AMERICAN EXPRESS
GLOBAL CREDIT AUTHORIZATION GUIDE
ISO 8583:1993 (VERSION 1)
APRIL 2016

GLOBAL MERCHANT SERVICES

Summary of Changes Table

The Summary of Changes is a broad overview of technical changes made to the specification since its last publication. This information may affect the way a Merchant, Third Party Processor or Vendor processes American Express Card transactions. Other changes, including but not limited to, clarification and consistency updates are included in the Revision Log located at the back of this guide.

Data Element or Section Number	Description of Change
	GENERAL CHANGES
	Added verbiage for Payment Token and/or Digital Wallet functionality to the following: • 1100 message: DF 2, DF 14, DF 22, DF 24, DF 60, DF 61 • 1110 message: DF 34, DF 60 • Section 1.5: Related Documents • Section 5.0 Card Acceptance Supported Services • Section 5.4.2.1 Expresspay Transit Transactions at Transit Access Terminals • Section 5.8 Digital Wallet Payments • Section 6.1 Payment Token Transactions
	Added verbiage for Derived Unique Key Per Transaction (DUKPT) functionality to the following: • 1100 message: DF 53 • Section 6.5.2 Derived Unique Key Per Transaction (DUKPT)
	1100 AUTHORIZATION REQUEST MESSAGE
DF 22: Point of Service Data Code	In the Point of Service Data Code tables, made the following changes and updates to include Payment Token functionality: • Position 1, removed value 'X' as a valid value. • Position 5, value 4, at the end of the description, added 'delayed shipment, split bill transactions'. • Position 6, added value 'Z' to identify Digital Wallet transactions. • Position 7, removed values 'X' and 'Y' as valid values. For value 5, added verbiage for Digital Wallet and Payment Token functionality.
	Removed references to magnetic stripe signature.
DF 24: Function Code	In the description, added verbiage to the function code table for '196=Expresspay Translation (PAN & Expiration Date Request)'.
DF 43: Card Acceptor Name/Location	Updated field for clarity around formatting for Payment Service Providers (Aggregators) and OptBlue Participants.
DF 62: Private Use Data	Removed references to magnetic stripe signature.

this page intentionally left blank

Table of Contents

Table of Contents

Table of Contents

this page intentionally left blank

1.0 About the Global Credit Authorization Guide

The *American Express Global Credit Authorization Guide (GCAG) ISO* contains software development instructions for use of the American Express Authorization System. These instructions enable programmers to code software in accordance with American Express requirements. American Express will allow users that conform to this specification and pass our certification tests to access the American Express Global Network to obtain authorizations for financial transactions. Use of this specification prior to certification is prohibited.

1.1 Who Should Use the GCAG ISO

The *GCAG ISO* is written for Merchants, authorized Third Party Processors, OptBlue Participants, Payment Service Providers (Aggregators) and Vendors.

In this guide, the terms Merchant, Seller, Service Establishment or SE, and Card Acceptor are used interchangeably to refer to businesses that are approved to accept American Express and/or American Express Partners' Cards as payment for goods and/or services.

The *GCAG ISO* is based on *International Standard ISO 8583:1993, Financial Transaction Card Originated Interchange Message Specifications*.

1.2 Document Changes

Changes to the *GCAG ISO* are identified in various ways.

Summary of Changes Table — The *GCAG ISO* begins with a Summary of Changes table that provides a broad overview of technical and/or data field changes since the last publication. The summary includes the following:

- The data field or section where revision occurred
- A brief description of the revision

Revision Mark — Throughout this document, revised areas that may affect the way a Merchant, Third Party Processor or Vendor processes transactions are indicated with a revision mark. This mark appears in the page margin, next to where a change was made. See example of a revision mark at left. Removed text will not have a revision mark. Changes may or may not be indicated with a revision mark.

Revision Log — The Revision Log is the last section in this document, and it contains a condensed overview of changes made in the last three publications.

1.3 Communication Process

This section outlines how changes to American Express Technical Specifications are communicated.

1.3.1 Semi-Annual Publication Process

The American Express Network publishes Technical Specifications twice each year, in April and October. Specification changes, which will require technical changes to implement or support, as well as any certification requirements and/or compliance dates, will be communicated six months prior to publication in a *Notice of Specification Changes (NOSC)*.

1.3.2 Notice of Specification Changes

Notice of Specification Changes (NOSC) are also published twice each year, in April and October. In each edition, changes to existing, or the introduction of new features and functionality will be announced. These changes will be incorporated into the next editions of the Technical Specifications.

- Changes published in the April *NOSC* will be incorporated into the October editions of the Technical Specifications.
- Changes published in the October *NOSC* will be incorporated into the April editions of the Technical Specifications.

1.3.3 Technical Bulletins

American Express will publish any changes occurring outside of the April and October publication schedule in *Technical Bulletins*. *Technical Bulletins* will generally contain the same level of detail found in the *NOSC*, including a description of the change, and the business and technical impacts of the change to customers.

Technical Bulletins may also communicate changes, corrections, and clarifications announced in previous Technical Specifications. Information communicated in *Technical Bulletins* will be incorporated into the next editions of the Technical Specifications.

1.4 Contact Information

To notify us when content clarifications are required, send an email to SpecQuestions@aexp.com. You may also send a copy of the document page in question.

You will receive confirmation of your request in 3-5 business days. Changes, corrections, and clarifications will be published in the next release.

For questions on modifications to existing functionality, contact your American Express representative.

1.5 Related Documents

- *American Express Global Financial Submission Guide (GFSG)*
- *American Express Global Codes & Information Guide*
- *American Express Online PIN Processing Implementation Guide for Merchants or Third Party Processors*
- *American Express Global Credit Authorization Guide ISO 8583:1993 (Version 1) Authorization Adjustment Addendum (AAA)*
- *American Express Network Communications Guide (MPLS & VPN)**
- *American Express ICC Payment (AEIPS) Chip Card Specification*
- *American Express ICC Payment (AEIPS) Terminal Specification*
- *American Express Merchant Regulations - U.S.*
- *American Express SafeKey℠ Acquirer — Merchant Implementation Guide*
- *Acquirer Chip Card Implementation Guide*
- *Implementing American Express EMV Acceptance on a Terminal*
- *Expresspay Terminal Specification*
- *Expresspay Card Specification*
- *Expresspay Card Specification Dual Interface Addenda*
- *Expresspay Communication Layer*
- *International Standard ISO 8583:1993, Financial Transaction Card Originated Interchange Messages — Interchange Message Specifications*
- *International Standard ISO/IEC 7813, Identification Cards — Financial Transaction Cards (Track I and Track II Specifications)*
- *American National Standards Institute ANSI X4.16, Financial Transaction Cards — Magnetic Stripe Encoding*
- *American National Standards Institute ANSI X9.24, Asymmetric Techniques for the Distribution of Symmetric Keys*
- *EMVCo Payment Tokenization Specification - Technical Framework*

*USA and Canada only. For information on connectivity solutions in other global regions, contact your American Express representative.

this page intentionally left blank

2.0 Implementation Planning

This section addresses the requirements and procedures needed for implementing authorization software. This section includes the following:

2.1 Overview of Implementation Planning

Merchants and authorized Third Party Processors who are interested in developing an interface to American Express must first contact an American Express representative. The American Express representative will discuss the business and basic technical issues involved with authorization, and if necessary, financial submission.

Once the business issues and decisions have been resolved, an American Express representative calls the Merchant and acts as the primary American Express contact during all phases of development until the software is approved for production use.

The American Express representative arranges for a technical conference call that includes members of the Merchant's technical staff and representatives of American Express. Prior to the first call, Merchants should become familiar with the contents of this document, as well as the following American Express documents:

- *American Express Global Codes & Information Guide*
- *American Express Global Financial Submission Guide* (if implementing both authorization and submission)
- *American Express Network Communications Guide (MPLS & VPN)**

* USA and Canada only. For information on connectivity solutions in other global regions, contact your American Express representative.

2.1 Overview of Implementation Planning (continued)

During the technical conference call, Merchants may ask the American Express staff detailed questions about hardware, communications protocol, and authorization service options. The American Express technical staff and American Express representative will provide detailed descriptions of processing options and message formats. The conference concludes when the Merchant and American Express agree on the authorization service options and interface requirements.

Following the initial conference calls, the American Express representative will arrange a technical conference call to review, in detail, the authorization message format selected by the Merchant.

2.2 Development Responsibilities

The following lists outline the basic installation responsibilities for both American Express and the Merchant.

American Express provides the following services:

- Allows scheduled access to American Express testing facilities.
- Allows 24-hour access to the American Express Consolidated Data Network (CDN) after the Merchant is approved for production activities.
- Installs and maintains circuit modems for a leased line authorization link, for qualified Merchants only. For more information, contact your American Express representative.

The Merchant provides the following:

- Develops or purchases credit authorization application and communications protocol software.
- Dedicates staff and computer resources to credit authorization software development within the project schedule agreed upon by American Express and the Merchant.

2.3 Development Steps

Most Merchants develop and implement their authorization software in these steps:

1. Participate in the technical conference call with American Express.
2. Receive and review the Business Requirements Document and Application Test Plan.
3. Develop authorization application and communications protocol software.
4. Test communications protocol with American Express. After protocol approval, test the authorization application software as stated in the Application Test Plan.
5. Receive American Express approval for production processing.

2.4 Hardware Requirements

The requirements for the hardware used by the Merchant are dependent on the types of products and services to be supported by the Merchant. For this reason, hardware requirements are established during conversations with the American Express representative.

2.5 Communications Options

For details, refer to the *American Express Network Communications Guide (MPLS & VPN)**

2.6 Leased Lines

Merchants who wish to use a leased line must qualify by transaction volume. This qualification is negotiated between the Merchant and the American Express representative. Qualified Merchants who choose a leased line may either use online or batch services.

The costs associated with using a leased line are contractually established between the Merchant and American Express. Merchants using their leased line to obtain MasterCard and VISA authorizations through the American Express authorizations system are assessed a small fee per transaction.

* USA and Canada only. For information on connectivity solutions in other global regions, contact your American Express representative.

this page intentionally left blank

3.0 Card Acceptance Guidelines

American Express enables Merchants and Third Party Processors to obtain financial transaction authorizations for the following:

- American Express Cards
- American Express-supported Network Cards
- American Express Prepaid Cards
- American Express Travelers Cheques

The Merchant or Third Party Processor must develop authorization software to enable the Merchant to collect Point of Sale (POS) information in any manner chosen by the Merchant's development team and also to submit that data to American Express in a format prescribed by this document.

American Express requires all Merchants and service providers, as part of their Card Acceptance or servicing agreements, to adhere to the American Express Data Security Operating Policy (DSOP). The policy requires Merchants to comply with the Payment Card Industry Security Standard to process, store or transmit Cardmember payment information. More information on the American Express DSOP and the PCI Data Security Standard can be found at www.americanexpress.com/datasecurity.

Users of this specification are often classified by regions which allow data field requirements and certification requirements to be applied to a specific region. When no country or region is listed for a requirement it is assumed to be a global requirement for all regions otherwise, the requirement applies to the countries and/or regions listed. The following acronyms are the recognized regional definitions:

- APA — Asia Pacific and Australia
- Canada — Canada
- EMEA — Europe, Middle East and Africa
- LA/C — Latin America and Caribbean
- USA — United States

For a complete list of regions and applicable countries, refer to the *American Express Global Codes & Information Guide*.

3.0 Card Acceptance Guidelines (continued)

Data from the following data fields in approved Authorization Request (1100) and Authorization Response (1110) messages should be retained by the Merchant since this information is required for financial submission:

- Primary Account Number (PAN)
- Amount, Transaction
- Date and Time, Local Transaction
- Approval Code
- Acquirer Reference Data (Transaction Identifier/TID)

Note: Other data may also be required. For more information on data requirements for financial submission, refer to the *American Express Global Financial Submission Guide (GFSG)*.

4.0 Guidelines for Using the GCAG ISO 8583 Message Formats

ISO 8583 standard provides for variable length messages that are bit map driven. A bit map consists of a 64-bit string contained within an eight-byte data field. The data content of a message is determined by the value (1) or (0) in a bit map data field. Each bit is associated with a unique data field. If the data content for a data field is available, the bitmap position should be set to one (1) and the respective data field should be sent. If the data content for a data field is not available, the bitmap position should be set to zero (0) and the respective data field should not be sent.

Data fields can be either fixed-length or variable-length. The Variable Length Indicator (VLI) indicates how many bytes of data will follow it. A length subfield or Variable Length Indicator (VLI) precedes the variable length data subfields. The length of the VLI will be encoded in either two or three character bytes. The length of the VLI is not included in the length of the variable data subfield it describes.

For example:

LLVAR — When present with a variable length data field specification, this indicates that the data field contains two subfields:

- "LL" indicates the number of positions in the VLI, and the value in the VLI shows the length of the variable-length data subfield that follows. The length may be 01 to 99 unless otherwise restricted.
- "VAR" is the variable length data subfield.

Example: A 27-byte data field with LLVAR indicates a VLI of 2 bytes with a maximum length of 25 bytes of variable data.

LLLVAR — When present with a variable length specification, this indicates that the data field contains two subfields:

- "LLL" indicates the number of positions in the variable-length data subfield that follows. Length may be 001 to 999, unless otherwise restricted.
- "VAR" is the variable length data subfield.

Example: A 503-byte data field with LLLVAR indicates a VLI of 3 bytes with a maximum length of 500 bytes of variable data.

4.0 Guidelines for Using the GCAG ISO 8583 Message Formats (continued)

- Unless otherwise specified, all fixed-length numeric data fields should be right justified and zero filled. Fixed-length alphanumeric data fields should be left justified and character space filled. Binary data fields should be in eight-bit blocks that are left justified and zero filled.
- The message content must be configured in the EBCDIC character set unless otherwise noted in the data field details.
- The communications protocol must support Transparency, due to the presence of binary data (e.g., bitmaps) that may be mistaken for communications control information.
- Some data fields are not supported in this version of the American Express ISO 8583 interface. However, to allow all processes to consistently and accurately deal with all data fields, all the attributes of all 64 data fields in the primary bit map are supplied beginning on page 53 and must be allowed while developing the interface. This allows a message to be sent even when it contains unsupported data. The data will not be processed by the recipient nor returned to the sender, but the definitions allow each system to step past unsupported data fields.
- Some data fields of the message are required to process the message while others are not required to process the message. Some data fields may be required in the response when present in the request. Data field requirements are as follows:

Mandatory	Data field and contents are required to process this message. Data field must contain the appropriate text or numeric information as indicated.
Mandatory - Echo returned	Data field is mandatory for processing this message; and whenever included in an originating request message, it will be preserved and returned in the response message without alteration.
Optional	Data field and contents are not mandatory for processing the message, but should be provided if available.
Optional - Echo returned	Data field is optional for processing this message; and whenever included in an originating request message, it will be preserved and returned in the response message without alteration.
Conditional	A data field may be conditional if it is only used in certain circumstances. See Data Field Descriptions for specific details.
Conditional - Echo returned	Data field is conditional for processing this message; and whenever included in an originating request message, it will be preserved and returned in the response message without alteration.

4.0 Guidelines for Using the GCAG ISO 8583 Message Formats (continued)

When Track 1 and/or Track 2 data is read from a magnetic stripe, the Merchant, their devices, systems, software, Vendors and Third Party Processors should capture all characters between the start and end sentinels, strip off the sentinels and LRC, and forward the remainder to American Express in the appropriate ISO 8583 Track 1 and/or Track 2 data field without regard to the specific lengths referenced in these sections. For more information, refer to the American Express Magnetic Stripe Formats in the *American Express Global Codes & Information Guide*.

Both Track 1 and Track 2 must be converted from ASCII to EBCDIC, and character spaces must not be stripped. In addition, data must not be padded to standardize track lengths, and it must be transmitted as read.

The Authorization Request (1100) message contains a data field that describes point-of-service processing capabilities (Data Field 22). Merchants and Third Party Processors must ensure that authorization data in Data Field 22 is accurate. Specifically, accuracy of Card Present, Cardholder Present and Track Data Indicators can significantly affect message processing, decrease POS disruptions and maximize customer satisfaction.

For more information, contact your American Express representative.

4.1 Variations in Messaging

No individual data field should exceed 290 bytes, except where specifically noted.

Messages transmitted to American Express must not exceed 900 bytes in total length.

For assistance in selecting optional data fields and determining the appropriate formats and variable data field lengths to use, contact your American Express representative.

American Express reserves the right to modify data field parameters (e.g., changing Data Field Type from numeric to alphanumeric, or vice-versa) to meet specific business and/or internal data and system requirements.

American Express Card creation standards for magnetic stripe layouts may include additional data undefined in currently published American Express implementations of ANSI X4.16 and ISO 7813 formats. Magnetic stripe data fields in current use will not be moved; however, discretionary or unused data fields may be redefined for use with future American Express Card products. Therefore, the data field definitions referenced in the American Express Magnetic Stripe and Expresspay Pseudo-Magnetic Stripe Formats are for reference only and may not reflect all American Express Card variations that may be encountered.

For additional information, refer to American Express Magnetic Stripe and Expresspay Pseudo-Magnetic Stripe Formats in the *American Express Global Codes & Information Guide*.

4.2 ISO 8583 Message Formats

American Express supports the International Organization for Standardization ISO 8583 format to exchange messages for authorizations.

4.2.1 Authorization Request/Response

- 1100 Message is used for Authorization Request messages
- 1110 Message is used for Authorization Response messages

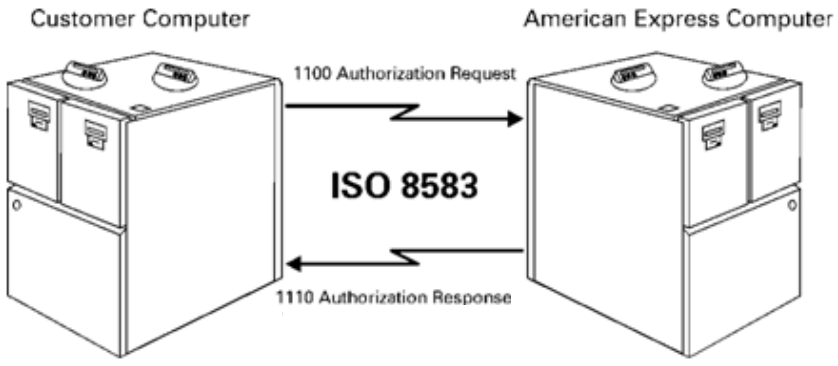


Figure 1-1. ISO 8583 Authorization Message Exchange

4.2.1 Authorization Request/Response (continued)

Merchants use the Authorization Request (1100) message to transmit credit authorization and/or Automated Address Verification (AAV) request messages to American Express. American Express uses the Authorization Response (1110) message to respond to a Merchant's Authorization Request (1100) message. American Express places the credit analysis results for the request in the Authorization Response (1110) message.

Merchant time-out values are determined during the technical conference call.

4.2.2 Reversal Advice Request/Response

- 1420 Message is used for Reversal Advice Request messages
- 1430 Message is used for Reversal Advice Response messages

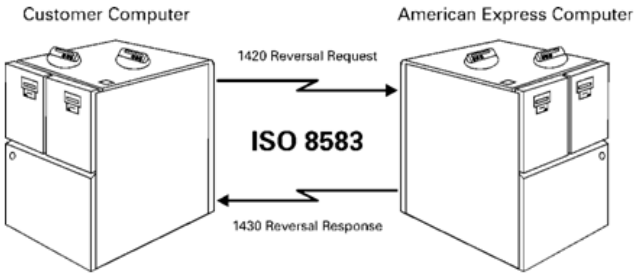


Figure 1-2. ISO 8583 Reversal Advice Message Exchange

These messages are constructed as specified in the ISO 8583-1993 standard. If your system supports a different version of ISO 8583, notify your American Express representative.

The Reversal Advice Request (1420) message allows the acquiring source to cancel the effects of a previous authorization transaction, completely. For more information, see page 219.

4.2.3 Network Management Request/Response

- 1804 Message is used for Network Management Request messages
- 1814 Message is used for Network Management Response messages

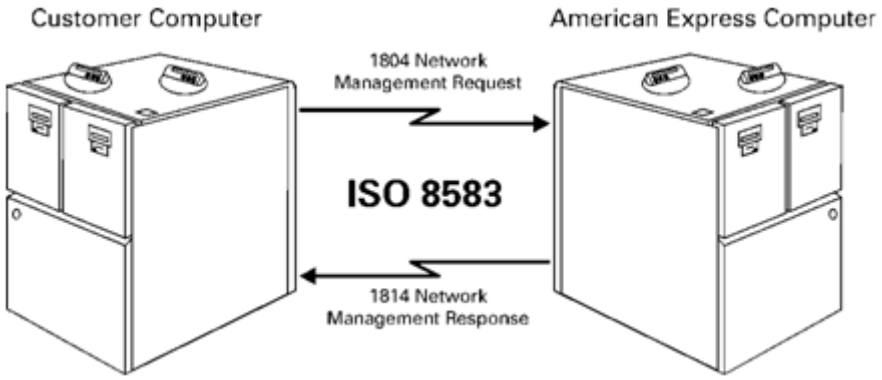


Figure 1-3. ISO 8583 Administration/Network Message Exchange

Network management messages are used to control the system security and operating condition of the interchange network and may be initiated by any interchanging party.

The Network Management Request (1804) message allows for either dynamic key exchange, an echo test or a signon/signoff request. When the Network Management Request (1804) message is received, it should be responded to by transmitting a Network Management Response (1814) message.

5.0 Card Acceptance Supported Services

American Express offers the following services for the products it supports:

- Online Authorizations — A Merchant who uses the online authorization service can transmit an authorization request and receive an authorization response, all in one individual session.
- American Express OptBlue Program— The American Express OptBlue Program is a program designed to increase acceptance of Cards among small Merchants by offering an integrated service and pricing through certain eligible third party Acquirers and payment processing companies.
- Prepaid Card Authorizations — This service allows a Merchant to accept and process an authorization request for American Express Prepaid Cards.
- Chip Card Authorizations (ICC) — American Express issues cards that in addition to a magnetic stripe, also contain an integrated chip that conforms to the industry EMV specifications.
- Recurring Billing and Standing Authorization — Recurring Billing transactions include periodic billings for regularly scheduled charges while Standing Authorization allows a Merchant to automatically charge a Cardmember's American Express Card.
- Batch Authorizations — A Merchant who uses the batch authorization service can transmit authorization request files containing multiple authorization request transactions periodically during a day or at the end of the business day. All authorization response transactions are batched into files and returned.
- Authorization Amount Adjustment — The Authorization Amount Adjustment can be used by any Merchant, Third Party Processor or Vendors that supports Automated Fuel Dispensers. This functionality allows for the release of held funds due to the actual sale amount being less than the original authorized amount.
- Digital Wallet Payments — This service allows Merchants to accept Digital Wallet transactions which provide Cardmembers a quick and flexible way to pay in store and within Mobile Applications (App) via various devices that Cardmembers frequently use.
- Other Authorization Services — A Merchant may process other financial transaction cards, as well as American Express Travelers Cheque authorizations.

5.1 Online Authorizations

The American Express online authorization process begins when a Cardmember uses the American Express Card to purchase goods or services from a Merchant. The purchase could occur at the physical location of the Merchant or remotely (e.g., a purchase through the internet, by mail-order or by telephone-order).

If the purchase occurs at the Merchant's location, the card is either swiped so that the Point of Sale terminal can read the magnetic stripe, inserted into a Chip Card capable terminal so the card data can be read from the embedded chip, tapped against the contactless interface, or manually keyed. If the purchase is made remotely, the Cardmember is required to provide their Card data to the Merchant to obtain authorization.

Once the information is complete, the data is transmitted to American Express. There are two services offered to Merchants who use online authorization:

- Non-Referral Link
- Referral Queue

5.1.1 Non-Referral Link

Non-Referral Link is the primary processing method used by most Merchants that accept the American Express Card and transmit authorization requests to American Express. Non-Referral Link allows an authorization to be processed without electronically referring the request to an American Express-employee Authorizer. When the electronic authorization request is transmitted to American Express via a non-referral link, American Express evaluates various information, which may include the Cardmember's spending, payment and credit history and risk criteria associated with the transaction. If the request passes this evaluation, the American Express authorization system approves the request, and returns an “APPROVED” message and approval code to the Merchant's system.

If the authorization request is not automatically approved, a message equivalent to “DENY” or “PLEASE CALL” is returned to the Merchant's system. When a Merchant receives a “PLEASE CALL” message, the POS Device Operator at the establishment must call American Express and speak to an Authorizer, who will verbally approve or deny the authorization request.

5.1.1 Non-Referral Link (continued)

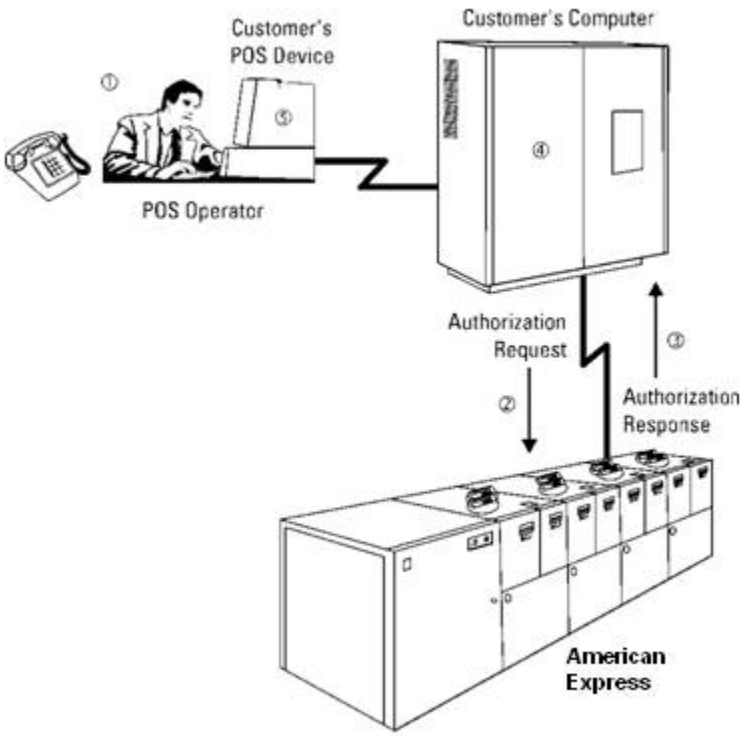


Figure 1-1. Non-Referral Link Processing

1. A POS Device Operator enters a transaction at the Merchant's system.
2. The Merchant's computer processes the transaction data and transmits an authorization request message to American Express.
3. American Express receives and processes the request then sends a response message to the Merchant's computer.
4. The Merchant's computer receives and processes the response message, then displays the response on the Merchant's system.
5. If American Express approves the request, an "APPROVED" message and an approval code are displayed at the Merchant's system.

   If American Express declines the request, a message equivalent to "DENY" is displayed at the Merchant's system.

   If American Express cannot make a decision, a "PLEASE CALL" message is displayed at the Merchant's system, and the POS Device Operator must then call an American Express Authorizer, who will analyze the transaction and verbally approve or deny the request.

5.1.2 Referral Queue

The referral queue option is available for both referral and non-referral processing links. The referral queue system assigns a four-digit referral number to each request that receives a "PLEASE CALL" authorization response, and places the request in a queue. The referral queue number is then included in the "PLEASE CALL" response message transmitted to the Merchant's system.

The POS Device Operator calls American Express and provides the referral queue number. Based on the referral queue number, the call is transferred to the assigned Authorizer, who reviews the information and either approves or denies the transaction. This procedure eliminates the re-entry of transaction data during the authorization call.

Illustrations of referral queue processing for non-referral links are shown on the next few pages.

5.1.2.1 Referral Queue — Non-Referral Mode

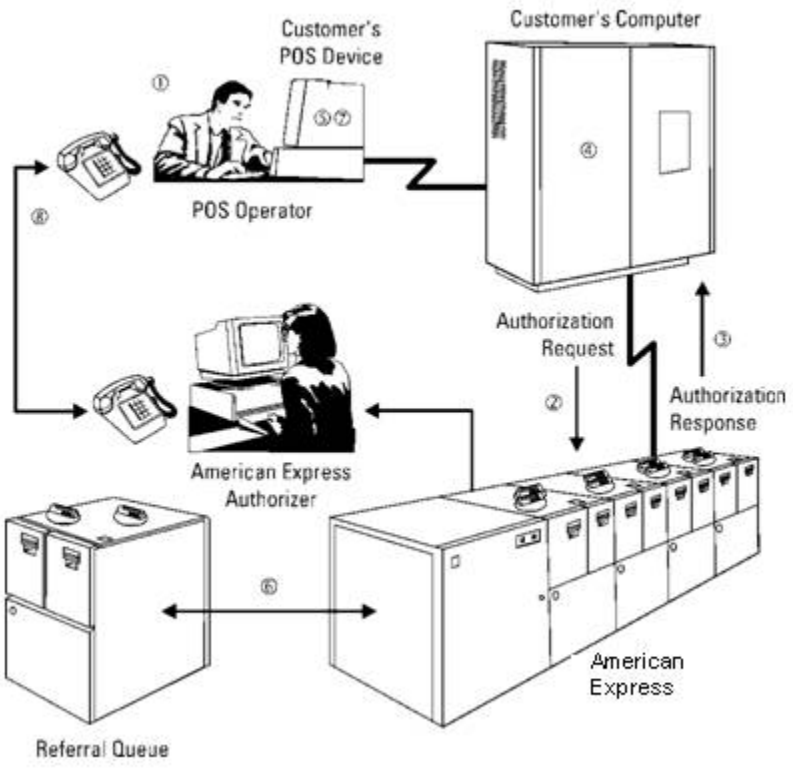


Figure 1-2. Referral Queue for Non-Referral Mode

5.1.2.1 Referral Queue — Non-Referral Mode (continued)

1. A POS Device Operator enters a transaction at the Merchant's system.
2. The Merchant's computer processes the transaction data and transmits an authorization request message to American Express.
3. American Express receives and processes the request then sends a response message to the Merchant's computer.
4. The Merchant's computer receives and processes the response message, then displays the response on the Merchant's system.
5. If American Express approves the request, an "APPROVED" message and an approval code are displayed at the Merchant's system.
6. If American Express declines the request, a message equivalent to "DENY" is displayed at the Merchant's system.
7. If American Express cannot make a decision, a "PLEASE CALL" message is displayed at the Merchant's system, and the POS Device Operator must then call an American Express Authorizer, who will analyze the transaction and verbally approve or deny the request.
8. The POS Device Operator calls American Express and provides the referral number. That number provides access to an American Express Authorizer.

5.1.3 Referral Queue — Referral Mode

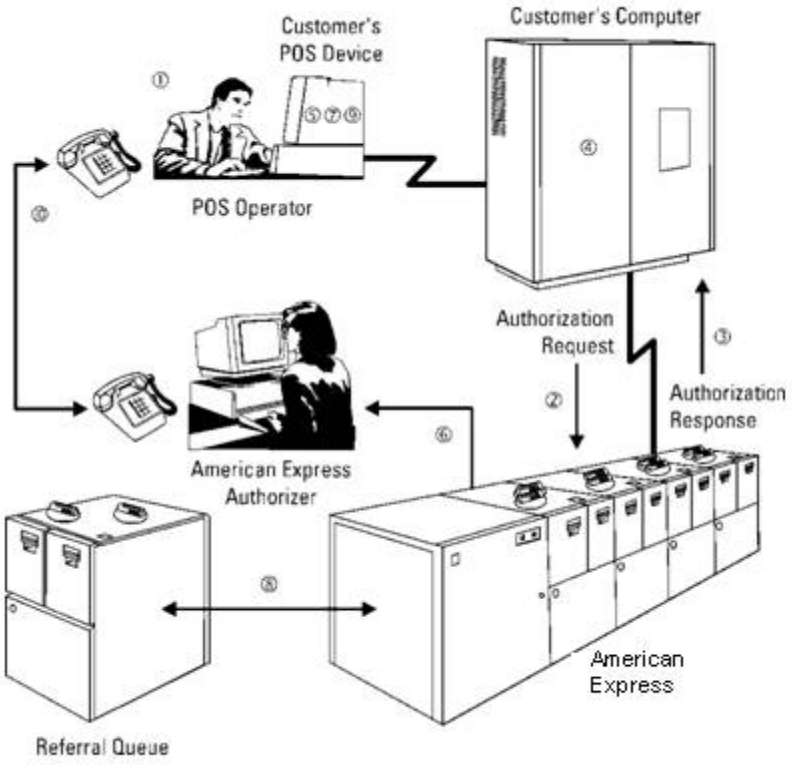


Figure 1-3. Referral Queue for Referral Mode

5.1.3 Referral Queue — Referral Mode (continued)

1. A POS Device Operator enters a transaction at the Merchant's system.
2. The Merchant's computer processes the transaction data and transmits an authorization request message to American Express.
3. American Express receives and processes the request then sends a response message to the Merchant's computer.
4. The Merchant's computer receives and processes the response message, then displays the response on the Merchant's system.
5. If American Express approves the request, an "APPROVED" message and an approval code are displayed at the Merchant's system.
6. If the Authorizer approves the request, an "APPROVED" response and an approval code are transmitted to the Merchant's computer. That computer processes the American Express response and sends the message to the Merchant's system.
7. If the Authorizer does not approve the request automatically, a referral number is assigned to the "PLEASE CALL" response message. The request is placed in the referral queue for easy access by American Express Authorizers.
8. The "PLEASE CALL" response message (with the referral number) is transmitted to the Merchant's computer, and both "PLEASE CALL" and the referral number are displayed on the Merchant's system.
9. The POS Device Operator calls American Express and provides the referral number. That number provides access to an American Express Authorizer.
10. After examining the request, spending history and payment history of the Cardmember, the Authorizer will verbally approve or deny the request.

5.2 American Express OptBlue® Program

The American Express OptBlue Program is designed to increase acceptance of Cards among small Merchants by offering integrated service and pricing through certain eligible third party Acquirers and payment processing companies. Program participants will be eligible to provide a full one-stop servicing solution for American Express Card acceptance to eligible small Merchants, including the flexibility to provide Merchants the benefit of a single statement, one settlement process, and one contact for all the major Card brands. For information on how to participate in the OptBlue program, contact your American Express representative.

5.3 Prepaid Card Authorizations

The Prepaid Card Partial Authorization and Authorization with Balance Return features are designed to help Merchants provide Card balance information to American Express Prepaid Cardholders at the point of sale. The Authorization Request/Response messages are exchanged to determine available funds to help the Merchant successfully complete Prepaid Card transactions in a timely manner.

Partial Authorization and Authorization with Balance Return features only apply to Prepaid Cards. Merchants who participate are not required to know which American Express products are prepaid. American Express will return the specified information for transactions that qualify otherwise, the responses will be the same as those they receive today.

5.3.1 Partial Authorization

American Express strongly recommends Partial Authorization, because it approves a request for the remaining balance rather than declining it when there are insufficient funds to cover the original amount.

The Partial Authorization feature allows American Express to authorize a transaction for an amount less than the original Merchant requested amount. Partial Authorization is used in circumstances where the Prepaid Card has insufficient funds to cover the original amount of the request. Rather than receiving a denial message, the transaction will be approved for the remaining balance of the Card. The Cardholder can then pay the Merchant the outstanding amount of the transaction via another form of payment.

Data Field 24 (Function Code) of the Authorization Request (1100) message is used to identify a Merchant that accepts partial authorizations. The approved amount is returned in Data Field 4 (Amount, Transaction) of the Authorization Response (1110) message. The original requested authorization amount is returned in Data Field 30 (Amounts, Original); and the available amount remaining on the Card (including a zero balance) may be returned in Data Field 54 (Amounts, Additional).

Merchants should develop internal instructions for using the Prepaid Card Partial Authorization or Authorization with Balance Return features at their point of sale. American Express will allow authorized Merchants that conform to this specification and pass our certification tests to access the American Express network to acquire Partial Authorization or Authorization with Balance Return.

Third Party Processors must develop support for both Partial Authorization and Authorization with Balance Return functionalities in order to provide the ability for their Merchants to utilize either feature. Additional information may be obtained from your American Express representative.

Balances may not be returned for some Prepaid Cards.

5.3.2 Authorization with Balance Return

In addition, American Express offers the Authorization with Balance Return feature.

The Authorization with Balance Return feature allows Merchants that choose not to use the Partial Authorization feature to receive the Prepaid Card balance on the Authorization Response (1110) message. Systems that do not support split tender capability which is required for Partial Authorizations can receive a response message containing the remaining balance (Authorization with Balance Return), This enables the customer to submit a new request for an amount less than or equal to the funds available or they can choose an alternate form of payment for the transaction.

Data Field 24 (Function Code) of the Authorization Request (1100) message is used to identify an Authorization with Balance Return request. The available balance may be returned to the Merchant in Data Field 54 (Amounts, Additional) in the Authorization Response (1110) message, even if the transaction is denied. Transactions that are denied for insufficient funds can be resubmitted for an amount equal to or less than the remaining balance provided in the Authorization Response (1110) message.

Prepaid Card Balance Inquiry may also be performed utilizing either the Partial Authorization or the Authorization with Balance Return feature. This can be done by simply entering an amount of zero in the Data Field 4 (Amount, Transaction). The transaction will be approved, and the available balance is returned in Data Field 54 (Amounts, Additional). A new authorization request can then be created for an amount equal to or less than the remaining balance.

Balances may not be returned for some Prepaid Cards.

5.4 Chip Card Authorizations

Two types of Chip Cards are issued by American Express, Contact (AEIPS) and Contactless (Expresspay):

- AEIPS — A Contact Chip Card is physically inserted into a Card Reader to enable it to communicate with the Terminal. The American Express contact solution is called AEIPS (American Express ICC Payment Specifications).
- Expresspay — A Contactless Chip Card uses radio frequency technology to communicate with the Terminal, and the card does not need to be inserted into a reader. Contactless transactions are typically faster than Contact transactions. The American Express contactless solution is called Expresspay.

In order to submit transactions from American Express Chip Cards for authorization and submission, the Merchant, authorized Third Party Processor or Vendor must submit data to American Express in the formats prescribed by the *GCAG ISO* and the *American Express Global Financial Submission Guide*.

Note: American Express requires chip card accepting devices to be approved by EMVCo. EMVCo approval can be obtained at an EMVCo approved laboratory. Further details can be obtained from the EMVCo website (www.emvco.com) or from your local American Express representative.

5.4.1 AEIPS

In an AEIPS transaction, the Card is inserted into the Card Reader in the terminal; and the Card data is read directly from the chip. Transaction data is created and populated in Data Field 55 (Integrated Circuit Card System Related Data) - special certification is required. For more information on the breakdown of Data Field 55, see page 138.

American Express mandates that in addition to populating Data Field 55, AEIPS transactions must include Data Field 35 (Track 2 Data).

For terminals that are EMV-enabled but not yet certified or for terminals that are EMV-enabled for other payment brands but not yet for American Express (AEIPS), transactions must be processed using any of the other non-EMV methods.

5.4.1 AEIPS (continued)

When submitting AEIPS transactions, Data Field 22 (Point of Service Data Code) must be populated based on acquiring method and adhere to the following guidelines:

- Position 1: Card Data Input Capability - Transactions must not be processed using value 5 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing.
- Position 7: Card Data Input Mode -
    - Transactions must not be processed using value 5 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing.
    - Transactions must not be processed using value 9 (Technical Fallback) unless the terminal and link are certified by American Express for EMV processing and used to indicate a fallback transaction.
- Position 9: Cardmember Authentication Entity- Transactions must not be processed using value 1 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing.
- Position: 10: Card Data Output Capability - Transactions must not be processed using value 3 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing.

5.4.2 Expresspay

In an Expresspay transaction, the data is passed between the chip and the terminal using Radio Frequency (RF) technology. Expresspay has two different modes in which the Card and Terminal can operate:

- Expresspay EMV Mode - This mode of operation is designed for those Issuers and Acquirers that support EMV data in the authorization messages. EMV capable terminals support both EMV and Magstripe Modes.
- Expresspay Magstripe Mode- This mode of operation is designed for both Issuers who can accept EMV data as well as Issuers and Acquirers who have not implemented EMV acceptance. Magstripe capable terminals only support Magstripe Mode.

