EPX Data Dictionary

Public - Security Level 0

April 2025

REVISION HISTORY

Date	Version	Author(s)	Comments
2/4/16	2.0	C. Meaney	Added sections CHIP_CONDITION_CODE, E2EE, AUTH_EMV_DATA, EMV_DATA, Partial Authorizations, REASON_CODE, revised Discover AVS Codes Revised CARD_ENT_METH value descriptions, CASH_BK_AMT description, ZIP_CODE description, SPECIAL_1 value descriptions.
5/20/16	2.1	C. Meaney	Revised CASH_BK_AMT field description.
10/14/16	2.2	C. Meaney	For VMT, replaced Special_N fields with corresponding TLV fields and updated values. For MasterCard, changed rePower verbiage to Money Transfer, updated ACI values, replaced Special_N fields with corresponding TLV fields.
10/24/16	2.3	C. Meaney	Added to the description of CAVV_UCAF.
4/20/17	2.4	C. Meaney	Added EMV tags 5F24, 8A, 9F39, 9F53. Removed tag 81. Sorted tags by hexadecimal order.
4/24/17	2.5	C. Meaney	Added new OCT BAI codes to Table 18, created Table 19 for AFT BAIs. Updated Table 8 with codes 10, 84, 88, ER, ES, ET, EU, EV
5/5/17	2.6	C. Meaney	Reformatting to accommodate change from TLV_*NN* tags to TLV_SETS tag.
5/19/17	2.7	C. Meaney	Revised descriptions for ADDRESS, ZIP_CODE, AUTH_AVS, CARD_ID.
6/21/17	2.8	C. Meaney	Added chapter for convenience fees. Deleted AUTH_SHA1 tag. Added CCxN transaction types to the TRAN_TYPE section.
9/8/17	2.9	C. Meaney	Revised descriptions for AMOUNT and CASH_BK_AMT.
4/12/18	2.10	C. Meaney	Edits to ACCOUNT_NBR, ACI, BARCODE_DATA, TRACK_DATA to reference EBT. Edits to TRAN_TYPE: removed Citi from retail, added DMS MC Send, added Citi-specific section, added EBT section, amended BATCH_ID example. Added Visa Debt Repayment Program chapter.
5/30/18	2.11	C. Meaney	Added PAYMENT_INITIATION_CHANNEL and NETWORK_RESPONSE tags, clarified AUTH_RESP tag.
10/19/18	2.12	M.Billips	Added ORIG_BATCH_ID , ORIG_TRAN_NBR , ORIG_TRAN_TYPE. Edit AUTH_RESP table.
6/11/19	2.13	M.Billips	Added CONVENIENCE_FEE , 3DS V2 and 3rd Party Token tags
9/6/2019	2.14	M.Billips	Change TDS_VER tag name to TDS_VER
12/18/2019	2.15	M.Billips	Added Partial Reversals support
6/15/2020	2.16	M.Billips	Add new tags and card types
11/2/2020	2.17	M.Billips	Add new ACI values, MIT_REASON and INDUSTRY_TYPE tags

Date	Version	Author(s)	Comments
3/31/2021	2.18	M.Billips	Add new EBT response tags
7/22/2021	2.19	M. Billips	Add ACI values AH
8/13/2021	2.20	M. Billips	Add EXI_EXT tag and COF / MIT specific request & response tags
9/1/2021	2.21	M. Billips	Add REGEX
10/14/2021	2.22	M. Billips	Update TRAN_FEE tag
10/25/2021	2.23	M. Billips	Add MPOS_TYPE and indicate DIRECTORY_SERVER_TRAN_ID is required for MC 3DS v2 transactions.
2/23/2022	2.24	M. Billips	Update response codes for Credit Card / PIN Debit
5/6/2022	2.25	M. Billips	Add MC merchant advice decline codes , response tag AUTH_RESP_TEXT_ENHANCED
7/25/2022	2.26	M. Billips	Remove MIT_REASON tag, update ACI_EXT with MIT code, update COF_PERIOD
2/2/2023	2.27	M. Billips	Deprecate ACI codes, add as ACI_EXT codes. Bring data dictionary current
3/3/2023	2.28	M. Billips	Bring ACH SEC codes current
6/6/2023	2.29	M. Billips	Add AUTH_PAR response tag
10/6/2023	2.30	M. Billips	Add DEVICE_ID request tag , Add MasterCard COF / MIT to ECI_EXT
6/14/2024	2.31	M. Billips	Bring AUTH_RESP tables current
8/22/2024	2.32	M. Billips	Add ACH AUTH_RESP code 'SX'
4/8/2025	2.33	M. Billips	Add MasterCard MPG ID Support & NACHA Account Status Declines. Remove MagneSafe sections.

Contents

Request Attributes 1
Four-Part Processing Key 1
Server Post XML Example 1
Server Post HTTPS Post Example 1
Batch XML Example 1
Batch File Attributes 2
Batch XML Example 2
Detail Element 3
Field Definitions 3
Transaction Request Fields 4
ACCOUNT_NBR 4
ACI 4
ACI_EXT 5
ACTION_CODE 6
ADDENDA_1 through 10 6
ADDRESS 6
AMOUNT 7
AUTH_SOURCE 7
BARCODE_DATA 8
BATCH_ID 8
BIRTH_DATE 8
CARD_ENT_METH 9
Card Entry Method Codes 9
CARD_ID 9
Card Identification Codes 10
CASH_BK_AMT 10
CHECK_NBR 11
CHECK_TYPE 11
CHIP_CONDITION_CODE 11
CITY 12
COF_PERIOD 12
CONVENIENCE_FEE 13
COUNTRY_CODE 13
CURRENCY_CODE 14

CVV2 14
DEVICE_ID 14
DL_NBR 14
DL_STATE 15
E2EE 15
EMV_DATA 15
Allowed / Maximum EMV Fields 16
ENHANCED_TLV 19
EXP_DATE 19
FIRST_NAME 19
FOLIO_NBR 20
IDENT_NBR 20
INDUSTRY_TYPE 20
INVOICE_NBR 21
ISSUE_NBR 21
LAST_NAME 22
MAC 22
MICR_DATA 22
MICR_TYPE 22
MPG ID (Merchant Payment Gateway Identifier) 23
MPOS_TYPE 24
ORDER_NBR 24
ORIG_AUTH_AMOUNT 25
ORIG_AUTH_GUID 25
ORIG_AUTH_TRAN_IDENT 25
ORIG_BATCH_ID 26
ORIG_TRAN_NBR 26
Partial Authorizations 27
Partial Reversals 27
PAYLOAD_1 27
PAYMENT_INITIATION_CHANNEL 27
Payment Initiation Channel Indicators 28
PHONE_CELL 29
PHONE_HM 30
PHONE_WK 30
PIN_BLK 30
READER_STATUS 31
REASON_CODE 31

RECV_NAME 32
REFERENCE_NBR 32
RENTAL_NBR 32
ROUTING_NBR 33
SERVER_OPR 33
SIGNATURE 33
SIGNATURE_FORMAT 34
SOFT_DESCRIPTOR and SOFT_DESCRIPTOR_2 34
SPECIAL_1 34
STATE 35
STD_ENTRY_CLASS 35
Standard Entry Class (SEC) Codes 35
START_DATE 36
TAVV 36
TAVV_ECI 37
TAX_AMT 37
TAX_EXEMPT 38
TAX_EXEMPT Values 38
TIP_AMT 38
TRACK_DATA 38
TRAN_FEE 39
TRAN_NBR 39
TRAN_TYPE 40
Ecommerce Transaction Types 40
Retail Transaction Types 41
MOTO Transaction Types 41
Debit Transaction Types 41
EBT Transaction Types 42
ACH Transaction Types 42
TeleCheck Transaction Types 42
Banking Transaction Types 42
Special Transaction Types 43
Visa Money Transfer Transaction Types 43
MasterCard Money Transfer Transaction Types 43
Citi Private Label Transaction Types 43
USER_DATA_1 through 10 43
VERBOSE_RESPONSE 44
ZIP_CODE 44

Transaction Response Fields 45
AUTH_AMOUNT 45
AUTH_AMOUNT_REQUESTED 45
AUTH_AVAILABLE_BAL 45
AUTH_AVS 46
Visa 46
MasterCard 47
Discover 47
AMEX 47
AUTH_CARD_TYPE 48
Card Types and Codes 48
AUTH_CODE 49
AUTH_CURRENCY_CODE 49
AUTH_CVV2 49
Visa 50
MasterCard 50
Discover 50
AMEX 50
AUTH_EBT_BAL_CASH 50
AUTH_EBT_BAL_FOOD 51
AUTH_EMV_DATA 51
AUTH_GUID 52
AUTH_PAR 52
AUTH_REF_ID 52
AUTH_REF_PHONE_NBR 53
AUTH_RESP 53
ACH Response Codes 53
NACHA Account Status Declines 54
AAU Response Codes 55
Credit Card / PIN Debit Response Codes 56
PINless Debit Response Codes 67
AUTH_RESP_DETAIL 69
AUTH_RESP_TEXT 69
AUTH_RESP_TEXT_ENHANCED 70
AUTH_SPECIAL_1 70
AUTH_SPECIAL_2 70
AUTH_SPECIAL_3 71

AUTH_TRAN_DATE_GMT 71
AUTH_TRAN_IDENT 71
BATCH_ID 72
LOCAL_DATE 72
NETWORK_RESPONSE 72
LOCAL_TIME 73
ORIG_TRAN_TYPE 73
TRAN_NBR 73
TRAN_TYPE 74

PayPage and Browser Post API Request Fields 75

CANCEL_URL 75
CUSTOM_CSS_URL 75
CUSTOM_JAVASCRIPT_URL 76
FORCE_CREDIT 76
FORCE_CREDIT Values 76
INVALID_REDIRECT_URL 77
INVALID_REDIRECT_URL Error Cases 77
RECEIPT 77
RECEIPT Values 77
REDIRECT_ECHO 78
REDIRECT_ECHO Values 78
REDIRECT_NON_APPROVALS 78
REDIRECT_NON_APPROVALS Values 78
REDIRECT_URL 79
RESPONSE_ECHO 79
RESPONSE_ECHO Values 79
RESPONSE_FORMAT 80
RESPONSE_URL 80
TAC 80
TIMEOUT_REDIRECT_URL 80
TRAN_CODE 81
TRAN_GROUP 81
Specified Groups 82

Browser Post Validation Response Fields 83

BP_FIELD_ERRORS 83
BP_RESP_CODE and BP_RESP_TEXT 83
Merchant Configuration Errors 84

REDIRECT_URL Validation Errors 84
Basic Validation Errors 85
Verified by Visa and MasterCard SecureCode Request Fields 86
CAVV_RESP 86
CAVV_RESP Values 86
CAVV_UCAF 87
DIRECTORY_SERVER_TRAN_ID 87
TDS_VER 88
TOKEN_TRAN_IDENT 88
Visa Money Transfer (VMT) Request & Response Fields 89
Request Fields 89
TLV tags 89
TLV tag 007 from TLV set "SENDER" 89
TLV tag 011 from TLV set "SENDER" 89
TLV tag 012 from TLV set "SENDER" 90
TLV tag 001 from TLV set "TRAN_DATA" 90
TLV tag 005 from TLV set "TRAN_DATA" 90
REFERENCE_NBR 92
Response Fields 92
AUTH_SPECIAL_1 92
AUTH_SPECIAL_10 92
MasterCard Money Transfer Request Fields 93
Request Fields 93
ACI_EXT 93
TLV tag 001 from TLV set "TRAN_DATA" 94
Transaction fees 95
Overview 95
Platform Support: 95
Flat Fee 95
Percentage 95
Transaction Response Fields 96
AUTH_FEE 96
AUTH_FEE_TEXT 96
Client Application Management / Support: 96
Visa Debt Repayment Program 97
Request Fields 97

ACI..... 97

Request Attributes

Four-Part Processing Key

The EPX Four-Part Key consists of four attributes: CUST_NBR, MERCH_NBR, DBA_NBR, and TERMINAL_NBR. The values for these fields are required to process transactions with the EPX platform in both test and production environments. Definitions for these attributes, as well as examples of how they are used shown below.

- CUST_NBR—The sponsoring or entity level of the hierarchy with EPX / NAB.
- MERCH_NBR—The "settle to" level of hierarchy within EPX internal systems, and contains the banking account numbers for settlement, billing, and funding.
- DBA_NBR—The "doing business as" (DBA) level of hierarchy within EPX internal systems, and contains descriptor information.
- TERMINAL_NBR—The terminal (the device or solution that is processing the transactions) level of hierarchy within EPX internal systems. The terminal can be a physical device, gateway, website, virtual terminal, etc.

Server Post XML Example

```
<DETAIL CUST_NBR="1234" MERCH_NBR="1234567" DBA_NBR="1" TERMINAL_NBR="1">
…
</DETAIL>
```

Server Post HTTPS Post Example

```
CUST_NBR=1234&MERCH_NBR=1234567&DBA_NBR=1&TERMINAL_NBR=1&…
```

Batch XML Example

```
<BATCH CUST_NBR="1234" MERCH_NBR="1234567" DBA_NBR="1" TERMINAL_ NBR="1"
BATCH_ID="210901" BATCH_TRAN_COUNT="28" BATCH_TOTAL_AMOUNT="150.00">
…
</BATCH>
```

Batch File Attributes

Along with the four-part key, the XML Batch file format uses additional attributes.

NOTE: With these additional attributes, it is important to note that when creating a batch file, the BATCH_ID is used as an attribute rather than as a field element when it is used for real-time processing.

The table below provides the definitions for the additional attributes; the text below the table provides examples of their use.

Additional Attributes for Batch Files

Attribute	Description
file_id	The file_id attribute is a field that is identical to the value of the file_id that is part of the file name for the current batch file. See the Batch Processing API guide for more information on the file_id and file naming convention.
file_total_amount	The file_total_amount attribute contains the sum of all transaction amounts within the batch file.
file_tran_count	The file_tran_count attribute contains the total number of transactions within the batch file.
batch_total_amount	The batch_total_amount attribute contains the sum of all transaction amounts within the batch_id within the file.
batch_tran_count	The batch_tran_count attribute contains the total number of transactions within the batch_id within the file.

Batch XML Example

```
<FILE FILE_ID=”20210901A" FILE_TOTAL_AMOUNT="150.00" FILE_TRAN_ COUNT="28">
<BATCH CUST_NBR="1234" MERCH_NBR="1234567" DBA_NBR="1" TERMINAL_ NBR="1"
BATCH_ID="202109011" BATCH_TRAN_COUNT="20" BATCH_TOTAL_ AMOUNT="126.00">
…
</BATCH>
<BATCH CUST_NBR="1234" MERCH_NBR="7654321" DBA_NBR="1" TERMINAL_ NBR="1"
BATCH_ID="202109012" BATCH_TRAN_COUNT="8" BATCH_TOTAL_ AMOUNT="24.00">
…
</BATCH>
</FILE>
```

Detail Element

The DETAIL Element of your transaction request will have many child elements that make up the fields needed to process transactions on the EPX payment gateway. The fields required for each transaction are dependent upon which transaction type (TRAN_TYPE) you would like to use. Refer to your *Transaction Specifications* document to view a list of mandatory and optional fields to use with the transactions in your industry type.

Field Definitions

The following sections contain a complete list of available fields and descriptions for use in the EPX payment gateway. Refer to your *Transaction Specifications* document to view a list of mandatory and optional fields associated with the transactions you use.

- Transaction Request Fields
- Transaction Response Fields
- PayPage Request Fields
- Browser Post Validation Response Fields
- Verified by Visa and MasterCard SecureCode Request Fields

Transaction Request Fields

This chapter describes the fields that can be used in a transaction request to the EPX payment gateway.

ACCOUNT_NBR

The ACCOUNT_NBR field contains the account number to be acted upon during the transaction.

- Variable Type: Numeric
- Max Length: 19
- REGEX: ^([0-9,*]){4,19}$

Example:

```
<ACCOUNT_NBR>4111111111111111</ACCOUNT_NBR>
```

ACI

The Authorization Characteristics Indicator (ACI) field is used to identify specific characteristics of the transaction for the Networks. The table below describes the possible values.

ACI Values for card types

ACI Value	Description	Card Type
AC	Payment Authorization and Capture (CCxT)	Citi Private Label
AH	Return Authorization and Capture Hold	MasterCard Discover, and Visa
D	Debt Repayment / Consumer Loan	MasterCard and Visa
Q	Quasi Cash	MasterCard and Visa

NOTE: There are additional ACI values listed in the MasterCard Money Transfer and Visa Debt Repayment sections.

- Variable Type: Alphanumeric
- Max Length: 2

Example:

```
<ACI>Q</ACI>
```

ACI_EXT

The Authorization Characteristics Indicator Extension (ACI_EXT) field is used to identify additional characteristics of the transaction for the Networks. The table below describes the possible values. The below table describes the possible values.

ACI Extension Values for card types

ACI_EXT Value	Description	Card Type
AE	Estimated Amount	Discover
AF	Final Authorization	MasterCard
AO	Open Authorization	MasterCard
CA	AFD Completion Advice Host will add this to transaction based on TRAN_TYPE	Visa
CC	CryptoCurrency	MasterCard and Visa
DS	Delayed Card Sale	Discover, MasterCard, & Visa
HR	High-risk Securities	MasterCard
IA	Incremental Authorization	Visa, MC, Discover, & Amex
IP	Installment Payment	Discover, MasterCard, & Visa
NS	No Show charges	Discover, MasterCard, & Visa
PS	Partial Shipment	Discover, MasterCard, & Visa
RA	Re-authorization	Discover and Visa
RB	Recurring Billing	All card types including ACH
RS	Resubmission of Card Sale	Discover, MasterCard, & Visa
SA	Subscription/Standing Authorization	Discover, MasterCard, & Visa
UP	Unscheduled Payment	Discover, MasterCard, & Visa

If the four-part processing key requires a CVV2 value to process an authorization, sending the ACI_EXT field will override this requirement, as recurring or installment transactions do not require a CVV2 value. This field should always be submitted when performing a recurring or installment authorization or sale transactions.

This field may also be used for recurring ACH transactions with a Standard Entry Class value of WEB. Sending the field with a value of "RA" will allow the transaction to clear as recurring rather than as the default value, S (Single).

- Variable Type: Alphanumeric
- Max Length: 2

Example:

```
<ACI_EXT>RB</ACI_EXT>
```

ACTION_CODE

The ACTION_CODE field contains the action code U that indicates that the account should be updated by Visa or MasterCard. This action should be taken against an ORIG_AUTH_GUID during an Automatic Account Updater Service transaction.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<ACTION_CODE>U</ACTION_CODE>
```

ADDENDA_1 through 10

The ADDENDA_X fields, where X is a number between 1 and 10, are used in the ACH environment to attach an addendum to a transaction.

- Variable Type: Alphanumeric
- Max Length: 80

Example:

```
<ADDENDA_6>Customer Checking Account</ADDENDA_6>
```

ADDRESS

The ADDRESS field contains the street address associated with the account number. This field, along with ZIP_CODE, is part of the credit card address verification as the numeric value contained in this field will be validated against the value recorded at the issuing bank for the account when doing a credit card authorization. The response for this verification is found in the AUTH_AVS field. EPX supports all AVS formats supported by the card networks.

- Variable Type: Alphanumeric
- Max Length: 30
- REGEX: ^([a-zA-Z0-9\/\.\-_,#'&+\s\xc0-\xff]){0,30}$

Example:

```
<ADDRESS>123 My Street</ADDRESS>
```

AMOUNT

The AMOUNT field contains the positive dollar amount of funds to be moved during the transaction. The AMOUNT should be the amount of goods and service including any reference field amount; for example, TIP_AMT, TAX_AMT.

AMOUNT should not include cashback amounts.

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13

Example:

```
<AMOUNT>12.34</AMOUNT>
```

AUTH_SOURCE

The AUTH_SOURCE field should be sent with a value of OTHER when attempting to capture a transaction using an AUTH_CODE and an ORIG_AUTH_GUID that does not reference a Pre-Authorization in the EPX System. In a situation where a voice authorization is needed, this field allows a BRIC such as one from a BRIC Storage transaction to be used to reference the account information, while also using the voice authorization/approval code during the transaction.

Example:

```
<AUTH_SOURCE>OTHER</AUTH_SOURCE>
```

BARCODE_DATA

The BARCODE_DATA field contains the data produced from a barcode scan. This field must be sent with CARD_ENT_METH value of "A" and supports non-encrypted PAN or Visa TLV formats. The value for the BARCODE_DATA tag must be formatted as described in the following table.

Position	Size	Format type	Description
1 - 3	3	numeric	Type • 000 = PAN - No encryption • 001 = Visa TLV - No encryption
4 - N	Variable	ANS	Barcode data

- REGEX: ^([0-9A-Fa-f]){4,1024}$

Consider an example where the barcode scan of a PAN (with no encryption) returns 3123456789012345678. The data that follows shows how this result needs to be submitted to EPX.

```
<BARCODE_DATA>0003123456789012345678</BARCODE_DATA>
<CARD_ENT_METH>A</CARD_ENT_METH>
```

BATCH_ID

The BATCH_ID field contains a unique number created by the operator to identify a batch of transactions. This field works in conjunction with the TRAN_NBR field. The same BATCH_ID/TRAN_NBR combination cannot be used more than once under a single merchant number (MERCH_NBR). Commonly, this field contains the date in a number format, which groups the transactions into a daily batch.

- Variable Type: Numeric
- Max Length: 10
- REGEX: ^([0-9]){0,10}$

Example:

```
<BATCH_ID>180412</BATCH_ID>
```

BIRTH_DATE

The BIRTH_DATE field is an optional field that contains the birth date of the customer associated with the account number for the transaction.

- Variable Type: Numeric
- Format: MMDDYYYY
- Max Length: 8

Example:

```
<BIRTH_DATE>11261980</BIRTH_DATE>
```

CARD_ENT_METH

The CARD_ENT_METH field is used to indicate how the card number was entered for the transaction.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<CARD_ENT_METH>X</CARD_ENT_METH>
```

Card Entry Method Codes

- A—Used when scanning a Bar Code
- B—OCR
- D—Used when sending Swiped Track 2 data
- E—Key Entered Card Number via Ecommerce
- G—Chip (EMV contact)
- H—Used when sending Swiped Track 1 data
- M—Used when sending MICR data
- Q—Proximity / Contactless MSD non-EMV (Track 2 data is required)
- R—Proximity / Contactless EMV-based (Track 2 data is required)
- T—Token from third party
- X—Key Entered MICR or Card Number (Typed in using keyboard or keypad)
- Z—BRIC/GUID Token Transaction
- 0—Used when sending Key Entered Card data from MagneSafe 1.x Reader (Legacy)
- 1—Used when sending Encrypted Track 1 data from MagneSafe 1.x Reader (Legacy)
- 2—Used when sending Encrypted Track 2 data from MagneSafe 1.x Reader (Legacy)
- 3—Used when sending Encrypted Track 1 and 2 data from MagneSafe 2.x Reader (Legacy)
- 4—Mobile Commerce (mCommerce) / Digital Wallet (Discover Only)
- 5—PAN Auto Entry via Server (issuer, acquirer, or third party vendor system)
- 6—PAN Entry via COF (Merchant's Card On File)

CARD_ID

The CARD_ID field contains the code that represents the industry used for the transaction requested.