If supporting Expresspay, Merchants, authorized Third Party Processors and Vendors must support EMV and Magstripe Mode including the Expresspay Pseudo-Magnetic Stripe Format. It is mandatory for all Third Party Processors and Vendors to certify they can pass Expresspay data. Refer to Expresspay Pseudo-Magnetic Stripe Formats in the *American Express Global Codes & Information Guide*.

In order to submit transactions from Expresspay Cards for authorization and submission, the Merchant, authorized Third Party Processor or Vendors must submit data to American Express in the formats prescribed by the *GCAG ISO* and the *American Express Global Financial Submission Guide*.

Expresspay Requirements

Magstripe Capable Terminals	EMV Capable Terminals
• Track 1 (Data Field 45) and/or Track 2 (Data Field 35) must be present. For information on *Expresspay Pseudo-Magnetic Stripe Formats*, refer to the *American Express Global Codes & Information Guide*.	• ICC System Related Data (Data Field 55) must be present. • Track 2 Data (Data Field 35)
• POS Data Code (Data Field 22) o Position 6 = "X" (Contactless transactions, including American Express Expresspay) o Position 7= "2" (Magnetic stripe read; Track 1 and/or Track 2) or "W" (Swiped transaction with keyed CID/4DBC/4CSC)	• POS Data Code (Data Field 22) o Position 6 = "X" (Contactless transactions, including American Express Expresspay) o Position 7 = "5" (Integrated Circuit Card [ICC]; EMV and Track 2 data captured from chip)

Notes:

1. Expresspay transactions must originate at a contactless reader and cannot be manually keyed.
2. It is important to note that pseudo-magnetic stripe data from a chip card contactless reader differs slightly from track data obtained from a magnetic stripe read. For this reason, when Magstripe-Capable Terminals, Track 1 and/or Track 2 pseudo-magnetic stripe data is supplied intact, the start and end sentinels should be stripped off; and all remaining characters between the sentinels (including the Interchange Designator and Service Code) should be forwarded to American Express without alteration, in the appropriate ISO 8583 Track 1 and/or Track 2 data field (Data Fields 45 and/or 35, respectively). For complete lists of allowable Interchange Designator/Service Code combinations, refer to the *American Express Global Codes & Information Guide*.

5.4.2.1 Expresspay Transit Transactions at Transit Access Terminals

The American Express Expresspay Transit solution will supplement existing American Express Network functionality to meet the transit industry's need for high speed, low risk transactions. The resulting service enables the customer to experience American Express acceptance at a transit fare gate like any other retail Merchant's contactless POS terminal.

Technical coding components of Expresspay Transit transactions at Transit Access Terminals (TAT) include:

1. Data Field 26 -Card Acceptor Business Codes (Merchant Category Code)

   One of the five transit specific Card Acceptor Business Codes (Merchant Category Code) must be populated for Transit - TAT transactions:

   - 4111 - Local and Suburban Commuter Passenger Transportation, including Ferries
   - 4112 - Passenger Railways
   - 4131 - Bus Lines
   - 4784 - Tolls and Bridge Fees
   - 7523 - Parking Lots and Garages

2. Data Field 22 - Point of Service Data Code

   In the Authorization Request (1100) message - Position 4, Value Z for Transit Access Terminal - TAT must be populated for Transit -TAT transactions.

3. Data Field 24 - Function Code

   There are several Function Codes available for Transit -TAT transactions.

   - Function Code 190 = Account Status Check
     - Used when requesting a check on the Cardmember's account for viability.
     - The outcome of the request will be an Action Code provided in Data Field 39 of the Authorization Response (1110) message.
   - Function Code 191 = ATC Synchronization
     - Used to indicate an Application Transaction Counter (ATC) value is being provided to the Issuer.
     - The outcome of the request will be an Action Code provided in Data Field 39 of the Authorization Response (1110) message.

5.4.2.1 Expresspay Transit Transactions at Transit Access Terminals (continued)

- Function Code 194 = Expresspay Translation (PAN request)
  - Used to indicate that the Primary Account Number (PAN) associated with an Expresspay-enabled card is being requested from the Issuer.
  - The response will be provided in Data Field 34 - Primary Account Number, Extended in the Authorization Response (1110) message.
- Function Code 196 = Expresspay Translation (PAN and Expiration Date request)
  - Used to indicate the Primary Account Number (PAN) and Expiration Date associated with an Expresspay-enabled card/device is being requested from the Merchant.
  - The response will be provided in Data Field 34 - Primary Account Number, Extended in the Authorization Response (1110) message.

4. Data Field 34 - Primary Account Number, Extended in the Authorization Response (1110) message.

5.5 Recurring Billing and Standing Authorization

Recurring Billing transactions include periodic billings such as membership fees to health clubs, magazine subscriptions, insurance premiums and other regularly scheduled charges. These transactions are typically requested the same time every month for the same dollar amount.

Standing Authorization allows a Merchant to automatically charge a Cardmember's American Express Card, when the Cardmember's billing information is on file, and goods have been delivered/ or services have been rendered. Billing frequency and amount can be variable (e.g., travel, car rental, lodging, frequent customer, etc.).

5.6 Batch Authorizations

The American Express Batch Authorization System accepts and processes files containing multiple authorization transactions; and the structure, content and format of batch Authorization Request (1100) messages are detailed in this specification. All Authorization Request (1100) message files submitted for batch processing must contain valid, properly constructed, Authorization Request (1100) message records.

The American Express batch authorization process begins when a Cardmember uses the American Express Card to purchase goods or services from a Merchant. The Merchant's point of sale (POS) operator enters purchase information into the POS device. This may or may not include keyboard entry of Cardmember account information and/or swiping the Card so that the POS device can read data stored in the magnetic stripe. More information on the American Express Data Security Operating Policy (DSOP) and the PCI Data Security Standard can be found at www.americanexpress.com/datasecurity.

Upon completion of data entry (which may occur periodically during the workday, or at the end of shift or business day), information accumulated from numerous transactions is transmitted to American Express in a file. The American Express Batch Authorization processor manages the exchange of request and response transactions between Merchant's system and American Express. Once processing of a file is completed, the Merchant retrieves the response batch file from American Express.

Message format errors or communication problems between Merchant and/or Authorized Third Party Processor systems and the American Express Batch Authorization System, may result in original, authorization request messages being returned in batch authorization response files.

Therefore, when processing responses from American Express, Merchant and/or Authorized Third Party Processor systems must recognize and separate original authorization requests, for retransmission (in a new batch authorization request file) or voice authorization.

Important Note: The Internet Direct IP Payments Gateway does not support the American Express Batch Authorization process. For more information, contact your American Express representative.

5.6.1 Message Separation

ISO 8583 messages are variable length and contain a combination of binary and character-encoded (primarily EBCDIC) text and numeric values. As a result, an ISO 8583 message must be treated as a stream of bytes in a file, rather than sequences of characters. Also, the binary data in some data fields makes it impractical to use end-of-record terminator characters as delimiters to separate sequential records in the stream of data that comprises a file. However, the last two bytes of a fixed length file layout, Authorization Request (1100) message are reserved and echo returned as the last two bytes in the corresponding Authorization Response (1110) message; and these two characters may be used as Merchant-specified, end-of-line (EOL) terminators, if necessary. For more information, see page 36.

American Express utilizes a Message Length Indicator (MLI), transmitted as a prefix to each individual authorization request, to specify the exact message length. The MLI is not part of the ISO 8583 Authorization Request (1100) message defined in this specification. Instead, it is considered part of the communication/transport mechanism.

The Message Length Indicator (MLI) is a two-byte, unsigned, short integer in binary, network short/ big-endian format (i.e., most significant byte, followed by least significant byte), which reflects the combined length of the two-byte MLI and the individual Authorization Request (1100) message that immediately follows.

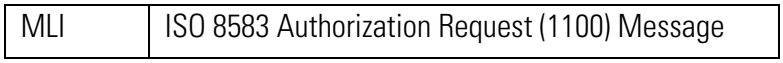


Figure 1-4. Message Length Indicator & ISO 8583 Authorization

Messages in the batch response file are similarly formatted and contain a two-byte MLI that indicates the combined length of the MLI and the Authorization Response (1110) message.

5.6.2 Supported File Layouts

The American Express Batch Authorization System supports two file layout formats:

- Variable Length Format
- Fixed Length Format

During certification, Merchants must indicate which format they wish to use, and once certified, all files must be submitted in that format. Merchants wishing to change formats must recertify. American Express uses the same format for a batch response file as was used for the corresponding batch request file.

For both layouts, the Batch Authorization System uses the MLI to determine actual message length.

The following table contains sample message data that appears on the following pages in both variable- and fixed-length formats. Note that ISO 8583 defines some data fields as variable length, with data in these data fields preceded by a Variable Length Indicator (VLI), in much the same manner as each message is preceded by an MLI. For this reason, individual message length varies in actual production files.

Data Field	Name	Required	Data Field Length	Sample Data	Hex Value
—	MESSAGE TYPE IDENTIFIER	M	4 bytes, fixed	1100	F1 F1 F0 F0
—	BIT MAP	M	8 bytes, 64 bits	703425C000408000	70 34 25 C0 00 40 80 00
2	PRIMARY ACCOUNT NUMBER (PAN)	M	21 bytes, LLVAR	370012345612345	F1 F5 F3 F7 F0 F0 F1 F2 F3 F4 F5 F6 F1 F2 F3 F4 F5*
3	PROCESSING CODE	M	6 bytes, fixed	004000	F0 F0 F4 F0 F0 F0
4	AMOUNT, TRANSACTION	M	12 bytes, fixed	000000000100	F0 F0 F0 F0 F0 F0 F0 F0 F0 F1 F0 F0
11	SYSTEMS TRACE AUDIT NUMBER	M	6 bytes, fixed	000001	F0 F0 F0 F0 F0 F1
12	DATE AND TIME, LOCAL TRANSACTION	M	12 bytes, fixed	090100000000	F0 F9 F0 F1 F0 F0 F0 F0 F0 F0 F0 F0
14	DATE, EXPIRATION	M	4 bytes, fixed	1301	F1 F3 F0 F1
19	COUNTRY CODE, ACQUIRING INSTITUTION	M	3 bytes, fixed	840	F8 F4 F0
22	POINT OF SERVICE DATA CODE	M	12 bytes, fixed	101150600120	F1 F0 F1 F1 F5 F0 F6 F0 F0 F1 F2 F0

Figure 5-5. Authorization Request Sample Data

* This data field contains the Cardmember Account Number, preceded by a two-digit, Variable Length Indicator (VLI). The VLI must indicate the exact length of the account number, and no additional characters should be added to this data field.

5.6.2 Supported File Layouts (continued)

.

Data Field	Name	Required	Data Field Length	Sample Data	Hex Value
24	FUNCTION CODE	O	3 bytes, fixed	180	F1 F8 F0
25	MESSAGE REASON CODE	M	4 bytes, fixed	1234*	F1 F2 F3 F4
26	CARD ACCEPTOR BUSINESS CODE	M	4 bytes, fixed	5399	F5 F3 F9 F9
42	CARD ACCEPTOR IDENTIFICATION CODE	M	15 bytes, fixed	12345678	F0 F0 F0 F0 F0 F0 F0 F1 F2 F3 F4 F5 F6 F7 F8
49	CURRENCY CODE, TRANSACTION	M	3 bytes, fixed	840	F8 F4 F0

Figure 1-5. Authorization Request Sample Data (continued)

Note: Sample data in the preceding table and the following examples show values in hexadecimal notation for illustration purposes only. Actual batch authorization messages are transmitted as raw binary data. Total length of sample data is 113 bytes.

5.6.2.1 Variable Length Layout

The variable length file layout is preferred for batch authorization files. Variable length files have no padding, nor end-of-record terminators; and, as a result, they are smaller than fixed length files that transport the same data.

The Message Length Indicator (MLI) is used in exactly the same manner in both the variable and fixed length file layouts, and the MLI indicates the combined length of the MLI and the variable data that comprises the actual Authorization Request (1100) message.

Variable Length Layout (113 bytes to 122 bytes, Variable Message Length)

Message 1	MLI (2 bytes)	Authorization Request (1100) Message (113 bytes)
Message 2	MLI (2 bytes)	Authorization Request (1100) Message (120 bytes)
Message 3	MLI (2 bytes)	Authorization Request (1100) Message (115 bytes)
Message 4	MLI (2 bytes)	Authorization Request (1100) Message (110 bytes)

Figure 1-6. Variable Length Layout

Message 1 is composed of a two-byte MLI preceding a 113-byte Authorization Request (1100) message. The MLI value is "115" ("00 73", hex).

* "1234" is sample data only. Actual Message Reason Code is provided during Merchant certification.

5.6.2.1 Variable Length Layout (continued)

Message 2 is 120 bytes in length. The MLI is "122" ("00 7A", hex).

```
00 73 F1 F1 F0 F0 70 34 25 C0 00 40 80 00 F1 F5 F3 F7 F0 F0 F1 F2
F3 F4 F5 F6 F1 F2 F3 F4 F5 F0 F0 F4 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0
F0 F0 F1 F0 F0 F0 F0 F0 F0 F0 F1 F0 F9 F0 F1 F0 F0 F0 F0 F0 F0 F0
F0 F1 F3 F0 F1 F8 F4 F0 F1 F0 F1 F1 F5 F0 F6 F0 F0 F1 F2 F0 F1 F8
F0 F1 F9 F0 F0 F5 F3 F9 F9 F1 F2 F3 F4 F5 F6 F7 F8 40 40 40 40 40
40 40 F8 F4 F0 00 7A F1 F1 F0 F0 70 30 25 40 00 40 80 00 F1 F5 F3
F7 F0 F0 F1 F2 F3 F4 F5 F6 F1 F2 F3 F4 F5 ...
```

Figure 1-7. Sample Data in Variable Length Format

In the example above:

- Message 2 is shown in shaded text.
- There is no padding, nor end-of-record terminator, between messages.

5.6.2.2 Fixed Length Layout

The fixed length file layout may be used by Merchants who utilize record-based file systems (e.g., a mainframe computer). In addition, Merchants who have difficulty creating files that conform to variable length file layout requirements may also use this alternate format. However, during certification, those Merchants must specify the fixed record length they will use (see 150-byte example in Figure 5-8). A subsequent change to this fixed record length requires recertification.

The Message Length Indicator (MLI) is used in exactly the same manner in both the fixed and variable length file layouts, and the MLI indicates the combined length of the MLI and the variable message data that comprises the actual Authorization Request (1100) message without padding.

The fixed length file layout requires that messages of different lengths each be padded to the merchant-specified, fixed record length using EBCDIC character spaces (0x40). In addition, the fixed record length must be at least four bytes longer than the maximum message length that will populate the file, to allow for the two-byte MLI, plus two-bytes for padding or an end-of-line (EOL) terminator.

When calculating maximum message length, the combined lengths of all fixed-length data fields and maximum lengths of all variable-length data fields used in a message must be accounted for. In Figure 5-8, the fixed record length is 150 bytes, which means that the maximum message length used to populate a file must not exceed 146 bytes.

The last two bytes of a fixed length request record are reserved and echo returned as the last two bytes in the corresponding response. These two characters must be present; and they may be a Merchant-specified EOL terminator or padded spaces if an EOL terminator is not used. Typical EOL values may include the following:

- "`0D 0A`" hex ("EOL", Windows character set)
- "`20 0A`" hex ("Space/EOL", Unix character set)
- "`40 25`" hex ("Space/EOL", EBCDIC character set)

5.6.2.2 Fixed Length Layout (continued)

Fixed Length Layout (150 Bytes, Fixed Record Length)

Message 1	MLI (2 bytes)	Authorization Request (1100) Message (113 bytes)	Padding (33 bytes)	Padding/EOL (2 bytes)
Message 2	MLI (2 bytes)	Authorization Request (1100) Message (120 bytes)	Padding (26 bytes)	Padding/EOL (2 bytes)
Message 3	MLI (2 bytes)	Authorization Request (1100) Message (115 bytes)	Padding (31 bytes)	Padding/EOL (2 bytes)
Message 4	MLI (2 bytes)	Authorization Request (1100) Message (110 bytes)	Padding (36 bytes)	Padding/EOL (2 bytes)

Figure 1-8. Fixed Length Layout

Message 1 is composed of a two-byte MLI preceding a 113-byte Authorization Request (1100) message. The MLI value is "115" ("00 73", hex).

Message 2 is 120 bytes in length. The MLI is "122" ("00 7A", hex).

```
00 73 F1 F1 F0 F0 70 34 25 C0 00 40 80 00 F1 F5 F3 F7 F0 F0 F1 F2
F3 F4 F5 F6 F1 F2 F3 F4 F5 F0 F0 F4 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0
F0 F0 F1 F0 F0 F0 F0 F0 F0 F0 F1 F0 F9 F0 F1 F0 F0 F0 F0 F0 F0 F0
F0 F1 F3 F0 F1 F8 F4 F0 F1 F0 F1 F1 F5 F0 F6 F0 F0 F1 F2 F0 F1 F8
F0 F1 F9 F0 F0 F5 F3 F9 F9 F1 F2 F3 F4 F5 F6 F7 F8 40 40 40 40 40
40 40 F8 F4 F0 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40
40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 00 7A F1 F1
F0 F0 70 30 25 40 00 40 80 00 F1 F5 F3 F7 F0 F0 F1 F2 F3 F4 F5 F6
F1 F2 F3 F4 F5 ...
```

Figure 1-9. Sample Data in Fixed Length Format, without EOL Terminator

In the example above:

- The file is composed of variable length messages, each padded to exactly 150-bytes.
- Message 2 is shown in shaded text.
- A minimum of two padded spaces (shown in **reversed text**) are used between messages in lieu of an EOL terminator.

5.6.2.2 Fixed Length Layout (continued)

```
00 73 F1 F1 F0 F0 70 34 25 C0 00 40 80 00 F1 F5 F3 F7 F0 F0 F1 F2
F3 F4 F5 F6 F1 F2 F3 F4 F5 F0 F0 F4 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0
F0 F0 F1 F0 F0 F0 F0 F0 F0 F0 F1 F0 F9 F0 F1 F0 F0 F0 F0 F0 F0 F0
F0 F1 F3 F0 F1 F8 F4 F0 F1 F0 F1 F1 F5 F0 F6 F0 F0 F1 F2 F0 F1 F8
F0 F1 F9 F0 F0 F5 F3 F9 F9 F1 F2 F3 F4 F5 F6 F7 F8 40 40 40 40 40
40 40 F8 F4 F0 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40
40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 0D 0A 00 7A F1 F1
F0 F0 70 30 25 40 00 40 80 00 F1 F5 F3 F7 F0 F0 F1 F2 F3 F4 F5 F6
F1 F2 F3 F4 F5 ...
```

Figure 1-10. Sample Data in Fixed Length Format, with EOL Terminator

In the example above:

- The file is composed of variable length messages, each padded to exactly 150-bytes.
- Message 2 is shown in shaded text.
- An EOL terminator (shown in **reversed text**) is used between messages.

5.7 Authorization Amount Adjustment

The authorization amount adjustment is designed to release funds held when the actual sale amount is less than the original amount authorized. This ISO 8583 message can be leveraged by Merchants to advise American Express of the exact amount of the completed sale. The Authorization Adjustment will release the difference between the original amount authorized and the final sale amount to the Cardmember's available credit or "open to buy". Merchants must only send an adjustment advice if the final sale amount is less than the original, approved authorized amount.

This is an optional message format, but American Express strongly recommends its use.

The authorization amount adjustment applies to any Merchant, Third Party Processor or Vendor that supports Automated Fuel Dispensers. For details on specific authorization amount adjustment requirements, contact your American Express representative and request the *American Express Global Credit Authorization Guide ISO 8583:1993 (Version 1) Authorization Adjustment Addendum (AAA).*

5.8 Digital Wallet Payments

Digital Wallet functionality allows for the processing of transactions initiated through the use of Mobile Apps or Digital Wallets found on Cardmember devices. Digital Wallet transactions can occur in store or through In-App transactions initiated in any location. All Digital Wallet transactions must be identified through the correct use of the Point of Service Data Codes in order to process properly.

5.8.1 In-Store Digital Wallet Transactions

In-Store Digital Wallet Transactions are considered Card Present and can be Contactless or Magnetic Secure Transmission (MST).

- **Contactless Near Field Communications (NFC) Transactions** — The Mobile NFC capable device completes a Card Present charge by tapping the device in close proximity to a Contactless NFC enabled POS system. Technical coding components of Contactless NFC transactions utilizing Payment Tokenization include:

  Data Field 22 - Point of Service Data Code Values

  - Position 6 - Card Present must be X
    (Contactless transactions, including American Express Expresspay)
  - Position 7 - Card Data Input Mode, must be one of the following:
    - Value 2 (Magnetic stripe read; Track 1 and /or Track 2)
    - Value 5 (Integrated Circuit Card [ICC], EMV and Track 2 data captured from chip)
    - Value W (Swiped transaction with keyed CID/4CSC)

5.8.1 In-Store Digital Wallet Transactions (continued)

- **Magnetic Secure Transmission (MST) Transactions** — The Mobile NFC and MST capable device completes a Card Present charge by tapping the device in close proximity to a Magnetic Swipe enabled POS device. MST can be utilized at almost any POS capable of accepting Magnetic Stripe. The Point of Service Data Code should reflect an MST transaction in the same manner as a typical Magnetic Stripe transaction.

5.8.2 In-App Transactions

The Cardmember initiates a Card Not Present charge using a software application loaded onto their mobile device. In-App transactions utilize Payment Tokenization and must be coded accordingly. Technical coding components of In-App transactions utilizing Payment Tokenization include:

Authorization Request (1100) Message

1. Data Field 22 - Point of Service Data Code Values
   - Position 6 - Card Present must be Z (Digital Wallet - application initiated (including application initiated Payment Token)) transactions
   - Position 7 - Card Data Input Mode, must be 5 (Integrated Circuit Card [ICC])
2. Data Field 60 - National Use Data
3. Data Field 61 - National Use Data

Authorization Response (1110) Message

Data Field 34 - Primary Account Number, Extended

For further information on Payment Tokenization see Section 6.1 Payment Token Transactions.

5.9 Other Authorization Services

American Express offers its Merchants authorization services for products other than American Express Cards. Those services are:

- American Express Travelers Cheque verifications
- Non-American Express card authorizations

5.9.1 American Express Travelers Cheque Verifications

American Express Travelers Cheques can be verified through the American Express system to ensure that the Travelers Cheque is not lost or stolen.

5.9.2 Non-American Express Card Authorizations

American Express will forward MasterCard, VISA, Diners Club and JCB transactions to the appropriate Issuer for authorization and return the response from the Issuer to the Merchant's system at the establishment.

Authorized Third Party Processors are specifically excluded from this function. Merchants must notify American Express of their intent to implement this function before it is used, as transaction data for non-American Express supported bankcards are normally rejected upon receipt. In addition, American Express cannot guarantee bankcard interchange compliance. For more information, contact your American Express representative.

Limited processing instructions for non-American Express-supported bankcards are included in this guide. This information is provided for Merchants routing transactions via American Express during bankcard network outages and is not intended as an alternative path for traditional bankcard transaction processing.

this page intentionally left blank

6.0 Fraud Prevention Services

A Merchant may send key data fields with the authorization request that can help prevent fraud at the point of authorization. Some of these services include Payment Token, Verification Services and Electronic Verification Services.

6.1 Payment Token Transactions

All Payment Token transactions must be identified through the correct use of Point of Service Data Codes in order to process properly.

Payment Tokens - Contactless[1] transactions:

- Position 6 - Card Present must be X (Contactless transactions, including American Express Expresspay)
- Position 7 - Card Data Input Mode, must be one of the following:
  - Value 2 (Magnetic stripe read; Track 1 and/or Track 2)
  - Value 5 (Integrated Circuit Card [ICC], EMV and Track 2 data captured from chip)
  - Value W (Swiped transaction with keyed CID/4DBC/4CSC)

Payment Tokens - Application Initiated transactions / Digital Wallet - application initiated (including application initiated Payment Token) transactions:

- Position 6 - Card Present, must be Z (Digital Wallet - application initiated (including application initiated Payment Token)) transactions[2]
- Position 7 - Card Data Input Mode, must be 5 (Integrated Circuit Card [ICC])

Payment Tokens - Card on File/Recurring Billing:

- Position 5 - Cardholder Present, must be either:
  - Value 4 (Cardmember not present, standing authorization) or
  - Value 9 (Cardmember not present, recurring billing)
- Position 6 - Card Present, must be 0 (Card not present)

---

[1] Contactless transaction processing remains unchanged, utilizing track data and the existing authorization process. There are no Merchant or Third Party Processor changes for Contactless.

[2] If populated with value "Z", Data Field 61, National Use Data, is required.

6.2 Verification Services

American Express offers a number of tools by which Merchants can electronically verify information in the authorization process for Card Present and Card Not Present transactions. These tools enable comparison of customer provided data with Cardmember information on file with the Issuer. American Express recommends these verification tools be used simultaneously with other fraud mitigation tools such as Enhanced Authorization in multiple layers to help a Merchant mitigate the risk of fraud. These tools are not a guarantee that the transaction is in fact bona fide, or that the Merchant will not be subject to a Chargeback. For policy questions regarding transaction processing, refer to one or more of the following:

- *American Express Merchant Regulations - U.S.*
- *Canada Merchant Operating Manual (MOM)*
- Local market Terms of Conditions or Contracts for those markets outside of the U.S. and Canada

6.2.1 Enhanced Authorization

The Enhanced Authorization tool helps mitigate fraud before a transaction is authorized by analyzing key transaction data fields submitted with authorization requests. When these additional data fields are included in authorization requests, the Issuer can make a more thorough risk assessment, enabling a more informed authorization decision.

Merchants may already capture Enhanced Authorization data fields and other Card information as part of the ordering process. While sending all data fields is the most effective use of Enhanced Authorization, any additional data fields can provide a more informed authorization response.

6.2.1 Enhanced Authorization (continued)

Enhanced data fields may include:

Data Type	Data Element Supported		Location
Internet Data	• IP address • Email address • Product SKU (Stock Keeping Unit)		ITD format, Data Field 47
Phone Data	Order telephone number		205-byte format, Data Field 63
Airline Data	• Passenger Name • Origin airport • Destination airport • Travel date • Routing	• Class of service/Fare Basis • Number of passengers • Airline carrier codes • Email address • IP address	IAC format, Data Field 47
Shipping Data	• Ship-to address • Postal code • Country code	• Telephone number • First and last name • Shipping method	205-byte format, Data Field 63
Goods Sold Data	Gift Cards in Card Present transactions		Goods Sold format, Data Field 47

6.3 Electronic Verification Services

The Electronic Verification Services supported include the following:

- Card Identification (CID) Verification
- Automated Address Verification (AAV)
- ZIP Code Verification
- Telephone Number Verification
- Email Address Verification

6.3.1 Card Identifier (CID) Verification

The Card Identifier (CID; a.k.a., 4DBC or 4CSC) Verification tool helps mitigate fraud on keyed and swiped transactions. The CID number is associated with each individual Card. Merchants request the four-digit CID printed on the Card from the Cardmember at the time of purchase and then submit the CID with the Authorization request. Verification of the CID is one method to authenticate whether an individual making a purchase has possession of the Card.

The CID is a four-digit, (flat) number that is printed on every American Express Card. The CID is usually located above the Cardmember Account Number on the face of the Card. In each of the following illustrations of American Express Card products, the CID is circled. For details on CID/ 4DBC/4CSC entry in the Authorization Request (1100) message, see page 135. See also, related topics on pages 82 and 194.

For more information on American Express Keyed CID/4DBC/4CSC, contact your American Express representative.

6.3.2 Automated Address Verification (AAV)

The Automated Address Verification tool compares the name, street address, and Zip Code provided by the customer with the Cardmember's information on file with the Issuer.

Merchants, especially those operating in a Card Not Present environment (e.g., mail-order, telephone-order and Internet), use Automated Address Verification (AAV) to evaluate Cardmember identity by comparing information provided by the customer at the point of sale with Cardmember information on file with the Issuer.

Merchants use the Authorization Request (1100) message to transmit an independent AAV request, or a combination authorization/AAV request. To use AAV, a Merchant transmits a Cardmember's name as it appears on the Card, street address, and/or postal code for Issuer verification.

Issuer systems compare the information provided by the Merchant with Cardmember data listed in the card Issuer's records, and transmit a response in Data Field 44, Additional Response Data, of the Authorization Response (1110) message, indicating if all information is valid or if the Cardmember name, address, and/or postal code do not match. American Express does not return Cardmember data to the Merchant.

American Express encourages Merchants who physically deliver merchandise to include Ship-to address information as part of Enhanced Authorization tool (EA), which is available in the 205-byte version of Data Field 63 of the Authorization Request (1100) message.

AAV Response Data

Merchants certified for AAV must use Data Field 63, Private Use Data, in the Authorization Request (1100) message. After processing, American Express returns the AAV Response Code in Data Field 44, Additional Response Data, or Data Field 62, Private Use Data, of the corresponding Authorization Response (1110) message. For more information, see pages 158, 198 and 212.

6.3.3 ZIP Code Verification

In the United States, the ZIP Code Verification tool is part of Automated Address Verification (AAV). It compares the ZIP Code provided by the Cardmember with the ZIP Code on file with the Issuer. The Cardmember is prompted to enter the ZIP Code at the point of sale.

Care should be taken when implementing this feature, because postal codes are not associated with all American Express Card numbers. One example of an American Express Card with no associated address would be a non-personalized American Express Prepaid Card. Improper Automated Address Verification programming can disrupt POS authorizations; for example, when no postal code is on file.

6.3.3 ZIP Code Verification (continued)

ZIP Code Response Data

Merchants certified for ZIP Code verification must use Data Field 63, Private Use Data, in the Authorization Request (1100) message. After processing, American Express returns the ZIP Code Response Code in Data Field 44, Additional Response Data, or Data Field 62, Private Use Data, of the corresponding Authorization Response (1110) message. For more information, see pages 158, 198 and 212.

6.3.4 Telephone Number Verification

The Telephone Number Verification tool compares the telephone number provided by the Customer at the point of sale with the Cardmember's telephone number on file with the Issuer. This tool helps Merchants evaluate the validity of a charge by reviewing information about the Cardmember not available on the Card.

Telephone Number Response Data

Telephone Number Verification works much the same as Automated Address Verification (AAV). However, a certified Merchant transmits a telephone number in the Authorization Request (1100) message, Data Field 63, Private Use Data. The Issuer compares the information provided by the Merchant with the Cardmember's records, and returns the Response Code for Cardmember Phone Number in the Authorization Response (1110) message, Data Field 62, Private Use Data. Data Field 62 also contains the matching results for the additional Automated Address Verification (AAV) subfields (i.e., Cardmember postal code, street address, and name) and Email Address verification. For more information, see pages 158 and 212. As with all verification services, American Express does not return Cardmember data to the Merchant.

6.3.5 Email Address Verification

The Email Address Verification tool compares the email address provided by the Customer at the point of sale, with the Cardmember's email address on file with the Issuer. This tool helps Merchants evaluate the validity of a charge by reviewing information about the Cardmember not available on the Card.

Email Address Response Data

A certified Merchant transmits the Cardmember Email Address in the Authorization Request (1100) message in Data Field 47, Additional Data - National, using Card Not Present - Internet Telephone Data [ITD] or Internet Airline Customer [IAC] formats, and the formats of Data Field 63, Private Use Data, with RTI = "AE", to receive a response code for Email Address Verification. The Issuer compares the information provided by the Merchant with the Cardmember's records, and returns the Response Code for Email Address in Data Field 62, Private Use Data, in the Authorization Response (1110) message. Matching results for additional Automated Address Verification (AAV) subfields (i.e., Cardmember postal code, street address and name) and Telephone number verification are also provided. For more information, see pages 117, 158 and 212. As with all verification services, American Express does not return Cardmember data to the Merchant.

6.4 American Express SafeKey℠

American Express SafeKey enables online authentication of Cardmember transactions. American Express SafeKey works by providing an additional layer of security in online transactions as the Cardmember enters their payment information. American Express SafeKey helps prevent unauthorized online use before it happens by confirming the Cardmember's identity with an additional password or unique value.

American Express SafeKey is based on the 3-D Secure® protocol, which provides an additional level of security for online transactions. American Express continues to expand American Express SafeKey functionality into additional countries. Refer to the following website: AmexSafeKey for the most current enablement updates.

6.5 Online PIN

Online Personal Identification Number (PIN) validation is a Cardholder Verification Method (CVM) used to authenticate the Cardmember at the Point of Sale (POS). This will provide the ability for Third Party Processors and Merchants to allow the use of an online PIN as an acceptable CVM to complete a Card Present transaction. This method entails sending an online Authorization Request (1100) message which carries encrypted PIN data entered by the Cardmember at the POS to American Express for validation during Authorization processing.

6.5.1 Master/Session Key Management Methodology

The Master/Session Key management method is used to encrypt online PIN data. Master Key is the key exchange key also known as the Zone Master Key (ZMK). Session Key refers to the PIN encryption key also known as the Zone PIN Key (ZPK).

American Express supports two different implementations, Static and Dynamic, of the Master/Session methodology. Both of these implementations support Merchants and Third Party Processors at the host-link level..

Implementation	Description
STATIC	• Unique fixed key applied to all PINs. • Master key is exchanged manually as part of initial setup. • Session keys are refreshed every three years or upon request.
DYNAMIC	• Unique session key applied to all PINs. • Master key is exchanged manually as part of initial setup to protect exchange of session key. • Session key is frequently exchanged via network messaging. • Session key is refreshed on an agreed period (e.g., daily).

***STATIC Key Exchange:**

1. Manual key exchange for ZMK and ZPK. Refer to the *American Express Online PIN Processing Implementation Guide for Merchants or Third Party Processors*.
2. Merchant sends Authorization Request (1100) message with encrypted block in Data Field 52 - Personal Identification Number (PIN) Data.

*For the *American Express Online PIN Processing Implementation Guide* for *Merchants or Third Party Processors*, contact your American Express representative.

6.5.1 Master/Session Key Management Methodology (continued)

*DYNAMIC Key Exchange:

1. Merchant or Third Party Processor successfully requests a session key exchange in the Network Management Request (1804) message:
   - Data Field 24 – Function Code 811 = Dynamic key exchange request
2. New PIN key and Key Check Values (KCV) are returned for a successful exchange in the Network Management Response (1814) message:
   - Data Field 39 – Action Code = 800 (Accepted)
   - Data Field 96 – Key Management Data - New PIN key and Key Check Values (KCV)
3. Merchant sends Authorization Request (1100) message with PIN and KCV:
   - Data Field 52 – Personal Identification Number (PIN) Data = Encrypted PIN block encrypted using the Key that was exchanged from subfield SESSION PIN KEY in Data Field 96 - Key Management Data, in the Network Management Response (1814) message.
   - Data Field 96 – Key Management Data = In subfield, SESSION PIN KEY CHECK VALUE, the value found in Data Field 96 of the Network Management Response (1814) message must be copied, without alteration, into Data Field 96 of the Authorization Request (1100) message. This value is used to identify the Key used.

*For the *American Express Online PIN Processing Implementation Guide* for *Merchants or Third Party Processors*, contact your American Express representative.

6.5.2 Derived Unique Key Per Transaction (DUKPT)

American Express supports the Derived Unique Key Per Transaction (DUKPT) implementation. The DUKPT encryption methodology is preferred for Terminal to Host connectivity. Refer to the *ANSI X9.24 Standard* for further details on DUKPT implementation and associated requirements.

.

Implementation	Description
DUKPT	• A base key is provided by American Express to Key Injection Facility (KIF). • Base key is used to derive a key which is injected into the terminal. • Terminal key is used with terminal data to derive a unique key which is applied to each PIN transaction. • A unique key applied to each PIN transaction encrypts the data from the domain of the Secure PIN entry device through to the American Express network.

***DUKPT (Derived Unique Key Per Transaction) Exchange:**

1. A base key is provided by American Express to Key Injection Facility (KIF). For additional information, contact your American Express representative.
2. Merchant sends Authorization Request (1100) message with Key Serial Number (KSN):
    - Merchant sends Authorization Request (1100) message with encrypted block in Data Field 52 - Personal Identification Number (PIN) Data.
    - Data Field 53 - Security Related Control Information = Key Serial Number (KSN) provided for PIN translation

*For the *American Express Online PIN Processing Implementation Guide* for *Merchants or Third Party Processors*, contact your American Express representative.

7.0 ISO 8583 Message Bit Map Table

ISO 8583 supports two 64-position bit maps, which are designated as the Primary and Secondary Bit Maps, to indicate which of up to 128 data fields are contained in a message. All 128 data fields and bit positions are listed in the following tables.

Note: Data fields shown in **reversed text** (white letters on a black background) are not used by American Express, and unauthorized use of these data fields may cause message rejection.

7.1 Primary Bit Map

Data Field	Data Field Name	Max. Data Field Length	Data Field Type
---	MESSAGE TYPE IDENTIFIER (MTI)	4 bytes, fixed	Numeric
---	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary
1	BIT MAP - SECONDARY	8 bytes, 64 bits	Binary
2	PRIMARY ACCOUNT NUMBER (PAN)	21 bytes, LLVAR	Numeric
3	PROCESSING CODE	6 bytes, fixed	Numeric
4	AMOUNT, TRANSACTION	12 bytes, fixed	Numeric
5	AMOUNT, RECONCILIATION	12 bytes, fixed	Numeric
6	AMOUNT, CARDHOLDER BILLING	12 bytes, fixed	Numeric
7	DATE AND TIME, TRANSMISSION	10 bytes, fixed	Numeric
8	AMOUNT, CARDHOLDER BILLING FEE	8 bytes, fixed	Numeric
9	CONVERSION RATE, RECONCILIATION	8 bytes, fixed	Numeric
10	CONVERSION RATE, CARDHOLDER BILLING	8 bytes, fixed	Numeric
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric
13	DATE, EFFECTIVE	4 bytes, fixed	Numeric
14	DATE, EXPIRATION	4 bytes, fixed	Numeric
15	DATE, SETTLEMENT	6 bytes, fixed	Numeric
16	DATE, CONVERSION	4 bytes, fixed	Numeric
17	DATE, CAPTURE	4 bytes, fixed	Numeric
18	MERCHANT TYPE	4 bytes, fixed	Numeric
19	COUNTRY CODE, ACQUIRING INSTITUTION	3 bytes, fixed	Numeric
20	COUNTRY CODE, PRIMARY ACCOUNT NUMBER	3 bytes, fixed	Numeric
21	COUNTRY CODE, FORWARDING INSTITUTION	3 bytes, fixed	Numeric
22	POINT OF SERVICE DATA CODE	12 bytes, fixed	Alphanumeric
23	CARD SEQUENCE NUMBER	3 bytes, fixed	Numeric
24	FUNCTION CODE	3 bytes, fixed	Numeric
25	MESSAGE REASON CODE	4 bytes, fixed	Numeric

7.1 Primary Bit Map (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type
26	CARD ACCEPTOR BUSINESS CODE	4 bytes, fixed	Numeric
27	APPROVAL CODE LENGTH	1 byte, fixed	Numeric
28	DATE, RECONCILIATION	6 bytes, fixed	Numeric
29	RECONCILIATION INDICATOR	3 bytes, fixed	Numeric
30	AMOUNTS, ORIGINAL	24 bytes, fixed	Numeric
31	ACQUIRER REFERENCE DATA	50 bytes, LLVAR	Alphanumeric & special characters
32	ACQUIRING INSTITUTION IDENTIFIFCATION CODE	13 bytes, LLVAR	Numeric
33	FORWARDING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric
34	PRIMARY ACCOUNT NUMBER, EXTENDED	30 bytes, LLVAR	Numeric
35	TRACK 2 DATA	39 bytes, LLVAR	Alphanumeric & special characters
36	TRACK 3 DATA	107 bytes, LLLVAR	Numeric & special characters
37	RETRIEVAL REFERENCE NUMBER	12 bytes, fixed	Alphanumeric & special characters
38	APPROVAL CODE	6 bytes, fixed	Alphanumeric & spaces
39	ACTION CODE	3 bytes, fixed	Numeric
40	SERVICE CODE	3 bytes, fixed	Numeric
41	CARD ACCEPTOR TERMINAL IDENTIFICATION	8 bytes, fixed	Alphanumeric & special characters
42	CARD ACCEPTOR IDENTIFICATION CODE	15 bytes, fixed	Alphanumeric & special characters
43	CARD ACCEPTOR NAME/LOCATION	101 bytes, LLVAR	Alphanumeric & special characters
44	ADDITIONAL RESPONSE DATA	27 bytes, LLVAR	Alphanumeric & special characters
45	TRACK 1 DATA	78 bytes, LLVAR	Alphanumeric & special characters
46	AMOUNTS, FEES	207 bytes, LLLVAR	Alphanumeric
47	ADDITIONAL DATA - NATIONAL	304 bytes, LLLVAR	Alphanumeric & special characters
48	ADDITIONAL DATA - PRIVATE	43 bytes, LLLVAR	Alphanumeric & special characters
49	CURRENCY CODE, TRANSACTION	3 bytes, fixed	Numeric
50	CURRENCY CODE, RECONCILIATION	3 bytes, fixed	Alpha or Numeric
51	CURRENCY CODE, CARDHOLDER BILLING	3 bytes, fixed	Alpha or Numeric
52	PERSONAL IDENTIFICATION NUMBER (PIN) DATA	8 bytes, 64 bits	Binary
53	SECURITY RELATED CONTROL INFORMATION	19 bytes, LLVAR	Alphanumeric
54	AMOUNTS, ADDITIONAL	123 bytes, LLLVAR	Alphanumeric & special characters
55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA	259 bytes, LLLVAR	Alphanumeric & special characters, BCD or binary
56	ORIGINAL DATA ELEMENTS	37 bytes, LLVAR	Numeric
57	AUTHORIZATION LIFE CYCLE CODE	3 bytes, fixed	Numeric
58	AUTHORIZING AGENT INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric

7.1 Primary Bit Map (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type
59	TRANSPORT DATA	1002 bytes, LLLVAR	Alphanumeric & special characters
60	NATIONAL USE DATA	106 bytes, LLLVAR	Alphanumeric & special characters
61	NATIONAL USE DATA	103 bytes, LLLVAR	Alphanumeric & special characters
62	PRIVATE USE DATA	63 bytes, LLLVAR	Alphanumeric & special characters or binary
63	PRIVATE USE DATA	208 bytes, LLLVAR	Alphanumeric & special characters
64	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary

7.2 Secondary Bit Map

Data Field	Data Field Name	Max. Data Field Length	Data Field Type
65	RESERVED FOR ISO USE	8 bytes, 64 bits	Binary
66	AMOUNTS, ORIGINAL FEES	204 bytes, LLLVAR	Alphanumeric & special characters
67	EXTENDED PAYMENT DATA	2 bytes, fixed	Numeric
68	COUNTRY CODE, RECEIVING INSTITUTION	3 bytes, fixed	Numeric
69	COUNTRY CODE, SETTLEMENT INSTITUTION	3 bytes, fixed	Numeric
70	COUNTRY CODE, AUTHORIZING AGENT INSTITUTION	3 bytes, fixed	Numeric
71	MESSAGE NUMBER	8 bytes, fixed	Numeric
72	DATA RECORD	999 bytes, LLLVAR	Alphanumeric & special characters
73	DATE, ACTION	6 bytes, fixed	Numeric
74	CREDITS, NUMBER	10 bytes, fixed	Numeric
75	CREDITS, REVERSAL NUMBER	10 bytes, fixed	Numeric
76	DEBITS, NUMBER	10 bytes, fixed	Numeric
77	DEBITS, REVERSAL NUMBER	10 bytes, fixed	Numeric
78	TRANSFER, NUMBER	10 bytes, fixed	Numeric
79	TRANSFER, REVERSAL NUMBER	10 bytes, fixed	Numeric
80	INQUIRIES, NUMBER	10 bytes, fixed	Numeric
81	AUTHORIZATIONS, NUMBER	10 bytes, fixed	Numeric
82	INQUIRIES, REVERSAL NUMBER	10 bytes, fixed	Numeric
83	PAYMENTS, NUMBER	10 bytes, fixed	Numeric
84	PAYMENTS, REVERSAL NUMBER	10 bytes, fixed	Numeric
85	FEE COLLECTIONS, NUMBER	10 bytes, fixed	Numeric

7.2 Secondary Bit Map (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type
86	CREDITS, AMOUNT	16 bytes, fixed	Numeric
87	CREDITS, REVERSAL AMOUNT	16 bytes, fixed	Numeric
88	DEBITS, AMOUNT	16 bytes, fixed	Numeric
89	DEBITS, REVERSAL AMOUNT	16 bytes, fixed	Numeric
90	AUTHORIZATIONS, REVERSAL NUMBER	10 bytes, fixed	Numeric
91	COUNTRY CODE, TRANSACTION DESTINATION INSTITUTION	3 bytes, fixed	Numeric
92	COUNTRY CODE, TRANSACTION ORIGINATOR INSTITUTION	3 bytes, fixed	Numeric
93	TRANSACTION DESTINATION INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric
94	TRANSACTION ORIGINATOR INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric
95	CARD ISSUER REFERENCE DATA	99 bytes, LLVAR	Alphanumeric & special characters
96	KEY MANAGEMENT DATA	999 bytes, LLLVAR	Binary
97	AMOUNT, NET RECONCILIATION	16 bytes, fixed	X + N (see note at end of table)
98	PAYEE	25 bytes, LLVAR	Alphanumeric & special characters
99	SETTLEMENT INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Alphanumeric
100	RECEIVING INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric
101	FILE NAME	17 bytes, LLVAR	Alphanumeric & special characters
102	ACCOUNT IDENTIFICATION 1	28 bytes, LLVAR	Alphanumeric & special characters
103	ACCOUNT IDENTIFICATION 2	28 bytes, LLVAR	Alphanumeric & special characters
104	TRANSACTION DESCRIPTION	100 bytes, LLLVAR	Alphanumeric & special characters
105	CREDITS, CHARGEBACK AMOUNT	16 bytes, fixed	Numeric
106	DEBITS, CHARGEBACK AMOUNT	16 bytes, fixed	Numeric
107	CREDITS, CHARGEBACK NUMBER	10 bytes, fixed	Numeric
108	DEBITS, CHARGEBACK NUMBER	10 bytes, fixed	Numeric
109	CREDITS, FEE AMOUNTS	84 bytes, LLVAR	Alphanumeric & special characters
110	DEBITS, FEE AMOUNTS	84 bytes, LLVAR	Alphanumeric & special characters
111	RESERVED FOR ISO USE	999 bytes, LLLVAR	Alphanumeric & special characters
112	RESERVED FOR ISO USE	999 bytes, LLLVAR	Alphanumeric & special characters
113	RESERVED FOR ISO USE	999 bytes, LLLVAR	Alphanumeric & special characters

Note: For Data Field 97, X = "C" credit or "D" debit, concatenated with "N" numeric amount.

7.2 Secondary Bit Map (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type
114	RESERVED FOR ISO USE	999 bytes, LLLVAR	Alphanumeric & special characters
115	RESERVED FOR ISO USE	999 bytes, LLLVAR	Alphanumeric & special characters
116	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
117	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
118	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
119	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
120	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
121	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
122	RESERVED FOR NATIONAL USE	999 bytes, LLLVAR	Alphanumeric & special characters
123	RESERVED FOR PRIVATE USE	999 bytes, LLLVAR	Alphanumeric & special characters
124	RESERVED FOR PRIVATE USE	999 bytes, LLLVAR	Alphanumeric & special characters
125	RESERVED FOR PRIVATE USE	999 bytes, LLLVAR	Alphanumeric & special characters
126	RESERVED FOR PRIVATE USE	999 bytes, LLLVAR	Alphanumeric & special characters
127	RESERVED FOR PRIVATE USE	999 bytes, LLLVAR	Alphanumeric & special characters
128	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary

this page intentionally left blank

8.0 ISO 8583 Authorization Request/Response Message Formats

This section describes the Authorization Request (1100) and Authorization Response (1110) messages, as defined for the ISO 8583 format. These messages are constructed as specified in the ISO 8583-1993 standard. If your system supports a different version of ISO 8583, notify your American Express representative.

8.1 1100 Authorization Request

Length of Record: 900 bytes maximum (recommended)

Note: Messages transmitted to American Express must not exceed 900 bytes in total length. Since all data fields in the Authorization Request (1100) message section are not used for a given transaction, this maximum would not be exceeded. For example, Data Fields 45 and 35 (Track 1 Data and Track 2 Data) are not used in Card Not Present transactions. For assistance in selecting optional data fields, and determining the appropriate formats and variable data field lengths to use, contact your American Express representative.

Any attempt to use the Authorization Request (1100) message as a preauthorization, will be treated as a normal authorization transaction.

Description: This message is used to transmit an Authorization and/or Automated Address Verification (AAV) Request to American Express.

.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
—	MESSAGE TYPE IDENTIFIER	4 bytes, fixed	Numeric	Mandatory	62
—	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary	Mandatory	62
1	BIT MAP - SECONDARY	8 bytes, 64 bits	Binary	See page ➔	64
2	PRIMARY ACCOUNT NUMBER (PAN)	21 bytes, LLVAR	Numeric	Mandatory	65
3	PROCESSING CODE	6 bytes, fixed	Numeric	Mandatory	66
4	AMOUNT, TRANSACTION	12 bytes, fixed	Numeric	Mandatory	67
7	DATE AND TIME, TRANSMISSION	10 bytes, fixed	Numeric	Optional	69
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters	Mandatory	70
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric	Mandatory	71
13	DATE, EFFECTIVE	4 bytes, fixed	Numeric	See page ➔	72

8.1 1100 Authorization Request (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
14	DATE, EXPIRATION	4 bytes, fixed	Numeric	See page ➔	73
15	DATE, SETTLEMENT	6 bytes, fixed	Numeric	N/A	74
18	MERCHANT TYPE	4 bytes, fixed	Numeric	N/A	75
19	COUNTRY CODE, ACQUIRING INSTITUTION	3 bytes, fixed	Numeric	Mandatory	75
22	POINT OF SERVICE DATA CODE	12 bytes, fixed	Alphanumeric	Mandatory	76
24	FUNCTION CODE	3 bytes, fixed	Numeric	See page ➔	86
25	MESSAGE REASON CODE	4 bytes, fixed	Numeric	See page ➔	91
26	CARD ACCEPTOR BUSINESS CODE	4 bytes, fixed	Numeric	Mandatory	92
27	APPROVAL CODE LENGTH	1 byte, fixed	Numeric	Optional	93
31	ACQUIRER REFERENCE DATA	50 bytes, LLVAR	Alphanumeric & special characters	N/A	94
32	ACQUIRING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Optional	95
33	FORWARDING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Optional	96
35	TRACK 2 DATA	39 bytes, LLVAR	Alphanumeric & special characters	Conditional	97
37	RETRIEVAL REFERENCE NUMBER	12 bytes, fixed	Alphanumeric & special characters	Optional	100
41	CARD ACCEPTOR TERMINAL IDENTIFICATION	8 bytes, fixed	Alphanumeric & special characters	See page ➔	101
42	CARD ACCEPTOR IDENTIFICATION CODE	15 bytes, fixed	Alphanumeric & special characters	Mandatory	102
43	CARD ACCEPTOR NAME/LOCATION	101 bytes, LLVAR	Alphanumeric & special characters	See page ➔	104
45	TRACK 1 DATA	78 bytes, LLVAR	Alphanumeric & special characters	See page ➔	109
47	ADDITIONAL DATA - NATIONAL	304 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	113

8.1 1100 Authorization Request (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
48	ADDITIONAL DATA - PRIVATE	43 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	130
49	CURRENCY CODE, TRANSACTION	3 bytes, fixed	Numeric	Mandatory	133
52	PERSONAL IDENTIFICATION NUMBER (PIN) DATA	8 bytes, 64 bits	Binary	See page ➔	134
53	SECURITY RELATED CONTROL INFORMATION	19 bytes, LLVAR	Alphanumeric	See page ➔	135
55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA	259 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	138
60	NATIONAL USE DATA	106 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	143
61	NATIONAL USE DATA	103 bytes, LLLVAR	Alphanumeric, special characters & binary	See page ➔	149
62	PRIVATE USE DATA	103 bytes, LLLVAR	Alphanumeric, special characters & binary	See page ➔	153
63	PRIVATE USE DATA	103 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	157
96	KEY MANAGEMENT DATA	17 bytes, LLLVAR	Binary	See page ➔	177
128	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary	N/A	178

8.1 1100 Authorization Request (continued)

Data Field — None	MESSAGE TYPE IDENTIFIER
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	`1100`
Field Requirement:	Mandatory
Description:	The constant literal "`1100`" signifies the ISO 8583 Authorization Request message.

Data Field — None	BIT MAP - PRIMARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory
Description:	Each bit in this data field signifies the presence (value 1) or absence (value 0) of a data field in the Authorization Request (1100) message. If the data field is mandatory, or is optional and the Merchant elects to use that data field, its assigned bit map position must contain a value of "1", to indicate the data field is present. If the data field is optional and not used, its assigned bit map position must contain a value of "0", to indicate the data field is omitted.

8.1 1100 Authorization Request (continued)

Data Field — None **BIT MAP - PRIMARY (continued)**

The following diagram illustrates a 64-bit string contained within an eight-byte data field. Each bit signifies the presence (1) or absence (0) of the data field used within the Authorization Request (1100) message format:

1	0	9	0	17	0	25	1	33	1	41	1	49	1	57	0
2	1	10	0	18	0	26	1	34	0	42	1	50	0	58	0
3	1	11	1	19	1	27	1	35	1	43	1	51	0	59	0
4	1	12	1	20	0	28	0	36	0	44	0	52	0	60	0
5	0	13	1	21	0	29	0	37	1	45	1	53	1	61	0
6	0	14	1	22	1	30	0	38	0	46	0	54	0	62	0
7	1	15	0	23	0	31	0	39	0	47	1	55	0	63	1
8	0	16	0	24	1	32	1	40	0	48	1	56	0	64	0

The following diagram illustrates how to calculate the hexadecimal equivalent of the bit map from the table shown above:

Position 1-8	Position 17-24	Position 33-40	Position 49-56
0111 = **7**	0010 = **2**	1010 = **A**	1000 = **8**
0010 = **2**	0101 = **5**	1000 = **8**	1000 = **8**
Position 9-16	**Position 25-32**	**Position 41-48**	**Position 57-64**
0011 = **3**	1110 = **E**	1110 = **E**	0000 = **0**
1100 = **C**	0001 = **1**	1011 = **B**	0010 = **2**

Hexadecimal equivalents for bit map:

```
0000 = 0  1000 = 8
0001 = 1  1001 = 9
0010 = 2  1010 = A
0011 = 3  1011 = B
0100 = 4  1100 = C
0101 = 5  1101 = D
0110 = 6  1110 = E
0111 = 7  1111 = F
```

The hexadecimal equivalent for the bit map in this Authorization Request (1100) message (as shown above) is:

72 3C 25 E1 A8 EB 88 02

8.1 1100 Authorization Request (continued)

Data Field 1	BIT MAP - SECONDARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory — For Data Fields 65 through 128
Description:	Each bit in this data field signifies the presence (value 1) or absence (value 0) of a data field in the Authorization Request (1100) message. If the data field is mandatory, or is optional and the Merchant elects to use that data field, its assigned bit map position must contain a value of "1", to indicate the data field is present. If the data field is optional and not used, its assigned bit map position must contain a value of "0", to indicate the data field is omitted.

8.1 1100 Authorization Request (continued)

Data Field 2	PRIMARY ACCOUNT NUMBER (PAN)
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 21 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 19 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	• Mandatory — American Express Card transactions, other Card products and bankcard transactions 1. American Express supports Diner's Club, JCB, VISA and MasterCard processing. For details, contact your American Express representative. 2. Vendors and Third Party Processors doing business in Australia, Canada, India, Mexico and New Zealand must be certified to process JCB transactions. • Not used — American Express Travelers Cheques

Description:	This data field contains the Cardmember Account Number, or Payment Token Account Number, preceded by a two-digit, Variable Length Indicator (VLI). The VLI must indicate the exact length of the account number, and no additional characters should be added to this data field.
	For example, the 15-digit American Express Account Number derived from an ANSI track data field that has embedded spaces (e.g., "`3714 496353 11004`") would have the spaces removed and appear as:
	`0 1`
	`12345678901234567`
	`153714496353110 04`
	Check digit validation is required. For details, refer to Check Digit Validation in the *American Express Global Codes & Information Guide*.
	Note: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 3	PROCESSING CODE
Length of Field:	6 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field indicates the financial service being requested. Valid Processing Codes: `004000` = Card Authorization Request `004800` = Combination Automated Address Verification (AAV) and Authorization `034000` = AMEX Emergency Check Cashing `064000` = AMEX Travelers Cheque Encashment `174800` = Transaction for Automated Address Verification (AAV) Only **Note**: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 4	AMOUNT, TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, right justified, zero filled
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the total transaction amount (including tax), in the currency designated by the Currency Code Transaction (Data Field 49). For example, for U.S. Dollar (840) transactions, two decimal places are implied. Thus, the value $100.00 would be entered as: "`000000010000`" For Japanese Yen (392) transactions, zero decimal places are implied. Thus, the value ¥10,000 would be entered as: "`000000010000`" American Express limits the maximum allowable value in this data field based on the U.S. Dollar equivalent calculated by American Express. Transmitted transaction amounts greater than the maximum allowed will result in an "invalid amount" edit error. For more information on maximum allowable values, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*.

8.1 1100 Authorization Request (continued)

Data Field 4	AMOUNT, TRANSACTION (continued)

Notes:

1. If Data Field 3, Processing Code, is "`174800`" (Transaction for Automated Address Verification [AAV] Only), then this data field must be zero filled.
2. A Prepaid Card Balance Inquiry for American Express Prepaid Card products can be submitted by zero filling Data Field 4 (Amount, Transaction), if Data Field 24 (Function Code) value is "`181`" (Partial Authorization) or "`182`" (Authorization with Balance Return). The available balance is returned in Data Field 54 (Amounts, Additional) of the Authorization Response (1110) message. However, balance inquiries cannot be processed for Card products other than American Express Prepaid Cards.
3. If this data field is zero filled for transactions other than for American Express Prepaid Card products, and Data Field 3 (Processing Code) is "`004000`" (Card Authorization) or "`004800`" (Combination AAV and Authorization), an edit error will result. Consequently, any supplemental data field verification requests, such as AAV (Automated Address Verification) or CID (Card Identifier), will not be performed. For these invalid requests, Data Field 54 will not be returned and Data Field 39 (Action Code) will contain an edit error code in the corresponding Authorization Response (1110) message.
4. This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration, except for Prepaid Card transactions. For more information, see page 183.

American Express Travelers Cheque Encashment

For American Express Travelers Cheques, this data field is used to capture the total amount of Travelers Cheques that will be encashed by a single customer, in the currency designated by the Currency Code, Transaction (Data Field 49). Processing Code (Data Field 3) must be "`064000`".

For example, if a customer presents five, $100 USD Travelers Cheques for encashment, this entry would be "`000000050000`" ($500.00).

8.1 1100 Authorization Request (continued)

Data Field 7	DATE AND TIME, TRANSMISSION
Length of Field:	10 bytes, fixed length
Field Type:	Numeric, MMDDhhmmss
Constant:	None
Field Requirement:	Optional
Description:	This data field contains the system date and time (e.g., GMT) when the Merchant transmits the transaction information to American Express. The format is MMDDhhmmss. The value of this data field must be a valid date and time.

Subfield	Definition	Digits	Range
MM	Month	2	01-12
DD	Day	2	01-31
hh	Hour	2	00-23
mm	Minute	2	00-59
ss	Second	2	00-59

Note: This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 11	SYSTEMS TRACE AUDIT NUMBER
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric (upper case) & special characters
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain a unique trace number, assigned by the Merchant, to help identify an individual transaction. A different number must be assigned to each transaction. **Note**: This data field is mandatory for processing this message and it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 12	DATE AND TIME, LOCAL TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, YYMMDDhhmmss
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the year, month, day and local time when the transaction took place at the card acceptor location. The format is YYMMDDhhmmss. The value of this data field must be a valid date and time:

Subfield	Definition	Digits	Range
YY	Year	Last 2 only	00-99
MM	Month	2	01-12
DD	Day	2	01-31
hh	Hour	2	00-23
mm	Minute	2	00-59
ss	Second	2	00-59

Note: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 13	DATE, EFFECTIVE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric, YYMM
Constant:	None
Field Requirement:	• Conditional — American Express Card transactions • Not applicable — Other transactions
Description:	This data field contains the effective date embossed on the face of the American Express or American Express-supported Card. If entered manually, the format is YYMM. The value of this data field must be a valid date. If the effective date is unavailable, omit this data field. No default values or all zeros will be accepted (e.g., "0000").

Subfield	Definition	Digits	Range
YY	Year	Last 2 only	00-99
MM	Month	2	01-12

Notes:

1. Most American Express Card products are embossed with the effective and/or expiration dates in format MMYY. This requires the Acquirer, their devices, systems, Vendor software and Third Party Processors that prompt for or accept these dates in MMYY format, to convert this data by reversing the month and year values, so that the entry in this data field appears in YYMM format.
2. This data field is not required if the message contains Track 1 (preferred) or Track 2 data.

8.1 1100 Authorization Request (continued)

Data Field 14	DATE, EXPIRATION
Length of Field:	4 bytes, fixed length
Field Type:	Numeric, YYMM
Constant:	None
Field Requirement:	• Conditional — American Express and American Express supported Cards • Mandatory — Digital Wallet - application initiated (including application initiated Payment Token) transactions • Mandatory — VISA
Description:	This data field contains the expiration date embossed on the face of the American Express or American Express-supported Card. If entered manually, the format is YYMM. For Digital Wallet - application initiated (including application initiated Payment Token) transactions, the Payment Token Expiration Date will be passed through the Authorization Request (1100) message in lieu of Primary Account Number (PAN) Expiration Date. **Note**: This data field is not required if the message contains Track 1 (preferred) or Track 2 data successfully read from a valid Card swipe or read; or if this is a recurring billing or standing authorization transaction. For more information, see page 30. The value of this data field must be a valid date. No default values or all zeros will be accepted (e.g., "0000"). **VISA Transactions Only** This data field is mandatory for Merchants routing VISA transactions via the American Express Card Acceptance and Processing Network to non-American Express networks, during bankcard network outages. While American Express does not verify or validate this entry, VISA may reject transactions that do not include a valid card expiration date. For more information, contact your VISA representative.

Subfield	Definition	Digits	Range
YY	Year	Last 2 only	00-99
MM	Month	2	01-12

8.1 1100 Authorization Request (continued)

Data Field 15	DATE, SETTLEMENT
Length of Field:	6 bytes, fixed length
Field Type:	Numeric, YYMMDD
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

8.1 1100 Authorization Request (continued)

Data Field 18	MERCHANT TYPE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is reserved for internal American Express use only. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

Data Field 19	COUNTRY CODE, ACQUIRING INSTITUTION
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the numeric country code corresponding to the country in which the Merchant is located. For example, the numeric country code for a Merchant located in the USA is "840". For more information on numeric country codes, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*.

8.1 1100 Authorization Request (continued)

Data Field 22	POINT OF SERVICE DATA CODE
Length of Field:	12 bytes, fixed length
Field Type:	Alphanumeric, upper case
Constant:	None
Field Requirement:	Mandatory

Description:	The Point of Service (POS) Data Code is a series of codes that identify terminal capability, security data and specific conditions present at the time the transaction occurred at the point of service. The POS Data Code consists of twelve positions, each with its own list of values. For example, Position 1 indicates the Card Data Input Capability, which may be one of several values such as Magnetic Stripe Read, Integrated Circuit Card (ICC), Key Entered and so on. Similarly, each of the other positions identifies a particular value related to the transaction.
	
	Merchants must populate all positions in Data Field 22 with valid data. However, if the applicable information is unavailable or unknown, the Merchant should consult with their American Express representative to determine the appropriate value.
	
	The POS Data Code must be determined from the table of values listed on page 78.
	
	`0 1`
	`123456789012`
	`261101200120`
	
	In the above example:
	Position 1= `2` Position 5 = `0` Position 9 = `0`
	Position 2= `6` Position 6 = `1` Position 10 = `1`
	Position 3= `1` Position 7 = `2` Position 11 = `2`
	Position 4= `1` Position 8 = `0` Position 12 = `0`

8.1 1100 Authorization Request (continued)

Data Field 22	POINT OF SERVICE DATA CODE (continued)
Description:	**Important notes for POS Data Code tables that follow:** 1. Values shown in **reversed text** (white letters on a black background) are defined by ISO, but are reserved for future use or not currently defined by American Express. For information on these values, contact your American Express representative. 2. The POS Data Codes used in this data field must also be included in the corresponding submission file. 3. For recurring billing and standing authorization information, see page 30.

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 1 Code	Card Data Input Capability — This subfield indicates the maximum capability of the device used to originate this transaction.
0	Unknown
1	Manual, no terminal
2	Magnetic stripe read
3	Bar code
4	Optical Character Recognition (OCR)
5	Integrated Circuit Card (ICC) **Note**: American Express-certified EMV terminal and link
6	Key entered
7	Reserved for ISO use
8	Reserved for national use
9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

Note: For information on how to properly identify American Express ICC transactions, see Section 5.4.1 AEIPS

POS. 2 Code	Cardholder Authentication Capability — This subfield indicates the primary means used to verify the Cardmember's identity at this terminal.
0	No electronic authentication or unknown
1	PIN
2	Electronic signature analysis
3	Biometrics
4	Biographic
5	Electronic authentication inoperative
6	Other
7	Reserved for ISO use
8	Reserved for national use
9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 3 Code	Card Capture Capability — This subfield indicates if the terminal is capable of capturing card data.
0	None or unknown (Card Capture Capability unknown to Acquirer)
1	Capture
2-4	Reserved for ISO use
5-7	Reserved for national use
8-9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

POS. 4 Code	Operating Environment — This subfield indicates the terminal's location, and if it is attended by the card acceptor.
0	No terminal used or unknown
1	On premises of card acceptor, attended
2	On premises of card acceptor, unattended (e.g., Oil CAT/Customer Activated Terminals, kiosks, self-checkout, etc.)
3	Off premises of card acceptor, attended (e.g., portable POS device at trade shows, service calls, taxis, etc.)
4	Off premises of card acceptor, unattended (e.g., Food/Beverage vending machines, DVD vending machines, etc.)
5	On premises of Cardmember, unattended
6-7	Reserved for ISO use
8	Reserved for national use
9	Delivery mode unknown, unspecified
A-I	Reserved for ISO use
J-R	Reserved for national use
S	Electronic delivery of product (e.g., music, software, electronic tickets, etc., downloaded via Internet)
T	Physical delivery of product (e.g., music, software, tickets, etc., delivered by mail/courier)
U-W	Reserved for American Express network use
X-Y	Reserved for private use
Z	Transit Access Terminal - TAT

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 5 Code	Cardholder Present — This subfield indicates if the Cardmember is present at the point of service; and if not, the reason why.
0	Cardmember present
1	Cardmember not present, unspecified, unknown
2	Cardmember not present, mail order
3	Cardmember not present, telephone
4	Cardmember not present, standing authorization - To be used for situations where Cardmember information is on record (card on file); however, the billing frequency and amount are variable (e.g., travel, car rental, lodging, preferred clubs, frequent customer, delayed shipment, split bill transactions, etc.).
5-6	Reserved for ISO use
7-8	Reserved for national use
9	Cardmember not present, recurring billing - Used for regular recurring transactions, such as periodic billings (e.g., membership dues, subscribed services, insurance premiums, wireless services, newspaper and other regularly scheduled charges). The recurring billing amount can vary.
A-I	Reserved for ISO use
J-R	Reserved for national use
S	Cardmember not present, electronic transaction (e.g., Internet)
T	Reserved for American Express network use
U-Z	Reserved for private use

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 6 Code	Card Present — This subfield indicates if the card is present at the point of service.
0	Card not present
1	Card present
2-4	Reserved for ISO use
5-7	Reserved for national use
8-9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-V	Reserved for private use
W	Transponder (RFID token) — For transactions initiated by an electronic, radio-frequency device (transponder or RFID, e.g., Speedpass), this value may be used alone, or in conjunction with Data Field 62 transponder security/ID (code AXTN). Alternately, a transponder security/ID code may be entered in Data Field 62 without Value W in Data Field 22, Position 6. Ideally, both items are transmitted. For more details, see Section 5.4.2 Expresspay. **Note**: Do not use this value for American Express Expresspay transactions.
X	Contactless transactions, including American Express Expresspay. For more information, see Section 5.4.2 Expresspay.
Y	Mobile Proximity Payment - American Express internal use only
Z	Digital Wallet - application initiated (including application initiated Payment Token) transactions **Note**: Position 6, value Z must be used with Position 7, value 5.

Note: For additional information on Payment Token processing, see page 43.

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 7 Code	Card Data Input Mode — This subfield indicates the method used to capture information from the card.
0	Unspecified, unknown, track data present but incomplete or truncated
1	Manual, no terminal
2	Magnetic stripe read. (**Note**: Byte 7 = 2 only if this transaction contains Track 1 [preferred] and/or Track 2 data captured intact from the magnetic stripe.)
3	Bar code
4	Optical Character Recognition (OCR)
5	Integrated Circuit Card (ICC). **Notes**: 1. Byte 7 = 5 only if this transaction contains EMV and Track 2 data captured intact from the chip (non-Payment Token transactions). 2. If value Z is present in Position 6 Digital wallet - application initiated Payment Token) transactions, then Position 7, value 5 (Integrated Circuit Card ICC) must be present. 3. American Express-certified EMV terminal and link.
6	Key entered
7	Reserved for ISO use
8	Reserved for national use
9	Technical fallback - Transaction initiated as chip but was processed using an alternative technology (such as magnetic stripe).
A-I	Reserved for ISO use
J-R	Reserved for national use
S	Manually entered or keyed transaction with keyed CID/4DBC/4CSC. Data Field 53, Security Related Control Information must be present.
T-U	Reserved for private use
V	Reserved for American Express network use
W	Swiped transaction with keyed CID/4DBC/4CSC. Data Field 53, Security Related Control Information must be present.
X-Z	Reserved for private use

Notes:

- See CID/4DBC/4CSC location on typical American Express Card products.
- For more information on how to properly identify American Express ICC transactions, see Section 5.4.1 - AEIPS.
- For additional information on Payment Token processing, see page 43.

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 8 Code	Cardmember Authentication Method — This subfield indicates the method for verifying the Cardmember identity.
0	Not authenticated, unknown
1	PIN
2	Electronic signature analysis
3	Biometrics
4	Biographic
5	Manual signature verification
6	Other manual verification (e.g., drivers license)
7	Reserved for ISO use
8	Reserved for national use
9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S	Electronic Ticket Environment
T-Z	Reserved for private use

POS. 9 Code	Cardmember Authentication Entity — This subfield indicates component or person who verified Cardmember identity reported in Cardmember Authentication (Position 8).
0	Not authenticated, unknown
1	Integrated Circuit Card (ICC) **Note**: American Express-certified EMV terminal and link
2	Card Acceptor Device (CAD)
3	Authorizing agent (identified in authorizing agent institution identification code)
4	By Merchant
5	Other
6	Reserved for ISO use
7	Reserved for national use
8-9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 10 Code	Card Data Output Capability — This subfield indicates the ability of the terminal to update the card.
0	Unknown
1	None
2	Magnetic stripe write
3	Integrated Circuit Card (ICC) **Note**: American Express-certified EMV terminal and link
4-5	Reserved for ISO use
6-7	Reserved for national use
8-9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

POS. 11 Code	Terminal Output Capability — This subfield indicates the ability of the terminal to print and/or display messages.
0	Unknown
1	None
2	Printing
3	Display
4	Printing and display
5-6	Reserved for ISO use
7-8	Reserved for national use
9	Reserved for private use
A-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

8.1 1100 Authorization Request (continued)

Data Field 22 POINT OF SERVICE DATA CODE (continued)

POS. 12 Code	PIN Capture Capability — This subfield indicates the PIN length that the terminal is capable of capturing.
0	No PIN capture capability
1	Device PIN capture capability unknown
2-3	Reserved for ISO use
4	Four characters
5	Five characters
6	Six characters
7	Seven characters
8	Eight characters
9	Nine characters
A	Ten characters
B	Eleven characters
C	Twelve characters
D-I	Reserved for ISO use
J-R	Reserved for national use
S-Z	Reserved for private use

8.1 1100 Authorization Request (continued)

Data Field 24	FUNCTION CODE
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	• Optional — Batch Authorization transactions • Mandatory — Specific Merchants identified for Prepaid Card functionality. All identified Merchants are informed by their American Express representative. • Optional — All other Merchants for Prepaid Card functionality, but strongly recommended. • Mandatory — Transit transactions at Transit Access Terminals (TAT)
Certification Requirement:	USA & Canada Mandatory — Third Party Processors and/or Vendors must be certified to pass Prepaid Card data, Function Codes 181 and 182, in this data field. After certification, all Merchant-provided Prepaid Card data must be forwarded in this data field.

8.1 1100 Authorization Request (continued)

Data Field 24	FUNCTION CODE (continued)

Description: This data field contains a value that indicates the specific purpose of this message, within its message class. The following table lists the valid codes:

Function Code
`100` - Authorization Request
`180` - Batch Authorization
`181` - Prepaid Card Partial Authorization
`182` - Prepaid Card Authorization with Balance Return
`190` - Account Status Check
`191` - ATC Synchronization
`194` - Expresspay Translation (PAN Request)
`196` - Expresspay Translation (PAN & Expiration Date Request)

See the following for more detailed information.

`100` = Authorization Request - This transaction can be used for normal Authorization Requests, including those used for processing a Payment Plan Authorization such as DPP or EPP. Use of code "`100`" is optional.

`180` = Batch Authorization -— This transaction is part of a batch of non-time-critical authorization requests, which do not require the rapid response normally provided for real-time transactions. Use of code "`180`" for batch processing allows American Express to assign an appropriate priority in relation to transactions submitted from real-time POS environments. Typically, a Merchant utilizing Batch Authorization would not also participate in the special, Prepaid Card Partial Authorization services, described on the next page. A Merchant using Batch Authorization can accept American Express Prepaid Cards as normal authorizations.

8.1 1100 Authorization Request (continued)

Data Field 24	FUNCTION CODE (continued)
Description (continued):	The following codes enhance acceptance, functionality and usage of American Express Prepaid Card products at the POS. For these special Prepaid Card services, authorized Third Party Processors and Vendor software are required to support both Prepaid Card functions, specifically Partial Authorization and Authorization with Balance Return. This enables their Merchants to select either option. Direct Link Merchants have the choice of selecting the feature(s) they want to support. American Express strongly recommends Partial Authorization, because it approves a request for the remaining balance rather than declining it when there are insufficient funds to cover the original amount. `181` = Prepaid Card Partial Authorization Supported - Indicates that the Merchant's system accepts and processes Prepaid Card response messages for partial authorization of transaction amounts less than the full value originally submitted for authorization. Note that the Merchant must collect the remainder from the Cardmember via another form of payment. Merchants certified for Prepaid Card Partial Authorization should use code "`181`" for all transactions, and American Express systems will determine which Card products require a partial authorization response. Specifically, non-Prepaid Card products are ineligible for Partial Authorization; and using code "`181`" will not affect normal authorization requests. When applicable, Partial Authorization-related data is returned in the following Authorization Response (1110) message Data Fields: • Data Field 4 — Amount, Transaction • Data Field 30 — Amounts, Original • Data Field 39 — Action Code • Data Field 54 — Amounts, Additional Balances may not be returned for some Prepaid Cards.

8.1 1100 Authorization Request (continued)

Data Field 24	FUNCTION CODE (continued)
Description (continued):	181 = (continued) These data fields represent the amount authorized, the amount requested, the action taken and the balance remaining on the Prepaid Card. For details, see pages 183, 187, 194 and 203, respectively. 182 = Prepaid Card Authorization with Balance Return Supported - Indicates that the Merchant's system and/or POS device accepts and processes Prepaid Card balances in response messages. This alternative for systems that do not support partial authorizations returns the Prepaid Card balance to the Merchant so that an authorization request can be resubmitted for the available amount when transactions are denied for insufficient balance. Another form of payment (i.e., split tender) can be requested for the remainder. Merchants certified for Prepaid Card Authorization with Balance Return should use code "182" for all transactions, and American Express systems will determine which Card products require a response related to Authorization with Balance Return. Specifically, non-prepaid Card products are ineligible for Authorization with Balance Return; and using code "182" will not affect normal authorization requests. Using code "182" indicates that the Merchant is requesting an authorization for the full amount, and that their system supports the return of Prepaid Card balance information from American Express. When applicable, Authorization with Balance Return-related data is returned in the following Authorization Response (1110) message Data Fields: • Data Field 39 — Action Code • Data Field 54 — Amounts, Additional These data fields represent the action taken and the balance remaining on the Prepaid Card. For details, see pages 194 and 203, respectively. Balances may not be returned for some Prepaid Cards.

8.1 1100 Authorization Request (continued)

Data Field 24	FUNCTION CODE (continued)
Description (continued):	`182` = (continued) **Note**: A Prepaid Card Balance Inquiry for American Express Prepaid Card products can be submitted by zero filling Data Field 4 (Amount, Transaction), if Data Field 24, Function Code, value is "`181`" (Partial Authorization) or "`182`" (Authorization with Balance Return). The available balance is returned in Data Field 54, Amounts, Additional, of the Authorization Response (1110) message. However, balance inquiries cannot be processed for Card products other than American Express Prepaid Cards. `190` = Account Status Check — Transit Merchants requesting an account status check on transit transactions only. `191` = ATC Synchronization — Indicates an Application Transaction Counter (ATC) value is being provided to the Issuer. Issuers can use this synchronization feature to maintain their internal ATC data. `194` = Expresspay Translation (PAN request) — Indicates the Primary Account Number (PAN) associated with an Expresspay-enabled card/device is being requested from the Issuer. The response will be returned in Data Field 34,Primary Account Number, Extended, for Transit transactions only. `196` = Expresspay Translation (PAN & Expiration Date request) — Indicates the Primary Account Number (PAN) and Expiration Date associated with an Expresspay-enabled card/device is being requested from the Issuer. The response will be returned in Data Field 34,Primary Account Number, Extended, for Transit transactions only.

8.1 1100 Authorization Request (continued)

Data Field 25	MESSAGE REASON CODE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	• Mandatory — American Express Card (and American Express-supported Card) transactions • Optional — VISA, MasterCard and JCB transactions • Optional — American Express Travelers Cheques
Description:	This data field contains a four-digit Message Reason Code, which is provided by American Express during certification. The code used varies with the type of request submitted for processing by the Merchant or Third Party Processor. Proper use of this data field indicates that the Authorization Request is certified by American Express. For information on valid codes and their use, contact your American Express representative.

8.1 1100 Authorization Request (continued)

Data Field 26	CARD ACCEPTOR BUSINESS CODE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the Merchant Category Code (MCC) that corresponds to the Merchant's type of business. If the Merchant is considered a Payment Service Provider (Aggregator) or an OptBlue Participant, billing for services/goods rendered by another entity, the MCC code should reflect the classification for the specific entity rendering the goods or services. Therefore, this value may vary for each transaction dependent on the category applicable to the Payment Service Provider (Aggregator) or OptBlue Participant's specific Sellers. For a list of Merchant Category Codes, refer to the *American Express Global Codes & Information Guide*. **Notes**: 1. For Oil Company Industry Merchants, the Card Acceptor Business Code data field should reflect the specific type of business conducted (e.g., 5542 - Automated Fuel Dispensers or 5541 - Service Stations, including in-store transactions). Oil Company Industry Merchants that use a single Merchant ID for more than one business type should populate this data field with the appropriate Merchant Category Code (MCC), for each transaction. For more information, contact your American Express representative. 2. For Transit - TAT transactions, the Card Acceptor Business Code data field must be populated by one of the following Merchant Category Codes: 4111 = Local and Suburban Commuter Passenger Transportation, including Ferries 4112 = Passenger Railways 4131 = Bus Lines 4784 = Tolls and Bridge Fees 7523 = Parking Lots and Garages

8.1 1100 Authorization Request (continued)

Data Field 27	APPROVAL CODE LENGTH
Length of Field:	1 byte, fixed length
Field Type:	Numeric
Constant:	6 or 2
Field Requirement:	Optional
Description:	The American Express preferred standard Approval Code for the Authorization Response (1110) message is a six-digit approval code. U.S. and Canadian Merchants must comply with this standard. However, for all other global regions, American Express has the ability to provide either a two-digit or a six-digit approval code. When applicable, American Express representatives must be informed during the initial setup of the Merchant interface, that Data Field 27 will be used to determine the Approval Code length in the Authorization Response (1110) message. American Express will then set up procedures to check the value in Data Field 27 and provide the appropriate Approval Code length in the Authorization Response (1110) message. When the valid values of either "2" or "6" are present in this data field, American Express will honor the request to send an Approval Code of the appropriate length. If the Merchant or Third Party Processor then submits the data field with no value, American Express will follow additional rules to determine the proper length of the Approval Code. This procedure allows the Approval Code length to vary, which may suit the Merchant's specific business rules. If the Merchant or Third Party Processor prefers not to use Data Field 27, American Express will still set up the link to return either a two-digit or six-digit Approval Code.