- Variable Type: Alphanumeric
- Max Length: 1

Example:

```
<CARD_ID>P</CARD_ID>
```

Card Identification Codes

Following are the possible Card Identification Codes:

- 0—CARDHOLDER PRESENT
- 1—CARDHOLDER NOT PRESENT
- M—CARDHOLDER PRESENT, Card not readable
- T—Discover "PayButton"
- P—PIN (online PIN)

If no value is supplied, the industry default applies.

CASH_BK_AMT

The amount specified in the CASH_BK_AMT field is added to the transaction amount indicated in the AMOUNT field when the request is sent to the networks for approval. For example, for a purchase transaction with an AMOUNT containing $20.00 and a cash-back amount (CASH_BK_AMT) containing $10.00, the amount (AUTH_AMOUNT_REQUESTED) is sent to the networks as a total of $30.00.

Partial approvals do not apply for the cash back amount. EPX includes the approved total amount in response tag AUTH_AMOUNT.

Note: CASH_BK_AMT is not a reference field

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13

Example:

```
<CASH_BK_AMT>10.00</CASH_BK_AMT>
```

CHECK_NBR

The CHECK_NBR field contains the check number associated to with an ACH transaction.

- Variable Type: Numeric
- Max Length: 8

Example:

```
<CHECK_NBR>1402</CHECK_NBR>
```

CHECK_TYPE

The CHECK_TYPE field contains the type of check being read during a TeleCheck transaction.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<CHECK_TYPE>M</CHECK_TYPE>
```

Possible values:

- P—Consumer/Business
- C—Company
- X—Travelers
- S—Payroll
- M—Cash
- T—Two Party
- G—Government

CHIP_CONDITION_CODE

The CHIP_CONDITION_CODE tag is used to indicate the reason for the EMV fallback transaction. EMV fallback transactions are presented as a standard swipe transaction and the CHIP_CONDITION_CODE must be present and set to the appropriate value.

CHIP_CONDITION_CODE Values

Value	Description
0	Not applicable to fallback transactions. For VSDC transactions must be '0'
1	Transaction was initiated from a magnetic stripe with a service code beginning with 2 or 6 and the last read at VSDC terminal was a successful chip read or was not a chip transaction.

Value	Description
2	Transaction was initiated at a chip-capable terminal from a magnetic stripe that contains service code 2 or 6, and the previous transaction initiated by that terminal was an unsuccessful chip read.

- Variable Type: Numeric
- Max Length: 1

Example:

```
<CHIP_CONDITION_CODE>2</CHIP_CONDITION_CODE>
```

CITY

The CITY field contains the city associated with the account number for the transaction.

- Variable Type: Alphanumeric
- Max Length: 25
- REGEX: ^([a-zA-Z0-9\/\.\-_,#'&+\s\xc0-\xff]){0,25}$

Example:

```
<CITY>Phoenix</CITY>
```

COF_PERIOD

The COF_PERIOD tag is used to indicate a base transaction for Card on File and Merchant Initiated Transactions. The COF_PERIOD tag designates the BRIC / GUID as COF / MIT and the number of months to keep the BRIC / GUID available for usage. This tag is only used during the base transaction request or customer initiated transaction. All subsequent COF / MIT transactions should not contain this tag.

- If COF_PERIOD is not supplied with "CCx0" AVS Only, "CCx1" Sale, and "CCx2" Auth Only transactions, EPX will by default mark as COF with the standard 13 month life usage window.
- If COF_PERIOD is supplied with a value of 1 – 24, EPX will mark as COF with the numeric value indicating the amount of months the BRIC / GUID will be available for usage. If the EPX BRIC / GUID is used within the initially specified window of time, EPX will reset the usage window to the original requested number of months; essentially restoring it with a new life cycle.
- If COF_PERIOD is supplied with a value of "0", EPX will ***NOT*** mark as COF. The BRIC can only be used to perform "CCx4" Capture Only, "CCx7" Reversal, "CCx9" Return, and "CCxX" Void transactions. The BRIC cannot be used to process any new "CCx0" AVS Only, "CCx1" Sale, and "CCx2" Auth Only transactions. The cardholder must provide their account information to process new transactions with the ACCOUNT_NBR, EXP_DATE, and CVV2.

The table below indicates the possible values and usage for COF_PERIOD.

COF_PERIOD Values

Value	Description
0	Specifies the transaction will ***NOT*** be sent out with the COF indicator to the Networks and the BRIC cannot be used to process any new AVS, Auth Only, or Sale transactions.
1 - 24	Specifies the amount of months the EPX BRIC / GUID is available for usage.

- Variable Type: Numeric
- Max Length: 2
- REGEX: ^([1-9] | 1[0-9] | 2[0-4]){0,1}$

Example:

```
<COF_PERIOD>24</COF_PERIOD>
```

CONVENIENCE_FEE

The CONVENIENCE_FEE field is a reference field that contains the convenience fee amount which is included in the amount of the transaction. This field does not get added to the AMOUNT field during the transaction, it is only referencing the convenience fee amount already included. The client application is responsible for adding the convenience fee into the total AMOUNT prior to initiating the transaction request.

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13

Example:

```
<CONVENIENCE_FEE>3.50</CONVENIENCE_FEE>
```

COUNTRY_CODE

The COUNTRY_CODE field contains the standard ISO code used to identify the country of card origination. For example, USA (United States of America) has a code of 840 which is also the numeric code for US (United States).

- Variable Type: Numeric
- Max Length: 3

Example:

```
<COUNTRY_CODE>840</COUNTRY_CODE>
```

CURRENCY_CODE

The CURRENCY_CODE field contains the standard ISO code used to identify the type of currency in the AMOUNT field. For example, USD (US Dollar) has a code of 840 which is also the numeric code for US (United States).

- Variable Type: Numeric
- Max Length: 3

Example:

```
<CURRENCY_CODE>840</CURRENCY_CODE>
```

CVV2

The CVV2 field contains the credit card's CVV2 number.

- Variable Type: Numeric
- Max Length: 4
- REGEX: ^([0-9]){3,4}$

Example:

```
<CVV2>123</CVV2>
```

DEVICE_ID

The DEVICE_ID field is used to provide the unique ID of the physical device that's initiating the transaction.

- Variable Type: alphanumeric
- Max Length: 40
- REGEX: ^([a-zA-Z0-9-.]){0,40}$

Example:

```
<DEVICE_ID>ajh-kfmkq-nrnjsp</DEVICE_ID>
```

DL_NBR

The DL_NBR field contains the customer's driver's license number during a TeleCheck transaction.

- Variable Type: Alphanumeric
- Max Length: 22

Example:

```
<DL_NBR>A123456789</DL_NBR>
```

DL_STATE

The DL_STATE field contains the state that the customer's driver's license was issued in during a TeleCheck transaction.

- Variable Type: Alpha
- Max Length: 2

Example:

```
<DL_STATE>DE</DL_STATE>
```

E2EE

The E2EE tag (End to End Encryption) identifies which type of encryption is in use. Use this tag in correspondence with the CARD_ENT_METH tag.

Valid values are as follows:

E2EE value	Description
0	Use CARD_ENT_METH tag to identify Format
1	MagTek V2 Format
2	3DES Format (generic)

- Variable Type: Numeric
- Max Length: 1

Example:

```
<E2EE>2</E2EE>
```

EMV_DATA

The EMV_Data tag contains the request data from the EMV kernel as a variable list of tags and their data in TLV format.

- Variable Type: Alphanumeric
- Max Length: 510

Example:

```
<EMV_DATA>9F34030200009F260828BF9D3AFCC8DD529F2701809F1008010103A0000000009F37044A
BAA8C49F3602008595054040040000820258009F3303E0F8C89F1A0208409F3501229F1E0832323135
333731309F03060000000000009A031504309C01009F02060000000010005F2A0208409F090200025F
3401009F4104000000039F0607A0000000041010</EMV_DATA>
```

Allowed / Maximum EMV Fields

The maximum length for the EMV_DATA tag is 510 bytes.

NOTE: The table below provides all EMV fields that EPX will accept. Not every transaction will contain all of these fields. If the field is present in the EMV data and is referenced in the table, include it in the EMV_DATA tag in any order. **Do not** include a field that is **not** present in the following table**Error! Reference source not found.**.

Allowed EMV fields

Field	Max Length (byte)	Field Name	Field Description
71	Variable	Issuer Script Template 1	Contains proprietary issuer data for transmission to the ICC before the second GENERATE AC command. *Tag data is normally in the response from the issuer. (Usually not included in the EMV data from the card, however EPX will allow this in the door if by chance it is)
72	Variable	Issuer Script Template 2	Contains proprietary issuer data for transmission to the ICC after the second GENERATE AC command Tag data is normally in the response from the issuer. (Usually not included in the EMV data from the card, however EPX will allow this in the door if by chance it is)
82	8	Application Interchange Profile	Indicates the capabilities of the card to support specific functions in the application
84	20	Dedicated File (DF) Name	Identifies the name of the DF as described in ISO/IEC 7816-4
8A	2	Authorization Response Code (ARC)	Data element generated by the Issuer Host System or the Reader indicating the disposition of the transaction.
91	20	Issuer Authentication Data	
95	14	Terminal Verification Results	Status of the different functions as seen from the terminal

Field	Max Length (byte)	Field Name	Field Description
9A	10	Transaction Date	Local date that the transaction was authorized
9C	6	Transaction Type	Indicates the type of financial transaction, represented by the first two digits of ISO 8583:1987 Processing Code
C0	Var	Secondary PIN Block	Visa specific, Secondary PIN Block
5F24	6	Application Expiration Date	Date after which the card application expires. (*YYMMDD*)
5F2A	10	Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217
5F34	8	Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards with the same PAN
9F02	18	Amount, Authorized (Numeric)	Authorized amount of the transaction (excluding adjustments)
9F03	18	Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cashback amount
9F06	38	Application Identifier (AID) – terminal	Identifies the application as described in ISO/IEC 7816-5
9F07	10	Application Usage Control (AUC)	Indicates issuer's specified restrictions on the geographic usage and services allowed for the card application.
9F09	10	Application Version Number	Version number assigned by the payment system for the application
9F10	70	Issuer Application Data	Contains proprietary application data for transmission to the issuer in an online transaction
9F1A	10	Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166
9F1E	22	Interface Device (IFD) Serial Number	Unique and permanent serial number assigned to the IFD by the manufacturer
9F26	22	Application Cryptogram	Cryptogram returned by the ICC in response of the GENERATE AC command

Field	Max Length (byte)	Field Name	Field Description
9F27	8	Cryptogram Information Data	Indicates the type of cryptogram and the actions to be performed by the terminal
9F33	12	Terminal Capabilities	Indicates the card data input, CVM, and security capabilities of the terminal
9F34	12	Cardholder Verification Method (CVM) Results	Indicates the results of the last CVM performed
9F35	8	Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control
9F36	10	Application Transaction Counter (ATC)	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)
9F37	14	Unpredictable Number	Value to provide variability and uniqueness to the generation of a cryptogram
9F39	2	Point-of-Service (POS) Entry Mode	Indicates the method by which the PAN was entered, according to the first two digits of the ISO POS Entry Mode
9F41	14	Transaction Sequence Counter	Counter maintained by the terminal that is incremented by one for each transaction
9F53	2	Transaction Category	MasterCard specific, Transaction Category Code 9F53
9F5B		Issuer Script Results	Indicates the results of Issuer Script processing. When the reader/terminal transmits this data element to the acquirer, in this version of Kernel 3, it is acceptable that only byte 1 is transmitted, although it is preferable for all five bytes to be transmitted.
9F6E	4	Form Factor Indicator (qVSDC)	Indicates the form factor of the consumer payment device and the type of contactless interface over which the transaction was conducted. This information is made available to the issuer host.
9F7C	32	Customer Exclusive Data (CED)	Contains data for transmission to the issuer. Note: This tag is contained in U.S. contactless transactions and contains issuer proprietary information in TLV format. The tag is personalized on the card or device. If present in an interregional transaction, the tag is treated as supplemental data.

ENHANCED_TLV

The ENHANCED_TLV field contains enhanced / level III data in TLV format. Reference the *EPX Data Dictionary – Enhanced / Level II & III Data* for additional information.

- Variable Type: Alphanumeric
- Format: TLV
- Max Length: 2000

Example:

```
<ENHANCED_TLV>0010006VISA_G00200510010009CUSTCODE7005000523.0000900038400110006031
42200300900010007COMCODE0020009ITEM,DESC0030008PRODCODE004000130050004EACH00600063
00.000100006600.00</ENHANCED_TLV>
```

EXP_DATE

The EXP_DATE field contains the credit card's expiration date.

- Variable Type: Numeric
- Format: YYMM
- Max Length: 4
- REGEX: ^(([0-9][0-9](0[1-9] | 1[0-2])) | 0000)$

Example:

```
<EXP_DATE>2104</EXP_DATE>
```

NOTE: This example represents April 2021.

FIRST_NAME

The FIRST_NAME field contains the first name the customer associated with the account number for the transaction.

- VariableType: Alpha
- Max Length: 25

Example:

```
<FIRST_NAME>John</FIRST_NAME>
```

FOLIO_NBR

The FOLIO_NBR field is an optional field that contains the folio number of the customer associated with the account number for the transaction.

- Variable Type: Alphanumeric
- Max Length: 25

Example:

```
<FOLIO_NBR>1582</FOLIO_NBR>
```

IDENT_NBR

The IDENT_NBR field is an optional field that the merchant can use to store an identification number related to the transaction.

- Variable Type: Alphanumeric
- Max Length: 15

Example:

```
<IDENT_NBR>765412</IDENT_NBR>
```

INDUSTRY_TYPE

The use of the INDUSTRY_TYPE tag allows any Retail, CAT, Banking, ECOM, or MOTO transaction to be sent to the same 4-part key and eliminates the need to use unique TERMINAL_NBR(s) configured specifically for each industry type.

If the INDUSTRY_TYPE tag is not present in the request, the EPX platform will determine the best value to use based on the rest of the items in the request, specifically TRAN_TYPE.

The INDUSTRY_TYPE value has the following effects:

- For the credit card transaction class, the INDUSTRY_TYPE value will override the industry code value found in all credit card class "CCIx" TRAN_TYPE(s), where "I" is the industry type.
- For all other transaction classes (CK, DB, EB, SS, SM, and SV), which do not have the industry code embedded, the INDUSTRY_TYPE value will determine the proper POS characteristics for each transaction.

The table below indicates the TRAN_TYPE values with the corresponding INDUSTRY_TYPE value mapping and descriptions.

	INDUSTRY_TYPE	
TRAN_TYPE industry code	**INDUSTRY_TYPE value mapping**	**INDUSTRY_TYPE description**
C, B, R	P	Cardholder Present (Retail, CAT, Banking)
E	E	ECOM
M	M	MOTO

- Variable Type: Alpha
- Max Length: 1
- REGEX: ^([EMP]){1}$

Example:

```
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
```

INVOICE_NBR

The INVOICE_NBR field is an optional field that will contain the invoice number of the customer associated with the account number for the transaction.

- Variable Type: Alphanumeric
- Max Length: 25

Example:

```
<INVOICE_NBR>12354</INVOICE_NBR>
```

ISSUE_NBR

The ISSUE_NBR field contains the credit card's issue number. This is commonly found on Maestro, Switch, or Solo credit cards that have been re-issued and may be required when processing such card types.

- Variable Type: Numeric
- Max Length: 3

Example:

```
<ISSUE_NBR>2</ISSUE_NBR>
```

LAST_NAME

The LAST_NAME field contains the last name the customer associated with the account number for the transaction.

- Variable Type: Alpha
- Max Length: 25

Example:

```
<LAST_NAME>Doe</LAST_NAME>
```

MAC

The MAC field contains either the Merchant Authorization Code (PayPage) or the TIC value generated by EPX. The MAC can also be enabled in the Merchant Profile as a required field for API processing. The MAC would then need to be sent with transactions in addition to the 4-part key.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
MAC=pZCt1KnhTZQbSl1V5tfo4Y51AR35sfus
```

MICR_DATA

The MICR_DATA field contains the MICR data in raw TOAD MICR format from the check being scanned at the register.

NOTE: EPX cannot support MICR data from business checks that have an Auxiliary On-Us field present. EPX cannot support any check greater than $25,000.

- Variable Type: Alphanumeric

Example:

```
<MICR_DATA>T999999991T      12345678900 1234</MICR_DATA>
```

MICR_TYPE

The MICR_TYPE field contains the type of MICR being sent when processing a TeleCheck transaction.

- VariableType: Numeric
- Max Length: 2

Example:

```
<MICR_TYPE>09</MICR_TYPE>
```

Possible Values:

- 09—Raw MICR
- 14—Canadian Manual MICR
- 18—Routing and Account Number Only
- 19—Manual MICR

MPG ID (Merchant Payment Gateway Identifier)

The MasterCard MPG ID (Merchant Payment Gateway Identifier) is used to identify the gateway or processing solution that is initiating card not present transactions. The MC MPG ID value can be dynamically included with transaction requests by utilizing the TLV_SETS API tag with data set "NETWORK" & TLV tag "008" (MC MPG ID). The table below contains specific details including a sample of the TLV string.

Note: If the MPG ID is not included with MasterCard transaction requests, the EPX platform will use a default value. This is intended specifically for card not present transactions. The gateway or processing solution will need to register directly with MasterCard to obtain a unique value indicator.

MC MPG ID – TLV_SETS “NETWORK”

TLV Tag	TLV Data	TLV Max Data	REGEX	Request	Response	Additional Details
000	DATA_SET= NETWORK					
008	MasterCard MPG ID (merchant payment gateway ID)	numeric..11	^([0-9]){1,11}$	If present it will be included with MasterCard transactions.	NA	The MPG ID is included with MC authorizations and will not be echoed back in the response
Example of NETWORK request information in TLV format - MC MPG ID						
Tag = 000; Value = "NETWORK"						**TLV Element = "000007NETWORK"**
Tag = 008; Value = "7654321" (MC MPG ID)						**TLV Element = "0080077654321"**
Total length of the TLV elements is 26						
TVL_SETS = "0026000007NETWORK0080077654321"						

- Variable Type: Numeric
- Max Length: 11

Example:

```
<TLV_SETS>0026000007NETWORK0080077654321</TLV_SETS>
```

MPOS_TYPE

The mPOS Type field is used to indicate the type of reader used by the mPOS device. This field is required for all card brands for transactions that are initiated from a true mPOS device. An mPOS device is not a terminal, rather a mobile device that is running a payment app and possibly using an external reader of some type. The table below describes the possible values.

Note: The EPX platform will add new values as they are provided by the Networks to define each type of mPOS reader.

mPOS values

mPOS Value	Description
0	AC - mPOS Accessory/dongle with contact and contactless interfaces, with or without PIN pad.
1	AS - mPOS Accessory/dongle with contact and contactless interfaces and PIN on Glass support (SCRP, Software-based PIN on COTS).
2	CC - Contactless Payment on COTS (CPoC) - Mobile device based contactless only mPOS without PIN support.
3	CS - Contactless Payment on COTS (CPoC) - Mobile device based contactless only mPOS with PIN on Glass support

- Variable Type: AlphaNumeric
- Max Length: 3
- REGEX: ^([0-3]){1}$

Example:

```
<MPOS_TYPE>0</MPOS_TYPE>
```

ORDER_NBR

The ORDER_NBR field is an optional field that will contain the order number of the customer associated with the account number for the transaction.

- Variable Type: Alphanumeric

- Max Length: 25

Example:

```
<ORDER_NBR>65421</ORDER_NBR>
```

ORIG_AUTH_AMOUNT

The ORIG_AUTH_AMOUNT tag contains the original authorization amount that was returned in the AUTH_AMOUNT response tag from the original base Card on File CCx0 AVS, CCx1 Sale, and CCx2 Auth Only transaction requests. EPX will include this value in the COF / MIT authorization request to the Networks.

Note: This tag is specifically used to support PAN based COF / MIT transactions, and is non-applicable to EPX BRIC / GUID based COF / MIT transactions.

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13
- REGEX: ^(([0-9]){1,12}?(\.[0-9]{0,4}) | ([0-9]){0,12}?(\.[0-9]{1,4}))$

Example:

```
<ORIG_AUTH_AMOUNT>77.00</ORIG_AUTH_AMOUNT>
```

ORIG_AUTH_GUID

The ORIG_AUTH_GUID field contains the BRIC/GUID (Globally Unique Identifier) of the original transaction being referenced in the current transaction. This field is used in transactions such as a capture of an existing authorization or the void of an existing unsettled sale. This field is also used when doing a BRIC/GUID-based token transaction such as a new Authorization or Sale.

- Variable Type: Alphanumeric
- Max Length: 20

Example:

```
<ORIG_AUTH_GUID>0V7017HDJXK00PNZKBE</ORIG_AUTH_GUID>
```

ORIG_AUTH_TRAN_IDENT

The ORIG_AUTH_TRAN_IDENT tag contains the NTID (Network Transaction ID) value that was returned in the AUTH_TRAN_IDENT response tag from the original base Card on File CCx0 AVS,

CCx1 Sale, and CCx2 Auth Only transaction requests. EPX will include this value in the COF / MIT authorization request to the Networks.

Note: This tag is specifically used to support PAN based COF / MIT transactions, and is non-applicable to EPX BRIC / GUID based COF / MIT transactions.

- Variable Type: Alphanumeric
- Max Length: 20
- REGEX: ^([A-Z0-9]){0,20}$

Example:

```
<ORIG_AUTH_TRAN_IDENT>210817175754976</ORIG_AUTH_TRAN_IDENT>
```

ORIG_BATCH_ID

The ORIG_BATCH_ID field contains the BATCH_ID from the original Purchase transaction. This field is currently required in all Food Stamp Return (EB01) request messages. However, based on Underwriting / Risk rules, in some circumstances a merchant account may require this tag to be present in all Return/Refund request messages (beyond EBT transactions). Additionally, one or more card networks might mandate the use of this tag in the future.

- Variable Type: Numeric
- Max Length: 10
- REGEX: ^([0-9]){1,10}$

Example:

```
<ORIG_BATCH_ID>123</ORIG_BATCH_ID>
```

ORIG_TRAN_NBR

The ORIG_TRAN_NBR field contains the TRAN_NBR from the original Purchase transaction. This field is currently required to be included in all Food Stamp Return (EB01) request messages. However, based on Underwriting / Risk rules, in some circumstances a merchant account may require this tag to be present in all Return/Refund request messages (beyond EBT transactions). Additionally, one or more card networks might mandate the use of this tag in the future.

- Variable Type: Numeric
- Max Length: 10
- REGEX: ^([0-9]){1,10}$

Example:

```
<ORIG_TRAN_NBR>17</ORIG_TRAN_NBR>
```

Partial Authorizations

The Partial Authorization capability is enabled and disabled through a merchant account profile setting. It is imperative that the merchant profile be set up completely for partial approvals/authorizations. The merchant must specify this capability during the initial merchant set up process.

For a Partial Authorization, the transaction response contains an AUTH_RESP value of 10 with the partial amount approved reflected in the AUTH_AMOUNT tag.

To generate the response in the UAP Test environment, use the test trigger cards with the amount of 1.59.

Partial Reversals

The Partial Reversal is to allow the merchant to make a correction on an open Sale CCx1 or a non-captured CCx2 Authorization Only prior to settlement. The amount specified in the AMOUNT request tag will be the actual amount that will remain authorized, i.e. the amount the corrected Authorization should be.

For example, the original transaction Authorization AMOUNT was for 150.00 and the corrected/final transaction amount is 120.00. The partial CCx7 reversal request would be sent with an AMOUNT of 120.00.

PAYLOAD_1

The PAYLOAD_1 field is used for generic payload information for specific transactions.

- Variable Type: Alphanumeric
- Format: Base64

Example:

```
<PAYLOAD_1>IkZvcmQsIiBoZSBzYWlkLCAieW91J3JlIHR1cm5pbaW4uIFN0b3AgaXQuIg</PAYLOAD_1>
```

PAYMENT_INITIATION_CHANNEL

The MasterCard Payment Initiation Channel provides information about the device type used to identify mobile-initiated, MSD Contactless, and EMV Contactless-based transactions. Contactless-enabled applications are required to transmit the device type indicator value for MasterCard transactions in the Sale or Authorization request POST messages.

This field will indicate the type of device used at the terminal. In the scope of EMV transactions it must be populated using the device type field value from tag 9F6E.

This is required for MasterCard Contactless transactions containing the below Card Entry Methods:

- **Q**—Proximity / Contactless MSD non-EMV (Track 1 or Track 2 allowed)
- **R**—Proximity / Contactless EMV-based (Track 2 data is required)
- Variable Type: Numeric
- Fixed Length: 2
- REGEX: ^([0-9]){1,2}$

Example:

```
<PAYMENT_INITIATION_CHANNEL>21</PAYMENT_INITIATION_CHANNEL>
```

Payment Initiation Channel Indicators

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

- 00—Card
- 01—Mobile Network Operator (MNO) controlled removable secure element (SIM or UICC) personalized for use with a mobile phone or smartphone
- 02—Key Fob
- 03—Watch using a contactless chip or a fixed (non-removable) secure element not controlled by the MNO
- 04—Mobile Tag
- 05—Wristband
- 06—Mobile Phone Case or Sleeve
- 07—Mobile phone or smartphone with a fixed (non-removable) secure element controlled by the MNO, for example, code division multiple access (CDMA)
- 08—Removable secure element not controlled by the MNO, for example, memory card personalized for used with a mobile phone or smartphone
- 09—Mobile Phone or smartphone with a fixed (non-removable) secure element not controlled by the MNO
- 10—MNO controlled removable secure element (SIM or UICC) personalized for use with a tablet or ebook
- 11—Tablet or e-book with a fixed (non-removable) secure element controlled by the MNO
- 12—Removable secure element not controlled by the MNO, for example, memory card personalized for use with a tablet or e-book
- 13—Tablet or e-book with fixed (non-removable) secure element not controlled by the MNO
- 14—Mobile phone or smartphone with a payment application running in a host processor
- 15—Tablet or e-book with a payment application running in a host processor

- 16—Mobile phone or smartphone with a payment application running in the Trusted Execution Environment (TEE) of a host processor
- 17—Tablet or e-book with a payment application running in the TEE of a host processor
- 18—Watch with a payment application running in the TEE of a host processor
- 19—Watch with a payment application running in a host processor

NOTE: Values from 20–33 exclusively indicate the form factor only, without also indicating the storage technology.

- 20—Card
- 21—Phone: Mobile phone
- 22—Tablet/e-reader: Tablet computer or e-reader
- 23—Watch/Wristband: Watch or wristband, including a fitness band, smart strap, disposable band, watch add-on, and security/ID band
- 24—Sticker
- 25—PC: PC or laptop
- 26—Device Peripheral: Mobile phone case or sleeve
- 27—Tag: Key fob or mobile tag
- 28—Jewelry: Ring, bracelet, necklace, and cuff links
- 29—Fashion Accessory: Handbag, bag charm, and glasses
- 30—Garment Dress
- 31—Domestic Appliance: Refrigerator, washing machine
- 32—Vehicle: Vehicle, including vehicle attached devices
- 33—Media/Gaming Device: Media or gaming device, including a set top box, media player, and television

PHONE_CELL

The PHONE_CELL field is an optional field that contains the cell phone number of the customer associated with the account number for the transaction.

- Variable Type: Numeric
- Max Length: 10

Example:

```
<PHONE_CELL>3025551234</PHONE_CELL>
```

PHONE_HM

The PHONE_HM field is an optional field that contains the home phone number of the customer associated with the account number for the transaction.

- Variable Type: Numeric
- Max Length: 10

Example:

```
<PHONE_HM>3025551234</PHONE_HM>
```

PHONE_WK

The PHONE_WK field is an optional field that contains the work phone number of the customer associated with the account number for the transaction.

- Variable Type: Numeric
- Max Length: 10

Example:

```
<PHONE_WK>3025551234</PHONE_WK>
```

PIN_BLK

The data provided within the PIN_BLK field should be the 16-character hexadecimal encrypted pin block (EPD) followed by the DUKPT key serial number KSN. Depending on the specific PIN entry device (PED) this data may need to be reformatted.

Example:

```
EPB = 1B9C1845EB993A7A KSN = FFFF9876543210E00001
PIN_BLK = 1B9C1845EB993A7AFFFF9876543210E00001
```

READER_STATUS

The READER_STATUS field contains the status of the MICR Reader when processing a TeleCheck transaction.

- Variable Type: Alphanumeric
- Max Length: 3

Example:

```
<READER_STATUS>15</READER_STATUS>
```

Possible Values:

- 15—Valid read by MICR Reader
- 15I—Valid read by MICR Reader
- 3—Mag ink present but failed read
- 5—No Mag ink present
- 9—Manual only – No read attempts

REASON_CODE

The REASON_CODE field is used to indicate the reason for the reversal of an EMV-based transaction approval.

REASON_CODE Values

REASON_CODE	Description
0	User Cancel
1	Error Condition

- Variable Type: Numeric
- Max Length: 1

Example:

```
<REASON_CODE>1</REASON_CODE>
```

RECV_NAME

The RECV_NAME field contains the customer's full name associated with the account number for an ACH transaction.

- Variable Type: Alpha
- Max Length: 22

Example:

```
<RECV_NAME>John Doe</RECV_NAME>
```

REFERENCE_NBR

The REFERENCE_NBR field is a required field for PIN-less Debit transactions that contain the consumer's account information, such as electrical, telephone, loan, or policy number for the bill that is being paid during the transaction.

- Variable Type: Alphanumeric
- Max Length: 25

Example:

```
<REFERENCE_NBR>12345678</REFERENCE_NBR>
```

RENTAL_NBR

The RENTAL_NBR field is an optional field that contains the rental number of the customer associated with the account number for the transaction.

- Variable Type: Alphanumeric
- Max Length: 25

Example:

```
<RENTAL_NBR>4512</RENTAL_NBR>
```

ROUTING_NBR

The ROUTING_NBR field contains the Bank's routing number associated with the account number for an ACH transaction.

- Variable Type: Numeric
- Max Length: 9

Example:

```
<ROUTING_NBR>031100092</ROUTING_NBR>
```

SERVER_OPR

The SERVER_OPR field is an optional field that contains the user name of the person running the application that is submitting the transaction.

- Variable Type: Alpha
- Max Length: 25

Example:

```
<SERVER_OPR>JDoe</SERVER_OPR>
```

SIGNATURE

The SIGNATURE field is an electronic representation of the signature, most often binary code, which is Base64 encoded so it can be transmitted over the Internet. Refer to the *Signature Capture Transaction Specifications* document for information on how and when to use the SIGNATURE field.

- Variable Type: Alphanumeric
- Max Length: 8k

Example:

```
<SIGNATURE>[Base64 encoded data]</SIGNATURE>
```

SIGNATURE_FORMAT

The SIGNATURE_FORMAT field is used to represent the actual device that captured the transaction, since each device may have its own proprietary format for the signature data. EPX is currently coded for the following formats: OPOS (Open Point of Sale) is an attempt to standardize message formats, interfaces, etc. for different hardware vendors, so that one API can be used among multiple devices; FPE (Forms Processing Engine) is proprietary to Hypercom Inc.

- Variable Type: Numeric (0 = OPOS Format, 1 = FPE Format, 2 = Ingenico, 3 = MagTek IPAD)
- Max Length: 3

Example:

```
<SIGNATURE_FORMAT>0</SIGNATURE_FORMAT>
```

SOFT_DESCRIPTOR and SOFT_DESCRIPTOR_2

The SOFT_DESCRIPTOR fields contain replacement descriptor information that will be used when the field is sent in with a transaction, rather than using the default descriptor set up in the merchant's profile. This is commonly used when a merchant is using the same four-part key for a number of DBAs. In order for you to use this field, your profile must be set up in production.

Refer to the *Soft Descriptors User's Manual* for more information on the use of these fields. Contact the EPX Integration Team if this manual was not part of your integration package.

- Variable Type: Alpha
- Max Length: 40

Example:

```
<SOFT_DESCRIPTOR>Jac D's Construction</SOFT_DESCRIPTOR>
```

SPECIAL_1

The SPECIAL_1 field can contain different values based on the transaction type being sent. When used with a Citi Private Label Auth or Sale transaction, this field should contain the credit plan number. When used in a Debit Batch Hold Release transaction, this field should contain the batch close sequence number that will be stored with each debit transaction and returned in the debit reconciliation file.

- Variable Type: Numeric

Example:

```
<SPECIAL_1>123456</SPECIAL_1>
```

STATE

The STATE field contains the two-character representation of the state associated with the account number for the transaction. This field is not a required field.

- Variable Type: Alphanumeric
- Max Length: 3
- REGEX: ^([a-zA-Z0-9\/\.\-_,#'&+\s]){0,3}$

Example:

```
<STATE>AZ</STATE>
```

STD_ENTRY_CLASS

The STD_ENTRY_CLASS field is used to indicate the standard entry class (SEC) code for an ACH transaction. If this field and code is not included with the ACH transaction request, the SEC code that is set within the merchant profile will be used by default.

- Variable Type: Alpha
- Max Length: 3

Example:

```
<STD_ENTRY_CLASS>PPD</STD_ENTRY_CLASS>
```

Standard Entry Class (SEC) Codes

SEC Codes

Code		Definition
ARC	Accounts Receivable Entry	Used in debit applications when a consumer check is received via mail or at a drop-box location for payment of goods or services. The check is used to collect the amount as well as the consumer's routing, account, and check serial number.
CCD	Cash Concentration or Disbursement	Used in either credit or debit applications where funds are distributed or consolidated between corporate entities.
CIE	Customer Initiated Entry	Used in credit applications where the consumer initiates the transfer of funds to a company for payment of funds owed to the company, typically through some type of home banking product or bill payment service provider.
CTX	Corporate Trade Exchange	Used in an application that supports the transfer of funds (debit or credit) within a trading partner relationship in which full ANSI ASC X12 message or payment related UN/EDIFACT information is sent with the funds transfer. This information is placed in multiple addenda records.