8.1 1100 Authorization Request (continued)

Data Field 31	ACQUIRER REFERENCE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 50 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 48 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is reserved for internal American Express use only. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

8.1 1100 Authorization Request (continued)

Data Field 32	ACQUIRING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Optional

Description:	This data field contains the identification code of the party processing the request, preceded by a two-digit, Variable Length Indicator (VLI).
	For example, the 11-digit acquiring institution identification code "`4567891234`5" would appear as:
	`0 1`
	`1234567890123`
	`1145678912345`
	Note: This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 33	FORWARDING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Optional

Description:	This data field contains the forwarding institution's identification code, preceded by a two-digit Variable Length Indicator (VLI).
	For example, the 11-digit, forwarding institution identification code "`4567891234`5" would appear as:
	`0 1`
	`1234567890123`
	`1145678912345`
	Note: In certain unique implementations, this data field may be redefined. For example, in the U.S., for non-American Express (i.e., bankcard) requests, this data field may contain the ID number assigned to the POS network by the non-American Express service association (i.e., the ID number assigned by the network provider processing transactions on the acquiring bank's behalf).
	If you wish to populate this data field with data outside the basic definition of "the forwarding institution's identification code", contact your American Express representative for assistance in determining the appropriate value to use.

8.1 1100 Authorization Request (continued)

Data Field 35	TRACK 2 DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 39 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 37 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Conditional
Certification Requirement:	Global — All regions During certification, Merchants must demonstrate the ability to populate and transmit Track 1, Track 2 and/or Integrated Circuit Card (ICC) Data (Data Fields 45, 35 and 55, respectively, for Card Present transactions when track or ICC data is successfully read from a valid Card swipe, EMV card read or Contactless card read. Similarly, authorized Third Party Processors and Vendors must demonstrate the ability to populate and transmit Track 1, Track 2 and/or ICC Data, Data Fields 45, 35 and 55, respectively, for Card Present transactions when track or ICC data is successfully read from a valid Card swipe, EMV card read or a Contactless card read. After certification, Merchants, Third Party Processors and Vendors must forward all Point of Sale-provided track and/or ICC data in the appropriate data field(s).
Description:	This data field contains the information encoded in a valid Track 2 magnetic stripe, an Integrated Circuit Card (ICC) or a Contactless card, preceded by a two-digit Variable Length Indicator (VLI). Actual Track 2 data is composed of the EBCDIC digits 0 9 and a data field separator value. If POS Data Code, Position 7 = "2", "5" or "W", then the full Track Data must be present. If Position 7 = "9", then the full Track Data may or may not be present. Data Field 45 must be present if Data Field 35 is not present.

8.1 1100 Authorization Request (continued)

Data Field 35	TRACK 2 DATA (continued)
Description (continued):	If Data Field 45, Track 1, is not present, Data Field 35, Track 2, must be populated with either the information encoded in a Track 2 magnetic stripe read for swiped transactions, or the Track 2 data stored on the chip of a Chip Card for ICC transactions. **Note**: Track 1 and Track 2 data formats may vary slightly between various American Express products. The data field definitions referenced in the American Express Magnetic Stripe and Expresspay Pseudo-Magnetic Stripe Formats are for reference only and may not reflect all variations that may be encountered. For this reason, when Track 1 or Track 2 data is supplied intact, the Acquirer, their devices, systems, Vendor software and authorized Third Party Processors should capture all characters between the start and end sentinels, strip off the sentinels and LRC, and forward the remainder to American Express in the appropriate ISO 8583 Track 1 or Track 2 data field, without regard to the specific lengths referenced in these sections. For more information, refer to the American Express Magnetic Stripe Formats and Expresspay Pseudo-Magnetic Stripe Formats in the *American Express Global Codes & Information Guide*.

ANSI X4.16 Format	In the following example below, the two-digit VLI is "29" and the digits that follow are the 29 bytes of Track 2 data in ANSI X4.16 format. The character "=" is used to depict the data field separator. The total length of this example is 31 bytes.
	
	`0 1 2 3`
	`12345678901234567890123456789 01`
	
	`29371449635311004=1211081112345`

ISO 7813 Format	In the following example, the two-digit VLI is "37" and the digits that follow are the 37 bytes of Track 2 data in ISO 7813 format. The character "=" is used to depict the data field separator. The total length of this example is 39 bytes.
	
	`0 1 2 3`
	`12345678901234567890123456789012345678 9`
	
	`373714496353110040=21110108111234567800`

8.1 1100 Authorization Request (continued)

Data Field 35	TRACK 2 DATA (continued)

Expresspay Pseudo-Magnetic Stripe Format	In the following example, the two-digit VLI is "37" and the digits that follow are the 37 bytes of Track 2 data shown in Expresspay Pseudo-Magnetic Stripe Format. The character "=" is used to depict the data field separator. The total length of this example is 39 bytes.
	`0 1 2 3`
	`12345678901234567890123456789012345678 9`
	`3737144963531100 4=1112702123424743123 45`
	Notes:
	1. If Tracks 1 and 2 are both captured, both should be forwarded. If only one track is captured, Track 1 is preferred (see page 109). For systems that capture only Track 2, this less desirable alternative may be supplied in lieu of Track 1.
	2. American Express security requirements prohibit the storage of track data within Merchant or processor systems.

8.1 1100 Authorization Request (continued)

Data Field 37	RETRIEVAL REFERENCE NUMBER
Length of Field:	12 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Optional
Description:	This data field contains a unique, 12-character reference number. **Note**: This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 41	CARD ACCEPTOR TERMINAL IDENTIFICATION
Length of Field:	8 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Mandatory — American Express transactions in EMEA, LA/C & APA **Note**: Merchants in EMEA & LA/C that are unable to provide a unique value for each terminal, can provide a central location Terminal ID • Optional — American Express transactions in the USA and Canada (strongly recommended), and non-VISA transactions • Mandatory — VISA PS2000
Description:	This data field contains a unique code that identifies a specific terminal at a Merchant location. It is used when Data Field 42, Card Acceptor Identification Code, does not uniquely identify the physical location of this transaction. **Note**: This data field may or may not be mandatory for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 42	CARD ACCEPTOR IDENTIFICATION CODE
Length of Field:	15 bytes, fixed length
Field Type:	Alphanumeric & special characters, left justified, character space filled
Constant:	None
Field Requirement:	Mandatory
Description:	This data field identifies the Merchant in a POS transaction and is required for ALL requests. The Merchant ID assigned to the POS location shall be one of the following, and must be left justified and character space filled: • 10-digit American Express SE Number. • Two-character alphanumeric Airline Code. • IATA[1] Travel Agent ID (T + 5-8 digits). If the American Express SE Number is used in this data field, check digit validation is required. For details, refer to SE Number Check Digit Computation (Modulus 9 Check) in the *American Express Global Codes & Information Guide*. ***Airline Code*** If a two-character alphanumeric Airline Code is used in this data field, additional information may be included using the following format: **XX~T12345678** See Airline Code instructions on the next page.

[1] IATA = International Air Transport Association.

8.1 1100 Authorization Request (continued)

Data Field 42	CARD ACCEPTOR IDENTIFICATION CODE (continued)
Description (continued):	In the example on the previous page, "XX" is the two-character alphanumeric Airline Code, "~" is a character space, the alpha character "T" is a constant that indicates that the value that follows is a travel agent number, and "12345678" is a 7-8 digit IATA Travel Agent ID, where the eight digits have the following significance: 12 = Two-digit State or Country Code 34567 = Five-digit Core Number 8 = Check Digit (optional). If unused, pad with a character space. **Notes**: 1. For American Express transactions, use of formats other than the 10-digit American Express SE Number requires additional certification. 2. This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 43	CARD ACCEPTOR NAME/LOCATION
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 101 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 99 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Global — All regions • Mandatory — Oil Company Industry, including Card Acceptor Terminal (CAT) transactions where a single Service Establishment Number is not used for each physical location • Mandatory — Payment Service Providers (Aggregators) & OptBlue Participants • Mandatory — VISA PS2000 • Optional — All other transactions
Certification Requirement:	Global — All regions Mandatory — Third Party Processors and/or Vendors must be certified to pass data in this data field. After certification, all Merchant-provided data must be forwarded in this data field. **Note**: While this data field is optional for many transactions, American Express strongly recommends that all Merchants populate this data field in every authorization request.
Description:	This data field contains the card acceptor name and location, which consists of six data elements with up to 99 characters total, preceded by a two-digit, Variable Length Indicator. The first three elements (subfield 1) are variable length and are separated from each other and the remaining elements by a back slash (\). Maximum allowable values include backslashes. See Subfield Table on the next page.

8.1 1100 Authorization Request (continued)

Data Field 43 CARD ACCEPTOR NAME/LOCATION (continued)

	Oil Co. CAT	VISA PS2000	Payment Service Provider (Aggregator) and OptBlue Participants	Other Trans.	Subfield Length	Subfield Type	Description
LLVAR	M	M	M	M	2 bytes	Numeric	Variable Length Indicator
Subfield 1	M[1]	N/A[2]	M[3]	O	83 bytes max.	Alphanumeric & special characters	**Oil Co. CAT**[1] Name \ \ \ Must replace Name with unique merchant-assigned, station location code. **Payment Service Providers (Aggregators) and OptBlue Participants**[3] ***Payment Service Provider***: PSP's supported within an OptBlue Participant must follow the Payment Service Provider format: Payment Service Provider (Aggregator)=Seller DBA\Seller Street\Seller City\ A. Payment Service Provider (Aggregator) and Seller Name - 38 bytes (max.) and should be constructed of two elements separated by an "=" delimiter: 1. Payment Service Provider (Aggregator) 2. Seller Name B. Street - 30 bytes (max.) C. City - 15 bytes (max.) ***OptBlue Participants***: = Seller DBA\Seller Street\Seller City\ A. =Seller Name - 38 bytes (max.) and should always begin with an "=" B. Street - 30 bytes (max.) C. City - 15 bytes (max.)

M = Mandatory O = Optional N/A = Subfield is unused

8.1 1100 Authorization Request (continued)

Data Field 43 CARD ACCEPTOR NAME/LOCATION (continued)

	Oil Co. CAT	VISA PS2000	Payment Service Provider (Aggregator) and OptBlue Participants	Other Trans.	Subfield Length	Subfield Type	Description
Subfield 1 (continued)							**Note**: The elements provided in this subfield should be spelled out completely. If necessary, truncate the information to meet the length requirements rather than using abbreviations. Additional data requirements are found in Data Field 60, National Use Data. **All Other Merchants - Optional** Name\Street\City\
Subfield 2	M	M	M[4]	O	10 bytes Fixed	Alphanumeric & special characters, left justified	Postal Code
Subfield 3	N/A[5]	N/A[4]	M[4]	O[5]	3 bytes Fixed	Alphanumeric & special characters, left justified	Region Code must correspond to the Country Code provided. For information on country and region codes, refer to the *American Express Global Codes & Information Guide*.
Subfield 4	N/A[5]	N/A[5]	M[4]	O[5]	3 bytes Fixed	Alphanumeric	Country Code must correspond to the Region Code provided. For information on country and region codes, refer to the *American Express Global Codes & Information Guide*.

M = Mandatory O = Optional N/A = Subfield is unused

8.1 1100 Authorization Request (continued)

Data Field 43 CARD ACCEPTOR NAME/LOCATION (continued)

Notes:

1. For Oil Company Industry CAT transactions, Subfield 1 must contain a unique, Merchant-assigned, station location code in format "S#nnnnnnnnnnn\\\". While the previous example shows an 11-byte station location code, the actual value may vary in length within the 83-byte maximum allowed.
2. For VISA PS2000, Subfield 1 is omitted, indicated by three back slashes (\\\), one per element (Name, Street and City).
3. Payment Service Providers (Aggregators) and OptBlue Participants:
   a. For Payment Service Providers (Aggregators) - Subfield 1 must include the Payment Service Provider (Aggregator) as well as the Seller DBA. Both elements should be separated by an "="delimiter. The Payment Service Provider (Aggregator) must also provide the Seller's Street and Seller's City.

      Example of typical entry for Subfield 1:
      ANY~AGGREGATOR=KATIS~BEACH~UMBRELLAS\1234~ABC~STREET\
      ANYTOWN\

   b. For OptBlue Participants - Subfield 1 must include the Seller DBA preceded by an "=" delimiter. The OptBlue Participant must also provide the Seller's Street and Seller's City.

      Example of typical entry for Subfield 1:
      =KATIS~BEACH~UMBRELLAS\1234~ABC~STREET\ANYTOWN\

      Notes for #3a and #3b:

      1. In the example above, tilde (~) characters represent character spaces and the equal sign (=) represents a delimiter.
      2. Payment Service Providers (Aggregators) supported within an OptBlue Participant must follow the Payment Service Provider (Aggregator) format.

4. Subfields 2, 3 and 4 are mandatory for Payment Service Providers (Aggregators) and OptBlue Participants. Should data be unavailable, omitted subfields are indicated by character spaces. See examples on the next page.
5. Subfields 3 and 4 are omitted for Oil Company Industry CAT transactions. For all other Merchants subfields 3 and 4 are optional. Omitted subfields are indicated by back slashes (\), one per subfield. See examples on the next page.

See all examples on the next page.

8.1 1100 Authorization Request (continued)

Data Field 43 CARD ACCEPTOR NAME/LOCATION (continued)

Typical example for entry of Oil Company Industry "Station Location Code"

```
         1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
28S#12345678901\\\85054~~~~~\\
```

Typical example for entry of Payment Service Provider (Aggregator) and OptBlue Participants "Payment Service Provider (Aggregator)=Seller DBA","Seller Street", "Seller City", "Seller Postal Code", "Seller Region", and "Seller Country Code"

```
         1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
77ANY~AGGREGATOR=KATIS~BEACH~UMBRELLAS\1234~ABC~STREET\ANYTO

                                       1         1         1
         7         8         9         0         1         2
1234567890123456789012345678901234567890123456789012345678901234567890
WN\85054~~~~~AZ~840
```

Typical example for entry of Payment Service Provider (Aggregator) and OptBlue Participants "Payment Service Provider (Aggregator)=Seller DBA","Seller Street", "Seller City", and omitted "Seller Postal Code", "Seller Region", and "Seller Country Code"

```
         1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
77ANY~AGGREGATOR=KATIS~BEACH~UMBRELLAS\1234~ABC~STREET\ANYTO

                                       1         1         1
         7         8         9         0         1         2
1234567890123456789012345678901234567890123456789012345678901234567890
WN~~~~~~~~~~~~~~~~
```

Typical example for all other Merchants

```
         1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
58KATIS~BEACH~UMBRELLAS\1234~ABC~STREET\ANYTOWN\85054~~~~~\\
```

Note: In the examples above, tilde (~) characters represent character spaces and the equal sign (=) represents a delimiter.

8.1 1100 Authorization Request (continued)

Data Field 45	TRACK 1 DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 78 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 76 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Global — All regions • Mandatory — Oil Company Industry, Card Acceptor Terminal (CAT) transactions • Conditional — All other transactions with POS Data Code values noted in description
Certification Requirement:	Global — All regions During certification, Merchants must demonstrate the ability to populate and transmit Track 1 or Track 2 data, Data Fields 45 and 35, respectively, for Card Present transactions when track data is successfully read from a valid Card swipe or a Contactless card read. Similarly, authorized Third Party Processors and Vendors must demonstrate the ability to populate and transmit Track 1 and Track 2 data, Data Fields 45 and 35, respectively, for Card Present transactions when track data is successfully read from a valid Card swipe or a Contactless card read. After certification, Merchants, Third Party Processors and Vendors must forward all Point of Sale-provided track data in the appropriate data field(s).
Description:	This data field contains the information encoded in a valid Track 1 magnetic stripe or a Contactless card, preceded by a two-digit, Variable Length Indicator (VLI). The actual Track 1 data is composed of EBCDIC alphanumeric and special characters, and a data field separator value.

8.1 1100 Authorization Request (continued)

Data Field 45	TRACK 1 DATA (continued)
Description (continued):	If POS Data Code, Position 7 = "2", "5" or "W", then the full Track Data must be present. If Position 7 = "9", then the full Track Data may or may not be present. Data Field 35 must be present, if Data Field 45 is not present. If Data Field 35, Track 2, is not present, Data Field 45, Track 1, must be populated with the information encoded in a Track 1 magnetic stripe read for swiped transactions, or Pseudo-Track 1 or the Track 1 data stored on a Contactless card for contactless transactions. **Note**: Track 1 and Track 2 formats may vary slightly between various American Express products. The data field definitions referenced in the American Express Magnetic Stripe and Expresspay Pseudo-Magnetic Stripe Formats are for reference only and may not reflect all variations that may be encountered. For this reason, when Track 1 or Track 2 data is supplied intact, the Acquirer, their devices, systems, Vendor software and authorized Third Party Processors should capture all characters between the start and end sentinels, strip off the sentinels and LRC, and forward the remainder to American Express in the appropriate ISO 8583 Track 1 or Track 2 data field, without regard to the specific lengths referenced in these sections. For more information, refer to the American Express Magnetic Stripe Formats and Expresspay Pseudo-Magnetic Stripe Formats in the *American Express Global Codes & Information Guide*. **Oil Company CAT Transactions** This data field is required for Oil Company Industry Card Acceptor Terminal (CAT) transactions. (Forwarding Track 1 data, which includes primary account number, effective and expiration dates, and Cardmember name, reduces fraud by allowing comparison of actual card data to the American Express database.)

8.1 1100 Authorization Request (continued)

Data Field 45	TRACK 1 DATA (continued)
Examples:	See the following examples.

ANSI X4.16 Format

In the following example, the two-digit VLI is "59" and the digits that follow are the 59 bytes of Track 1 data in ANSI X4.16 format. The character "^" is used to depict the data field separator, and tildes (~) represent character spaces. The total length of this example is 61 bytes.

```
0         1         2         3         4         5         6
12345678901234567890123456789012345678901234567890123456789012345678901
59B3714~49653~11004^FROST/CHARLES~F.JR~~~~~~~~^9403910112345
```

ISO 7813 Format

In the following example, the two-digit VLI is "76" and the digits that follow are the 76 bytes of Track 1 data in ISO 7813 format. The character "^" is used to depict the data field separator, and tildes (~) represent character spaces. The total length of this example is 78 bytes.

```
0         1         2         3         4         5         6
12345678901234567890123456789012345678901234567890123456789012345678901234567890
76B371449635311004^FROST/CHARLES~F.JR~~~~~~~~^94031019101123

6         7
12345678901234567
4567890123456789012
```

8.1 1100 Authorization Request (continued)

Data Field 45	TRACK 1 DATA (continued)

Expresspay Pseudo-Magnetic Stripe Format

In the following example, the two-digit VLI is "60" and the digits that follow are the 60 bytes of Track 1 data shown in Expresspay Pseudo-Magnetic Stripe Format. The character "^" is used to depict the data field separator. The total length of this example is 62 bytes.

```
0         1         2         3         4         5         6
12345678901234567890123456789012345678901234567890123456789012
60B3714496353110O4^VALUED/CARDMEMBER~~~~12345^1211702123424743
```

Notes:

1. If Tracks 1 and 2 are both captured, both should be forwarded. If only one track is captured, Track 1 is preferred. For systems that capture only Track 2, this less desirable alternative may be supplied in lieu of Track 1 (see page 97).

2. American Express security requirements prohibit the storage of track data within Merchant or processor systems.

8.1 1100 Authorization Request (continued)

Data Field 47	ADDITIONAL DATA - NATIONAL
Length of Field: Variable Length Indicator: Length of Variable Data:	19 bytes minimum, 304 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 301 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Optional — Merchants in mail-, telephone- and internet-order industries that pass Card Not Present - Internet Telephone Data (ITD). • Optional — Merchants in the airline industry that pass Card Not Present Internet Airline Customer (IAC) data or Card Not Present - Airline Passenger Data (APD). • Optional — Merchants in Card Present transactions that pass Card Present - Goods Sold data.
Certification Requirement:	USA, Canada, EMEA & LA/C • Mandatory — Third Party Processors and/or Vendors must be certified to pass Card Not Present - Internet Telephone Data (ITD) in this data field. After certification, all Merchant-provided ITD data must be forwarded in this data field. • Mandatory — Third Party Processors and/or Vendors must be certified to pass Card Not Present Internet Airline Customer (IAC) data in this data field. After certification, all Merchant-provided IAC data must be forwarded in this data field. • Mandatory — Third Party Processors and/or Vendors must be certified to pass Card Not Present - Airline Passenger Data (APD) in this data field. After certification, all Merchant-provided APD data must be forwarded in this data field.

8.1 1100 Authorization Request (continued)

Data Field 47	ADDITIONAL DATA - NATIONAL (continued)
Certification Requirement (continued):	• Mandatory — Third Party Processors and/or Vendors must be certified to pass Card Present - Goods Sold data in this data field. After certification, all Merchant-provided Card Present - Goods Sold data must be forwarded in this data field.
Description:	This data field is composed of four formats: • The first format is for Merchants in mail-, telephone- and internet-order industries that submit Card Not Present - Internet Telephone Data (ITD). For Merchants using this format, ITD subfields may contain source data, including the Cardmember's Web and email addresses, host computer name, HTTP browser, product SKU (Stock Keeping Unit) inventory reference number, shipping method and country to which product will be shipped. • The second format is specific to airline industry Merchants that submit Card Not Present - Internet Airline Customer (IAC) data. For these Merchants, IAC subfields may contain additional travel-specific information, including the departure date, passenger name, travel origin and destination, routing cities, airline carriers, fare basis, number of passengers, and customer IP and email addresses.

8.1 1100 Authorization Request (continued)

Data Field 47	ADDITIONAL DATA - NATIONAL (continued)
Description:	• The third format is specific to airline industry Merchants that submit Card Not Present - Airline Passenger Data (APD). For these Merchants, APD subfields may contain additional travel-specific information, including the departure date, passenger and Cardmember names, travel origin and destination, routing cities, airline carriers, fare basis, number of passengers, e-ticket indicator and reservation code. **Note**: Within the Airline Industry, the IAC format is recommended over the APD format, as it is more comprehensive. The APD format has been retained for Merchants, Processors and Vendor software currently sending data in this format. Merchants that could fall under ITD, IAC or APD categories should contact their American Express representative, to determine which format is appropriate for their business. • The fourth format is specific to Card Present Goods Sold data. The Card Present - Goods Sold subfields contain Card Present information identifying the product being purchased which is Gift Cards.

8.1 1100 Authorization Request (continued)

Data Field 47	ADDITIONAL DATA - NATIONAL (continued)
Description (continued):	**Notes**: 1. Only one of the four formats may be used for a given transaction. The ITD format has a minimum length of 74 bytes and a maximum of 265, including VLI. The IAC format has a minimum of 132 bytes and a maximum of 304, including VLI. The APD format has a minimum of 151 bytes and a maximum of 290, including VLI. The Card Present - Goods Sold format has a minimum length of 19 bytes and a maximum of 19, including the VLI. 2. For all formats, unused fixed-length subfields must be character space or zero filled, as appropriate. 3. Unless otherwise indicated, for all formats, unused variable-length subfields must be a minimum of one byte, composed of a character space or zero, as appropriate. This is in addition to providing the preceding ID and VLI bytes. For example, the three-byte ID would be sent with two-byte VLI "`01`", and the one-byte subfield would contain a single character space or a zero, as appropriate. 4. Unless otherwise indicated, alphanumeric subfields are left justified, character space filled and not case sensitive; and numeric subfields are right justified and zero filled, as necessary.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Internet Telephone Data (ITD) For the Mail-, Telephone- and Internet-Order Industries Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	Secondary ID (Data Type Code). Valid IDs include: ITD = Card Not Present Data
9-11	CUSTOMER EMAIL ID (CE ID)	3 bytes	Alphanumeric	Customer Email ID is constant literal "CE~" (Customer Email).
12-13	VARIABLE LENGTH INDICATOR (CE VLI)	2 bytes	Numeric	CE VLI indicates length of CUSTOMER EMAIL variable data (not including CE ID or VLI).
14-37	CUSTOMER EMAIL	1-60 bytes	Alphanumeric & special characters	Customer's email address. Example: CFFROST@EMAILADDRESS.COM
38-40	CUSTOMER HOSTNAME ID (CH ID)	3 bytes	Alphanumeric	Customer HostName ID is constant literal "CH~" (Customer HostName).
41-42	VARIABLE LENGTH INDICATOR (CH VLI)	2 bytes	Numeric	CH VLI indicates length of CUSTOMER HOST-NAME variable data (not including CH ID or VLI).
43-56	CUSTOMER HOSTNAME	1-60 bytes	Alphanumeric & special characters	Name of server to which customer is connected. Example: PHX.QW.AOL.COM
57-59	HTTP BROWSER TYPE ID (HBT ID)	3 bytes	Alphanumeric	HTTP Browser Type ID is constant literal "HBT" (HTTP Browser Type).
60-61	VARIABLE LENGTH INDICATOR (HBT VLI)	2 bytes	Numeric	HBT VLI indicates length of HTTP BROWSER TYPE variable data (not including HBT ID or VLI).
62-107	HTTP BROWSER TYPE	1-60 bytes	Alphanumeric & special characters	Customer's HTTP browser type. Example: MOZILLA/4.0~(COMPATIBLE; ~MSIE~5.0;~WINDOWS~95)
108-110	SHIP TO COUNTRY ID (STC ID)	3 bytes	Alphanumeric	Ship To Country ID is constant literal "STC" (Ship To Country).
111-112	VARIABLE LENGTH INDICATOR (STC VLI)	2 bytes	Numeric	STC VLI indicates length of SHIP TO COUNTRY variable data. Must be constant literal "03".

Note: ~ = character space.

See example on page 120.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Internet Telephone Data (ITD) For the Mail-, Telephone- and Internet-Order Industries Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
113-115	SHIP TO COUNTRY	3 bytes	Alphanumeric	Three-byte, numeric Country Code. Refer to Country Codes in the *Global Codes & Information Guide*. Example for U.S.: `840`
116-118	SHIPPING METHOD ID (SM ID)	3 bytes	Alphanumeric	Shipping Method ID is constant literal "SM~" (Shipping Method).
119-120	VARIABLE LENGTH INDICATOR (SM VLI)	2 bytes	Numeric	SM VLI indicates length of SHIPPING METHOD variable data (not including SM ID or VLI). Must be constant literal "`02`".
121-122	SHIPPING METHOD	2 bytes	Alphanumeric	Two-byte, shipment-type code: `01` = Same Day `02` = Overnight / Next Day `03` = Priority, 2-3 days `04` = Ground, 4 or more days `05` = Electronic Delivery `06` = Ship-to Store* `07-ZZ` = Reserved for future use
123-125	MERCHANT PRODUCT SKU ID (MPS ID)	3 bytes	Alphanumeric	Merchant Product SKU ID is constant literal `"MPS"` (Merchant Product SKU).
126-127	VARIABLE LENGTH INDICATOR (MPS VLI)	2 bytes	Numeric	MPS VLI indicates length of MERCHANT PRODUCT SKU variable data (not including MPS ID or VLI).
128-135	MERCHANT PRODUCT SKU	1-15 bytes	Alphanumeric & special characters	Unique SKU (Stock Keeping Unit) inventory reference number of product associated with this authorization request. For multiple items, enter SKU for single, most expensive item. Example: `TKDC315U`
136-150	CUSTOMER IP	15 bytes	Alphanumeric & special characters	Customer's Internet IP address, left justified and character space filled (as necessary) to 15 bytes. Example 1: `127.142.151.223` Example 2: `127.142.5.56~~~` Example 3: `12.142.49.190~~`

Note: ~ = character space.

See example on page 120.

* Merchants populating the Shipping Method, using shipment-type code (06) Ship-to Store, are strongly encouraged to populate the address of the store location in Data Field 63 (Private Use Data) Ship-to Address in the 205-byte format.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Internet Telephone Data (ITD) For the Mail-, Telephone- and Internet-Order Industries Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
151-160	CUSTOMER ANI	10 bytes	Alphanumeric & special characters	ANI (Automatic Number Identification) specified 10-digit phone number that customer used to place order with Merchant. Leading or trailing zeros and/or virgules (/) are not permitted as filler. However, phone numbers less than 10-digits should be left justified and character space filled. USA, Canada and other countries that follow the NANP phone numbering system should send all 10-digits of the phone number, including the area code. For countries that do not follow this system, send the last 10-digits. Examples: United States of America (USA) phone number "602-555-1212" would be entered as "`6025551212`". United Kingdom (UK) phone number "44-1234-123456" would be entered as "`1234123456`".
161-162	CUSTOMER II DIGITS	2 bytes	Alphanumeric & special characters	Telephone company-provided ANI Information Identifier (II) digits associated with CUSTOMER ANI. II digits indicate call type. For example, cellular (61-63), payphone (27), toll free (24, 25), etc.

See example on the next page.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Internet Telephone Data (ITD) For the Mail-, Telephone- and Internet-Order Industries Example

The following example corresponds to the ITD Position Format Table on the preceding pages, and illustrates a data field entry for mail-, telephone- and internet-order Merchants that submit Card Not Present - Internet Telephone Data (Data Type Code "**ITD**").

```
          1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
159AXITDCE~24CFFROST@EMAILADDRESS.COMCH~14PHX.QW.AOL.COMHBT4

                                        1         1         1
6         7         8         9         0         1         2
1234567890123456789012345678901234567890123456789012345678901234567890
6MOZILLA/4.0~(COMPATIBLE;~MSIE~5.0;~WINDOWS~95)STC03840SM~02

1         1         1         1         1
2         3         4         5         6
12345678901234567890123456789012345678901234567890123456
02MPS08TKDC315U127.142.005.056602555121200
```

Notes:

1. In the example above, tilde (~) characters represent character spaces.

2. This example represents data for multiple scenarios of a Card Not Present - Internet Telephone Data (ITD) transaction. A typical transaction will probably not include all subfields (e.g., an Internet-order would not include Customer ANI and Customer II Digits; and a phone-order would not include Customer Hostname or Customer IP).

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present Internet Airline Customer (IAC) Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	Primary ID (Card Type Code) is constant literal `"AX"` (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	Secondary ID (Data Type Code). Valid IDs include: `IAC` = Internet Airline Customer
9-16	DEPARTURE DATE	8 bytes	Numeric	Departure Date (format `CCYYMMDD`). Example: `20030101`
17-19	AIRLINE PASSENGER NAME ID (APN ID)	3 bytes	Alphanumeric	Airline Passenger Name ID is constant literal `"APN"` (Airline Passenger Name).
20-21	VARIABLE LENGTH INDICATOR (APN VLI)	2 bytes	Numeric	APN VLI indicates length of Airline PASSENGER NAME variable data (not including APN ID or VLI).
22-44	PASSENGER NAME	23-40 bytes	Alphanumeric & special characters	Passenger Name in format: `SURNAME~FIRSTNAME~MIDDLEINITIAL~TITLE` Use character space as sub-element separator. Variable data must be 23-bytes minimum, space filled as necessary, 40-bytes maximum. Truncate at 40 bytes, if necessary. Example: `FROST~JANE~M~MRS~~~~~~~`
45-49	ORIGIN (Origin Airport)	5 bytes	Alphanumeric & special characters	First segment travel origination Airport, Note: Five-byte code sequence allows for anticipated expansion of present, three-character Airport Code. If necessary, left justify codes and character space fill each code sequence to five bytes. Example: `ABC~~`
50-54	DEST (First Segment Travel Destination Airport)	5 bytes	Alphanumeric & special characters	Destination Airport for first travel segment of trip; not necessarily the final destination. For example, if passenger flies from STL to MIA with layover at JFK, Destination Airport for first segment is JFK. Note: Five-byte code sequence allows for anticipated expansion of present, three-character Airport Code. If necessary, left justify codes and character space fill each code sequence to five bytes. Example: `XYZ~~`

Note: ~ = character space.

See example on page 124.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present Internet Airline Customer (IAC) Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
55-57	ROUTING ID (RTG ID)	3 bytes	Alphanumeric	Routing ID is constant literal "RTG" (Routing).
58-59	VARIABLE LENGTH INDICATOR (RTG VLI)	2 bytes	Numeric	RTG VLI indicates combined length of NUMBER OF CITIES and ROUTING CITIES variable data (not including RTG ID or VLI).
60-61	NUMBER OF CITIES	2 bytes	Numeric	Number of Airports or Cities on ticket (10 max).
62-120	ROUTING CITIES	11-59 bytes	Alphanumeric & virgule (/)	Routing Airport or City Codes for each leg on ticket (including ORIGIN and DEST) in five-byte segments with virgule (/) separator. Example: ABC~~/DEF~~/GHI~~/JKL~~/MNO~~/PQR~~/STU~~/VWX~~/YZA~~/XYZ~~
121-123	AIRLINE CARRIERS ID (ALC ID)	3 bytes	Alphanumeric	Airline Carriers ID is constant literal "ALC" (Airline Carrier).
124-125	VARIABLE LENGTH INDICATOR (ALC VLI)	2 bytes	Numeric	ALC VLI indicates combined length of NUMBER OF AIRLINE CARRIERS and AIRLINE CARRIERS variable data (not including ALC ID or VLI).
126-127	NUMBER OF AIRLINE CARRIERS	2 bytes	Numeric	Number of Airline Carriers entered in AIRLINE CARRIERS subfield (9 max). Example: 09
128-180	AIRLINE CARRIERS	5-53 bytes	Alphanumeric & virgule (/)	Airline Carrier Code for each leg on ticket (including ORIGIN and DEST) in five-byte segments with virgule (/) separator. Example: AB~~~/XY~~~/BC~~~/CD~~~/DE~~~/DE~~~/CD~~~/BC~~~/AB~~~ Each leg must have Airline Carrier Code entry, even if multiple (or all) legs are on same Airline.
181-204	FARE BASIS	24 bytes	Alphanumeric & special characters	Primary & secondary discount codes indicate class of service and fare level associated with ticket. Truncate at 24 bytes, if necessary. Example: ABC123DEF456GHI789JKL012
205-207	NUMBER OF PASSENGERS	3 bytes	Numeric	Number of passengers in party. Example: 001

Note: ~ = character space.

See example on page 124.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present Internet Airline Customer (IAC) Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
208-222	CUSTOMER IP	15 bytes	Alphanumeric & special characters	Customer's Internet IP address, left justified and character space filled (as necessary) to 15 bytes. Example 1: `127.142.151.223` Example 2: `127.142.5.56~~~` Example 3: `12.142.49.190~~`
223-225	CUSTOMER EMAIL ID (CE ID)	3 bytes	Alphanumeric	Customer Email ID is constant literal "`CE~`" (Customer Email).
226-227	VARIABLE LENGTH INDICATOR	2 bytes	Numeric	CE VLI indicates length of CUSTOMER EMAIL variable data (not including CE ID or VLI).
228-251	CUSTOMER EMAIL	1-60 bytes	Alphanumeric & special characters	Customer's email address. Example: `CFFROST@EMAILADDRESS.COM`

Note: ~ = character space.

See example on the next page.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present Internet Airline Customer (IAC) Example

The following example corresponds to the IAC Position Format Table on the preceding pages, and illustrates a data field entry for airline industry Merchants that submit Card not Present Internet Airline Customer data (Data Type Code "IAC").

```
          1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
248AXIAC20030101APN23FROST~JANE~M~MRS~~~~~~~ABC~~XYZ~~RTG611

                                        1         1         1
6         7         8         9         0         1         2
1234567890123456789012345678901234567890123456789012345678901234567890
0ABC~~/DEF~~/GHI~~/JKL~~/MNO~~/PQR~~/STU~~/VWX~~/YZA~~/XYZ~~

1         1         1         1         1         1         1
2         3         4         5         6         7         8
1234567890123456789012345678901234567890123456789012345678901234567890
ALC5509AB~~~/XY~~~/BC~~~/CD~~~/DE~~~/DE~~~/CD~~~/BC~~~/AB~~~

1         1         2         2         2         2         2
8         9         0         1         2         3         4
1234567890123456789012345678901234567890123456789012345678901234567890
ABC123DEF456GHI789JKL012001127.142.005.056CE~24CFFROST@EMAIL

2         2
4         5
1234567890
ADDRESS.COM
```

Note: In the example above, the tilde (~) characters represent character spaces.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Airline Passenger Data (APD) Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	Secondary ID (Data Type Code). Valid IDs include: APD = Internet Airline Customer
9-16	DEPARTURE DATE	8 bytes	Numeric	Departure Date (format CCYYMMDD). Example: 20030101
17-19	AIRLINE PASSENGER NAME ID (APN ID)	3 bytes	Alphanumeric	Airline Passenger Name ID is constant literal "APN" (Airline Passenger Name).
20-21	VARIABLE LENGTH INDICATOR (APN VLI)	2 bytes	Numeric	APN VLI indicates length of Airline PASSENGER NAME variable data (not including APN ID or VLI).
22-44	PASSENGER NAME	23-40 bytes	Alphanumeric & special characters	Passenger Name in format: SURNAME~ FIRSTNAME~MIDDLEINITIAL~TITLE Use character space as sub-element separator. Variable data must be 23-bytes minimum, space filled as necessary, 40-bytes maximum. Truncate at 40 bytes, if necessary. Example: FROST~JANE~M~MRS~~~~~~~
45-47	CARDMEMBER NAME ID (CN ID)	3 bytes	Alphanumeric	Cardmember Name ID is constant literal "CN~" (Cardmember Name).
48-49	VARIABLE LENGTH INDICATOR (CN VLI)	2 bytes	Numeric	CN VLI indicates length of CARDMEMBER NAME variable data (not including CN ID or VLI).
50-72	CARDMEMBER NAME	23-40 bytes	Alphanumeric & special characters	Cardmember Name in format: SURNAME~ FIRSTNAME~MIDDLEINITIAL~TITLE Use character space as sub-element separator. Variable data must be 23-bytes minimum, space filled as necessary, 40-bytes maximum. Truncate at 40 bytes, if necessary. Example: FROST~CHARLES~F~MR~~~~~

Note: ~ = character space.

See example on page 128.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Airline Passenger Data (APD) Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
73-77	ORIGIN (Origin Airport)	5 bytes	Alphanumeric & special characters	First segment travel origination Airport, Note: Five-byte code sequence allows for anticipated expansion of present, three-character Airport Code. If necessary, left justify codes and character space fill each code sequence to five bytes. Example: ABC~~
78-82	DEST (First Segment Travel Destination Airport)	5 bytes	Alphanumeric & special characters	Destination Airport for first travel segment of trip; not necessarily the final destination. For example, if passenger flies from STL to MIA with layover at JFK, Destination Airport for first segment is JFK. Note: Five-byte code sequence allows for anticipated expansion of present, three-character Airport Code. If necessary, left justify codes and character space fill each code sequence to five bytes. Example: XYZ~~
83-85	ROUTING ID (RTG ID)	3 bytes	Alphanumeric	Routing ID is constant literal "RTG" (Routing).
86-87	VARIABLE LENGTH INDICATOR (RTG VLI)	2 bytes	Numeric	RTG VLI indicates combined length of NUMBER OF CITIES and ROUTING CITIES variable data (not including RTG ID or VLI).
88-89	NUMBER OF CITIES	2 bytes	Numeric	Number of Airports or Cities on ticket (10 max).
90-148	ROUTING CITIES	11-59 bytes	Alphanumeric & virgule (/)	Routing Airport or City Codes for each leg on ticket (including ORIGIN and DEST) in five-byte segments with virgule (/) separator. Example: ABC~~/DEF~~/GHI~~/JKL~ /MNO~~/PQR~~/STU~~/VWX~~/YZA~~ /XYZ~~
149-151	AIRLINE CARRIERS ID (ALC ID)	3 bytes	Alphanumeric	Airline Carriers ID is constant literal "ALC" (Airline Carrier).
152-153	VARIABLE LENGTH INDICATOR (ALC VLI)	2 bytes	Numeric	ALC VLI indicates combined length of NUMBER OF AIRLINE CARRIERS and AIRLINE CARRIERS variable data (not including ALC ID or VLI).
154-155	NUMBER OF AIRLINE CARRIERS	2 bytes	Numeric	Number of Airline Carriers entered in AIRLINE CARRIERS subfield (9 max). Example: 09

Note: ~ = character space.

See example on page 128.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Airline Passenger Data (APD) Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description

156-208	AIRLINE CARRIERS	5-53 bytes	Alphanumeric & virgule (/)	Airline Carrier Code for each leg on ticket (including ORIGIN and DEST) in five-byte segments with virgule (/) separator. Example:
				`AB~~~/XY~~~/BC~~~/CD~~~/DE~~~/`
				`DE~~~/CD~~~/BC~~~/AB~~~`
				Each leg must have Airline Carrier Code entry, even if multiple (or all) legs are on same Airline.

209-232	FARE BASIS	24 bytes	Alphanumeric & special characters	Primary & secondary discount codes indicate class of service and fare level associated with ticket. Truncate at 24 bytes, if necessary. Example: `ABC123DEF456GHI789JKL012`
233-235	NUMBER OF PASSENGERS	3 bytes	Numeric	Number of passengers in party. Example: `001`
236	E-TICKET INDICATOR	1 byte	Alphanumeric & special characters	Indicates if ticket is electronic. `E` = E-Ticket ~ = Other ticket types (non-electronic ticket)
237-239	RESERVATION CODE ID (RES ID)	3 bytes	Alphanumeric	Reservation Code ID is the constant literal "`RES`". (Reservation Code).
240-241	VARIABLE LENGTH INDICATOR (RES VLI)	2 bytes	Numeric	RES VLI indicates length of Reservation Code variable data (not including RES ID or VLI). Example: `15`
242-256	RESERVATION CODE	6-15 bytes	Alphanumeric & special characters	Reservation Code (a precursor to a ticket number) corresponds to an airline ticket purchase reservation made by an airline or Global Distribution System (GDS). Example: `ABCDE1234567890`

Note: ~ = character space.

See example on the next page.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Not Present - Airline Passenger Data (APD) Example

The following example corresponds to the APD Position Format Table on the preceding pages, and illustrates a data field entry for airline industry Merchants that submit Airline Passenger Data (Data Type Code "APD").

```
          1         2         3         4         5         6
1234567890123456789012345678901234567890123456789012345678901234567890
253AXAPD20030101APN23FROST~JANE~M~MRS~~~~~~~CN~23FROST~CHARL

                                        1         1         1
6         7         8         9         0         1         2
1234567890123456789012345678901234567890123456789012345678901234567890
ES~F~MR~~~~~ABC~~XYZ~~RTG6110ABC~~/DEF~~/GHI~~/JKL~~/MNO~~/P

1         1         1         1         1         1         1
2         3         4         5         6         7         8
1234567890123456789012345678901234567890123456789012345678901234567890
QR~~/STU~~/VWX~~/YZA~~/XYZ~~ALC5509AB~~~/XY~~~/BC~~~/CD~~~/D

1         1         2         2         2         2         2
8         9         0         1         2         3         4
1234567890123456789012345678901234567890123456789012345678901234567890
E~~~/DE~~~/CD~~~/BC~~~/AB~~~ABC123DEF456GHI789JKL012001ERES1

2         2
4         5
12345678901234 56
5ABCDE1234567890
```

Note: In the example above, tilde (~) characters represent character spaces.

8.1 1100 Authorization Request (continued)

Data Field 47 ADDITIONAL DATA - NATIONAL (continued)

Card Present - Goods Sold Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	Secondary ID (Data Type Code). Valid IDs include: CPD = Card Present Data
9-10	VERSION NUMBER	2 bytes	Numeric	Card Present - Goods Sold data version. Valid numbers include: 01 - Version 1
11-13	GOODS SOLD ID (GS ID)	3 bytes	Alphanumeric	Goods Sold Code is constant literal "GS~" (Goods Sold).
14-15	VARIABLE LENGTH INDICATOR (GS VLI)	2 bytes	Numeric (EBCDIC)	GS VLI indicates length of GOODS SOLD variable data (not including GS ID or VLI)
16-19	GOODS SOLD PRODUCT CODE	4 bytes	Alphanumeric	Four-byte goods product indicator code. Valid codes include: 1000 = Gift Card

Note: ~ = character space.

Card Present - *Goods Sold Example*

The following example corresponds to the Goods Sold Format Table on the preceding pages, and illustrates a data field entry for Goods Sold Merchants that submit Card Present Gift Card data.

```
          1         2         3         4         5         6
12345678901234567890123456789012345678901234567890123456789012345678901
016AXCPD01GS~041000
```

In the example above, tilde (~) characters represent character spaces.

8.1 1100 Authorization Request (continued)

Data Field 48	ADDITIONAL DATA - PRIVATE
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 43 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 40 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Optional — American Express installment plan programs, (special certification required) • Optional — Other bankcards
Description:	This data field contains the American Express Extended Payment Indicator, which consists of the Plan Type and the Number of Installments, preceded by a three-digit, Variable Length Indicator (VLI). 0 1234567 **LLLPPNN** In the above example: LLL = Variable Length Indicator (VLI) PP = Plan Type NN = Number of Installments

8.1 1100 Authorization Request (continued)

Data Field 48	ADDITIONAL DATA - PRIVATE (continued)

Description (continued):	**Plan Type** — The Plan Type is used to indicate which payment plan is applicable to this transaction. Valid entries include:
	`03` = Legacy Plan N
	`05` = Legacy American Express Deferred Payment Plan (DPP) and Extended Payment Plan (EPP) - Merchant Deferred Payment Plan
	Number of Installments — The Number of Installments is used to indicate the number of installment payments applicable to this transaction.
	Note: In some global regions, these subfields are further defined to transport data that is used only in those areas. See regional definitions for Plan N, EPP and DPP below and on the following pages.
	Plan N — LA/C
	For transactions processed per Plan N, Merchants receive deferred payment installments from American Express, and Cardmembers are billed in deferred billing installments. By processing transactions using Plan N, the Merchant absorbs any interest accrual. See the following example for Plan N:
	`0`
	`1234567`
	`0040303`
	In the example above:
	`004` = VLI — Indicates that data length is 4 bytes.
	`03` = Plan Type — "`03`" = Plan N
	`03` = Number of Installments — "`03`" = 3 installments

8.1 1100 Authorization Request (continued)

Data Field 48	ADDITIONAL DATA - PRIVATE (continued)

Deferred Payment Plan (DPP) — LA/C & APA
Extended Payment Plan (EPP) — APA

For transactions processed per the Deferred Payment Plan (DPP) or the Extended Payment Plan (EPP), Merchants are paid in one installment; and American Express bills Cardmembers in deferred billing installments, with or without interest.

Additional requirement for DPP or EPP transactions:

- Function Code (Data Field 24) must be "100".

See the following DPP/EPP example:

0
1234567

0040503

In the example above:

004 = VLI — Indicates that data length is 4 bytes.

05 = Plan Type — "05" = DPP or EPP

03 = Number of Installments — "03" = 3 installments

Note: The Number of Installments default value (which varies by region and country) is specified during terminal or system setup. For more information, contact your American Express representative.

8.1 1100 Authorization Request (continued)

Data Field 49	CURRENCY CODE, TRANSACTION
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the numeric code that describes the currency used in this transaction. For example, the numeric currency code for U.S. Dollars is "840". For more information on numeric currency codes and decimal point positions, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*. **Notes**: 1. If Data Field 55 is populated, the currency code entries in Data Fields 49 and 55 (Transaction Currency Code subfield, Positions 72-73) must match. 2. This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

8.1 1100 Authorization Request (continued)

Data Field 52	PERSONAL IDENTIFICATION NUMBER (PIN) DATA
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	Conditional — Used only when PIN is available
Certification Requirement:	Mandatory — Third Party Processors and/or Vendors must be certified to pass data in this data field. After certification, all Merchant-provided data must be forwarded in this data field.
Description:	This data field is for use in markets that support online PIN verification, and it will transport encrypted PIN data for PIN-based Point of Sale (POS) transactions.Unauthorized use of this data field may cause message rejection.

8.1 1100 Authorization Request (continued)

Data Field 53	SECURITY RELATED CONTROL INFORMATION
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 19 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 17 bytes maximum, EBCDIC or Binary
Field Type:	Alphanumeric or unsigned binary numbers
Constant:	None
Field Requirement:	• Mandatory — PIN Transactions using DUKPT • Optional — American Express transactions • Not used — Other bankcards
Certification Requirement:	Global - All regions Mandatory — Third Party Processors and/or Vendors must be certified to pass data in this data field. After certification, all Merchant-provided data must be forwarded in this data field.
Description:	This field is used for American Express keyed Card Identifier (CID) code or Derived Unique Key Per Transaction (DUKPT) Key Serial Number (KSN) processing only. **Keyed 4 digit CID Code (a.k.a 4DBC or 4CSC)** This data field contains the American Express Card Identifier (CID) code (a.k.a., 4DBC or 4CSC), preceded by a two-digit Variable Length Indicator (VLI). If Data Field 53 is present, then POS Data Code, Data Field 22, Position 7, must be set to value "9", "S", "W" or "Y". Extract of POS Data Code table appears below, or see Data Field 22, Position 7.

9	Technical fallback - Transaction initiated as chip, but was processed using an alternative technology (such as magnetic stripe).
S	Manually entered or keyed transaction with keyed CID/4DBC/4CSC, Data Field 53 (Security Related Control Information) must be present.
W	Swiped transaction with keyed CID/4DBC/4CSC. Data Field 53 (Security Related Control Information) must be present.

8.1 1100 Authorization Request (continued)

Data Field 53	SECURITY RELATED CONTROL INFORMATION (continued)

Keyed 4 digit CID Code (a.k.a 4DBC or 4CSC) (continued):

This value is manually entered by keying the four-digit CID/4DBC/4CSC, which is printed on the face of the American Express Card. See the following formatting details for Manual Entry.

Format for Manual Entry - "`04XXXX`" where "`04`" is the Variable Length Indicator (VLI) and "`XXXX`" is the four-digit CID/4DBC/4CSC code from the face of the American Express Card. **Note**: See CID/4DBC/4CSC location on typical American Express Card products.

The following requirements must be met prior to sending a keyed CID/4DBC/4CSC value that will be actioned by American Express:

- From the Authorization Response (1110) message, system is prepared to accept all possible Action Codes found in Data Field 39 and all possible Response Indicators found in byte 2 of Data Field 44, and in any combination.
- System is prepared to send a second authorization request with revised 4DBC/4CSC value, if a response is not approved; or if it is treated as not approved due to a CID mismatch.

Notes:

1. American Express security requirements prohibit storage of keyed CID/4DBC/4CSC data within Merchant or Third Party Processor systems.
2. CID and KSN cannot be used in the same Authorization Request (1100) message

DUKPT KSN

This value is the Derived Unique Key Per Transaction (DUKPT) Key Serial Number (KSN). The Key Serial Number (KSN) ensures that each DUKPT transaction has a unique key.

Refer to the *ANSI X9.24 Standard* for additional details on the KSN format.

Note: CID and KSN cannot be used in the same Authorization Request (1100) message.

8.1 1100 Authorization Request (continued)

Data Field 53 SECURITY RELATED CONTROL INFORMATION (continued)

DUKPT KSN Format Table

Subfield Name	Subfield Length	Subfield Type	Description
VARIABLE LENGTH INDICATOR (VLI)	2 bytes	Numeric (EBCDIC)	VLI indicates total length of variable data in this data field (not including VLI).
PRIMARY ID	2 bytes	Alphanumeric	Primary ID (Card Type Code) is constant literal "AX" (American Express).
SECONDARY ID	3 bytes	Alphanumeric	Secondary ID (Data Type Code). Valid IDs include: KSN = Key Serial Number Data
VARIABLE LENGTH INDICATOR (VLI)	2 bytes	Numeric (EBCDIC)	VLI indicates the total length of variable data for KSN data (not including the VLI).
KSN	10 bytes	Binary	The Key Serial Number (KSN) ensures that each DUKPT transaction has a unique key.

8.1 1100 Authorization Request (continued)

Data Field 55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 259 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 256 bytes maximum, EBCDIC, BCD or binary
Field Type:	Alphanumeric & special characters, and binary coded decimal (BCD) or unsigned binary numbers **Note**: Data Field 55 contains some subfields that are forwarded for transmission to an integrated circuit card or terminal, and are specified as binary. This data is in binary format in 8 bit blocks, right justified and zero filled, per the following: 1. Binary Coded Decimal (BCD)* - Data items whose original formats are defined as numeric are represented with two digits per byte ("`00`" to "`99`"). Each digit is stored on four bits (one nibble) resulting in each byte storing two digits. For example, a date subfield containing numerals representing the date November 30, 2006 in `YYMMDD` format would be three-bytes holding the six digits "`06 11 30`". A numeric subfield with an odd number of digits is padded with a leading zero before packing. 2. Unsigned Binary Number† - Data items whose original formats are defined as binary are mapped directly as eight bits per byte, with the value for any binary byte of data varying from hexadecimal "`00`" to "`FF`". For example, the Application Transaction Counter (ATC) is defined as a two-byte, unsigned binary number. Thus, the ATC value "`26`" would be stored as "`00 1A`" hex.
Constant:	None

* Also referred to as *binary numeric* in some American Express documentation.
† Also referred to as *binary hexadecimal* in some American Express documentation.

8.1 1100 Authorization Request (continued)

Data Field 55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA (continued)
Field Requirement:	• Mandatory — AEIPS transactions (special certification required) • Mandatory — Expresspay EMV* transactions • Not used — Other transactions
Certification Requirement:	Global - All regions Mandatory — Third Party Processors and/or Vendors must be certified to pass Card Present transactions for Integrated Circuit Cards (ICCs) in this data field. After certification, all Merchant-provided ICC related data must be forwarded in this data field.
Description:	This data field contains Integrated Circuit Card (ICC) Related Data defined in the subfield table on the next page. If Data Field 22 (POS Data Code) Position 7 = "5", then this data field must be present. Data Field 22 describes the interaction between Data Field 22 and Data Field 55. Before Merchants may use this data field, special certification is required to process AEIPS or Expresspay transactions. For more information, reference the AEIPS Chip Card Specification and AEIPS Terminal Specification, in addition to contacting your American Express representative. **Note**: For Merchants who have not completed this certification, no data can be transmitted in this data field to American Express. Unauthorized use of this data field may result in message rejection. See table containing subfield details on the next page.

* EMV is the abbreviation for Europay/MasterCard/VISA, joint sponsors of the global standard for electronic financial transactions using "chip card" technology.

8.1 1100 Authorization Request (continued)

Data Field 55 INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA (continued)

EMV Tags	Relative Position	Subfield Name	Subfield Length	Subfield Type	Required	Description
	1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	Yes	VLI indicates total length of variable data in this data field (not including VLI).
	4-7	ICC HEADER VERSION NAME	4 bytes	Alphanumeric (EBCDIC)	Yes	Data Field 55 Version Header is constant literal "AGNS".
	8-9	ICC HEADER VERSION NUMBER	2 bytes	Binary coded decimal (BCD)	Yes	Data Field 55 Version Number is constant literal "0001".
9F26	10-17	APPLICATION CRYPTOGRAM	8 bytes	Unsigned binary number	Yes	The Application Cryptogram generated by the chip card in response to GENERATE AC Command. In an online authorization message, this will be the Authorization Request Cryptogram (ARQC).
9F10	18-50	ISSUER APPLICATION DATA (IAD)	33 bytes, max (LLVAR)	Unsigned binary number	Yes	One byte, unsigned-binary-number VLI indicates subfield length, and precedes up to 32 bytes of variable data. For example, the VLI for 32 bytes of variable data is = "20" (one byte) in hex. See explanation of unsigned binary number format on page 138. **Note**: This subfield contains proprietary, Issuer-defined application data transmitted from card to Issuer. For details, refer to the *American Express AEIPS Chip Card Specification*. Only card Issuer needs to know how to interpret. Networks and systems need only forward IAD in its entirety, without alteration, to card Issuer.
9F37	51-54	UNPREDICTABLE NUMBER	4 bytes	Unsigned binary number	Yes	A terminal-generated Unpredictable Number, which is a randomly generated value that adds variability and uniqueness to the creation of the application cryptogram value in the preceding APPLICATION CRYPTOGRAM data field.

8.1 1100 Authorization Request (continued)

Data Field 55 INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA (continued)

EMV Tags	Relative Position	Subfield Name	Subfield Length	Subfield Type	Required	Description
9F36	55-56	APPLICATION TRANSACTION COUNTER (ATC)	2 bytes	Unsigned binary number	Yes	Counter maintained by application on the card. Chip Card increments this value for each transaction. Because counter includes failed transactions, this value cannot be used alone to track last transaction.
95	57-61	TERMINAL VERIFICATION RESULTS (TVR)	5 bytes	Unsigned binary number	Yes	Status of various functions, as determined by terminal. For details, refer to the *American Express AEIPS Terminal Specification*.
9A	62-64	TRANSACTION DATE	3 bytes	Binary coded decimal (BCD)	Yes	Terminal-generated Transaction Date, in format "`YY MM DD`". Example: Jan. 1, 2007 = "`07 01 01`".
9C	65	TRANSACTION TYPE	1 byte	Binary coded decimal (BCD)	Yes	Code indicates type of financial transaction represented by the first two digits of the ISO 8583 Processing Code. Valid entries include: `00` = Debit
9F02	66-71	AMOUNT AUTHORIZED	6 bytes	Binary coded decimal (BCD)	Yes	Authorization amount of transaction, provided by terminal to the card. **Note**: This value is used in cryptogram generation, and it may differ from other amount data fields in this request message.
5F2A	72-73	TRANSACTION CURRENCY CODE	2 bytes	Binary coded decimal (BCD)	Yes	ISO currency code for this transaction. Example: "`124`" (Canadian Dollars) is entered as "`01 24`" in 2-byte, BCD format. **Note**: The currency code entries in this subfield and Data Field 49 (Currency Code, Transaction) must match.
9F1A	74-75	TERMINAL COUNTRY CODE	2 bytes	Binary coded decimal (BCD)	Yes	ISO country code for terminal location. Example: "`124`" (Canada) is entered as "`01 24`" in 2-byte, BCD format.

8.1 1100 Authorization Request (continued)

Data Field 55 INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA (continued)

EMV Tags	Relative Position	Subfield Name	Subfield Length	Subfield Type	Required	Description
82	76-77	APPLICATION INTERCHANGE PROFILE (AIP)	2 bytes	Unsigned binary number	Yes	Bitmap that indicates ability of the card to support specific functions. Contents of this subfield are described in the *American Express AEIPS Chip Card Specification*.
9F03	78-83	AMOUNT, OTHER	6 bytes	Binary coded decimal (BCD)	Yes	Secondary amount associated with transaction representing a cashback amount. Zero-fill, if cashback is not supported.
5F34	84	APPLICATION PAN SEQUENCE NUMBER	1 byte	Binary coded decimal (BCD)	Yes	Identifies and differentiates card applications with same PAN. Both PAN & PAN Sequence Number are required to validate Application Cryptogram.
9F27	85	CRYPTOGRAM INFORMATION DATA (CID)	1 byte	Unsigned binary number	Yes	Indicates type of cryptogram (TC, ARQC or AAC) returned by the card, and actions to be performed by terminal. Formatted per the *American Express AEIPS Chip Card Specification*.
	86-259	RESERVED FOR FUTURE USE	174 bytes, max (LLVAR)	N/A	No	This subfield is reserved for future use and should be completely omitted (including LLVAR). Specifically, no information should be forwarded, as all data will be ignored by both network and Issuer.

8.1 1100 Authorization Request (continued)

Data Field 60	NATIONAL USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	13 bytes minimum, 106 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 103 bytes maximum, EBCDIC or Binary
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Global — All regions • Mandatory — Payment Service Providers (Aggregators) & OptBlue Participants • Mandatory — Payment Token transactions where the Token Requester ID (TRID) is available • Not used — All other transactions
Certification Requirement:	• Global — All regions • Mandatory — Third Party Processors and/or Vendors must be certified to pass data in this data field. After certification, all Merchant-provided data must be forwarded in this data field.
Description:	This data field supports two types of transaction processing: Payment Service Provider (Aggregator)/OptBlue and Payment Token. These two types of transactions can be sent together or separately. This field currently consists of five bitmap subfields proceeded by a three-digit, Variable Length Indicator. **Payment Service Provider (Aggregator) and OptBlue Participants** Subfields 2, 3 and 4 support Payment Service Provider (Aggregator) and OptBlue Participant data. These subfields include Seller ID, Seller Email Address, and Seller Telephone Number. These subfields should be used in conjunction with Data Field 43, Card Acceptor Name/Location, Payment Service Provider (Aggregator) and OptBlue Participant format.

8.1 1100 Authorization Request (continued)

Data Field 60	NATIONAL USE DATA
Description (continued):	**Payment Token Transactions** Subfields 5 and 6 support Payment Token transaction processing. These subfields include Token Requestor ID (TRID) and Last 4 PAN Return Indicator. • Token Requestor ID — Received by the Merchant from the mobile device. • Last 4 PAN Return Indicator — Enables a Merchant to request the last four digits of the PAN be returned in Data Field 34, Primary Account Number, Extended of the Authorization Response (1110) message. See Subfield Table on the next page.

8.1 1100 Authorization Request (continued)

Data Field 60 NATIONAL USE DATA (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of *variable data* in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alphanumeric	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alphanumeric	M	Secondary ID (Data Type Code) is constant literal "AAD" (Additional Authorization Data)
9-12	BITMAP IDENTIFIER	4 bytes	Binary (hexadecimal configuration)	M	Bitmap Identifier Each bit in this data element identifies the presence (value 1) or absence (value 0) of a subfield. Following the Bitmap, the layout consists of at least (1) of the following subfields. Each bit position of the 32 bit/4-byte bitmap represents which market specific data are present. If a bit is "ON" in the bitmap, that corresponding subfield will be present.
Subfield					
1	Reserved for American Express Internal Use	N/A	N/A	N/A	N/A
2	Seller ID	20 bytes fixed	Alphanumeric	C[1]	20-digit, numeric, Seller ID, that uniquely identifies a Payment Service Provider's (Aggregators) or OptBlue Participant's specific Seller or Vendor. Left justified, character space filled.
LLVAR	Variable Length Indicator	2 bytes	Numeric	C[2]	VLI indicates total length of Seller Email Address variable data.
3	Seller Email Address	40 bytes max	Alphanumeric & special characters	C[1]	Email of the Payment Service Provider's (Aggregators) or OptBlue Participant's Seller.
4	Seller Telephone	20 bytes fixed	Alphanumeric	C[1]	Telephone number of the Payment Service Provider's (Aggregators) or OptBlue Participant's Seller. Left justified, character space filled.

C[1] = Mandatory for Payment Service Providers (Aggregators) and OptBlue Participants

C[2] = Mandatory if populating Subfield 3, Seller Email Address

8.1 1100 Authorization Request (continued)

Data Field 60 NATIONAL USE DATA (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
Subfield (continued)					
5	TOKEN REQUESTOR ID (TRID)	11 bytes, fixed	Alphanumeric	C[3]	Token Requestor ID (TRID) contains the 11-byte numeric value that uniquely identifies the Payment Token requestor. Refer to the *EMVCo Payment Tokenization Specification - Technical Framework* specification for additional information.
6	LAST 4 PAN RETURN INDICATOR	1 byte	Alphanumeric	O	Last 4 PAN Return Indicator is constant literal "Y".

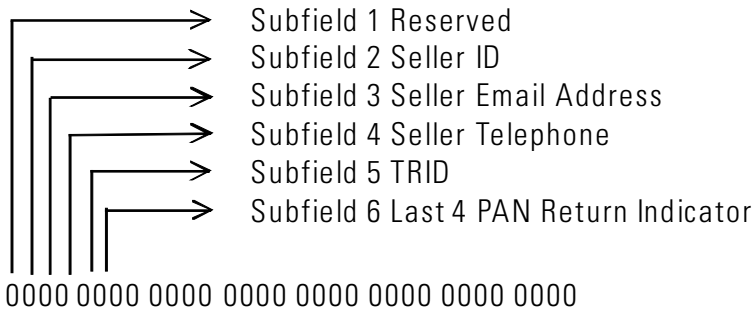
C[3] = Mandatory for Payment Token transactions where the Token Requestor ID (TRID) is available

8.1 1100 Authorization Request (continued)

Data Field 60 NATIONAL USE DATA (continued)

Data Field 60 NATIONAL USE DATA (continued)

Illustration of 32 Bit String Contained Within Four Byte Data Field



Following example includes Seller ID, Seller Email Address and Seller Telephone:

Position	Value
1-3	070
4-5	AX
6-8	AAD
9-12	01110000000000000000000000000000 X'70000000'
Subfields 2-4	22222222222222222222193333333333@33333334444444444~~~~~~~~~~

Following example includes Seller ID, Seller Email Address and Seller Telephone, TRID and LAST 4 Pan Return Indicator:

Position	Value
1-3	082
4-5	AX
6-8	AAD
9-12	01111100000000000000000000000000 X'7C000000'
Subfields 2-4	22222222222222222222193333333333@33333334444444444~~~~~~~~~~555555555556

8.1 1100 Authorization Request (continued)

Data Field 60 NATIONAL USE DATA (continued)

Following example includes Seller TRID and Last 4 PAN Return Indicator:

Position	Value
1-3	021
4-5	AX
6-8	AAD
9-12	00001100000000000000000000000000 X'0C000000'
Subfields 2-4	555555555556

8.1 1100 Authorization Request (continued)

Data Field 61	NATIONAL USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 103 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 100 bytes maximum, EBCDIC & Binary
Field Type:	Alphanumeric, special characters and unsigned binary numbers **Note**: Data Field 61 contains some subfields that are specified as binary. This data is in binary format in 8-bit blocks, right justified and zero filled. Unsigned Binary Number* - Data items whose original formats are defined as binary are mapped directly as eight bits per byte, with the value for any binary byte of data varying from hexadecimal "00" to "FF".
Constant:	None
Field Requirement:	• Mandatory — American Express SafeKey transactions (special certification required) • Mandatory — Digital Wallet - application initiated (including application initiated Payment Token) transactions • Not used — Other transactions
Certification Requirement:	See Section 6.4 for the website link to American Express SafeKey enabled countries. • Mandatory — Third Party Processors and/or Vendors must be certified to pass American Express SafeKey authentication data in this data field. • Mandatory — Third Party Processors and/or Vendors must be certified to pass Merchant-provided Payment Token data in this data field.

* Also referred to as *binary hexadecimal* in some American Express documentation.

8.1 1100 Authorization Request (continued)

Data Field 61	NATIONAL USE DATA (continued)
Description:	American Express SafeKey is an industry-standard Authentication method that provides greater security by authenticating the Cardmember during an online purchase and protecting payment card information as it is transmitted via the Internet. Before Merchants may use this data field, special certification is required to process American Express SafeKey transactions. For more information, refer to the *American Express SafeKey℠ Acquirer - Merchant Implementation Guide*, in addition to contacting your American Express representative. For American Express SafeKey transaction processing subfield details, see page 151. The American Express Payment Token transaction processing solution is based on an industry aligned and interoperable tokenization system that offers increased protection against fraud through the use of a Payment Token. A Payment Token will be used in place of sensitive Cardmember data such as Primary Account Number (PAN) to originate payment transactions. For American Express Payment Token transaction processing subfield details, see page 146. **Note**: For Merchants who have not completed certification for American Express SafeKey and/or Payment Token transactions, no data can be transmitted in this data field to American Express. Unauthorized use of this data field may result in message rejection.

8.1 1100 Authorization Request (continued)

Data Field 61 NATIONAL USE DATA (continued)

American Express SafeKey Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alpha	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alpha	M	Secondary ID (Data Type Code) is constant literal "ASK" (American Express SafeKey)
9-10	ELECTRONIC COMMERCE INDICATOR (ECI)	2 bytes	Alphanumeric	M	ECI is the level of security used when Cardmember provides payment information to the Merchant during American Express SafeKey authentication. Valid values include: 05 = Authenticated with AEVV 06 = Attempted with AEVV 07 = Not Authenticated
11-14	AMERICAN EXPRESS VERIFICATION VALUE (AEVV) ID	4 bytes	Alpha	C[1]	AEVV ID is constant literal "AEVV".
15-34	AMERICAN EXPRESS VERIFICATION VALUE (AEVV)	20 bytes	Unsigned binary number	C[2]	AEVV is a cryptographic value derived by the Issuer during the American Express SafeKey payment authentication that can provide evidence of the results of payment authentication during an online purchase.
35-37	AMERICAN EXPRESS SAFEKEY TRANSACTION ID (XID)	3 bytes	Alpha	C[3]	American Express SafeKey Transaction ID is constant literal "XID". **Note**: The XID Value is an optional Merchant-populated value.
38-57	AMERICAN EXPRESS SAFEKEY TRANSACTION ID VALUE	20 bytes	Unsigned binary number	C[3]	American Express SafeKey Transaction Identifier is determined by the Merchant during the American Express SafeKey payment authentication. **Note**: The American Express SafeKey Transaction ID is not the same as the Acquirer Reference Data - Transaction Identifier in Data Field 31 of the 1100/1110.

C[1] = Conditional - required if AEVV is present

C[2] = Conditional - required if the ECI is not "07"

C[3] = Conditional - required if American Express SafeKey Transaction ID Value is present

8.1 1100 Authorization Request (continued)

Data Field 61 NATIONAL USE DATA (continued)

American Express Payment Token Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alpha	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alpha	M	Secondary ID (Data Type Code) is constant literal "TKN" (Tokenization) **Note**: When using "TKN", Data Field 61 will not appear in the Authorization Response (1110) message.
9-10	ELECTRONIC COMMERCE INDICATOR (ECI)	2 bytes	Alphanumeric	M	ECI is the level of security used when Cardmember provides payment information to the Merchant during American Express authentication. Valid value includes: 20 = Payment Token data present
11-14	Token Data Block A ID	4 bytes	Alpha	M	Token Data Block A ID is constant literal "TDBA".
15-34	Token Data Block A	20 bytes	Unsigned binary number	M	Token Data Block A contains bytes 1-20 of the cryptographic value.
35-37	Token Data Block B ID	3 bytes	Alpha	C[1]	Token Data Block B ID is constant literal "DBB".
38-57	Token Data Block B	20 bytes	Unsigned binary number	C[2]	Token Data Block B contains bytes 21-40 of the cryptographic value.

C[1] = Conditional - required if Token Data Block B is present

C[2] = Conditional - required if the cryptographic value is greater than 20 bytes

8.1 1100 Authorization Request (continued)

Data Field 62	PRIVATE USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 63 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 60 bytes maximum, coding determined by data field use
Field Type:	Alphanumeric & special characters, and binary coded decimal (BCD) or unsigned binary numbers
Constant:	None
Field Requirement:	• Mandatory — American Express Travelers Cheques • Optional — Transponder transactions • Mandatory — VISA PS2000 transactions • Not used — Other transactions
Description:	This data field is used for American Express Travelers Cheques, Transponder or VISA PS2000 processing only. **Note**: Transactions containing Transponder data are considered Card Not Present transactions. **American Express Travelers Cheque Encashment** For American Express Travelers Cheques (TC), this data field is used to capture the denomination (face value) of the individual TC to be encashed, when the Travelers Cheque Number is manually entered in Data Field 63 (see page 157). This data field must contain the denomination of the Travelers Cheque, in whole currency units (no decimals), in the currency designated by the Currency Code, Transaction data field (Data Field 49). For Example, for a $50 USD Travelers Cheque, the variable data in this entry would be "`50`"; and for a $100 Travelers Cheque, it would be "`100`", etc. If multiple Travelers Cheques are presented for encashment, the entry in this data field must correspond to the Travelers Cheque Number entered in Data Field 63, Private Use Data.

8.1 1100 Authorization Request (continued)

Data Field 62	PRIVATE USE DATA (continued)

American Express Travelers Cheque Encashment (continued)

For American Express Travelers Cheques, the maximum length of variable data that can be transported in this data field is 11 bytes.

See the following examples:

```
0         1
12345678901234
```

LLLSSRRDDDDDDD

- "LLL" is the three-digit, Variable Length Indicator (VLI), right justified and zero filled, if necessary.
- "SS" is the two-character, Service Identifier (SI).
- "RR" is the two-character, Request Type Identifier (RTI).
- "DDDDDDD" is the Travelers Cheque denomination (seven-bytes, maximum).

American Express Travelers Cheque Example

```
123456789
```

006AXTC50

- "006" is the Variable Length Indicator (VLI).
- "AX" is the Service Identifier (constant literal "AX" = American Express).
- "TC" is the Request Type Identifier (constant literal "TC" = Travelers Cheque).
- "50" is the Travelers Cheque denomination ($50 USD).

8.1 1100 Authorization Request (continued)

Data Field 62	PRIVATE USE DATA (continued)

Transponder Transactions

This data field may contain a Merchant-captured, security/identification code associated with processing Authorization Request (1100) messages initiated by electronic, radio-frequency devices (transponders or RFIDs; e.g., Speedpass™). This unique, transponder-Issuer assigned code corresponds to a customer-designated form of payment and Cardmember Account Number, on the transponder-Issuer's system.

Note: For transactions initiated by an electronic, radio-frequency device (transponder or RFID, e.g., Speedpass), Data Field 62 (AXTN + transponder security/ID code) may be used alone or in conjunction with POS Data Code (Data Field 22), Position 6, value "W". Alternately, POS Data Code (Data Field 22), Position 6, value "W" may be used without a transponder security/ID entered in Data Field 62. Ideally, both items are transmitted. For more details, see page 81.

Card Type (primary) and Device Type (secondary) identifiers precede a variable-length security/identification code (19 bytes maximum), as illustrated in the following format:

```
0         1         2
12345678901234567890123456
LLLCCDDsssssssssssssssss
```

- "LLL" is the three-digit, Variable Length Indicator (VLI).
- "CC" is the two-character, Card Type code (always "AX").
- "DD" is the two-character, Device Type code (always "TN").
- "sssssssssssssssss" is the variable-length, security/ identification code (19 characters maximum, no padding).

Transponder Data Example

In the following example, "023" is the three-digit, Variable Length Indicator (VLI); "AX" is the two-character, Card Type code (AX = American Express); "TN" is the two-character, Device Type code (TN = transponder); and "1234567890 123456789" is the 19 character security/identification code.

```
0         1         2
12345678901234567890123456
023AXTN1234567890123456789
```

8.1 1100 Authorization Request (continued)

Data Field 62	PRIVATE USE DATA (continued)

VISA PS2000 Transactions

The following code is entered in this data field, if the transaction Acquirer wishes to have this Authorization Request (1100) message considered for VISA PS2000:

`001Y`

In this example, "`001`" is the Variable Length Indicator (VLI), and the "`Y`" indicates that this transaction is being submitted for VISA PS2000 qualification.

Note: Additional sub-element values may exist, subject to VISA requirements.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 208 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 205 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Mandatory — American Express Travelers Cheques • Optional — To participate in Automated Address Verification (AAV), ZIP Code Verification, Enhanced Authorization (Shipping), and Telephone Number Verification • Conditional — To participate in Email Address Verification (if RTI = "AE" and Data Field 47 is present) • Not used — Other transactions
Certification Requirement:	Global - All regions Mandatory — Third Party Processors and/or Vendors must be certified to pass 33-, 78- and 205-byte formats and Request Type Identifier (RTI) "AD" and "AE" of Automated Address Verification (AAV) and Telephone Number Verification data in this data field. After certification, all Merchant-provided AAV and Telephone Number data must be forwarded in this data field.
Description:	This data field contains data required to process certain types of Authorization Request (1100) messages, such as American Express Travelers Cheque, and verifications for Cardmember Name, Address, ZIP Code, and Telephone Number.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)
Description:	**Combination Address Verification & Authorization**

Authorization Verification Only

The format for this data field must be consistent with Processing Code, Data Field 3, codes "`004800`" (Combination Address Verification and Authorization) and "`174800`" (Address Verification Only). For details, see page 212.

See descriptions and examples below and on the following pages.

Electronic Verification

American Express supports Automated Address Verification (AAV) and Telephone Number Verification.

The three formats that correspond to the length of variable data in this data field (not including the three-digit VLI) are:

- **33-Byte Format** — AAV
- **78-Byte Format** — AAV
- **205-Byte Format** — AAV, Enhanced Authorization (Shipping) and Telephone Number Verification

These three formats transport different combinations of Cardmember and/or Ship-to data in various subfields, as specified by a three-digit Variable Length Indicator (VLI).

Descriptions of AAV-types with corresponding VLIs appear on the next few pages, with tables that illustrate how the three formats are utilized to transmit different amounts of data. On page 163, a summary table lists Data Field 63 subfield names, relative positions, lengths, data field types and usage.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)
	Data Field 63 descriptions for Cardmember information subfields appear on page 164, followed by Ship-to descriptions on page 168. Finally, examples of typical 33-, 78- and 205-byte format data appear on page 171 with an accompanying explanation.
AAV (RTI=AD) Optional Subfields: • CM Billing Postal Code • CM Billing Address • CM First & Last Name • CM Billing Phone Number • Ship-to Postal Code • Ship-to Address • Ship-to First & Last Name • Ship-to Phone Number • Ship-to Country Code	AAV with Request Type Identifier "AD" is used to submit various levels of Cardmember and shipping data for verification, as determined by the total data length of this data field (not including VLI). All subfields are optional, but within a given format, unused subfields must be character space filled. **33-Byte Format** — Used to forward the Cardmember's Billing Postal Code and/or Street Address. **78-Byte Format** — Used to append the Cardmember's First and Last Name to the preceding data. **205-Byte Format** — Used to append the Cardmember's Billing Telephone Number and Enhanced Authorization shipping information to the preceding data. Ship-to subfields may be populated for all shipping addresses. See typical examples of these three formats on page 171. Merchants are encouraged to use the 205-byte format to include the telephone number and shipping data on all shipments, even if Cardmember and Ship-to addresses are identical, because this data enhances the American Express ability to assess risk. Merchants populating Data Field 47 (Additional Data-National), ITD format, Shipping Method, using shipping-type code (06), Ship-to Store, are strongly encouraged to populate the address of the store location in the Ship-to Address in the 205-byte format. An AAV response is returned in the Authorization Response (1110) message in Data Field 44, Additional Response Data, relative position 3, as a one-byte code that indicates if the Cardmember Billing Postal Code, Address and/or First and Last Name match American Express records. For details, see page 197.

8.1 1100 Authorization Request (continued)

Data Field 63 **PRIVATE USE DATA (continued)**

AAV

The basic differences in AAV variants are illustrated in the following tables.

For AAV, the Request Type Identifier (RTI) is "AD".

	Request Type Identifier (RTI)	Authorization Request	Data Field 3 Processing Code	CM P Billing Postal Code	CM Billing Address	CM Name	CM Billing Phone Number	Ship-to Postal Code	Ship-to Address	Ship-to Name	Ship-to Phone	Ship-to Country Code	Length of Variable Data
33-Byte Format	AD	YES	004800	O	O								33
	AD	NO	174800	O	O								33
78-Byte Format	AD	YES	004800	O	O	O							78
	AD	NO	174800	O	O	O							78
205-Byte Format	AD	YES	004800	O	O	O	O	O	O	O	O	O	205
	AD	NO	174800	O	O	O	O	O	O	O	O	O	205

In the table, above:

O = Optional - Subfield may be populated.

Note: Optional subfields including CM Billing Phone Number, that are not populated, must be character space filled to meet 33-, 78- or 205-byte variable data length specified. For summary of subfield positions and lengths, see table on page 163.

8.1 1100 Authorization Request (continued)

Data Field 63 **PRIVATE USE DATA (continued)**

Telephone Number Verification (RTI=AE)

Merchants must submit Telephone Number data using the 205-byte format and Request Type Indicator (RTI) "AE".

In addition to AAV subfields, the CM Phone Number is also an optional subfield.

The Telephone Number Verification response is returned in the Authorization Response (1110) message in Data Field 62, as a series of one-byte codes that indicate if the Customer telephone number, in addition to Postal Code, Address and Name match Cardmember information on file with the Issuer. For details, see page 211.

	Request Type Identifier (RTI)	Authorization Request	Data Field 3 Processing Code	CM Billing Postal Code	CM Billing Address	CM Name	CM Billing Phone Number	Ship-to Postal Code	Ship-to Address	Ship-to Name	Ship-to Phone	Ship-to Country Code	Length of Variable Data
205-Byte Format	AE	YES	004800	O	O	O	O	O	O	O	O	O	205
	AE	NO	174800	O	O	O	O	O	O	O	O	O	205

In the table, above:

O = Optional - Subfield may be populated.

Note: Optional subfields including CM Billing Phone Number, that are not populated, must be character space filled to meet 33-, 78- or 205-byte variable data length specified. For summary of subfield positions and lengths, see table on page 163.

8.1 1100 Authorization Request (continued)

Data Field 63 **PRIVATE USE DATA (continued)**

Email Address Verification (RTI=AE)*

For Email Address Verification, Merchants must submit the 33-, 78- or 205-byte format with Request Type Indicator (RTI) "AE".

	Request Type Identifier (RTI)	Authorization Request	Data Field 3 Processing Code	CM Billing Postal Code	CM Billing Address	CM Name	CM Billing Phone Number	Ship-to Postal Code	Ship-to Address	Ship-to Name	Ship-to Phone	Ship-to Country Code	Length of Variable Data
33-Byte Format	AE	YES	004800	O	O								33
	AE	NO	174800	O	O								33
78-Byte Format	AE	YES	004800	O	O	O							78
	AE	NO	174800	O	O	O							78
205-Byte Format	AE	YES	004800	O	O	O	O	O	O	O	O	O	205
	AE	NO	174800	O	O	O	O	O	O	O	O	O	205

In the table, above:

O = Optional - Subfield may be populated.

Note: Optional subfields including CM Billing Phone Number, that are not populated, must be character space filled to meet 33-, 78- or 205-byte variable data length specified. For summary of subfield positions and lengths, see table on page 163.

* In order to use Email Address Verification, the RTI in this data field must be AE. However, Email Address is a subfield of Data Field 47, Additional Data - Private, in the ITD Format. For more information on Email Address, see page 117.

8.1 1100 Authorization Request (continued)

Data Field 63 **PRIVATE USE DATA (continued)**

Data Field 63 Subfield Summary Table

Note: RTI = AD or AE

See detailed descriptions of each subfield on the following pages.

Pos.	Data Field 63 Subfield Name	Length	Subfield Type	Subfield Requirement
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M
4-5	SERVICE IDENTIFIER	2 bytes	Alphanumeric	M
6-7	REQUEST TYPE IDENTIFIER	2 bytes	Alphanumeric	M
8-16	CARDMEMBER BILLING POSTAL CODE	9 bytes	Alphanumeric	O
17-36	CARDMEMBER BILLING ADDRESS	20 bytes	Alphanumeric	O
37-51	CARDMEMBER FIRST NAME	15 bytes	Alphanumeric	O
52-81	CARDMEMBER LAST NAME	30 bytes	Alphanumeric	O
82-91	CARDMEMBER BILLING PHONE NUMBER	10 bytes	Alphanumeric	O
92-100	SHIP-TO POSTAL CODE	9 bytes	Alphanumeric	O
101-150	SHIP-TO ADDRESS	50 bytes	Alphanumeric	O
151-165	SHIP-TO FIRST NAME	15 bytes	Alphanumeric	O
166-195	SHIP-TO LAST NAME	30 bytes	Alphanumeric	O
196-205	SHIP-TO PHONE NUMBER	10 bytes	Alphanumeric	O
206-208	SHIP-TO COUNTRY CODE	3 bytes	Numeric	O

M = Mandatory O = Optional

Optional subfields that are not populated must be character space filled to meet 33-, 78- or 205-byte length specified.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

AAV & Telephone Number Verification Subfield Descriptions

The following are detailed descriptions for the subfields that may be present in Data Field 63.

VLI, SI and RTI

The first 7 digits of the American Express Automated Address Verification (AAV) and Telephone Number Verification request are as follows:

0
1234567

LLLSSRR

- "LLL" is the three-digit, Variable Length Indicator (VLI), right justified and zero filled, if necessary.
- "SS" is the two-character, Service Identifier (SI).
- "RR" is the two-character, Request Type Identifier (RTI).

Cardmember Information Subfields

The following are detailed descriptions for the subfields that may be present in Data Field 63.

Cardmember Billing Postal Code

For non-U.S. addresses, the postal code may vary in length and contain alpha characters. Non-U.S. postal codes must be padded with character spaces to nine characters, left justified. Case-sensitive characters (those that have both upper and lower case options) must be upper case.

Merchant and Third Party Processor systems must be capable of submitting both numeric ZIP and alphanumeric non-U.S. postal codes in this subfield.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

If a Cardmember Billing Postal Code is not entered, this subfield must be character space filled.

```
0 1
890123456
```

NNNNNNNNN

"NNNNNNNNN" is the nine-character, Cardmember Billing Postal Code. For addresses in the U.S., this is a numeric 5+4 ZIP; or a five-digit ZIP, left justified and character space filled to nine characters.

Cardmember Billing Address

If a Cardmember Billing Address is not entered, this subfield must be character space filled.

```
1   2          3
78901234567890123456
```

AAAAAAAAAAAAAAAAAAAA

"AAAAAAAAAAAAAAAAAAAA" is the first 20 characters of the Cardmember Billing Address (including the unit, apartment, flat or suite number), left justified and character space filled, if necessary. Case-sensitive characters (those that have both upper and lower case options) must be upper case. Leading or trailing zeros and/or virgules (/) are not permitted as filler.

Note: For 33-byte format, Cardmember Billing Address is the last item in Data Field 63. See table on page 160.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Cardmember First and Last Name

Cardmember First Name and Last Name (as it appears on the Card) is left justified and character space filled, if necessary.

Case-sensitive characters (those that have both upper and lower case options) must be upper case. Leading or trailing zeros and/or virgules (/) are not permitted as filler. If a Cardmember First and Last Name are not entered, this subfield must be character space filled.

```
3  4          5          6          7          8
78901234567890123456789012345678901234567890123
FFFFFFFFFFFFFFLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
```

- "FFFFFFFFFFFFFFF" is the 15-character, Cardmember First Name
- "LLLLLLLLLLLLLLLLLLLLLLLLLLLLLL" is the 30-character, Cardmember Last Name

Note: For 78-byte format, Cardmember Last Name is the last item in Data Field 63. See table on page 160.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Cardmember Billing Phone Number — Use for Telephone Number Verification

USA, Canada and other countries that follow the NANP phone numbering system should send all 10 digits of the phone number, including the area code. For countries that do not follow this system, send the last 10 digits.

```
8         9
2345678901
```

PPPPPPPPPP

"PPPPPPPPPP" is the 10-digit, Cardmember Billing Phone Number. Leading or trailing zeros and/or virgules (/) are not permitted as filler. However, phone numbers less than 10 digits should be left justified and character space filled.

If a Cardmember Billing Phone Number is not entered, this subfield must be character space filled.

For example:

- United Kingdom (UK) phone number "44-1234-123456" would be entered as "1234123456".
- "Australia (AU) phone number "61292-11-1234" would be entered as "1292111234".
- "Portugal (PT) phone number "351-911-444-555" would be entered as "1911444555".

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Ship-to Subfields

The following are detailed descriptions for the Ship-to subfields that may be present in Data Field 63.

Ship-to Postal Code

For non-U.S. addresses, the postal code may vary in length and contain alpha characters. Non-U.S. postal codes must be padded with character spaces to nine characters left justified and character space filled to nine characters. Case-sensitive characters (those that have both upper and lower case options) must be upper case.

Merchant and Third Party Processor systems must be capable of submitting both numeric ZIP and alphanumeric non-US postal codes in this subfield.

If a Ship-to Postal Code is not entered, this subfield must be character space filled.

```
         1
9        0
234567890
```

ZZZZZZZZZ

"ZZZZZZZZZ" is the nine-character, Ship-to Postal Code. For addresses in the U.S., this is a numeric 5+4 ZIP; or a five-digit ZIP, left justified and character space filled to nine characters.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Ship-to Address

Case-sensitive characters (those that have both upper and lower case options) must be upper case. Leading or trailing zeros and/or virgules (/) are not permitted as filler.

If a Ship-to Address is not entered, this subfield must be character space filled.

```
1         1         1         1         1         1
0         1         2         3         4         5
12345678901234567890123456789012345678901234567890
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

"A...A" (50 characters) is the 50-character, Ship-to Address, left justified and character space filled, if necessary.

Ship-to First and Last Name

Ship-to First Name and Last Name, is left justified and character space filled, if necessary.

Case-sensitive characters (those that have both upper and lower case options) must be upper case. Leading or trailing zeros and/or virgules (/) are not permitted as filler. If a Ship-to First and Last Name are not entered, this subfield must be character space filled.

```
1         1         1         1         1
5         6         7         8         9
12345678901234567890123456789012345678901234567
SSSSSSSSSSSSSSSNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
```

- "SSSSSSSSSSSSSSS" is the first 15 characters of the Ship-to First Name
- "N...N" (30 characters) is the first 30 characters of the Ship-to Last Name

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Ship-to Phone Number

Leading or trailing zeros and/or virgules (/) are not permitted as filler. However, phone numbers less than 10 digits should be left justified and character space filled.

If a Ship-to Phone Number is not entered, this subfield must be character space filled.

USA, Canada and other countries that follow the NANP phone numbering system should send all 10 digits of the phone number, including the area code.

For countries that do not follow this system, send the last 10 digits.

```
1   2
9   0
6789012345
```

LLLLLLLLL

"LLLLLLLLL" is the 10-digit, Ship-to Phone Number.

For example:

- United Kingdom (UK) phone number "44-1234-123456" would be entered as "1234123456".
- "Australia (AU) phone number "61292-11-1234" would be entered as "1292111234".
- "Portugal (PT) phone number "351-911-444-555" would be entered as "1911444555".

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Ship-to Country Code

If a Ship-to Country Code is not entered, this subfield must be character space filled.

2
0
678

CCC

"CCC" is the three-digit, numeric, Ship-to Country Code. For more information on numeric country codes, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*.

Note: For 205-byte format, Ship-to Country Code is the last item in Data Field 63. See table on page 160.

Examples of Data Field 63 Formats

Unused and Optional subfields that are not populated must be character space filled to meet 33-, 78- or 205-byte format specified. Unit, apartment, flat and suite numbers are included in street addresses, in positions 17-36.

33-Byte Format (plus three-byte VLI) - AAV (RTI=AD) or Email Verification (RTI=AE)

```
0        1         2         3
12345678901234567890123456789012345678
033AXAD85054450018850~N~56~ST~#301~~
```

78-Byte Format (plus three-byte VLI) -AAV (RTI=AD) or Email Verification (RTI=AE)

```
          1         2         3         4         5         6
123456789012345678901234567890123456789012345678901234567890
078AXAD85054450018850~N~56~ST~#301~~JANE~~~~~~~~~~SMITH~~~~

6        7         8
12345678901234567890123
~~~~~~~~~~~~~~~~~~~~~~~
```

8.1 1100 Authorization Request (continued)

Data Field 63 PRIVATE USE DATA (continued)

205-Byte Format (plus three-byte VLI) - AAV (RTI=AD) or Email Verification (RTI=AE)

```
0         1         2         3         4         5         6
12345678901234567890123456789012345678901234567890123456789012345678901234567890
205AXAD85054450018850~N~56~ST~#301~~JANE~~~~~~~~~~SMITH~~~~

                                                  1         1         1
6         7         8         9         0         1         2
12345678901234567890123456789012345678901234567890123456789012345678901234567890
~~~~~~~~~~~~~~~~~~~~~~1234567890850221800 4102~N~289~PL~~~~~~~

1         1         1         1         1         1         1
2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ROBERT~~~~~~~~~JONES~~~~~~~~~~

1         1         2
8         9         0
123456789012345678901234 5678
~~~~~~~~~~~~~~~5555370000840
```

205-Byte Format (plus three-byte VLI) - Telephone Number and/or Email Verification (RTI=AE)

```
0         1         2         3         4         5         6
12345678901234567890123456789012345678901234567890123456789012345678901234567890
205AXAE85054450018850~N~56~ST~#301~~JANE~~~~~~~~~~SMITH~~~~

                                                  1         1         1
6         7         8         9         0         1         2
12345678901234567890123456789012345678901234567890123456789012345678901234567890
~~~~~~~~~~~~~~~~~~~~~~1234567890850221800 4102~N~289~PL~~~~~~~

1         1         1         1         1         1         1
2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ROBERT~~~~~~~~~JONES~~~~~~~~~~

1         1         2
8         9         0
123456789012345678901234 5678
~~~~~~~~~~~~~~~5555370000840
```

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

In the preceding examples:

- "033", "078" and "205" are the three-byte, Variable Length Indicators (VLI)[1].
- "AX" is the two-byte, Service Identifier (constant literal "AX" = American Express).
- "AD" is the two-byte, Request Type Identifier.
  "AD" = American Express AAV.

  "AE" = American Express Telephone Number Verification and/or Email Address Verification.
- "850544500" is the nine-byte, Cardmember Billing Postal Code.
- "18850~N~56~ST~#301~~" is the first 20 bytes of Cardmember Billing Address. Note that unit, apartment, flat or suite number must be included in street address, if applicable. See the following notes.
- "JANE~…~SMITH~…~" is the 15-byte, Cardmember First Name; and 30-character, Cardmember Last Name.
- "1234567890" is the 10-byte, Cardmember Billing Phone Number (used for Telephone Number Verification).
- "850221800" is the nine-byte, Ship-to Postal Code.
- "4102~N~289~PL~…~" is the 50-byte, Ship-to Address.
- "ROBERT~…~JONES~…~" is the 15-byte, Ship-to First Name; and 30-byte, Ship-to Last Name.
- "1234567890" is the 10-byte, Ship-to Phone Number.
- "840" is the three-digit, numeric, Ship-to Country Code. For more information on numeric country codes, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*

Notes:

1. Tilde (~) characters represent character spaces.
2. Refer to Street Codes in the *American Express Global Codes & Information Guide*.
3. See Data Field 63 Subfield Summary Table on page 163.

1 Not counting the Variable Length Indicator (VLI) that populates the first three positions in this data field.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

American Express Travelers Cheque Format

For American Express Travelers Cheque (TC) transactions, TC data may be machine read or manually entered.

The following are detailed descriptions for the subfields used to transmit TC information in Data Field 63.

TC Data — MICR Entry

For TC transactions in which the MICR (Magnetic Ink Character Recognition) data is machine read, this data field must contain the MICR data printed along the bottom edge of the TC.

```
0         1         2         3
12345678901234567890123456789 01
```

LLLSSRRNNNNNNNNNNNNNNNNNNNNNNN

- "LLL" is the three-digit, Variable Length Indicator (VLI), right justified and zero filled, if necessary.
- "SS" is the two-character, Service Identifier (SI).
- "RR" is the two-character, Request Type Identifier (RTI).
- "NNN..." is the 24-character, TC MICR line entry.

Example of TC MICR Line TC Data

```
0         1         2         3
12345678901234567890123456789 01
```

028AXTC123456789T12D12345678901

- "028" is the Variable Length Indicator (VLI).
- "AX" is the two-byte, Service Identifier (constant literal "AX" = American Express).
- "TC" is the two-byte, Request Type Identifier (constant literal "TC" = Travelers Cheque, MICR line data).
- "123..." is the 24-character, TC MICR line entry.

Note: Some symbols in the printed MICR line are data field separators, which are translated to alpha characters when machine read.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

TC Data — Manual Entry

For TC transactions in which the Travelers Cheque Number is manually entered, this data field must contain the TC Alpha Prefix and Serial Number from the upper, right-hand corner of Travelers Cheque.

Note: For manually entered TC Numbers only, the corresponding TC denomination must be forwarded in Data Field 62.

The TC Alpha Prefix (leading alpha characters) must be converted to numbers prior to populating this data field, because the TC Alpha Prefix and Serial Number must be transmitted as numerals. See the following Travelers Cheque Alpha Prefix Conversion Table:

Travelers Cheque Alpha Prefix Conversion Table

```
A = 1   J = 1
B = 2   K = 2    S = 2
C = 3   L = 3    T = 3
D = 4   M = 4    U = 4
E = 5   N = 5    V = 5
F = 6   O = 6    W = 6
G = 7   P = 7    X = 7
H = 8   Q = 8    Y = 8
I = 9   R = 9    Z = 9
```

Note: Bullet characters (used as separators) are not transmitted.

```
0         1
123456789012345678
```

LLLSSRRNNNNNNNNNNN

- "LLL" is the three-digit, Variable Length Indicator (VLI), right justified and zero filled, if necessary.
- "SS" is the two-character, Service Identifier (SI).
- "RR" is the two-character, Request Type Identifier (RTI).
- "NNNNNNNNNNN" is the 11-digit concatenation of the 2 digit numeric equivalent of the TC Alpha Prefix and the 9 digit, manually entered, Travelers Cheque Number.

8.1 1100 Authorization Request (continued)

Data Field 63	PRIVATE USE DATA (continued)

Example of Manually Entered TC Data

```
0         1
123456789012345678
```

015AXTS12123456789

- "015" is the Variable Length Indicator (VLI).
- "AX" is the two-byte, Service Identifier (constant literal "AX" = American Express).
- "TS" is the two-byte, Request Type Identifier (constant literal "TS" = Travelers Cheque, manually entered data).
- "12123456789" is the manually entered, TC Prefix (converted) and Travelers Cheque Number.

8.1 1100 Authorization Request (continued)

DATA FIELD 96	KEY MANAGEMENT DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 17 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 14 bytes maximum, EBCDIC & Binary
Field Type:	Unsigned binary number - Data items whose original formats are defined as binary are mapped directly as eight bits per byte, with the value of any binary byte of data varying from hexadecimal "00" to "FF".
Field Requirement:	• Mandatory — PIN, MAC or DATA encryption transactions using dynamic key exchange. • Not used — Other transactions
Description:	This data field contains information on cryptographic keys to support transactional encrypted data.

American Express Session Key Identifier Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alpha	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alpha	M	Secondary ID (Data Type Code) is constant literal "KCV" (Key Check Value).
9-11	SESSION PIN KEY CHECK VALUE	3 bytes	Binary	M	Check value is to be copied from the value found in the SESSION PIN KEY CHECK VALUE subfield in Data Field 96, Key Management Data, Network Management Response (1814) message.
12-14	SESSION MAC KEY CHECK VALUE	3 bytes	Binary	M	Binary-zero filled
15-17	SESSION DATA KEY CHECK VALUE	3 bytes	Binary	M	Binary-zero filled

8.1 1100 Authorization Request (continued)

Data Field 128	MESSAGE AUTHENTICATION CODE FIELD
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. This data field is used for the data value that protects both a message's integrity, as well as its authenticity, by allowing verifiers the ability to detect any changes to the message content. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

8.2 1110 Authorization Response

Length of Record: 801 bytes maximum

Description: This message is used by American Express to transmit an Authorization and/or Automated Address Verification (AAV) Response (1110) message to a Merchant.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
—	MESSAGE TYPE IDENTIFIER	4 bytes, fixed	Numeric	Mandatory	181
—	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary	Mandatory	181
2	PRIMARY ACCOUNT NUMBER (PAN)	21 bytes, LLVAR	Numeric	Mandatory - Echo returned	182
3	PROCESSING CODE	6 bytes, fixed	Numeric	Mandatory - Echo returned	182
4	AMOUNT, TRANSACTION	12 bytes, fixed	Numeric	See page ➔	183
7	DATE AND TIME, TRANSMISSION	10 bytes, fixed	Numeric	Conditional - Echo returned	184
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters	Mandatory - Echo returned	184
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric	Mandatory - Echo returned	185
15	DATE, SETTLEMENT	6 bytes, fixed	Numeric	See page ➔	186
30	AMOUNTS, ORIGINAL	24 bytes, fixed	Numeric	See page ➔	187
31	ACQUIRER REFERENCE DATA	50 bytes, LLVAR	Alphanumeric & special characters	Mandatory	188
32	ACQUIRING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Conditional - Echo returned	189
34	PRIMARY ACCOUNT NUMBER, EXTENDED	30 bytes, maximum	Alphanumeric	See page ➔	190
37	RETRIEVAL REFERENCE NUMBER	12 bytes, fixed	Alphanumeric & special characters	Conditional - Echo returned	192
38	APPROVAL CODE	6 bytes, fixed	Alphanumeric	See page ➔	193

8.2 1110 Authorization Response (continued)

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
39	ACTION CODE	3 bytes, fixed	Numeric	Mandatory	194
41	CARD ACCEPTOR TERMINAL IDENTIFICATION	8 bytes, fixed	Alphanumeric & special characters	See page ➔	196
42	CARD ACCEPTOR IDENTIFICATION CODE	15 bytes, fixed	Alphanumeric & special characters	Mandatory - Echo returned	196
44	ADDITIONAL RESPONSE DATA	27 bytes, LLVAR	Alphanumeric & special characters	See page ➔	197
49	CURRENCY CODE, TRANSACTION	3 bytes, fixed	Numeric	Mandatory - Echo returned	203
54	AMOUNTS, ADDITIONAL	123 bytes, LLVAR	Alphanumeric & special characters	See page ➔	203
55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA	259 bytes, LLLVAR	Alphanumeric, special characters & binary	See page ➔	205
60	NATIONAL USE DATA	106 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	208
61	NATIONAL USE DATA	103 bytes, LLLVAR	Alphanumeric	See page ➔	209
62	PRIVATE USE DATA	63 bytes, LLLVAR	Alphanumeric, special characters & binary	See page ➔	211
63	PRIVATE USE DATA	103 bytes, LLLVAR	Alphanumeric & special characters	See page ➔	217
64	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary	N/A	217

8.2 1110 Authorization Response (continued)

Data Field — None	MESSAGE TYPE IDENTIFIER
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	`1110`
Field Requirement:	Mandatory
Description:	The constant literal "`1110`" signifies the ISO 8583 Authorization Response message.

Data Field — None	BIT MAP - PRIMARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory
Description:	See Bit Map - Primary description on page 62 of the Authorization Request (1100) message.

8.2 1110 Authorization Response (continued)

Data Field 2	PRIMARY ACCOUNT NUMBER (PAN)
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 21 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 19 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Authorization Request (1100) message, and is echo returned without alteration in the Authorization Response (1110) message.

Data Field 3	PROCESSING CODE
Length of Field:	6 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Authorization Request (1100) message, and is echo returned without alteration in the Authorization Response (1110) message.

8.2 1110 Authorization Response (continued)

Data Field 4	AMOUNT, TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, right justified, zero filled
Constant:	None
Field Requirement:	• Mandatory — Echo returned for Non-Prepaid Card Authorization Requests • Conditional — Prepaid Card Partial Authorization Requests
Description:	This data field is mandatory in the Authorization Request (1100) message, and is generally echo returned without alteration in the Authorization Response (1110) message. **Partial Authorization - Prepaid Cards Only** If Function Code (Data Field 24) is "`181`" (Partial Authorization) in the Authorization Request (1100) message, and Action Code (Data Field 39) is "`002`" in this Authorization Response (1110) message, then this Amount, Transaction data field contains the approved, authorized amount, which will be less than the Amount, Transaction entry transmitted in the originating Authorization Request (1100) message. **Note**: Merchant certification is required to receive partial authorization responses.

8.2 1110 Authorization Response (continued)

Data Field 7	DATE AND TIME, TRANSMISSION
Length of Field:	10 bytes, fixed length
Field Type:	Numeric, `MMDDhhmmss`
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

Data Field 11	SYSTEMS TRACE AUDIT NUMBER
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric (upper case) & special characters
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Authorization Request (1100) message, and is echo returned without alteration in the Authorization Response (1110) message.

8.2 1110 Authorization Response (continued)

Data Field 12	DATE AND TIME, LOCAL TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, YYMMDDhhmmss
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Authorization Request (1100) message, and is echo returned without alteration in the Authorization Response (1110) message.

8.2 1110 Authorization Response (continued)

Data Field 15	DATE, SETTLEMENT
Length of Field:	6 bytes, fixed length
Field Type:	Numeric, YYMMDD
Constant:	None
Field Requirement:	• Mandatory — MasterCard transactions • Not used — Other transactions
Description:	This data field is used for MasterCard processing only. This data field contains the BankNet Settlement Date of the card, as returned by MasterCard. The format is: YYMMDD YY = Year (last two digits only) - Optional MM = Month (two digits) DD = Day (two digits)

8.2 1110 Authorization Response (continued)

Data Field 30	AMOUNTS, ORIGINAL
Length of Field:	24 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	• Conditional — Some American Express Prepaid Card transactions • Not used — All others
Description:	This data field contains the original amount requested when a partial amount is approved. Merchants must be certified for Partial Authorization for the original amount to be returned in this data field. See additional information on partial authorizations in Authorization Request (1100) message, Data Field 24, Function Code, on page 86. Positions 1-12 of this data field are the original transaction amount from Data Field 4, Amount, Transaction, in the originating Authorization Request (1100) message. Positions 13-24 are zero filled and reserved for future use.

8.2 1110 Authorization Response (continued)

Data Field 31	ACQUIRER REFERENCE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 50 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 48 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Mandatory **Note**: This data field is mandatory and created by the American Express Global Network, and always appears in response messages returned to Merchants and/or Third Party Processors.

Description:	This data field contains the 15-digit, numeric, Transaction Identifier (TID), a unique, American Express-assigned tracking number. The TID is used to identify and track a Cardmember transaction throughout its life cycle.
	The value in this data field must be retained by the Merchant's system and returned to American Express in the Transaction Advice Basic (TAB), Transaction Advice Detail (TAD) and Transaction Advice Addendum (TAA) financial submission records that correspond to this authorization response. For more information, refer to the *American Express Global Financial Submission Guide*.
	See the following example of a typical TID entry:
	`0 1`
	`12345678901234567`
	`15123456789012345`
	• "`15`" is the two-byte, Variable Length Indicator (VLI).
	• "`123456789012345`" is the 15-byte, numeric TID.

8.2 1110 Authorization Response (continued)

Data Field 32	ACQUIRING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

8.2 1110 Authorization Response (continued)

Data Field 34	PRIMARY ACCOUNT NUMBER, EXTENDED
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 30 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 28 bytes maximum, EBCDIC
Field Type:	Alphanumeric
Constant:	None
Field Requirement:	• Mandatory — Expresspay Translation (PAN request) transactions • Mandatory — Expresspay Translation (PAN & Expiration Date request) transactions • Conditional — Payment Token transactions • Not used — Other transactions
Description:	For Expresspay Translation (PAN request or PAN and Expiration Date request), in order to receive a response in this data field, Function Code 194 Expresspay Translation (PAN request) or Function Code 196, Expresspay Translation (PAN and Expiration Date request), must be populated in Data Field 24, Function Code in the request message. **Payment Token transactions** This field contains the last four digits of the PAN when Subfield 6 in Data Field 60, National Use Data, is populated in the Authorization Request (1100) message. Merchant's system(s) should be prepared to accept and process the responses detailed on the following page. When the Primary Account Number (PAN) is provided, this data field contains the disposition for the PAN. The first two digits are the Variable Length Indicator (VLI) followed by one digit alpha PAN request result followed by the PAN if valid.

8.2 1110 Authorization Response (continued)

Data Field 34	PRIMARY ACCOUNT NUMBER, EXTENDED (continued)

Description:	Valid PAN response codes:
	Y = PAN returned
	N = PAN not found/does not exist
	R = Reattempt PAN request
	F = Last four digits of the Primary Account Number
	E = PAN and Expiration Date returned
	Examples of PAN Responses:
	PAN Returned
	`LLY123456789012345`
	LL = Two-digit, Variable Length Indicator (VLI), right justified, and zero filled
	Y= One-character, PAN response code
	`123456789012345` = PAN
	Payment Token transactions
	`LLF1234`
	LL = Two-digit, Variable Length Indicator (VLI), right justified, and zero filled
	F = One-character, PAN response code
	`1234` = PAN
	Last 4 digits of the Primary Account Number
	`05F1234`
	PAN and Expiration Date Returned:
	`LLE1601123456789012345`
	LL = Two-digit, Variable Length Indicator (VLI), right justified, and zero filled
	E= One-character, PAN response code
	where "**1601**" = Expiration Date (YYMM)
	and "**123456789012345**" = PAN
	20E1601123456789012345

8.2 1110 Authorization Response (continued)

Data Field 34	PRIMARY ACCOUNT NUMBER, EXTENDED (continued)
Description:	**PAN Not Found/Does not exist** O1N **Reattempt PAN Request** O1R

Data Field 37	RETRIEVAL REFERENCE NUMBER
Length of Field:	12 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

8.2 1110 Authorization Response (continued)

Data Field 38	APPROVAL CODE
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric, left justified, character space filled
Constant:	None
Field Requirement:	• Mandatory — "Approved" transactions • Optional — "Please Call Issuer" - American Express • Not used — Other transactions
Description:	If Action Code (Data Field 39) is an approval, this data field contains an "authorization code" that corresponds to the Authorization Request (1100) message or Automated Address Verification (AAV) request in the originating request message. Formats include: **NNNNNN** = Authorization code for all U.S., Canadian and some regional American Express Merchants. **Note**: All U.S. and Canadian Merchants must comply with the American Express Six-Digit Approval Code policy. **NN~~~~** = Authorization code for American Express Travelers Cheques. **NN~~~~** = Authorization code for some regional American Express Merchants, only. **NNNNNN** = Authorization code for MasterCard, VISA and American Express-supported Cards. **NN~~~~** = Authorization code for Diners Club. If Action Code is "`107` - Please Call Issuer", this data field may optionally contain a four-digit, American Express (AMEX) Referral Queue Number. **NNNN~~** = AMEX Referral Queue Number (American Express option only - Not provided for all American Express products (e.g., Gift Cards). See Notes on the next page.

8.2 1110 Authorization Response (continued)

Data Field 38	APPROVAL CODE (continued)
Description (continued):	**Notes**: 1. All Approval Codes are numeric for American Express transactions, except for Address Verification Only transactions, when the Approval Code data field is blank. 2. For more information on the AMEX Referral Queue Number, see page 20. 3. In the examples above, "N" is an alphanumeric character, and the tilde (~) represents a character space.

Data Field 39	ACTION CODE
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the Action Code, indicating the American Express disposition for this transaction. See valid Action Codes on the next page.

8.2 1110 Authorization Response (continued)

Data Field 39	ACTION CODE (continued)
Description (continued):	Valid Action Codes:

`000` Approved
`001` Approve with ID
`002` Partial Approval (Prepaid Cards only)
`100` Deny
`101` Expired Card / Invalid Expiration Date
`106` Exceeded PIN attempts
`107` Please Call Issuer
`109` Invalid merchant
`110` Invalid amount
`111` Invalid account / Invalid MICR (Travelers Cheque)
`115` Requested function not supported
`117` Invalid PIN
`119` Cardmember not enrolled / not permitted
`122` Invalid card security code (a.k.a., CID, 4DBC, 4CSC)
`125` Invalid effective date
`181` Format error
`183` Invalid currency code
`187` Deny - New card issued
`189` Deny - Canceled or Closed Merchant/SE
`200` Deny - Pick up card
`900` Accepted - ATC Synchronization
`909` System Malfunction (Cryptographic error)
`912` Issuer not available

Notes:

1. The following requirement must be met prior to sending a keyed CID/4DBC/4CSC value that will be actioned by American Express. The system is prepared to accept all possible Action Codes found in Data Field 39 and all possible Response Indicators found in byte 2 of Data Field 44, and in any combination.
2. While Action Code "`115`" (Requested function not supported) means the Issuer does not support the requested function, it can also mean "Service not permitted" (i.e., the Merchant or Third Party Processor has requested an authorization feature or function for which it is not certified).
3. Action Code "`122`" indicates keyed four-digit CID/4DBC/ 4CSC failed validation. For CID/4DBC/ 4CSC location on Cards, see page 46.

8.2 1110 Authorization Response (continued)

Data Field 41	CARD ACCEPTOR TERMINAL IDENTIFICATION
Length of Field:	8 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Mandatory — Echo returned for VISA PS2000 • Conditional — Echo returned for American Express transactions in the USA and Canada, and non-VISA transactions
Description:	This data field may or may not be required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message without alteration.

Data Field 42	CARD ACCEPTOR IDENTIFICATION CODE
Length of Field:	15 bytes, fixed length
Field Type:	Alphanumeric & special characters, left justified, character space filled
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Authorization Request (1100) message, and is echo returned without alteration in the Authorization Response (1110) message.

8.2 1110 Authorization Response (continued)

Data Field 44	ADDITIONAL RESPONSE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 27 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 25 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Conditional — American Express Automated Address Verification (AAV) Validation • Conditional — Keyed CID/4DBC/4CSC Validation • Optional — American Express Dial Transfer • Not used — Other transactions
Description:	This data field contains additional response data for certain Authorization Request (1100) messages; and it is mandatory if American Express Automated Address Verification (AAV) and/or Keyed CID/4DBC/4CSC validation is requested in Data Field 63 and/or 53 (respectively) of the Authorization Request (1100) message. However, this data field may not be returned when certain error Action Codes (Data Field 39) are returned in the Authorization Response (1110) message (e.g., a "181" Format Error). Merchants that submit 33-, 78- or 205-byte format, Automated Address Verification (AAV) Requests in Authorization Request (1100) messages may receive the AAV responses described for this data field and in the table on the next page. Therefore, the Merchant's system(s) should be prepared to accept and process all of the responses detailed on the following pages. For more information on Automated Address Verification formats, see page 157.

8.2 1110 Authorization Response (continued)

Data Field 44 ADDITIONAL RESPONSE DATA (continued)

33-Byte Format	78-Byte Format	205-Byte Format	Code	Description
X	X	X	Y	Yes, CM Address and Postal Code are both correct.
X	X	X	N	No, CM Address and Postal Code are both incorrect.
X	X	X	A	CM Address only correct.
X	X	X	Z	CM Postal Code only correct.
X	X	X	U	Information unavailable.
X	X	X	S	SE not allowed AAV function.
X	X	X	R	System unavailable; retry.
	X	X	L	CM Name and Postal Code match.
	X	X	M	CM Name, Address and Postal Code match.
	X	X	O	CM Name and Address match.
	X	X	K	CM Name matches.
	X	X	D	CM Name incorrect, Postal Code matches.
	X	X	E	CM Name incorrect, Address and Postal Code match.
	X	X	F	CM Name incorrect, Address matches.
	X	X	W	No, CM Name, Address and Postal Code are all incorrect.

X = Possible response for indicated format.

8.2 1110 Authorization Response (continued)

Data Field 44	ADDITIONAL RESPONSE DATA (continued)

Variable Length Indicator (VLI)

The first two digits in this data field are the Variable Length Indicator (VLI). Besides indicating variable data length, the VLI is a key to the contents of this data field.

`01` = Variable data in the form of a one-byte response is used for American Express AAV. Example: "`01Y`".

`02` = Variable data in the form of a two-byte response, where the first byte (relative position 3) contains Address Verification results; and the second byte (relative position 4) contains Keyed CID/4DBC/4CSC Validation results. Example: **"`02NY`"**.

`15` = Variable data as a 15-byte data field is reserved for American Express Dial Transfer, Relay Phone Number data. This rarely used option transports a phone number dial-string to a terminal, to facilitate autodialing to an American Express U.S. Authorizations Center (so that the Merchant can speak to an Authorizer). For more information on this option, contact your American Express representative.

Note: See subfield layouts and examples that follow.

VLI = "01" Format

For AAV responses, the format for this data field is:

`123`

`LLX`

`LL` = Two-digit, Variable Length Indicator (VLI), right justified and zero filled.

`X` = One-character, Address Verification response code for American Express AAV requests.

8.2 1110 Authorization Response (continued)

Data Field 44	ADDITIONAL RESPONSE DATA (continued)

VLI = "01" Format (continued)

Valid Address Verification response codes include the following:

Y = Yes, CM Address and Postal Code are both correct.

N = No, CM Address and Postal Code are both incorrect.

A = CM Address only correct.

Z = CM Postal Code only correct.

U = Information unavailable.

S = SE not allowed AAV function.

R = System unavailable; retry.

L = CM Name and Postal Code match.

M = CM Name, Address and Postal Code match.

O = CM Name and Address match.

K = CM Name matches.

D = CM Name incorrect, Postal Code matches.

E = CM Name incorrect, Address and Postal Code match.

F = CM Name incorrect, Address matches.

W = No, CM Name, Address and Postal Code are all incorrect.

Example of VLI = "01"

The following is a typical example of an AAV, one-byte response:

123

01Y

01 = Two-digit, Variable Length Indicator (VLI).

Y = One-character, Address Verification response code.

8.2 1110 Authorization Response (continued)

Data Field 44	ADDITIONAL RESPONSE DATA (continued)

VLI = "02" Format

For AAV and/or Keyed CID/4DBC/4CSC Validation responses, the format for this data field is:

1234

LLXB

LL = Two-digit, Variable Length Indicator (VLI), right justified and zero filled.

X = One-character, Address Verification response code for American Express AAV requests. See valid codes on previous page.

Note: A character space in relative position 3, in lieu of an Address Verification response code, indicates that Data Field 63 (containing AAV data) was not present in the originating Authorization Request (1100) message.

B = One-character, CID/4DBC/4CSC response code for American Express Keyed CID/4DBC/4CSC Validation requests.

Valid CID/4DBC/4CSC response codes include the following:

Y = CID/4DBC/4CSC matched

N = CID/4DBC/4CSC did not match

U = CID/4DBC/4CSC was not checked

Example #1 of VLI = "02"

The following is a typical example of an AAV with Keyed CID/4DBC/4CSC Validation, two-byte response to an Authorization Request (1100) message that contained both Data Field 53 (CID/4DBC/ 4CSC from the face of the Card) and Data Field 63 (address verification information):

1234

02YN

02 = Two-digit, Variable Length Indicator (VLI).

Y = One-character, AAV response code.

N = One-character, Keyed CID/4DBC/4CSC Validation response code.

8.2 1110 Authorization Response (continued)

Data Field 44	ADDITIONAL RESPONSE DATA (continued)

Example #2 of VLI = "02"

The following is a typical example of a Keyed CID/4DBC/4CSC Validation, two-byte response to an Authorization Request (1100) message that contained Data Field 53 (CID/4DBC/4CSC from the face of the Card) and not Data Field 63 (address verification information):

1234

02~N

02 = Two-digit, Variable Length Indicator (VLI).

~ = Character space.

N = One-character, Keyed CID/4DBC/4CSC Validation response code.

Example of VLI = "15"

The following is a typical example of an American Express Dial Transfer, Relay Phone Number, 15 byte response:

0 1

12345678901234567

15441101234567890

15 = Two-byte, Variable Length Indicator (VLI).

441101234567890 = 15-byte, telephone number.

8.2 1110 Authorization Response (continued)

Data Field 49	CURRENCY CODE, TRANSACTION
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Authorization Request (1100) message, and is echo returned without alteration in the Authorization Response (1110) message. For more information on numeric currency codes and decimal point positions, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*.

Data Field 54	AMOUNTS, ADDITIONAL
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 123 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 120 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Optional — American Express Prepaid Cards • Not used — All others
Description:	This data field contains the available amount remaining on certain American Express Prepaid Card products. The amount is present in the response message, when Data Field 24, Function Code in the originating request message, contains codes "181" or "182". Merchants may wish to display this value on the POS terminal or print it on the customer receipt. For more information, see page 86. **Note**: Balances may not be returned for some Prepaid Cards.

8.2 1110 Authorization Response (continued)

Data Field 54	AMOUNTS, ADDITIONAL (continued)

Description (continued):

This data field is composed of a three-byte Variable Length Indicator (VLI) and 20 bytes of coded data that specifies the Account Type, Amount Type, Currency Code, Credit status and the Prepaid Card remaining balance. The format is:

```
          1         2
12345678901234567890123
```

VVVAABBCCCD123456789012

	Length	Pos.	Description
VVV	3 bytes	1-3	VLI / Variable Length Indicator (always "020")
AA	2 bytes	4-5	Account Type Code (always "00")
BB	2 bytes	6-7	Amount Type Code (always "05")
CCC	3 bytes	8-10	Numeric Currency Code (e.g., U.S. Dollars = "840"). For more information on numeric currency codes and decimal point positions, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*.
D	1 byte	11	Credit Code ("C" = Credit)
123...	12 bytes	12-23	12-digit, Prepaid Card balance, right justified, zero filled, with corresponding decimal implied (e.g., 840 / U.S. Dollars = two decimal places).

For example, a credit (remaining balance) of $10.00 in U.S. Dollars (840) would appear as:

```
          1         2
12345678901234567890123
```

0200005840C000000001000

8.2 1110 Authorization Response (continued)

Data Field 55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 259 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 256 bytes maximum, EBCDIC, BCD or binary
Field Type:	Alphanumeric & special characters, and binary coded decimal (BCD) or unsigned binary numbers **Note**: Data Field 55 contains some subfields that are forwarded for transmission to an integrated circuit card or terminal, and are specified as binary. This data is in binary format in 8 bit blocks, right justified and zero filled, per the following: 1. Data originally transmitted as numeric is formatted as binary coded decimal (BCD) with two digits per byte ("00" to "99"). Numeric subfields with an odd number of digits are padded with leading zeros. 2. Data originally transmitted as binary is mapped directly as eight bits per byte, with the value for any binary byte of data varying from hexadecimal "00" to "FF". For more information, see page 138.
Constant:	None
Field Requirement:	• Mandatory — ICC (EMV*) transactions (special certification required) • Not used — Other transactions

*EMV is the abbreviation for Europay/MasterCard/VISA, joint sponsors of the global standard for electronic financial transactions using "chip card" technology

8.2 1110 Authorization Response (continued)

Data Field 55	INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA (continued)
Certification Requirement:	Global - All regions Mandatory — Third Party Processors and/or Vendors must be certified to pass Card Present transactions for Integrated Circuit Cards (ICCs) in this data field. After certification, all card Issuer-provided ICC related data must be forwarded in this data field.
Description:	This data field contains Integrated Circuit Card (ICC) Related Data that is forwarded for transmission to the integrated circuit on a chip card. If ICC data was read from the Card and included in the originating request message, some subfields are echo returned in this response. Before Merchants may use this data field, special certification is required to process ICC transactions. For more information on ICC support, reference the *American Express AEIPS Chip Card Specification* and *American Express AEIPS Terminal Specification*, in addition to contacting your American Express representative. **Note**: For Merchants who have not completed this certification, no data will be transmitted in this data field from American Express. See subfield details on the next page:

8.2 1110 Authorization Response (continued)

Data Field 55 INTEGRATED CIRCUIT CARD SYSTEM RELATED DATA (continued)

EMV Tags	Relative Position	Subfield Name	Subfield Length	Subfield Type	Required	Description
	1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	Yes	VLI indicates total length of variable data in this data field (not including VLI).
	4-7	ICC HEADER VERSION NAME	4 bytes	Alphanumeric (EBCDIC)	Mandatory echo	Version header of the bit contents. Must be echoed without alteration from Network to Issuer Request, even if Bit 55 data (Issuer Authentication Data/ Issuer Script Data) is not present in the response. Required value: "AGNS"
	8-9	ICC HEADER VERSION NUMBER	2 bytes	Binary coded decimal (BCD)	Mandatory echo	Version number of the bit contents. Must be echoed without alteration from Network to Issuer Request, even if Bit 55 data (Issuer Authentication Data/ Issuer Script Data) is not present in the response. Required value: "0001"
91	10-26	ISSUER AUTHENTICATION DATA	17 bytes, max (LLVAR)	Unsigned binary number	Conditional	One byte, unsigned-binary-number VLI indicates subfield length, and precedes up to 16 bytes of variable data. For example, the VLI for 16 bytes of variable data is = "10" (one byte) in hex. See explanation of unsigned binary number format on page 138. **Note**: This subfield contains proprietary, Issuer-defined authentication data transmitted from Issuer to card. For details, refer to the *AEIPS Chip Card Specification*.
	27-155	ISSUER SCRIPT DATA	129 bytes, max (LLLVAR)	Unsigned binary number	Conditional	This subfield may be used only if Subfield 3, Issuer Authentication Data, is present. This subfield contains Issuer Script Template(s) and Command(s) to be communicated in the ICC Chip. The subfield length is the first byte, binary hexadecimal.
	156-259	RESERVED FOR FUTURE USE	104 bytes, max (LLVAR)	N/A	No	This subfield is reserved for future use and is completely omitted (including LLVAR).

8.2 1110 Authorization Response (continued)

Data Field 60	NATIONAL USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	13 bytes minimum, 106 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 103 bytes maximum, EBCDIC or Binary
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is mandatory for Payment Service Providers (Aggregators), OptBlue Participants and Payment Token transactions and not used for all other transactions in the Authorization Request (1100) message. This message is echo returned without alteration in the Authorization Response (1110) message (if previously submitted).

8.2 1110 Authorization Response (continued)

Data Field 61	NATIONAL USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 103 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 100 bytes maximum, EBCDIC & Binary
Field Type:	Alphanumeric
Constant:	None
Field Requirement:	• Mandatory — American Express SafeKey transactions (special certification required) • Not used — Other transactions
Certification Requirement:	See Section 6.4 for the website link to American Express SafeKey enabled countries. Mandatory — Third Party Processors and/or Vendors must be certified to pass American Express SafeKey authentication data in this data field. After certification, all Merchant-provided American Express SafeKey authentication related data must be forwarded in this data field.
Description:	American Express SafeKey is an industry-standard Authentication method that provides greater security, by authenticating the Cardmember during an online purchase and protecting payment card information as it is transmitted via the Internet. Before Merchants may use this data field, special certification is required to process American Express SafeKey transactions. For more information, reference the *American Express SafeKey℠ Acquirer - Merchant Implementation Guide*, in addition to contacting your American Express representative. **Note**: For Merchants who have not completed this certification, no data will be transmitted in this data field from American Express. See table containing subfield details on the next page.

8.2 1110 Authorization Response (continued)

Data Field 61 NATIONAL USE DATA (continued)

American Express SafeKey Format Table:

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alpha	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alpha	M	Secondary ID (Data Type Code) is constant liter "ASK" (American Express SafeKey)
9	AMERICAN EXPRESS VERIFICATION VALUE (AEVV) VALIDATION RESULT	1 byte	Alphanumeric	M	Valid values include: 0 = Reserved for future use 1 = AEVV Failed - Authentication, Issuer Key 2 = AEVV Passed - Authentication, Issuer Key 3 = AEVV Passed - Attempt, Issuer Key 4 = AEVV Failed - Attempt, Issuer Key 5 = Reserved for future use 6 = Reserved for future use 7 = AEVV Failed - Attempt, Issuer not participating, Network Key 8 = AEVV Passed - Attempt, Issuer not participating, Network Key 9 = AEVV Failed - Attempt, Participating, Access Control Server (ACS) not available, Network Key A = AEVV Passed - Attempt, Participating, Access Control Server (ACS) not available, Network Key B = Reserved for future use C = Reserved for future use D = Reserved for future use U = AEVV Unchecked

8.2 1110 Authorization Response (continued)

Data Field 62	PRIVATE USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 63 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 60 bytes maximum, coding determined by data field use
Field Type:	Alphanumeric & special characters, and binary coded decimal (BCD) or unsigned binary numbers
Constant:	None
Field Requirement:	• Mandatory — American Express transactions, Telephone Number and Email Verification • Mandatory — VISA PS2000 transactions, PS2000 requested • Not used — Other transactions
Certification Requirement:	Global - All regions Mandatory — All Third Party Processors and/or Vendors must certify to this data field. Merchants that submit Telephone Number and/or Email Address data in Data Field 63 and/or 47, respectively, in the Authorization Request (1100) message, must also certify to this data field. Therefore, the Merchant's system(s) should be prepared to accept and process all of the responses detailed on the following pages. For more information on Automated Address Verification (AAV), Telephone Number Verification and/or Email Address Verification formats, see pages 159, 161 and/or 162, respectively.
Description:	This data field is used for American Express Telephone Number Verification and/or Email Address Verification and VISA transaction responses. However, this data field may not be returned when certain error Action Codes in Data Field 39 are returned in the Authorization Response (1110) message (e.g., a "181" Format Error). American Express strongly recommends that Merchant/processor systems be capable of supporting the full 60-byte (variable data) maximum length specified for this data field for future expansion.

8.2 1110 Authorization Response (continued)

Data Field 62	PRIVATE USE DATA (continued)

Telephone Number and/or Email Address Verification Transactions:

This data field contains response codes that indicate if Cardmember information forwarded in an Address Verification Only (Processing Code "`174800`") or a Combination Address Verification and Authorization (Processing Code "`004800`") Authorization Request (1100) message is valid. In addition to Automated Address Verification (AAV) responses, this data field also provides Cardmember Telephone Number and Email Address verification.

Combination Address Verification & Authorization - Processing Code "004800"

The Cardmember Postal Code, Street Address, Name, Telephone Number and Email Address response codes returned in this data field, correspond to data transmitted by the Merchant for Combination Address Verification and Authorization (Processing Code "`004800`") in the Authorization Request (1100) message, Data Fields 63 and 47. For more information, see pages referenced in the table on the next page.

This response is composed of a series of response codes, preceded by a three-digit, Variable Length Indicator (VLI). Currently, the typical variable data portion of the response is only five characters.

Each character in the five-byte variable data response indicates the status for specific Cardmember (CM) data submitted in the Authorization Request (1100) message. For more information on the original data sent, see pages indicated in the table on the next page.

8.2 1110 Authorization Response (continued)

Data Field 62 **PRIVATE USE DATA (continued)**

American Express AAV, Telephone Number and Email Address Verification Response Message Subfields

Pos.	Subfield Name	Length	Comments (Message / Data Field Reference)	Page
1-3	VLI	3 bytes	3-digit Variable Length Indicator	—
4-5	SERVICE IDENTIFIER	2 bytes	Constant literal "AX" = American Express	—
6-7	REQUEST TYPE IDENTIFIER	2 bytes	Constant literal "AE" = Telephone Number and Email Address Verification Response	—
8	CARDMEMBER POSTAL CODE	1 byte	Authorization Request (1100) message / Data Field 63 — 33-, 78- and 205-byte format	164
9	CARDMEMBER STREET ADDRESS	1 byte	Authorization Request (1100) message / Data Field 63 — 33-, 78- and 205-byte format	165
10	CARDMEMBER FIRST AND LAST NAME	1 byte	Authorization Request (1100) message / Data Field 63 — 78- and 205-byte format	166
11	CARDMEMBER PHONE NUMBER	1 byte	Authorization Request (1100) message / Data Field 63 — 205-byte format	167
12	CUSTOMER EMAIL ADDRESS	1 byte	Authorization Request (1100) message / Data Field 47 — ITD and IAC	117

Valid response codes for subfield positions 8-12 include:

Y = Yes, data matches

N = No, data does not match

~ = Data not sent. **Note**: Tilde (~) represents character space.

U = Data unchecked

R = Retry

S = Service not allowed

8.2 1110 Authorization Response (continued)

Data Field 62	PRIVATE USE DATA (continued)

Layout for American Express AAV, Telephone Number and Email Address Verification Response

```
0         1
123456789012
```

LLLSSRRABCDE

- "LLL" is the three-digit, Variable Length Indicator (VLI), right justified and zero filled, if necessary.
- "SS" is the two-character, Service Identifier (SI).
- "RR" is the two-character, Request Type Identifier (RTI).
- "ABCDE" are the five response codes, where:
  - A = Response code for Cardmember Postal Code.
  - B = Response code for Cardmember Street Address.
  - C = Response code for Cardmember First and Last Name.
  - D = Response code for Cardmember Phone Number.
  - E = Response code for Customer Email Address.

Note: American Express strongly recommends that Merchant/processor systems be capable of supporting the full 60-byte (variable data) maximum length specified for this data field, for future expansion.

8.2 1110 Authorization Response (continued)

Data Field 62	PRIVATE USE DATA (continued)

Sample Data for American Express AAV, Telephone Number and Email Address Verification Response

```
          1
1234567890123
```

009AXAEYYNYY

- "009" is the Variable Length Indicator (VLI).
- "AX" is the Service Identifier (constant literal "AX" = American Express).
- "AE" is the Request Type Identifier (constant literal "AE" = American Express Telephone Number and Email Address Verification).
- "YYNYY" are the five response codes, where:
  - Y = Yes, Customer Postal Code matches Cardmember information on file with the Issuer.
  - Y = Yes, Customer Street Address matches Cardmember information on file with the Issuer.
  - N = No, Customer First and Last Name does not match Cardmember information on file with the Issuer.
  - Y = Yes, Customer Phone Number matches Cardmember information on file with the Issuer.
  - Y = Yes, Customer Email Address data matches Cardmember information on file with the Issuer.

8.2 1110 Authorization Response (continued)

Data Field 62	PRIVATE USE DATA (continued)

VISA PS2000 Transactions

When used for VISA processing, this data field contains the authorization response to the VISA card transaction data transmitted in the corresponding data field in the originating Authorization Request (1100) message.

If a VISA transaction is approved but it does *not* meet the VISA qualified rate requirements, this data field contains the Variable Length Indicator (VLI) "`001`" followed by the one-byte, payment service indicator "`N`".

Example: **`001N`**

If a VISA transaction is approved and it does meet the VISA qualified rate requirements, this data field contains the following response:

```
0         1         2         3         4
12345678901234567890123456789012345678900
```

`020Annnnnnnnnnnnnnnvvvv`

In the example above, "`020`" is the three-digit, Variable Length Indicator (VLI); "`A`" is the one-byte, payment service indicator; "`n...n`" is the 15-digit transaction identifier; and **`"vvvv"`** is the four-digit, alphanumeric validation code.

If a VISA transaction is denied, this data field is omitted in the Authorization Response (1110) message.

8.2 1110 Authorization Response (continued)

Data Field 63	PRIVATE USE DATA
Length of Field Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 103 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 100 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Mandatory — MasterCard transactions • Not used — Other transactions
Description	This data field contains the BankNet Reference Number (assigned by MasterCard) for a MasterCard transaction. This is a nine-digit alphanumeric number (preceded by a three-digit VLI/Variable Length Indicator) that must be passed to the submission record.

Data Field 64	MESSAGE AUTHENTICATION CODE FIELD
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	• Not used — All transactions
Description	This data field is unused and reserved for future use. This data field is used for the data value that protects both a message's integrity, as well as its authenticity, by allowing verifiers the ability to detect any changes to the message content.

this page intentionally left blank

9.0 ISO 8583 Reversal Advice Request/Response Message Formats

This section describes the Reversal Advice Request (1420) message and the Reversal Advice Response (1430) message, as defined for the ISO 8583 format. These messages are constructed as specified in the ISO 8583-1993 standard. If your system supports a different version of ISO 8583, notify your American Express representative.

The Reversal Advice Request/Response (1420/1430) message is mandatory for Merchant Initiated Reversals for U.S. Third Party Processors only and is an optional message for System Generated Reversals.

The Reversal Advice Request (1420) message can be generated by the Merchant in the following two situations:

- Merchant Initiated Reversal (Mandatory for U.S. Third Party Processors only): This is the cancellation of an already approved transaction that has not yet been submitted by the Merchant and which must equal the amount originally approved. This type of reversal can only be submitted after an Authorization Response (1110) message has been received. Merchants or Processors that certify for this feature can use it for all American Express products and any transaction for which they have received a prior approval that has not yet been submitted by the Merchant.
- System Generated Reversal (Optional): An Authorization Response (1110) message has not been received to an Authorization Request (1100) message within the transaction timeout period. This type of reversal indicates that a request has been forwarded by the card acceptance device and no response has been received within the allocated time out period.

The Reversal Advice Request (1420) message should be created by the electronic medium used to enter the original Authorization Request (1100) message. Only the original data field values used to generate the original Authorization Request (1100) message can be used to populate the data field values in the reversal message except for the System Trace Audit Number (Data Field 11) which should be a new value.

The acquiring source will receive a Reversal Advice Response (1430) message from the card Issuer's system indicating acknowledgement of the reversal request. This acknowledgement does not imply that any financial action has been taken to adjust the Cardmember's account standing. If the Merchant system does not get a Reversal Advice Response (1430) message to their initial Reversal Advice Request (1420) message, then resending the Reversal Advice Request (1420) message should not exceed more than three attempts.

The Reversal Advice Request (1420) message is not intended for debit or credit adjustments, for transactions that have already been settled, or for amounts other than the original approved amount.

Notes:

1. Reversals, of any type, are not allowed for Travelers Cheque transactions.
2. The Reversal Advice Request (1420) message contains many of the same data fields found in an Authorization Request (1100) message. When submitting a Reversal Advice Request (1420) message, only the defined data fields for that message should be sent.

9.1 1420 Reversal Advice Request

Length of Record: 318 bytes maximum

Description: This message is used by a Merchant to transmit a Reversal Advice Request (1420) message to American Express.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
—	MESSAGE TYPE IDENTIFIER	4 bytes, fixed	Numeric	Mandatory	222
—	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary	Mandatory	222
2	PRIMARY ACCOUNT NUMBER (PAN)	21 bytes, LLVAR	Numeric	See page ➔	223
3	PROCESSING CODE	6 bytes, fixed	Numeric	Mandatory	224
4	AMOUNT, TRANSACTION	12 bytes, fixed	Numeric	Mandatory	225
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters	Mandatory	225
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric	Mandatory	226
14	DATE, EXPIRATION	4 bytes, fixed	Numeric	Optional	227
19	COUNTRY CODE, ACQUIRING INSTITUTION	3 bytes, fixed	Numeric	Mandatory	228
22	POINT OF SERVICE DATA CODE	12 bytes, fixed	Alphanumeric	Mandatory	228
25	MESSAGE REASON CODE	4 bytes, fixed	Numeric	See page ➔	229
26	CARD ACCEPTOR BUSINESS CODE	4 bytes, fixed	Numeric	Mandatory	229
31	ACQUIRER REFERENCE DATA	50 bytes, LLVAR	Alphanumeric & special characters	Mandatory	230
32	ACQUIRING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Optional	231
33	FORWARDING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Optional	232

9.1 1420 Reversal Advice Request (continued)

.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
37	RETRIEVAL REFERENCE NUMBER	12 bytes, fixed	Alphanumeric & special characters	Optional	232
41	CARD ACCEPTOR TERMINAL IDENTIFICATION	8 bytes, fixed	Alphanumeric & special characters	See page ➔	233
42	CARD ACCEPTOR IDENTIFICATION CODE	15 bytes, fixed	Alphanumeric & special characters	Mandatory	234
49	CURRENCY CODE, TRANSACTION	3 bytes, fixed	Numeric	Mandatory	234
56	ORIGINAL DATA ELEMENTS	37 bytes, LLVAR	See page ➔	Mandatory	235
62	PRIVATE USE DATA	63 bytes, LLLVAR	Alphanumeric & special characters	N/A	236
64	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary	N/A	236

9.1 1420 Reversal Advice Request (continued)

Data Field — None	MESSAGE TYPE IDENTIFIER
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	`1420`
Field Requirement:	Mandatory
Description:	The constant literal "`1420`" signifies the ISO 8583 Reversal Advice Request message.

Data Field — None	BIT MAP - PRIMARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory
Description:	See Bit Map - Primary description on page 62 of the Authorization Request (1100) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 2	PRIMARY ACCOUNT NUMBER (PAN)
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 21 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 19 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	• Mandatory — American Express Card transactions • Mandatory — Other Card products and bankcard transactions **Note**: American Express supports Diner's Club, JCB, VISA and MasterCard processing. For details, contact your American Express representative. • Not used - American Express Travelers Cheques
Description:	This data field must contain the same Primary Account Number (PAN) value used in the original Authorization Request (1100) message. See Primary Account Number (PAN) description on page 65 of the Authorization Request (1100) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 3	PROCESSING CODE
Length of Field:	6 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field indicates the financial service being requested. Valid Processing Codes: `004000` = Card Reversal Advice — System Generated Reversal `024000` = Merchant Initiated Reversal **Notes**: 1. Reversals, of any type, are not allowed for Travelers Cheque transactions. 2. This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

9.1 1420 Reversal Advice Request (continued)

Data Field 4	AMOUNT, TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, right justified, zero filled
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the original transmitted amount. The decimal point is determined by the Currency Code, Transaction data field (Data Field 49). See Amount, Transaction description on page 67 of the Authorization Request (1100) message. **Note**: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

Data Field 11	SYSTEMS TRACE AUDIT NUMBER
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric (upper case) & special characters
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain a unique trace number, assigned by the Merchant, to help identify an individual transaction. A different number must be assigned to each transaction. **Note**: American Express returns this number without alteration in the Systems Trace Audit Number data field of the Reversal Advice Response (1430) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 12	DATE AND TIME, LOCAL TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, YYMMDDhhmmss
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the year, month, day and local time when the Reversal Advice Request (1420) message took place. The format is YYMMDDhhmmss. The value of this data field must be a valid date and time.

Subfield	Definition	Digits	Range
YY	Year	Last 2 only	00-99
MM	Month	2	01-12
DD	Day	2	01-31
hh	Hour	2	00-23
mm	Minute	2	00-59
ss	Second	2	00-59

Note: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration

9.1 1420 Reversal Advice Request (continued)

Data Field 14	DATE, EXPIRATION
Length of Field:	4 bytes, fixed length
Field Type:	Numeric, YYMM
Constant:	None
Field Requirement:	Optional
Description:	See Date, Expiration description on page 73 of the Authorization Request (1100) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 19	COUNTRY CODE, ACQUIRING INSTITUTION
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain the same Country Code, Acquiring Institution value used in the original Authorization Request (1100) message. See Country Code, Acquiring Institution description on page 75 of the Authorization Request (1100) message.

Data Field 22	POINT OF SERVICE DATA CODE
Length of Field:	12 bytes, fixed length
Field Type:	Alphanumeric, upper case
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain the same Point of Service Data Code values used in the original Authorization Request (1100) message. See Point of Service Data Code description on page 76 of the Authorization Request (1100) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 25	MESSAGE REASON CODE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	• Mandatory — American Express Card (and American Express-supported Card) transactions. • Optional — VISA, MasterCard and JCB transactions • Optional — American Express Travelers Cheques
Description:	See Message Reason Code description on page 91 of the Authorization Request (1100) message.

Data Field 26	CARD ACCEPTOR BUSINESS CODE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain the same Card Acceptor Business Code value used in the original Authorization Request (1100) message. See Card Acceptor Business Code description on page 92 of the Authorization Request (1100) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 31	ACQUIRER REFERENCE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 50 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 48 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Conditional — Merchant systems • System Generated Reversal — This data field is unused by Merchants and/or Third Party Processors. • Merchant Initiated Reversal — This data field must contain the same 15-digit Transaction Identifier provided in Data Field 31 of the Authorization Response (1110) mesage.

Description:	This data field contains the 15-digit, numeric, Transaction Identifier (TID), a unique, American Express-assigned tracking number. The TID is used to identify and track a Cardmember transaction throughout its life cycle.
	See the following example of a typical TID entry:
	`0 1`
	`1234567890123456`
	`151234567890123 45`
	• "`15`" is the two-byte, Variable Length Indicator (VLI).
	• "`123456789012345`" is the 15-byte, numeric TID.

9.1 1420 Reversal Advice Request (continued)

Data Field 32	ACQUIRING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Optional
Description:	This data field must contain the same Acquiring Institution Identification Code value used in the original Authorization Request (1100) message. See Acquiring Institution Identification Code description on page 95 of the Authorization Request (1100) message. **Note**: This data field may not be required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

9.1 1420 Reversal Advice Request (continued)

Data Field 33	FORWARDING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Optional
Description:	This data field must contain the same Forwarding Institution Identification Code value used in the original Authorization Request (1100) message. See Forwarding Institution Identification Code description on page 96 of the Authorization Request (1100) message.

Data Field 37	RETRIEVAL REFERENCE NUMBER
Length of Field:	12 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Optional
Description:	See Retrieval Reference Number description on page 100 of the Authorization Request (1100) message.

9.1 1420 Reversal Advice Request (continued)

Data Field 41	CARD ACCEPTOR TERMINAL IDENTIFICATION
Length of Field:	8 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	• Optional — American Express transactions in the USA and Canada, and non-VISA transactions • Mandatory — VISA PS2000
Description:	This data field must contain the same Card Acceptor Terminal Identification value used in the original Authorization Request (1100) message. See Card Acceptor Terminal Identification description on page 101 of the Authorization Request (1100) message. **Note**: This data field may or may not be mandatory for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message without alteration.

9.1 1420 Reversal Advice Request (continued)

Data Field 42	CARD ACCEPTOR IDENTIFICATION CODE
Length of Field:	15 bytes, fixed length
Field Type:	Alphanumeric & special characters, left justified, character space filled
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain the same Card Acceptor Identification Code value used in the original Authorization Request (1100) message. See Card Acceptor Identification Code description on page 102 of the Authorization Request (1100) message.

Data Field 49	CURRENCY CODE, TRANSACTION
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain the same Currency Code, Transaction value used in the original Authorization Request (1100) message. See Currency Code, Transaction description on page 133 of the Authorization Request (1100) message. **Note**: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

9.1 1420 Reversal Advice Request (continued)

Data Field 56	ORIGINAL DATA ELEMENTS
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 37 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 35 bytes maximum, EBCDIC
Field Type:	See individual subfields for Data Field Type
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains four data subfields from the original transaction being reversed. These four subfields may total up to 35 characters, and they are preceded by a two-digit, Variable Length Indicator (VLI). See the following table:

Subfield Name	Description	Subfield Type	Subfield Length
LL	VARIABLE LENGTH INDICATOR (VLI)	Numeric (EBCDIC)	2 bytes
Subfield 1	MESSAGE TYPE IDENTIFIER *	Numeric	4 bytes
Subfield 2	SYSTEM TRACE AUDIT NUMBER *	Alphanumeric & special characters	6 bytes
Subfield 3	DATE AND TIME, LOCAL TRANSACTION *	Numeric	12 bytes
Subfield 4	ACQUIRING INSTITUTION IDENTIFICATION CODE *	Numeric or special characters	13 bytes (max.) LLVAR

*This subfield must contain the same value used in the original Authorization Request (1100) message.

Note: If subfield 4 (in above table) is unused, this is indicated by one backslash (\).

9.1 1420 Reversal Advice Request (continued)

Data Field 62	PRIVATE USE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 63 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 60 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. If included in an originating request, it will not be preserved; and it may not be returned in the response. However, as long as it is properly formatted per this specification, its presence will not interfere with message processing.

Data Field 64	MESSAGE AUTHENTICATION CODE FIELD
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Message Authentication Code data field description on page 178 of the Authorization Request (1100) message.

9.2 1430 Reversal Advice Response

Length of Record: 181 bytes maximum

Description: This message is used by American Express to transmit a Reversal Advice Response (1430) message to a Merchant.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
—	MESSAGE TYPE IDENTIFIER	4 bytes, fixed	Numeric	Mandatory	238
—	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary	Mandatory	238
2	PRIMARY ACCOUNT NUMBER (PAN)	21 bytes, LLVAR	Numeric	Mandatory - Echo returned	239
3	PROCESSING CODE	6 bytes, fixed	Numeric	Mandatory - Echo returned	239
4	AMOUNT, TRANSACTION	12 bytes, fixed	Numeric	Mandatory - Echo returned	240
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters	Mandatory - Echo returned	240
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric	Mandatory - Echo returned	241
31	ACQUIRER REFERENCE DATA	50 bytes, LLVAR	Alphanumeric & special characters	See page ➔	242
32	ACQUIRING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Conditional - Echo returned	243
37	RETRIEVAL REFERENCE NUMBER	12 bytes, fixed	Alphanumeric & special characters	Conditional - Echo returned	243
39	ACTION CODE	3 bytes, fixed	Numeric	Mandatory	244
41	CARD ACCEPTOR TERMINAL IDENTIFICATION	8 bytes, fixed	Alphanumeric & special characters	Conditional - Echo returned	244
42	CARD ACCEPTOR IDENTIFICATION CODE	15 bytes, fixed	Alphanumeric & special characters	Mandatory - Echo returned	245
49	CURRENCY CODE, TRANSACTION	3 bytes, fixed	Numeric	Mandatory - Echo returned	245
64	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary	N/A	246

9.2 1430 Reversal Advice Response (continued)

Data Field — None	MESSAGE TYPE IDENTIFIER
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	`1430`
Field Requirement:	Mandatory
Description:	The constant literal "`1430`" signifies the ISO 8583 Reversal Advice Response message.

Data Field — None	BIT MAP - PRIMARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory
Description:	See Bit Map - Primary description on page 62 of the Authorization Request (1100) message.

9.2 1430 Reversal Advice Response (continued)

Data Field 2	PRIMARY ACCOUNT NUMBER (PAN)
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 21 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 19 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message.

Data Field 3	PROCESSING CODE
Length of Field:	6 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message.

9.2 1430 Reversal Advice Response (continued)

Data Field 4	AMOUNT, TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, right justified, zero filled
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message.

Data Field 11	SYSTEMS TRACE AUDIT NUMBER
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric (upper case) & special characters
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message.

9.2 1430 Reversal Advice Response (continued)

Data Field 12	DATE AND TIME, LOCAL TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, YYMMDDhhmmss
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message.

9.2 1430 Reversal Advice Response (continued)

Data Field 31	ACQUIRER REFERENCE DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 50 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 48 bytes maximum, EBCDIC
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Mandatory • System Generated Reversal — This data field is mandatory and created by the American Express Global Network, and it always appears in response messages returned to Merchants and/or Third Party Processors. • Merchant Initiated Reversal — This data field is mandatory in the Reversal Advice Request (1420) message and echo returned without alteration in the Reversal Advice Response (1430) message.

Description:	This data field contains the 15-digit, numeric, Transaction Identifier (TID), a unique, American Express-assigned tracking number. The TID is used to identify and track a Cardmember transaction throughout its life cycle.
	See the following example of a typical TID entry:
	`0 1`
	`123456789012345`
	`151234567890123 45`
	• "`15`" is the two-byte, Variable Length Indicator (VLI).
	• "`123456789012345`" is the 15-byte, numeric TID.

9.2 1430 Reversal Advice Response (continued)

Data Field 32	ACQUIRING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

Data Field 37	RETRIEVAL REFERENCE NUMBER
Length of Field:	12 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

9.2 1430 Reversal Advice Response (continued)

Data Field 39	ACTION CODE
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	`400`
Field Requirement:	Mandatory
Description:	This data field contains the Action Code, indicating the American Express disposition for this transaction. Valid Action Code: 400 = Reversal Accepted **Note**: American Express uses the Reversal Advice Response (1430) message as a response to Reversal Advice Request (1420) message reversals. This acknowledgement does not imply that financial action(s) have been taken to adjust the Cardmember's account standing.

Data Field 41	CARD ACCEPTOR TERMINAL IDENTIFICATION
Length of Field:	8 bytes, fixed length
Field Type:	Alphanumeric & special characters
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

9.2 1430 Reversal Advice Response (continued)

Data Field 42	CARD ACCEPTOR IDENTIFICATION CODE
Length of Field:	15 bytes, fixed length
Field Type:	Alphanumeric & special characters, left justified, character space filled
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message.

Data Field 49	CURRENCY CODE, TRANSACTION
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Reversal Advice Request (1420) message, and is echo returned without alteration in the Reversal Advice Response (1430) message. For more information on numeric currency codes and decimal point positions, refer to Country and Currency Codes for Authorizations in the *American Express Global Codes & Information Guide*.

9.2 1430 Reversal Advice Response (continued)

Data Field 64	MESSAGE AUTHENTICATION CODE FIELD
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Message Authentication Code Data Field description on page 178 of the Authorization Request (1100) message.

10.0 ISO 8583 Network Management Request/Response Message Formats

This section describes the Network Management Request (1804) message and the Network Management Response (1814) message, as defined for the ISO 8583 format. These messages are constructed as specified in the ISO 8583-1993 standard. If your system supports a different version of ISO 8583, notify your American Express representative.

The Network Management Request (1804) message allows for a Dynamic Key Exchange, Echo Test or Sign On/Sign Off request. When the Network Management Request (1804) message is received, it should be responded to by transmitting a Network Management Response (1814) message.

The Network Management Request (1804) message can be generated by the Merchant in the following situations:

- Dynamic Key Exchange: The Merchant must send in a Function Code (Data Field 24) of "`811`" requesting dynamic key exchange from American Express.
- Echo Test: Allows the Merchant to query American Express as to its availability.
- Sign On/Sign Off: This is only available in China. Indicates American Express readiness to transmit or stop transmitting financial transactions.

10.1 1804 Network Management Request

Length of Record: 1113 bytes maximum

Description: This message is used by a Merchant to transmit a Network Management Request (1804) message to American Express.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
—	MESSAGE TYPE IDENTIFIER	4 bytes, fixed	Numeric	Mandatory	249
—	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary	Mandatory	249
1	BIT MAP - SECONDARY	8 bytes, 64 bits	Binary	N/A	250
3	PROCESSING CODE	6 bytes, fixed	Numeric	Mandatory	250
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters	Mandatory	251
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric	Mandatory	252
24	FUNCTION CODE	3 bytes, fixed	Numeric	Mandatory	253
25	MESSAGE REASON CODE	4 bytes, fixed	Numeric	Mandatory	254
33	FORWARDING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Optional	255
93	TRANSACTION DESTINATION INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric	N/A	255
94	TRANSACTION ORIGINATOR INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric	N/A	256
96	KEY MANAGEMENT DATA	999 bytes, LLLVAR	Binary	N/A	256
100	RECEIVING INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric	N/A	257
128	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary	N/A	257

10.1 1804 Network Management Request (continued)

Data Field — None	MESSAGE TYPE IDENTIFIER
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	`1804`
Field Requirement:	Mandatory
Description:	The constant literal "`1804`" signifies the ISO 8583 Network Management Request (1804) message.

Data Field — None	BIT MAP - PRIMARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory
Description:	See Bit Map - Primary description on page 62 of the Authorization Request (1100) message.

10.1 1804 Network Management Request (continued)

Data Field 1	BIT MAP - SECONDARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. Bit Map - Secondary supports ISO Data Fields 65 through 128. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

Data Field 3	PROCESSING CODE
Length of Field:	6 bytes, fixed length
Field Type:	Numeric
Constant:	`000000`
Field Requirement:	Mandatory
Description:	This data field indicates the processing service being requested. At the present time, the only code being used is for communications verification. Valid Processing Code: `000000` = System Audit Control/Echo Message "Are you there?" Note: This data field is mandatory for processing this message and it will be preserved and returned in the response message without alteration.

10.1 1804 Network Management Request (continued)

Data Field 11	SYSTEMS TRACE AUDIT NUMBER
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric (upper case) & special characters
Constant:	None
Field Requirement:	Mandatory
Description:	This data field must contain a unique trace number, assigned by the Merchant, to help identify an individual transaction. A different number must be assigned to each transaction. Note: This data field is mandatory for processing this message and it will be preserved and returned in the response message without alteration.

10.1 1804 Network Management Request (continued)

Data Field 12	DATE AND TIME, LOCAL TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, YYMMDDhhmmss
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the year, month, day and local time when the transaction took place at the card acceptor location. The format is YYMMDDhhmmss. The value of this data field must be a valid date and time:

Subfield	Definition	Digits	Range
YY	Year	Last 2 only	00-99
MM	Month	2	01-12
DD	Day	2	01-31
hh	Hour	2	00-23
mm	Minute	2	00-59
ss	Second	2	00-59

Note: This data field is mandatory for processing this message, and it will be preserved and returned in the response message without alteration.

10.1 1804 Network Management Request (continued)

Data Field 24	FUNCTION CODE
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains a three-digit code indicating the specific purpose of the message, within its message class. The standard value for this data field is: `811` Dynamic Key Exchange `831` = System Audit Control / Echo Message "Are you there?" **The following additional values are accepted in China only:** `801` = Acquirer Session "Sign On" Indicator of Acquirer readiness to transmit financial transactions. `802` = Acquirer Session "Sign Off" Indicator that Acquirer will no longer be transmitting financial transactions. Note: This data field is mandatory for processing this message and it will be preserved and returned in the response message without alteration.

10.1 1804 Network Management Request (continued)

Data Field 25	MESSAGE REASON CODE
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains a four-digit Message Reason Code, which is provided by American Express during certification. The code used varies with the type of request submitted for processing by the Merchant or Third Party Processor. Proper use of this data field indicates that the Network Management Request is certified by American Express. For information on valid codes and their use, contact your American Express representative.

10.1 1804 Network Management Request (continued)

Data Field 33	FORWARDING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Optional
Description:	See Forwarding Institution Identification Code description on page 96 of the Authorization Request (1100) message. This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

Data Field 93	TRANSACTION DESTINATION INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 11 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 9 bytes maximum, EBCDIC
Field Type:	Numeric
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. This data field is used to identify the institution for a transaction's destination. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

10.1 1804 Network Management Request (continued)

Data Field 94	TRANSACTION ORIGINATOR INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 11 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 9 bytes maximum, EBCDIC
Field Type:	Numeric
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. This data field is used to identify the institution for a transaction's originator. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

Data Field 96	KEY MANAGEMENT DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 999 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 996 bytes maximum, EBCDIC
Field Type:	Binary
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. This data field contains information on session keys and tokens. For more information, contact your American Express representative. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

10.1 1804 Network Management Request (continued)

Data Field 100	RECEIVING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 11 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 9 bytes maximum, EBCDIC
Field Type:	Numeric
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. This data field is used to identify the receiving institution. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

Data Field 128	MESSAGE AUTHENTICATION CODE FIELD
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Message Authentication Code Data Field description on page 178 of the Authorization Request (1100) message. Data must not be transmitted to American Express in this data field. Unauthorized use of this data field may cause message rejection.

10.2 1814 Network Management Response

Length of Record: 1112 bytes maximum

Description: This message is used by American Express to transmit a Network Management Response (1814) message to a Merchant.

Data Field	Data Field Name	Max. Data Field Length	Data Field Type	Data Field Requirements	Page
—	MESSAGE TYPE IDENTIFIER	4 bytes, fixed	Numeric	Mandatory	259
—	BIT MAP - PRIMARY	8 bytes, 64 bits	Binary	Mandatory	259
1	BIT MAP - SECONDARY	8 bytes, 64 bits	Binary	See page ➔	260
3	PROCESSING CODE	6 bytes, fixed	Numeric	Mandatory - Echo returned	260
11	SYSTEMS TRACE AUDIT NUMBER	6 bytes, fixed	Alphanumeric & special characters	Mandatory - Echo returned	261
12	DATE AND TIME, LOCAL TRANSACTION	12 bytes, fixed	Numeric	Mandatory - Echo returned	261
24	FUNCTION CODE	3 bytes, fixed	Numeric	Mandatory - Echo returned	262
33	FORWARDING INSTITUTION IDENTIFICATION CODE	13 bytes, LLVAR	Numeric	Conditional - Echo returned	262
39	ACTION CODE	3 bytes, fixed	Numeric	Mandatory	263
93	TRANSACTION DESTINATION INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric	N/A	263
94	TRANSACTION ORIGINATOR INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric	N/A	264
96	KEY MANAGEMENT DATA	999 bytes, LLLVAR	Binary	See page ➔	265
100	RECEIVING INSTITUTION IDENTIFICATION CODE	11 bytes, LLVAR	Numeric	N/A	268
128	MESSAGE AUTHENTICATION CODE FIELD	8 bytes, 64 bits	Binary	N/A	268

10.2 1814 Network Management Response (continued)

Data Field — None	MESSAGE TYPE IDENTIFIER
Length of Field:	4 bytes, fixed length
Field Type:	Numeric
Constant:	1814
Field Requirement:	Mandatory
Description:	The constant literal "1814" signifies the ISO 8583 Network Management Response message.

Data Field — None	BIT MAP - PRIMARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory
Description:	See Bit Map - Primary description on page 62 of the Authorization Request (1100) message.

10.2 1814 Network Management Response (continued)

Data Field 1	BIT MAP - SECONDARY
Length of Field:	8 bytes, 64 bits, fixed length for each bit map
Field Type:	Binary (hexadecimal configuration)
Constant:	None
Field Requirement:	Mandatory — For Data Fields 65 through128
Description:	See Bit Map - Secondary description on page 64 of the Authorization Request (1100) message.

Data Field 3	PROCESSING CODE
Length of Field:	6 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Network Management Request (1804) message, and is echo returned without alteration in the Network Management Response (1814) message.

10.2 1814 Network Management Response (continued)

Data Field 11	SYSTEMS TRACE AUDIT NUMBER
Length of Field:	6 bytes, fixed length
Field Type:	Alphanumeric (upper case) & special characters
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Network Management Request (1804) message, and is echo returned without alteration in the Network Management Response (1814) message.

Data Field 12	DATE AND TIME, LOCAL TRANSACTION
Length of Field:	12 bytes, fixed length
Field Type:	Numeric, `YYMMDDhhmmss`
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	This data field is mandatory in the Network Management Request (1804) message, and is echo returned without alteration in the Network Management Response (1814) message.

10.2 1814 Network Management Response (continued)

Data Field 24	FUNCTION CODE
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory — Echo returned
Description:	See Function Code description on page 253 of the Network Management Request (1804) message. This data field is mandatory in the Network Management Request (1804) message, and is echo returned without alteration in the Network Management Response (1814) message.

Data Field 33	FORWARDING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 13 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 11 bytes maximum, EBCDIC
Field Type:	Numeric
Constant:	None
Field Requirement:	Conditional — Echo returned
Description:	This data field is not required for processing this message; however, if included in an originating request message, it will be preserved and returned in the response message, without alteration.

10.2 1814 Network Management Response (continued)

Data Field 39	ACTION CODE
Length of Field:	3 bytes, fixed length
Field Type:	Numeric
Constant:	None
Field Requirement:	Mandatory
Description:	This data field contains the Action Code, indicating the American Express disposition for this transaction. Valid Action Codes: 115 = Requested Function not Supported 181 = Format Error 800 = Accepted 909 = System Malfunction (Cryptographic Error)

Data Field 93	TRANSACTION DESTINATION INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 11 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 9 bytes maximum, EBCDIC
Field Type:	Numeric
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Transaction Destination Institution Identification Code description on page 255 of the Network Management Request (1804) message.

10.2 1814 Network Management Response (continued)

Data Field 94	TRANSACTION ORIGINATOR INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 11 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 9 bytes maximum, EBCDIC
Field Type:	Numeric
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Transaction Originator Institution Identification Code description on page 256 of the Network Management Request (1804) message.

10.2 1814 Network Management Response (continued)

Data Field 96	KEY MANAGEMENT DATA
Length of Field: Variable Length Indicator: Length of Variable Data:	4 bytes minimum, 999 bytes maximum, (LLLVAR) 3 bytes, EBCDIC, right justified, zero filled 996 bytes maximum, EBCDIC & Binary
Field Type:	Unsigned binary number – Data items whose original formats are defined as binary are mapped directly as eight bits per byte, with the value of any binary byte of data varying from hexadecimal "00" to "FF"
Field Requirement:	• Mandatory — PIN, MAC or DATA encryption transactions using dynamic key exchange. • Not used — Other transactions
Description:	This data field contains key management related data that can be transmitted either in transaction messages to convey information about cryptographic keys used to secure the current transaction, or in cryptographic service messages to convey information about cryptographic keys to be used to secure future transactions. Note: This data field is returned only after a successful dynamic key exchange request containing Function Code 811 (Dynamic Key Exchange) in the Network Management Request (1804) message.

10.2 1814 Network Management Response (continued)

Data Field 96 KEY MANAGEMENT DATA (continued)

American Express Session Key Exchange Format Table

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
1-3	VARIABLE LENGTH INDICATOR (VLI)	3 bytes	Numeric (EBCDIC)	M	VLI indicates total length of variable data in this data field (not including VLI).
4-5	PRIMARY ID	2 bytes	Alpha	M	Primary ID (Card Type Code) is constant literal "AX" (American Express).
6-8	SECONDARY ID	3 bytes	Alpha	M	Secondary ID (Data Type Code) is constant literal "SKX" (Session Key Exchange).
9-24	SESSION PIN KEY	16 bytes	Binary	M	Session Key created for encrypting a Personal Identification Number (PIN).
25-40	SESSION MAC KEY	16 bytes	Binary	M	Reserved for future use. Session Key created for the generation of Message Authentication Code. Not currently in use, must binary zero-fill.
41-56	SESSION DATA KEY	16 bytes	Binary	M	Reserved for future use. Session Key created for encrypting of Personal Identifiable Information (PII). Not currently in use, must binary zero-fill.
57-59	SESSION PIN KEY CHECK VALUE	3 bytes	Binary	M	Check Value is derived by American Express identifying the Session PIN Key sent in the Network Response (1814) message received from American Express. Note: This value is returned, without alteration, in the SESSION PIN KEY CHECK VALUE subfield in Data Field 96, Key Management Data, of the Authorization Response (1110) message.
60-62	SESSION MAC KEY CHECK VALUE	3 bytes	Binary	M	Reserved for future use. Check value derived from the Session MAC Key received from American Express. Not currently in use, must binary zero-fill.

10.2 1814 Network Management Response (continued)

Data Field 96 KEY MANAGEMENT DATA (continued)

American Express Session Key Exchange Format Table (continued)

Relative Position	Subfield Name	Subfield Length	Subfield Type	Required (M/O/C)	Description
63-65	SESSION DATA KEY CHECK VALUE	3 bytes	Binary	M	Reserved for future use. Check value derived from the Session DATA Key received from American Express. Not currently in use, must binary zero-fill.

Note: The subfields SESSION PIN KEY CHECK VALUE, SESSION MAC KEY CHECK VALUE, and SESSION DATA KEY CHECK VALUE will be encrypted by American Express with the Master Key (ECB Mode X9.17) prior to transmitting the message.

10.2 1814 Network Management Response (continued)

Data Field 100	RECEIVING INSTITUTION IDENTIFICATION CODE
Length of Field: Variable Length Indicator: Length of Variable Data:	3 bytes minimum, 11 bytes maximum, (LLVAR) 2 bytes, EBCDIC, right justified, zero filled 9 bytes maximum, EBCDIC
Field Type:	Numeric
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Receiving Institution Identification Code description on page 257 of the 1804 Network Management Request (1804) message.

Data Field 128	MESSAGE AUTHENTICATION CODE FIELD
Length of Field:	8 bytes, 64 bits
Field Type:	Binary
Constant:	None
Field Requirement:	Not used — All transactions
Description:	This data field is unused and reserved for future use. See Message Authentication Code Data Field description on page 178 of the Authorization Request (1100) message.

11.0 Examples of Typical Message Formats

This section shows examples of typical layouts for each message-type class. However, not all possible data field and functionality combinations, which are described in applicable data field descriptions are shown. **Note**: Formats are American Express unless otherwise noted.

11.1 1100 Authorization Request Message — Card Present Transaction with AAV & CID/4DBC/4CSC — American Express

This diagram illustrates the message layout for a typical, American Express, **Card Present** transaction where both AAV and CID/4DBC/4CSC are transmitted. The following Data Fields are included: 2, 3, 4, 11, 12, 19, 22, 24, 25, 26, 32, 33, 35, 37, 41, 42, 43, 45, 49, 53 and 63.

Data Field:	MTI	Bit Map	2	3	4	11
Bytes Max:	4	8	21	6	12	6
Data:	1100	70 30 25 C1 A8 E8 88 02	15371449635311004	004800	000000010000	123456

Data Field:	12	19	22	24	25	26	32	33
Bytes Max:	12	3	12	3	4	4	13	13
Data:	041217145000	840	261101W00120	181	1234	1234	1145678912345	1145678912345

Data Field:	35	37	41	42
Bytes Max:	39	12	8	15
Data:	3737144963531 1004=94031019101123456 7800	ABCDE1234567	123ABC45	5021011432~~~~~

Data Field:	43	45
Bytes Max:	101	78
Data:	45AA~CLEANERS\1234~MAIN~ST\ANYTOWN\85054~~~~~\\	76B3714496353110 04^

Data Field:	45 (continued)	49	53
Bytes Max:	78 (continued)	3	10
Data:	FROST/CHARLES~F.JR~~~~~~~~^9403101910112345678901234567 8901	840	049999

Data Field:	63
Bytes Max:	208
Data:	033AXAD850544500~~~~~~~~~~~~~~~~~~~~

11.1 Card Present Transaction with AAV & CID/4DBC/4CSC — American Express (continued)

In the example above:

Page

- Data Field 3 is mandatory and contains Processing Code "`004800`", which indicates that this message is a Combination Automated Address Verification and Authorization Request. 66
- Data Field 22 is mandatory and contains the POS Data Code. Position 7, Code "`W`", indicates that this is a swiped transaction with keyed CID/4DBC/4CSC. This example shows that both Tracks 1 and 2 were captured. Note that Track 1 and Track 2 data examples illustrate the ISO 7813 format. For more information on Track formats, see pages 9, 97, and 109. 76
- Data Field 24 contains the Function Code. The value **`"181"`** indicates that the Merchant's system supports Prepaid Card Partial Authorizations. 86
- Data Field 25 is mandatory and contains the Message Reason Code. However, note that **`"1234"`** is a placeholder only, and this value is not a valid entry. American Express assigns Message Reason Codes to Merchants during certification. 91
- Data Field 43 is optional and contains the Card Acceptor Name/Location, which in this example is the Merchant's company name, street address, city and ZIP. 104
- Data Field 53 is conditional and contains Security Related Control Information, which in this example is the keyed CID/4DBC/4CSC code. 135
- Data Field 63 is mandatory for certain American Express transactions, including Automated Address Verification, and contains Private Use Data, which in this example is basic 33-byte format, AAV (ZIP only) data associated with the swiped transaction. 157

11.2 1100 Authorization Request Message — Card Not Present Transaction with AAV & CID/4DBC/4CSC — American Express

This diagram illustrates the message layout for a typical, American Express, **Card Not Present** transaction where both AAV and CID/4DBC/4CSC are transmitted. The following Data Fields are included: 2, 3, 4, 11, 12, 14, 19, 22, 24, 25, 26, 32, 33, 37, 41, 42, 43, 49, 53 and 63.

Note: Data Field 47 is not shown, because of its length. However, American Express defines specific Card Not Present formats for Data Field 47. For more details and examples of typical layouts, see pages 113-117.

.

Data Field:	MTI	Bit Map	2	3	4	11
Bytes Max:	4	8	21	6	12	6
Data:	1100	70 34 25 C1 88 E0 88 02	15371449635311004	004800	000000010000	123456

Data Field:	12	14	19	22	24	25	26	32	33
Bytes Max:	12	4	3	12	3	4	4	13	13
Data:	041217145000	0512	840	160020S00110	181	1234	1234	1145678912345	1145678912345

Data Field:	37	41	42	43
Bytes Max:	12	8	15	101
Data:	ABCDE1234567	123ABC45	5021011432~~~~~	45AA~SOFTWARE\5678~MAIN~ST\ANYTOWN\

Data Field:	43 (continued)	49	53	63
Bytes Max:	101 (continued)	3	10	208
Data:	85054~~~~~\\	840	049999	033AXAD8505445004588~LOWELL~BLVD~~~

In the example above:

	Page
• Data Field 3 is mandatory and contains Processing Code "004800", which indicates that this message is a Combination Automated Address Verification and Authorization Request.	66
• This Example shows that Data Field 14, Expiration Date, was provided, because Track 1 or Track 2 was not captured. Data Field 22 is mandatory and contains the POS Data Code. Position 7, Code "S", indicates that this is a Card Not Present transaction with keyed CID/4DBC/4CSC.	73
• Data Field 22 is mandatory and contains the POS Data Code. Position 7, Code "S", indicates that this is a Card Not Present transaction with keyed CID/4DBC/4CSC.	76

11.2 Card Not Present Transaction with AAV & CID/4DBC/4CSC — American Express (continued)

In the example above (continued): **Page**

- Data Field 24 contains the Function Code. The value **"181"** indicates that the Merchant's system supports Prepaid Card Partial Authorizations. 86
- Data Field 25 is mandatory and contains the Message Reason Code. However, note that **"1234"** is a placeholder only, and this value is not a valid entry. American Express assigns Message Reason Codes to Merchants during certification. 91
- Data Field 43 is optional and contains the Card Acceptor Name/Location, which in this example is the Merchant's company name, street address, city and ZIP. 104
- Data Field 53 is conditional and contains Security Related Control Information, which in this example is the keyed CID/4DBC/4CSC code. 135
- Data Field 63 is mandatory for certain American Express transactions, including Automated Address Verification, and contains Private Use Data, which in this example is only the 33-byte AAV (Postal ZIP and Street Address only) data. However, American Express prefers Card Not Present transactions to contain the 208-byte AAV data. As this is a large data field, it is not shown here. Refer to the detail of Data Field 63 for a detailed example of the 208-byte AAV format. 157

11.3 1110 Authorization Response Message — American Express

This diagram illustrates the message layout for a typical response to the authorization request submitted in the preceding examples. The following Data Fields are included: 2, 3, 4, 11, 12, 31, 32, 37, 38, 39, 41, 42, 44 and 49; and most entries are echo returned from the original Authorization Request (1100) message.

Data Field:	MTI	Bit Map	2	3	4	11
Bytes Max:	4	8	21	6	12	6
Data:	1110	70 30 00 03 0E D0 80 00	15371449635311004	004800	000000010000	123456

Data Field:	12	31	32	37	38	39	41
Bytes Max:	12	50	13	12	6	3	8
Data:	041217145000	15123930120140500	1145678912345	ABCDE1234567	NNNNNN	000	123ABC45

Data Field:	42	44	49
Bytes Max:	15	27	3
Data:	5021011432~~~~~	02ZY	840

In the example above:

Page

- Data Field 31 is mandatory and contains Acquirer Reference Data, which in this example is the Transaction Identifier (TID) inserted by the American Express Network. 94
- Data Field 38 is mandatory for approved transactions and contains an Approval Code, because the value in Data Field 39 indicates that this transaction was approved. 193
- Data Field 39 is mandatory and contains an Action Code that indicates that the transaction was approved. 194
- Data Field 44 is mandatory for American Express Automated Address Verification and Keyed CID/ 4DBC/4CSC Validation, and contains Additional Response Data, which in this example is a four-byte entry composed of a two byte VLI and a two-byte AAV/CID/ 4DBC/4CSC response. The "Z" in relative position 3 indicates that the Postal (ZIP) Code matched, and the "Y" in relative position 4 indicates that the keyed CID/4DBC/4CSC was valid. 197

11.4 1420 Reversal Advice Request Message

This diagram illustrates the message layout for a typical, American Express Reversal Advice Request (1420) message system reversal, which contains many of data field entries from the original Authorization Request (1100) message. The following data fields are included: 2, 3, 4, 11, 12, 14, 19, 22, 25, 26, 32, 33, 37, 41, 42, 49 and 56.

Data Field:	MTI	Bit Map	2	3	4	11
Bytes Max:	4	8	21	6	12	6
Data:	1420	70 34 24 C1 88 C0 81 00	15371449635311004	004000	000000010000	123456

Data Field:	12	14	19	22	25	26	32	33
Bytes Max:	12	4	3	12	4	4	13	13
Data:	041217145000	0502	840	261101200120	1234	1234	1145678912345	1145678912345

Data Field:	37	41	42	49	56
Bytes Max:	12	8	15	3	37
Data:	ABCDE1234567	123ABC45	5021011432~~~~~	840	2311001234560501201405305\

In the example above:

Page

- Data Field 14 is optional and contains the Card Expiration Date embossed on the face of the American Express or American Express-supported Card. 227
- Data Field 25 is mandatory and contains the Message Reason Code. However, note that **"1234"** is a placeholder only, and this value is not a valid entry. American Express assigns Message Reason Codes to Merchants during certification. 229
- Data Field 32 is optional and contains the Acquiring Institution Identification Code of the party processing the request. 231
- Data Field 33 is optional and contains the Forwarding Institution Identification Code, which for non-AMEX requests may be the ID number assigned by the network provider processing transactions on the acquiring bank's behalf. 232
- Data Field 37 is optional and contains the Retrieval Reference Number. 232

11.4 1420 Reversal Advice Request Message (continued)

In the example above (continued): **Page**

- Data Field 41 is optional and contains the Card Acceptor Terminal Identification code. Use of this data field is strongly recommended for American Express transactions and mandatory for VISA PS2000 and other bankcards. 233
- Data Field 56 is mandatory and contains the Original Data Elements from the Authorization Request (1100) message, which identify the transaction needing correction or reversal. In this example, Subfield 4, Acquiring Institution Identification Code, is not provided; and this unused subfield is indicated by one backslash (\). 235

11.5 1430 Reversal Advice Response Message

This diagram illustrates the message layout for a typical response to the Reversal Advice Request (1420) message submitted in the preceding example. The following Data Fields are included: 2, 3, 4, 11, 12, 31, 32, 37, 39, 41, 42 and 49; and most entries are echo returned from the original Reversal Advice Request (1420) message.

Data Field:	MTI	Bit Map	2	3	4	11
Bytes Max:	4	8	21	6	12	6
Data:	1430	70 30 00 03 0A C0 80 00	15371449635311004	004000	000000010000	123456

Data Field:	12	31	32	37	39	41
Bytes Max:	12	50	13	12	3	8
Data:	041217145000	15111117891234543	1145678912345	ABCDE1234567	400	123ABC45

Data Field:	42	49
Bytes Max:	15	3
Data:	5021011432~~~~~	840

In the example above: **Page**

- Data Field 31 is mandatory and contains Acquirer Reference Data, which in this example is the Transaction Identifier (TID) inserted by the American Express Network. 242
- Data Field 39 is mandatory and contains Action Code value "400" that indicates "reversal acknowledged". 244

  Note: American Express uses the Reversal Advice response (1430) message as a response to Reversal Advice Request (1420) message system reversals only. This acknowledgement does not imply that financial action(s) have been taken to adjust the Cardmember's account standing.

11.6 1804 Network Management Request Message

This diagram illustrates the message layout for a typical, American Express, Network Management Request (1804) message. The following Data Fields are included: 3, 11, 12, 24 and 25.

Data Field:	MTI	Bit Map	3	11	12	24	25
Bytes Max:	4	8	6	6	12	3	4
Data:	1804	20 30 01 80 00 00 00 00	000000	123456	041217145000	831	1234

11.7 1814 Network Management Response Message

This diagram illustrates the message layout for a typical, American Express, Network Management Response (1814) acknowledgement message. The following Data Fields are included: 3, 11 and 12.

Data Field:	MTI	Bit Map	3	11	12
Bytes Max:	4	8	6	6	12
Data:	1814	20 30 00 00 00 00 00 00	000000	123456	041217145000

this page intentionally left blank

12.0 Revision Log

The Revision Log goes back three publications, current publication plus the last two. For earlier versions, contact SpecQuestions@aexp.com.

The Revision Log contains a condensed overview of the *GCAG ISO* changes. The Revision Log is divided into the following types of changes:

- General - Changes made due to reorganization, clarification, consistency, or for informative purposes
- Global - Changes made in multiple locations, not specific to a data field
- Specific data field changes - Changes made to specific data field(s) as noted
- Specific section changes - Changes made to specific section(s) as noted

Publication: April 2016 | Global Data Quality & Standards (GDQ&S) | Contact: SpecQuestions@aexp.com

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
General Changes		Changed '*Global Financial Settlement Guide (GFSG)*' to '*Global Financial Submission Guide (GFSG)*'.
Specific Data Field Changes *1100 Authorization Request*	DF 2: Primary Account Number (PAN)	In the description, changed the first paragraph to 'This data field contains the Cardmember Account Number, or Payment Token Account Number, preceded by a two-digit, Variable Length Indicator (VLI). The VLI must indicate the exact length of the account number, and no additional characters should be added to this data field'.
	DF 14: Date, Expiration	Updated field to include Payment Token functionality.
		In the description, removed ICC verbiage from the Note.
	DF 22: Point of Service Data Code	In the Point of Service Data Code tables, made the following changes and updates to include Payment Token functionality: • Position 1, removed value 'X' as a valid value. • Position 5, value 4, at the end of the description, added 'delayed shipment, split bill transactions'. • Position 6, added value 'Z' to identify Digital Wallet transactions. • Position 7, removed values 'X' and 'Y' as valid values. For value 5, added verbiage for Digital Wallet and Payment Token functionality.
		Removed references to magnetic stripe signature.
	DF 24: Function Code	In the description, added verbiage to the function code table for '196=Expresspay Translation (PAN & Expiration Date Request)'.
	DF 43: Card Acceptor Name/Location	Updated field for clarity around formatting for Payment Service Providers (Aggregators) and OptBlue Participants.
	DF 53: Security Related Control Information	Updated field to include Derived Unique Key Per Transaction (DUKPT) Key Exchange process.

12.0 Revision Log (continued)

Publication: April 2016 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
1100 Authorization Request (continued)	DF 60: National Use Data	Updated field to include Payment Token functionality.
	DF 61: National Use Data	Updated field to include Payment Token functionality.
	DF 62: Private Use Data	Removed references to magnetic stripe signature.
1110 Authorization Response	DF 34: Primary Account Number, Extended	Updated field to include Payment Token functionality.
	DF 60: National Use Data	Updated field to include Payment Token functionality.
1420 Reversal Advice Request	DF 4: Amount, Transaction	In the description, changed the first sentence from 'This data field contains the amount of the original (that is being reversed)' to 'This data field contains the original transmitted amount'.
	DF 14: Date, Expiration	Changed the field requirement from 'Conditional-If the value was submitted in the original Authorization Request (1100) message' to 'Optional'.
Specific Section Changes	Section 1.5 Related Documents	Added bullets for: • *American National Standards Institute ANSI X9.24, Asymmetric Techniques for the Distribution of Symmetric Keys* • *EMVCo Payment Tokenization Specification - Technical Framework*
		Removed bullet for '*American Express XML Global Financial Submission Guide*'.
	Section 5.0 Card Acceptance Supported Services	Updated section to include Payment Token functionality.
	Section 5.4.2.1 Expresspay Transit Transactions at Transit Access Terminals	Updated section to include Payment Token functionality.
	Section 5.8 Digital Wallet Payments	Added new section for Digital Wallet functionality.
	Section 6.1 Payment Token Transactions	Added new section for Payment Token functionality.
	Section 6.5.1 Master/Session Key Management Methodology	Updated section to include the DUKPT Key Exchange process.

12.0 Revision Log (continued)

Publication: April 2016 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes (continued)	Section 6.5.2 Derived Unique Key Per Transaction (DUKPT)	Added new section for DUKPT Key Exchange process.
	Section 7.1 Primary Bit Map	For DF 53, changed the max. data field length from '110 bytes LLVAT' to '19 bytes LLVAR'.
	Section 8.1 1100 - Authorization Request	For DF 60, changed max. data field length from '94 bytes, LLLVAR' to '106 bytes, LLLVAR'.

12.0 Revision Log (continued)

Publication: October 2015 | Global Data Quality & Standards (GDQ&S) | Contact: SpecQuestions@aexp.com

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
General Changes		The following sections have been moved to the *Global Codes & Information Guide*: • Check Digit Verification • SE Number Check Digit Computation (Modulus 9 Check) • Cardmember Number Check Digit Computation (Modulus 10 Check) • Appendix The following sections and applicable references have been removed entirely: • Document Clarification Request • ISO 8583 Network Management Notification (1844) Format • ISO 8583 Message Tables for VISA, MasterCard, Diner's Club and JCB • Examples of Typical Message Formats for VISA and MasterCard • Data and Certification Testing • Certification Tests
	Summary of Changes Table	Updated the paragraph description for clarity which includes 'This information may affect the way a Merchant, Third Party Processor or Vendor software processes American Express Card transactions'.
Specific Data Field Changes *Authorization Request (1100)*	DF 22: Point of Service Data Code	Added 'Note: American Express-certified EMV terminal and link' to the following: POS. 1, value 5 POS. 7, value 5 POS. 9, value 1 POS. 10, value 3

12.0 Revision Log (continued)

Publication: October 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Authorization Request (1100) (continued)	DF 43: Card Acceptor Name/Location	In Subfield 1, updated the description column for Payment Service Providers (Aggregators) and OptBlue Participants.
		Updated the notes and examples for Payment Service Providers (Aggregators) and OptBlue Participants.
	DF 60: National Use Data	Changed length of field to '20 bytes minimum, 94 bytes maximum, (LLLVAR)'
		Changed length of variable data to '91 bytes maximum, EBCDIC or Binary'.
		For subfields 3 and 4, after (Aggregators), added 'or OptBlue participant's...'.
		For Subfield 3, changed the subfield type from 'Alphanumeric' to 'Alphanumeric & special characters
		Added an example which includes Seller ID, Seller Email Address and Seller Telephone.
	DF 64: Message Authentication Code Field	Changed 'Data Field 64' to 'Data Field 128'and moved it after Data Field 96.
	DF 96: Key Management Data	For relative position 9-11, changed subfield name from 'Session Key PIN Check Value' to 'Session PIN Key Check Value'.
		Changed the description to 'Check value is to be copied from the value found in the SESSION PIN KEY CHECK VALUE subfield in Data Field 96, Key Management Data, Network Management Response (1814) message'.
		For relative position 12-14, changed subfield name from 'Session Key MAC Check Value' to 'Session MAC Key Check Value'.
		For relative position 15-17, changed subfield name from 'Session Key Data Check Value' to 'Session Data Key Check Value'.
Authorization Response (1110)	DF 60: National Use Data	Changed length of field to '20 bytes minimum, 94 bytes maximum, (LLLVAR)'
		Changed length of variable data to '91 bytes maximum, EBCDIC or Binary'.
	DF 62: Private Use Data	For the example in American Express AAV, Telephone Number and Email Address Verification Response, the VLI changed from '012AXAEYYNYY' to '009AXAEYYNYY'. In the first bullet, VLI changed from '012' to '009'.
Reversal Advice Request (1420)	DF 12: Date and Time, Location Transaction	In the description, changed the first sentence from 'This data field contains the year, month, day and local time when this transaction took place' to 'This data field contains the year, month, day and local time when the Reversal Advice Request (1420) message took place.

12.0 Revision Log (continued)

Publication: October 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Network Management Response (1814)	DF 96: Key Management Data	For Relative Positions 9-24, 25-40, 41-56, 57-59, 60-62 and 63-65, changed the subfield names to: • Session Key PIN to Session PIN Key • Session Key MAC to Session MAC Key • Session Key DATA to Session DATA Key • Session Key PIN Check Value to Session PIN Key Check Value • Session Key MAC Check Value to Session MAC Key Check Value • Session Key DATA Check Value to Session DATA Key Check Value
		For Session PIN Key Check Value, changed the description to 'Check Value is derived by American Express identifying the Session PIN Key sent in the Network Response (1814) message received from American Express. Note: This value is returned, without alteration, in the SESSION PIN KEY CHECK VALUE subfield in Data Field 96, Key Management Data, of the Authorization Response (1110) message'.
		For Session MAC Key Check Value, removed 'the POS device' and 'Acquirer System'. Changed 'Session Key MAC' to 'Session MAC Key'.
		For Session DATA Key Check Value, removed 'the POS device' and 'Acquirer System'. Changed 'Session Key DATA' to 'Session DATA Key'.
		In the note, changed subfield names to: SESSION PIN KEY CHECK VALUE, SESSION MAC KEY CHECK VALUE, and SESSION DATA KEY CHECK VALUE.
Specific Section Changes	Section 1.2 Document Changes	Under Revision Log, changed the description to 'The Revision Log is the last section in this document, and it contains a condensed overview of the changes made in the last three publications'.
	Section 1.4 Contact Information	Added new Section 1.4 Contact Information to document.
	Section 1.5 Related Documents	Added the following documents: • American Express Global Codes & Information Guide • American Express Online PIN Processing Implementation Guide for Merchants and Third Party Processors.
		For the Expresspay documents, removed the version number '2.0'.
	Section 2.1 Overview of Implementation Planning	Added a bullet for 'Global Codes & Information Guide'.
	Section 4.0 Guidelines for Using the GCAG ISO 8583 Message Formats	In the second paragraph, changed the first sentence from 'Some of the data fields can be either fixed-length and others are variable-length' to 'Data fields can be either fixed-length or variable-length'.

12.0 Revision Log (continued)

Publication: October 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes (continued)	Section 5.0 Card Acceptance Supported Services	Changed the Authorization Amount Adjustment description to 'The Authorization Amount Adjustment can be used by any Merchant, Third Party Processor or Vendor software provider that supports Automated Fuel Dispensers. This functionality allows for the release of held funds due to the actual sale amount being less than the original authorized amount'.
	Section 5.2 American Express OptBlue Program	Updated the paragraph description for clarity.
	Section 5.4.1 AEIPS	For Position 7, added a bullet for 'Transactions must not be processed using value 5 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing'.
		Added bullet for 'Position 9: Cardmember Authentication Entity- Transactions must not be processed using value 1 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing'.
		Added bullet for 'Position 10: Card Data Output Capability - Transactions must not be processed using value 3 (Integrated Circuit Card - ICC) unless the terminal and link are certified by American Express for EMV processing'.
	Section 5.4.2 Expresspay	In the paragraph following the bullets, at the end of the first sentence, added 'including the Expresspay Pseudo-Magnetic Stripe Format'. At the end of the paragraph, added reference to the Global Codes & Information Guide.
	Section 6.1 Verification Services	Changed the last sentence to 'For policy questions regarding transaction processing, refer to one or more of the following: American Express Merchant Regulations - U.S., Canada Merchant Operating Manual (MOM) - Local market Terms of Conditions/Contracts for those markets outside of the U.S. and Canada'.
	Section 6.4 Online PIN	Updated section for Online PIN to add clarity around Static and Dynamic Key Exchange.
	Section 7.0 ISO 8583 Message Bit Map Table	Removed the Secondary Bit Map restrictions.
	Section 7.1 Primary Bit Map	For DF 60, changed the max. data field length to '94 bytes, LLLVAR'.
	Section 8.1 ISO 8583 Authorization Request (1100)	For DF 60, changed the max. data field length to '94 bytes, LLLVAR'.
		Changed Message Authentication Code Field from Data Field 64 to Data Field 128 and moved it after Data Field 96.

12.0 Revision Log (continued)

Publication: October 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes (continued)	Section 8.2 ISO 8583 Authorization Response (1110)	For DF 60, changed the max. data field length to '94 bytes, LLLVAR'.
	Section 9.0 ISO 8583 Reversal Advice Request/Response Message Formats	Changed Merchant Initiated Reversals making them mandatory for U.S. Third Party Processors only.
		In the first sentence of the first bullet, changed the text in the parentheses to 'Mandatory for U.S. Third Party Processors only'.
	Section 12.0 Revision Log	Added the sentence 'The Revision Log goes back three publications, current publication plus the last two. For earlier versions, contact SpecQuestions@aexp.com'.
		Changed the first bullet to 'General - Changes made due to reorganization, clarification, consistency, or for informative purposes'.

12.0 Revision Log (continued)

Publication: April 2015 | Global Data Quality & Standards (GDQ&S) | Contact: SpecQuestions@aexp.com

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
General Changes	Cover	Changed date from 'OCTOBER 2014' to 'APRIL 2015'.
	Footer	Changed date from 'October 17, 2014' to 'April 17, 2015'.
	Copyright	Changed copyright from '2004-2014' to '2004-2015'.
	Document Clarification Request	In the second paragraph, removed the quotes around 'SpecQuestions.com'.
	Table of Contents	Moved the '1' after the word 'Guide' to the right to align with page numbers.
Specific Data Field Changes *Authorization Request (1100)*	DF 1: Bit Map - Secondary	Added new data field to document.
	DF 22: Point of Service Data Code	In POS. 5, values 4 & 9, removed the last sentence 'For more information, see page 20'.
	DF 43: Card Acceptor Name/Location	Changed this data field significantly for Payment Service Providers (Aggregators). Please read in its entirety.
	DF 52: Personal Identification Number (PIN) Data	Changed the field requirement to 'Conditional - Used only when PIN is available'.
		Added certification requirement 'Mandatory — Third Party Processors and/or Vendor software must be certified to pass data in this data element. After certification, all Merchant-provided data must be forwarded in this data element'.
		Changed the description to 'This data field is for use in markets that support online PIN verification, and it will transport encrypted PIN data for PIN-based POS transactions. Unauthorized use of this data field may cause message rejection'.

12.0 Revision Log (continued)

Publication: April 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Authorization Request (1100) (continued)	DF 53: Security Related Control Information	In the description, changed '...must be set to value "S", W" or "Y" to '...must be set to value "9", "S", "W" or "Y".
	DF 53: Security Related Control Information (continued)	In the description, in the table, added a row for '9 - Technical fallback - Transaction initiated as chip, but was processed using an alternative technology (such as magnetic stripe)'.
	DF 60: National Use Data	Changed this data field significantly for Payment Service Providers (Aggregators). Please read in its entirety.
	DF 61: National Use Data	Changed the certification requirement to 'See Section 4.3 for the website link to American Express SafeKey enabled countries'.
	DF 63: Private Use Data	In the 205-byte format examples, changed the phone number for AE and AD from '1234567890' to '5555370000'.
	DF 96: Key Management Data	Added new data field.
Authorization Response (1110)	DF 39: Action Code	In the description, added code '909-System Malfunction (Cryptographic error)'.
	DF 60: National Use Data	In length of field, changed '303 bytes maximum, (LLLVAR)' to '92 bytes maximum, (LLLVAR)'.
		In length of variable data, changed '300 bytes maximum, EBCDIC' to '89 bytes maximum, EBCDIC'.
		Changed the field requirement to Conditional - Echo returned'.
	DF 61: National Use Data	Changed the certification requirement to 'See Section 4.3 for the website link to American Express SafeKey enabled countries'.
Network Management Request (1804)	DF 24: Function Code	In the description, added '811-Dynamic Key Exchange'. Changed the sentence 'The following additional values are accepted in China only' to bold.
	DF 96: Key Management Data	Corrected spelling of data field name from 'Key Management Data' to 'Key Management Data'.

12.0 Revision Log (continued)

Publication: April 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Network Management Response (1814)	DF 1: Bit Map - Secondary	Changed the field requirement to 'Mandatory — For Data Fields 65 and 128'.
		Changed the description to 'See Bit Map - Secondary description on page 58 of the Authorization Request (1100) message'.
	DF 24: Function Code	Changed the constant from '831' to 'None'.
	DF 39: Action Code	Changed constant from '800' to 'None'.
		In the description, changed 'Valid action code' to 'Valid action codes'.
		Added the following codes: '115 = Requested function not support, 181 = Format error, and 909 = System Malfunction (Cryptographic Error)'.
	DF 96: Key Management Data	Changed this data field significantly for Payment Service Providers (Aggregators). Please review in its entirety.
Specific Section Changes	Section 1.2 Document Changes	For revision mark, added the sample revision mark in the left margin.
	Section 1.4 Related Documents	In the 2nd bullet, added '(XML GFSG)' after the document title. Changed the bullet 'American Express Card Acceptance and Processing Network Communications Guide' to 'American Express Network Communications Guide (MPLS & VPN)'.
	Section 4.3 American Express SafeKey	Originally Section 4.2.6. Changed the section number to '4.3'.
		In the second paragraph, removed the last 2 sentences and replaced with 'Refer to the following website link: 'AmexSafeKey' for the most current enablement updates'.
	Section 3.5.2 Supported File Layouts	In the table, for DF 2, changed the '1' to an '*'. In the footnote, changed the '1' to an '*'.
	3.5.2.1 Variable Length Layout	In the table, for DF 25, changed the '2' to an '*'. In the footnote, changed the '2' to an '*'.
	Section 4.3 American Express SafeKey	Originally Section 4.2.6. Changed the section number from '4.2.6' to '4.3'.
		In the second paragraph, removed the last 2 sentences and replaced with 'Refer to the following website link: 'AmexSafeKey' for the most current enablement updates'.

12.0 Revision Log (continued)

Publication: April 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes (continued)	Section 4.4 Online PIN and Dynamic Key Exchange	Added new Section 4.4 Online PIN Processing to document.
	Section 5.1 Overview of Implementation Planning	Changed the bullet 'American Express Card Acceptance and Processing Network Communications Guide' to 'American Express Network Communications Guide (MPLS & VPN)'.
	Section 5.5 Communications Options	Changed the bullet 'American Express Card Acceptance and Processing Network Communications Guide' to 'American Express Network Communications Guide (MPLS & VPN)'.
	Section 5.7.3 Network Management Request/Response	In the last paragraph, changed the first sentence to 'The Network Management Request (1804) message allows for either dynamic key exchange, an echo test or a signon/signoff request'.
	Section 6.2.1 Primary Bit Map	For DF 60: changed max. data field length from '303 bytes LLLVAR' to '92 bytes LLLVAR'.
	Section 6.2.2 Secondary Bit Map	Formatted table so the field numbers align correctly.
	Section 7.1 ISO 8583 Authorization Request (1100)	Added DF 1: Bit Map-Secondary and DF 96: Key Management Data to section.
		In the table, for DF 60: changed the max. data field length from '303 bytes LLLVAR' to '92 bytes LLLVAR'. Changed data field requirement to 'See page'.
	Section 7.2 ISO 8583 Authorization Request (1110)	In the table, for DF 60: changed the max. data field length from '303 bytes LLLVAR' to '92 bytes LLLVAR'. Changed data field requirement to 'See page'.
	Section 7.2.1 Card Identifier (CID) Verification	Remove the word 'program' from 'For more information on American Express CID/4DBC/4CSC Program, contact your American Express representative'.
	Section 8.0 ISO 8583 Reversal Advice Request/Response Formats	Changed the second paragraph to 'The Reversal Advice Request/Response (1420/1430) is mandatory for Merchant Initiated Reversals and is an optional message for System Generated Reversals'. For the two bullet points, switched the order and added '(Mandatory)' for Merchant Initiated Reversals and '(Optional)' for System Generated Reversals.

12.0 Revision Log (continued)

Publication: April 2015 (continued)

Type of Change/ Message Type	Data Field (DF)/ Section # / Title	Description
Specific Section Changes (continued)	Section 9.0 ISO 8583 Network Management Request/Responses	In the second paragraph, added information for encryption key management and signon and signoff.
	Section 9.2 ISO 8583 Network Management Response (1814)	For DF 1 and DF 96, changed the data field requirement to 'See Page'.
	Section 12.10 Network Management Request (1804) Message	In the paragraph, removed 'Are You There?'.
	Section 13.2 Certification Tests	Changed the bullet 'American Express Card Acceptance and Processing Network Communications Guide' to 'American Express Network Communications Guide (MPLS & VPN)'.
	Section 14.0 Appendix	Removed 14.8 American Express SafeKey Related Countries from the Appendix and renumbered accordingly.
	Section 14.6.2.1 Currency Code - Country/Entity Name Order	Changed the Algerian Dinar from 0 decimal places to 2 decimal places. Removed the '2' from the Notes column.
	Section 14.6.2.1 Currency Code - Country/Entity Name Order (continued)	Changed 'Lithuania' Litas to 'Euro' and code to '978'
	Section 14.6.2.2 Currency Code - Currency Name Order	Changed the Algerian Dinar from 0 decimal places to 2 decimal places. Removed the '2' from the Notes column.
		Changed 'Lithuania' Litas to 'Euro' and code to '978'
	Section 14.8 American Express SafeKey Enabled Countries	Removed section from document.
	Section 15.0 Revision Log	In October 2014 - moved the last change in data field 47 to Data Field 48.

this page intentionally left blank