Code		Definition
DNE	Death Notification Entry	Used in applications that are utilized by a Federal Government Agency, such as Social Security Administration, to notify a depository financial institution that the recipient of a government benefit payment has died.
PPD	Pre-arranged Payment and Deposit Entry	For direct deposit, this is used in credit applications that transfer funds into a consumer's account at the Receiving Depository Financial Institution. For a pre-authorized payment, this is used in a debit application that the company, with the customer's consent, will initiate periodic charges to the customer's account as bills become due.
RCK	Represented Check Entry	Merchant collection of checks that had been returned as NSF or Uncollected Funds.
TEL	Telephone Initiated Entry	Used in applications that will debit a consumer's account pursuant to an oral authorization obtained from the consumer via the telephone.
WEB	Internet Initiated Entry	Used in signal entry or recurring debit of a consumer's account pursuant to an authorization that is obtained from the Receiver via the Internet.

START_DATE

The START_DATE field contains the credit card's issue date. This is commonly found on Maestro, Switch, or Solo credit cards and may be required when processing such card types.

- Variable Type: Alpha
- Format: YYMM
- Max Length: 4

Example:

```
<START_DATE>1610</START_DATE>
```

NOTE: This example represents October 2016.

TAVV

The TAVV field contains the cryptogram returned by the Token Provider and can contain up to 81 characters. This is very similar to the CAVV value and how 3DS and MC SecureCode function.

When sending a MasterCard request, the Cryptogram data string is required in Base64 format.

When sending a Visa request, if the string length is 28, the data will be considered to be in Base64 format; if the string length is 40 it will be considered to be in HEX format; if its length is not equal to 28 or 40 it will not be included in the authorization request.

The optional XID can be in BASE64 or HEX (40) representation. If present, place a "|" (vertical bar) after the TAVV and then append the XID value.

NOTE: For Base64, if the cryptogram string contains a "+" character, ensure that it remains in the string and that it is not replaced with a "space".

- Variable Type: Alphanumeric
- Max Length: 81

Example (HEX):

```
<TAVV>0000010732799312345678901279930000000000</TAVV>
```

Example (Base64):

```
<TAVV>AAABAWFlmQAAAABjRWWZEEFgFz+=</TAVV>
```

TAVV_ECI

The TAVV_ECI field contains the ECI response returned by the Token Provider.

NOTE: This field is optional; however, EPX strongly recommends that if a value is returned from the Token Provider that this value should be included with the transaction.

- Variable Type: Numeric
- Max Length: 2

Example:

```
<TAVV_ECI>5</TAVV_ECI>
```

TAX_AMT

The TAX_AMT field is a reference field that contains the tax amount which is included in the amount of the transaction. This field does not get added to the Amount field during the transaction, it is only referencing the tax amount already included.

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13

Example:

```
<TAX_AMT>1.35</TAX_AMT>
```

TAX_EXEMPT

The TAX_EXEMPT field is a reference field that contains an indication as to whether the transaction is tax exempt. This field assists in qualifying a transaction for Level II processing using the following rule. If a transaction is tax-exempt, then there is no need to send a tax amount, and if it is not then the tax amount should be supplied in the TAX_EXEMPT field.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<TAX_EXEMPT>Y</TAX_EXEMPT>
```

TAX_EXEMPT Values

- Y—Sending a tag with a value of Y indicates that the transaction is tax exempt and tax amount does not need to be provided for Level II qualification.
- N—Sending a tag with a value of N indicates that the transaction is not tax exempt and tax amount needs to be provided for Level II qualification.

TIP_AMT

The TIP_AMT field is a reference field that contains the tip amount which is included in the amount of the transaction. This field does not get added to the Amount field during the transaction, it is only referencing the tip amount already included.

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13

Example:

```
<TIP_AMT>1.35</TIP_AMT>
```

TRACK_DATA

The TRACK_DATA field contains the track data from the credit or debit card. This field works with the CARD_ENT_METH field and may be in clear text or encrypted based on the card reader used during the transaction. When sending track data, track 1 is to be used when processing a credit card transaction, and track 2 is to be used if track 1 is unavailable or when processing a debit or EBT transaction. Refer to sections ***Error! Reference source not found.*** or ***Error! Reference source not found.*** for additional information regarding the required format of the encrypted TRACK_DATA value.

NOTE: In some cases, coding environments will perform a URL post of data to EPX. In these cases Track Data may contain special characters, like '%', '+', or '=', that may need to be URL Encoded so that they are communicated correctly.

- Variable Type: Alphanumeric
- Max Length: 256

Example:

```
<TRACK_DATA>B4111111111111111^CARD/TEST^10121010000012345678</TRACK_ DATA>
```

TRAN_FEE

The TRAN_FEE is used to indicate the surcharge fee amount applied to a specific transaction. The amount specified in the TRAN_FEE field is added to the transaction amount indicated in the AMOUNT field when the request is sent to the networks for approval. For example, a purchase transaction with an "AMOUNT" containing $20.00 and a transaction surcharge fee amount "TRAN_FEE" containing $2.50, the amount (AUTH_AMOUNT_REQUESTED) is sent to the networks as a total of $22.50.

EPX includes the approved total amount in response tag AUTH_AMOUNT.

Note: TRAN_FEE is not a reference field

- Variable Type: Numeric (Decimal Point Required)
- Format: N.NN
- Max Length: 13

Example:

```
<TRAN_FEE>2.50</TRAN_FEE>
```

TRAN_NBR

The TRAN_NBR field contains a unique number created by the operator to identify a transaction within a batch. This field works in conjunction with the BATCH_ID field. The same BATCH_ID/TRAN_NBR combination cannot be used more than once under a single merchant number (MERCH_NBR). Commonly, this field contains an invoice number, or is just incremented throughout the day.

- Variable Type: Numeric
- Max Length: 10
- REGEX: ^([0-9]){0,10}$

Example:

```
<TRAN_NBR>28</TRAN_NBR>
```

TRAN_TYPE

The TRAN_TYPE field contains the TRAN_TYPE code specific to the type of transaction which is to be performed on the account number during the request. Below are lists defining the valid Transaction Type field values. (For details about specific transaction types, refer to the EPX transaction specification document for the selected industry.)

> IMPORTANT!
>
> In some scenarios, and based on certain processing rules, the EPX platform may automatically change the TRAN_TYPE value before sending the transaction to the Card Networks for approval. In these cases, the TRAN_TYPE field in the response returned from EPX will contain a new value that represents the transaction type that the transaction was processed as to accommodate certain processing rules.
>
> Because of this reason, the client application must never hardcode to the TRAN_TYPE field in the response message to prevent any potential issues from occurring. Instead, the client application can reference the ORIG_TRAN_TYPE field in the transaction response field section, since it will contain the original TRAN_TYPE value from the client request, which can be used for matching purposes.

- Variable Type: Alphanumeric
- Max Length: 4

Example:

```
<TRAN_TYPE>CCE1</TRAN_TYPE>
```

Ecommerce Transaction Types

- CCE0—Ecommerce Account Verification transaction
- CCE1—Ecommerce Purchase Authorization & Capture transaction
- CCE2—Ecommerce Purchase Authorization Only transaction
- CCE4—Ecommerce Purchase Capture Only transaction
- CCE7—Ecommerce Purchase Authorization Reversal
- CCE8—Ecommerce BRIC Storage transaction
- CCE9—Ecommerce Return Capture transaction
- CCEA—Ecommerce Return Authorization & Capture transaction
- CCEC—Ecommerce Visa Debt Repayment Authorization and Capture
- CCEG—Ecommerce Return Authorization & Capture Hold Release
- CCEM—Ecommerce Payment Authorization & Capture transaction

- CCEN—Ecommerce Edit Authorization and Capture transaction
- CCEX—Ecommerce Void transaction
- CCEZ—Ecommerce Close Batch transaction

Retail Transaction Types

- CCR0—Retail Account Verification transaction
- CCR1—Retail Purchase Authorization & Capture transaction
- CCR2—Retail Purchase Authorization Only transaction
- CCR4—Retail Purchase Capture Only transaction
- CCR7—Retail Purchase Authorization Reversal
- CCR8—Retail BRIC Storage or Updates transaction
- CCR9—Retail Return Capture transaction
- CCRA—Retail Return Authorization & Capture transaction
- CCRG—Retail Return Authorization & Capture Hold Release
- CCRN—Retail Edit Authorization and Capture transaction
- CCRX—Retail Void transaction
- CCRY—Open to Buy/Balance Inquiry transaction. Citi Private Label only
- CCRZ—Retail Close Batch transaction

MOTO Transaction Types

NOTE: MOTO = Mail Order and Telephone Order

- CCM0—MOTO Account Verification transaction
- CCM1—MOTO Purchase Authorization & Capture transaction
- CCM2—MOTO Purchase Authorization Only transaction
- CCM4—MOTO Purchase Capture Only transaction
- CCM7—MOTO Purchase Authorization Reversal
- CCM8—MOTO BRIC Storage or Update Transactions
- CCM9—MOTO Return Capture transaction
- CCMA—MOTO Return Authorization & Capture transaction
- CCMC—MOTO Visa Debt Repayment Authorization and Capture
- CCMG—MOTO Return Authorization & Capture Hold Release
- CCMN—MOTO Edit Authorization and Capture transaction
- CCMX—MOTO Void transaction
- CCMZ—MOTO Close Batch transaction

Debit Transaction Types

- DB00—DEBIT Purchase (Default) transaction
- DB01—DEBIT Return (Default) transaction
- DB0P—DEBIT PIN-less Purchase (Default) transaction

- DB0S—DEBIT PIN-less Return (Default) transaction
- DB0V—DEBIT Void and/or Reversal
- DB0Z—DEBIT Hold Release

EBT Transaction Types

- EB00—EBT Food Stamp Purchase / Voucher transaction
- EB01—EBT Food Stamp Return transaction
- EB02—EBT Food Stamp Bal Inq. transaction
- EB05—EBT Cash Benefits Purchase (Cash Back optional) transaction
- EB07—EBT Cash Benefits Balance Inq. transaction
- EB0V—EBT Reversal/Void/Cancel transaction

ACH Transaction Types

- CKC0—Checking Pre-note Debit transaction
- CKC1—Checking Pre-note Credit transaction
- CKC2—Checking Account Debit transaction
- CKC3—Checking Account Credit transaction
- CKC8—Checking BRIC Storage transaction
- CKCX—Checking Account Debit Void
- CKS0—Savings Pre-note Debit transaction
- CKS1—Savings Pre-note Credit transaction
- CKS2—Savings Account Debit transaction
- CKS3—Savings Account Credit transaction
- CKS8—Savings BRIC Storage transaction
- CKSX—Savings Account Debit Void

TeleCheck Transaction Types

- CKCE—Check Follow Up Transaction
- CKCF—Check Pre-Auth Transaction
- CKCG—Check Verify/Guarantee Transaction

Banking Transaction Types

- CCBJ—BANKING Cash Authorization & Capture transaction
- CCBK—BANKING Cash Authorization Only transaction
- CCBL—BANKING Cash Capture Only transaction
- CCBN—BANKING Edit Authorization and Capture transaction

Special Transaction Types

- SS01—Sending a signature capture
- SS02—Batch Totals
- SS03—Account Query
- SS0E—Enhanced TLV Edit / Add

Visa Money Transfer Transaction Types

- SM0G—VMT Account Funding Transaction (AFT)
- CCEW—VMT Watch List Screening Transaction (WLS)
- SM0H—VMT Original Credit Transaction (OCT)

MasterCard Money Transfer Transaction Types

NOTE: The representation of value "x" can be substituted with "R" for Retail, "M" for MOTO, and "E" Ecommerce industry types.

- SM0G—SMS Funding Transaction
- SM0K—SMS Payment Transaction

Citi Private Label Transaction Types

NOTE: The representation of value "x" can be substituted with "R" for Retail, "M" for MOTO, and "E" Ecommerce industry types. EPX additionally supports standard processing transaction types for Citi, reference the *Transaction Specs – Visa Debt Repayment* guide.

- CCxH—Citi Card Payment Adjustment Capture and Hold transaction
- CCxI—Citi Card Payment Adjustment Capture and Hold Release transaction
- CCxT—Citi Card Payment Capture and Hold transaction
- CCxU—Citi Card Payment Capture and Hold Release transaction
- SS07—Citi Account Lookup Transaction
- SS08—Citi New Account Request / Apply for Credit Transaction

USER_DATA_1 through 10

The USER_DATA_*X* fields are optional fields that the merchant can use to store additional information about the transaction where *X* equals a number between 1 and 10.

- Variable Type: Alphanumeric
- Max Length: 80

Example:

```
<USER_DATA_3>XL Shirt</USER_DATA_3>
```

VERBOSE_RESPONSE

The VERBOSE_RESPONSE field determines if the verbose transaction response will be enabled. When enabled, the field contains a Y and all request and response elements are returned.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<VERBOSE_RESPONSE>Y</VERBOSE_RESPONSE>
```

ZIP_CODE

The ZIP_CODE field contains the Zip code associated with the account number for the transaction. This field is not required.

This field, along with ADDRESS, is part of the credit card address verification as the value contained in this field will be validated against the value recorded at the issuing bank for the account when doing a credit card authorization. The response for this verification is found in the AUTH_AVS field. EPX supports all AVS formats supported by the card networks.

NOTE: A hyphen "-" should not be present when sending a numeric 9-digit US zip code.

- Variable Type: Alphanumeric
- Max Length: 10
- REGEX: ^([A-Za-z0-9\-\s]){0,10}$

Examples:

```
<ZIP_CODE>198041258</ZIP_CODE>
```

```
<ZIP_CODE>T6V 1X7</ZIP_CODE>
```

Transaction Response Fields

This chapter describes the fields that are returned in the response from EPX after running a transaction.

AUTH_AMOUNT

The AUTH_AMOUNT tag contains the actual dollar amount that the transaction request was approved for.

- VariableType: Numeric
- Max Length: 13
- Format: N.NN

Example:

```
<FIELD KEY="AUTH_AMOUNT">379.00</FIELD>
```

AUTH_AMOUNT_REQUESTED

The AUTH_AMOUNT_REQUESTED field contains the dollar amount that was used during the transaction request.

- VariableType: Numeric
- Max Length: 13
- Format: N.NN

Example:

```
<FIELD KEY="AUTH_AMOUNT_REQUESTED">500.00</FIELD>
```

AUTH_AVAILABLE_BAL

The AUTH_AVAILABLE_BAL field contains the available balance / open to buy amount for the cardholder account. EPX will include this data in the response if returned by the issuing bank.

- Variable Type: Numeric
- Max Length: 13

Example:

```
<FIELD KEY="AUTH_AVAILABLE_BAL">500.00</FIELD>
```

AUTH_AVS

The AUTH_AVS field contains the Address Verification System response for the transaction requested. The address information sent in with the transaction is validated against the information at the issuing bank. This is a bank response that is passed along by EPX. EPX supports all AVS formats supported by the card networks.

The network-specific sections that follow define the possible response values for the Address Verification System (AVS) field.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<FIELD KEY="AUTH_AVS">M</FIELD>
```

Visa

- A—Address matches, ZIP code does not. Acquirer rights not implied
- B—Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)
- C—Street address and postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)
- D—Street addresses and postal codes match.
- F—Street address and postal code match. Applies to U.K. only.
- G—Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for this account.
- I—Address information not verified.
- M—Street address and postal code match.
- N—No match. Acquirer sent postal/ZIP code only, or street address only, or both postal code and street address. Also used when acquirer requests AVS but sends no AVS data in field 123.
- P—Postal code match. Acquirer sent both postal code and street address, but street address not verified due to incompatible formats.
- R—Retry: System unavailable or timed out. Issuer ordinarily performs AVS but was unavailable. The code R is used by V.I.P. when issuers are unavailable. Issuers should refrain from using this code.
- S—Not applicable. If present, replaced with “U” (for domestic) or “G” (for international) by V.I.P. Available for U.S. issuers only.

- U—Address not verified for domestic transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for this account.
- W—Not applicable. If present, replaced with "Z" by V.I.P. Available for U.S. issuers only.
- X—Not applicable. If present, replaced with "Y" by V.I.P. Available for U.S. issuers only.
- Y—Street address and postal code match.
- Z—Postal/ZIP matches; street address does not.

MasterCard

- A—Address matches, postal code does not
- N—Neither address nor postal code matches
- R—Retry, system unable to process
- S—AVS currently not supported
- U—No data from issuer/Authorization Platform
- W—For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not
- X—For U.S. addresses, nine-digit postal code and address matches; for addresses outside the U.S., postal code and address match
- Y—For U.S. addresses, five-digit postal code and address matches
- Z—For U.S. addresses, five-digit postal code matches, address does not

Discover

- Y—Address matches, five-digit Postal Code matches
- X—Address matches, nine-digit Postal Code matches
- A—Address matches, Postal Code does not
- Z—Five-digit Postal Code matches, address does not
- W—Nine-digit Postal Code matches, address does not
- G—Address information not verified for international Transaction
- S—AVS not supported at this time
- Z—Nothing matches
- R—Approved AVS N/A
- U—Retry, system unable to process

AMEX

- A—Billing Address only correct
- D—CM Name incorrect, Billing Postal Code matches

- E—CM Name incorrect, Billing Address and Postal Code match
- F—CM Name incorrect, Billing Address matches
- K—CM Name matches
- L—CM Name and Billing Postal Code match
- M—CM Name, Billing Address and Postal Code match
- N—No match, Billing Address and Postal Code are both incorrect
- O—CM Name and Billing Address match
- R—System unavailable; retry
- S—SE not allowed AAV function
- U—Information unavailable
- W—No, CM Name, Billing Address and Postal Code are all incorrect
- Y—Yes, Billing Address and Postal Code are both correct
- Z—Billing Postal Code only correct

AUTH_CARD_TYPE

The AUTH_CARD_TYPE field contains the card type code for the card used in the transaction request. The possible response values for the Card Type field are listed below.

- Variable Type: Alphanumeric
- Max Length: 1

Example:

```
<FIELD KEY="AUTH_CARD_TYPE">V</FIELD>
```

Card Types and Codes

- 0—Maestro
- 1—Solo Card
- 2—Switch Card
- 3—China Union
- 4—Citi Private Label
- 5—Synchrony
- 6—Stored Value / Gift Card
- 7—Voyager
- 8—WEX
- A—AliPay
- E—EBT
- J—JCB
- L—Private
- M—MasterCard

- N—Diners
- O—Other Debit
- R—Discover
- S—American Express
- V—Visa

AUTH_CODE

The AUTH_CODE field contains the approval code for the transaction requested. In the event that there is no approval, this field will be empty. Some issuers will return an authorization code on declined transactions. Use the AUTH_RESP value to determine if a transaction was approved.

- Variable Type: Alphanumeric
- Max Length: 6

Example:

```
<FIELD KEY="AUTH_CODE">000601</FIELD>
```

AUTH_CURRENCY_CODE

The AUTH_CURRENCY_CODE field contains the currency code used in the transaction request.

- Variable Type: Numeric
- Max Length: 3

Example:

```
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
```

AUTH_CVV2

The AUTH_CVV2 field contains the CVV2 response for the transaction requested. The CVV value sent in with the transaction is validated against the information at the issuing bank. This is a bank response that is passed along by EPX. The table below defines the possible response values for the CVV2 field based on valid card type.

- Variable Type: Alpha
- Max Length: 1

Example:

```
<FIELD KEY="AUTH_CVV2">N</FIELD>
```

Visa

- Space—No result
- M—CVV2 match
- N—CVV2 does not match
- P—Not processed
- S—CVV2 should be on the card, but the merchant indicates that it is not
- U—Issuer is not certified or has not provided Visa with encryption keys, or both.

MasterCard

- M—CVV2 match
- N—CVV2 no match
- P—Not processed
- S—CVV2 is on the card, but the merchant has indicated that CVV2 is not present.
- U—Issuer is not Visa-certified for CVV2, has not provided Visa encryption keys, or both.

Discover

- M—CID Match
- N—CID No Match
- P—Not Processed
- S—CID should be on the Card, but the Merchant has indicated that it is not present
- U—Issuer is not certified

AMEX

- N—CID/4DBC/4CSC did not match
- U—CID/4DBC/4CSC was not checked
- Y—CID/4DBC/4CSC matched

AUTH_EBT_BAL_CASH

The AUTH_EBT_BAL_CASH field contains the available EBT Cash balance / open to buy amount for the cardholder account. EPX will include this data in the response if returned by the Networks.

- Variable Type: Numeric
- Max Length: 13

Example:

```
<FIELD KEY="AUTH_EBT_BAL_CASH">250.00</FIELD>
```

AUTH_EBT_BAL_FOOD

The AUTH_EBT_BAL_FOOD field contains the available EBT Food balance / open to buy amount for the cardholder account. EPX will include this data in the response if returned by the Networks.

- Variable Type: Numeric
- Max Length: 13

Example:

```
<FIELD KEY=" AUTH_EBT_BAL_FOOD">375.00</FIELD>
```

AUTH_EMV_DATA

The AUTH_EMV_DATA tag is provided in the response and the data must be provided back to the EMV kernel. The tag currently can contain up to 3 EMV tags from the issuer: Tags 91, 71, and 72. Data will be returned within this tag in the response nearly always.

- Tag 91 Issuer Authentication Data will be present 99.9% of the time.
- Tag 71 Issuer Script Template 1 will be present .01% of the time
- Tag 72 Issuer Script Template 1 will be present .01% of the time

Issuer scripts 0x71 and 0x72 can be very large, up to 128 bytes each, which is presented in HEX ASCII, so 256 characters each.

NOTE: The EPX UAP / Demo environment does not return this tag as we are unable to replicate this in Demo mode.

- Variable Type: Alphanumeric
- Max Length: variable

Example:

```
<FIELD KEY="AUTH_EMV_DATA">910AD1020739E23C7D443035</FIELD>
```

AUTH_GUID

The AUTH_GUID field contains the globally unique identifier (GUID), also commonly referred to as the EPX BRIC for the transaction requested. This value is unique throughout the EPX platform. When retained, the BRIC / GUID can be used later to reference the transaction for other transactions, such as a refund. It can also be used by the relationship manager to refer to specific transactions.

- Variable Type: Alphanumeric
- Max Length: 20

Example:

```
<FIELD KEY="AUTH_GUID">0v703WNY8DD00KXNQG1</FIELD>
```

AUTH_PAR

The AUTH_PAR response field contains the PAR (Payment Account Reference). EPX will include this field and value in the response if returned by the Networks. The PAR serves as a universal ID that can be used to tie all underlying tokens associated with a specific PAN (Primary Account Number).

NOTE: The EPX terminal profile must be set to Response Version "Dynamic XML".

- Variable Type: Alphanumeric
- Max Length: 40

Example:

```
<FIELD KEY="AUTH_PAR"></FIELD>
```

AUTH_REF_ID

The AUTH_REF_ID field contains the TeleCheck Trace ID for a TeleCheck transaction.

- Variable Type: Numeric
- Max Length: 25

Example:

```
<FIELD KEY="AUTH_REF_ID">8888888</FIELD>
```

AUTH_REF_PHONE_NBR

The AUTH_REF_PHONE_NBR field contains the Referral Phone Number for a Citi Bank Private Label Auth or Sale transaction.

- Variable Type: Numeric
- Max Length: 10

Example:

```
<FIELD KEY="AUTH_REF_PHONE_NBR">8005551234</FIELD>
```

AUTH_RESP

The AUTH_RESP field contains the response code for the transaction requested and should be used to determine the result of the transaction. This information is passed along from the issuing bank. Refer to the following tables for additional information on the ACH, CC, and PIN-less Debit response codes. In the ACH environment, the transaction receives an AUTH_CODE indication if there is anything wrong with the transaction that would cause it not to settle, including an invalid routing number.

Since ACH is not real time, EPX checks for a valid Routing Number and that all other required fields are available. Once the transaction is submitted to the Federal Reserve, merchants are notified via a return or notice of change if there is an issue or change with the account.

- Variable Type: Alphanumeric
- Max Length: 3

Example:

```
<FIELD KEY="AUTH_RESP">00</FIELD>
```

ACH Response Codes

ACH Response Codes

CODE	DISPLAY	DESCRIPTION
00	ACCEPTED	ACCEPTED
03	INVALID MERCHANT	INVALID MERCHANT OR SERVICE PROVIDER
06	ERROR	ERROR
12	INVALID TRANS	INVALID TRANSACTION
13	AMOUNT ERROR	INVALID AMOUNT
14	INVALID ACCT NBR	INVALID ACCOUNT NUMBER
19	RE ENTER	RE-ENTER TRANSACTION
21	NO ACTION TAKEN	NO ACTION TAKEN

CODE	DISPLAY	DESCRIPTION
25	UNABLE TO LOCATE	UNABLE TO LOCATE RECORD ON FILE
52	NO CHECK ACCOUNT	NO CHECKING ACCOUNT
53	NO SAVE ACCOUNT	NO SAVINGS ACCOUNT
58	SERV NOT ALLOWED	TRANSACTION NOT ALLOWED AT TERMINAL
61	DECLINE	ACTIVITY AMOUNT LIMIT EXCEEDED
76	NO ACTION TAKEN	UNABLE TO LOCATE PREVIOUS MESSAGE (NO MATCH ON RRN)
77	NO ACTION TAKEN	NO MATCH ON ORIGINAL MESSAGE
78	INVALID RTN NBR	INVALID ROUTING NUMBER
80	DATE ERROR	INVALID DATE
96	SYSTEM ERROR	SYSTEM ERROR
E1	INVALID SEC	Invalid or unsupported Standard Entry Class (SEC) code
E7	TERMINAL ID ERROR	TERMINAL ID ERROR
EA	AUTH TO OLD	AUTH TO OLD
EQ	NO NETWORK GATEWAY AVAILABLE	NO NETWORK GATEWAY AVAILABLE
ES	DECLINE	Transaction not allowed due to failure of internal validations
SX	DO NOT TRY AGAIN	A previous ACH Fatal Return linked to the bank account in use
RR	ERROR	If you receive this response code, contact the customer support team for further instructions
SX	DO NOT TRY AGAIN	Decline due to a previous ACH Fatal Return linked to the bank account in use – Do not try again

NACHA Account Status Declines

NACHA Account Status Declines

The following NACHA Status Declines can be returned in real time with EPX AUTH_RESP codes '14' & '25'

EPX AUTH_RESP Code	NACHA Account Status	Reason - Information	Description
14	Disabled	Account reported closed. Consumer Affairs 855-673-7310.	Account has been reported closed.
14	Disabled	Account number invalid. Consumer Affairs 855-673-7310.	Account number has less than the minimum number of digits or contains an invalid character.
14	Disabled	History of account closed. Consumer Affairs 855-673-7310.	Account has been reported closed with no reports of negative activity in the previous 12 months.
14	Disabled	Past history of account not found or invalid account number. Consumer Affairs 855-673-7310.	History of R03 or R04 returns on account in the previous 12 months.
14	Disabled	Account number has been reported as invalid or no account found. Consumer Affairs 855-673-7310	Account has experienced returns indicating account number invalid or account closed.

EPX AUTH_RESP Code	NACHA Account Status	Reason - Information	Description
14	Disabled	Routing number invalid. Consumer Affairs 855-673-7310.	Routing number provided is not a valid US routing number.
14	Disabled	Consumer Affairs 855-673-7310.	Account is not available for ACH.
14	Disabled	Account reported closed. Consumer Affairs 855-673-7310.	Account has been reported closed with outstanding items.
14	Disabled	Past history of account not found or invalid account number. Consumer Affairs 855-673-7310.	Account has been reported closed with outstanding items.
25	Unable to Locate	Account structure.	Format of account number for provided routing number does not match expected format.

AAU Response Codes

AAU Response Codes

Card Type	AUTH_RESP	Display / Description
MasterCard	blank	Match made; update data provided
MasterCard	blank	Match made; account closed
MasterCard	blank	Match made; expiration date changed
MasterCard	blank	No updates were found but the account is valid
MasterCard	blank	The account number could not be found in the ABU database
MasterCard	blank	Non-numeric Account Number
MasterCard	blank	Invalid Expiration Date
MasterCard	blank	Merchant Not Registered
MasterCard	V	Matches the account as reported by the issuer
MasterCard	P	No match, participating BIN/issuer
MasterCard	N	No match, non-participating BIN/issuer
Visa	A	Account number change message
Visa	C	Closed account advice
Visa	E	Expiration date change message
Visa	N	Non-participating BIN
Visa	P	Participating BIN, no match
Visa	Q	Contact cardholder advice
Visa	V	Match made, account number and expiration date unchanged

Credit Card / PIN Debit Response Codes

Visa Response Codes

VISA		
CODE	**DISPLAY**	**DESCRIPTION**
00	APPROVAL	APPROVED
01	CALL	REFER TO CARD ISSUER
02	CALL	REFER TO CARD ISSUER, SPECIAL CONDITION
03	TERM ID ERROR	INVALID MERCHANT OR SERVICE PROVIDER
04	HOLD-CALL	PICK UP CARD (NO FRAUD)
05	DECLINE	DO NOT HONOR
06	ERROR	ERROR
07	HOLD-CALL	PICK UP CARD, SPECIAL CONDITION (POSSIBLE FRAUD)
10	PARTIAL APPROVED	APPROVED PARTIAL
12	INVALID TRANS	INVALID TRANSACTION
13	AMOUNT ERROR	INVALID AMOUNT
14	CARD NO. ERROR	INVALID ACCOUNT NUMBER
15	NO SUCH ISSUER	NO SUCH ISSUER
19	RE ENTER	RE-ENTER TRANSACTION
21	NO ACTION TAKEN	NO ACTION TAKEN
25	UNABLE TO LOCATE	UNABLE TO LOCATE RECORD IN FILE
28	NO REPLY	FILE IS TEMPORARILY UNAVAILABLE
30	FORMAT ERROR	FORMAT ERROR
34	CALL	CALL
39	NO CREDIT ACCT	NO CREDIT ACCOUNT
41	HOLD-CALL	LOST CARD, PICK UP CARD (FRAUD ACCOUNT)
43	HOLD-CALL	STOLEN CARD, PICK UP (FRAUD ACCOUNT)
46	DECLINE	CLOSED ACCOUNT
51	INSUFF FUNDS	INSUFFICIENT FUNDS
52	NO CHECK ACCOUNT	NO CHECKING ACCOUNT
53	NO SAVE ACCOUNT	NO SAVINGS ACCOUNT
54	EXPIRED CARD	EXPIRED CARD
55	WRONG PIN	INCORRECT PIN
57	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ISSUER/CARDHOLDER
58	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ACQUIRER/TERMINAL
59	CALL	SUSPECTED FRAUD
61	DECLINE	EXCEEDS APPROVAL AMOUNT LIMIT
62	DECLINE	RESTRICTED CARD - INVALID IN REGION OR COUNTRY
63	SEC VIOLATION	SECURITY VIOLATION
64	DECLINE AML	TRANSACTION DOES NOT FULFILL AML REQUIREMENT
65	DECLINE	ACTIVITY COUNT LIMIT EXCEEDED
75	PIN EXCEEDED	ALLOWABLE NUMBER OF PIN ENTRY TRIES EXCEEDED
76	NO ACTION TAKEN	UNABLE TO LOCATE PREVIOUS MESSAGE
77	NO ACTION TAKEN	NO MATCH ON ORIGINAL MESSAGE
78	BLOCKED 1ST USE	BLOCKED FIRST USE BY CARDHOLDER
80	DECLINED	NO FINANCIAL IMPACT

VISA		
81	ENCRYPTION ERROR	PIN CRYPTOGRAPHIC ERROR FOUND
82	CVV ERROR	INCORRECT CVV
83	CANT VERIFY PIN	UNABLE TO VERIFY PIN
85	NOT DECLINED	Issuer has no reason to decline the transaction (CCx0 Account Verification & CCx9/CCxA Return/Refund)
86	CANT VERIFY PIN	CAN NOT VERIFY PIN
91	NO REPLY	ISSUER UNAVAILABLE OR SWITCH INOPERATIVE
92	INVALID ROUTING	DESTINATION CANNOT BE FOUND FOR ROUTING
93	DECLINE	TRANSACTION CANNOT BE COMPLETED, VIOLATION
94	CALL	DUPLICATE TRANSMISSION DETECTED
96	SYSTEM ERROR	SYSTEM MALFUNCTION
1A	DECLINE	ADDITIONAL CUSTOMER AUTHENTICATION REQUIRED
6P	DECLINE	Verification data failed
B1	DECLINE	Surcharge amount not permitted on Visa cards
DA	INVALID FLEET	Required fleet prompts invalid or missing
E2	AVS REQUIRED	AVS data required
E3	CVV2 REQUIRED	CVV2 data required
E4	SERV NOT ALLOWED	SERV NOT ALLOWED
E5	SERV NOT ALLOWED	SERV NOT ALLOWED
E6	SERV NOT ALLOWED	SERV NOT ALLOWED
E7	TERM ID ERROR	TERMINAL ID ERROR
E9	NO REPLY	NO REPLY NETWORK
EA	ACCT LENGTH ERR	ACCOUNT LENGTH ERROR
EB	CHK DIGIT ERROR	CHECK DIGIT ERROR
EC	CID FORMAT ERROR	CID FORMAT ERROR
ED	EXPIRED AUTH	AUTH IS TO OLD FOR CAPTURE
EE	RESTRICTED CARD	CARD PRODUCT BLOCKED
EF	INVALID TRANS	BRIC ON PIN TRAN NOT ALLOWED
EH	CEM INVALID	INVALID CARD ENTRY METHOD
EI	CARD_ID INVALID	INVALID CARD ID
EJ	NO PIN BLK	NO PIN BLK
EK	SERV NOT ALLOWED	PINLESS ROUTING NOT ALLOWED
EL	STORAGE FAILED	BRIC STORAGE FAILED
EM	DEBIT SWIPE ONLY	DEBIT SWIPE ONLY
EN	BRIC RESPONSE TO	BRIC RESPONSE TIMEOUT
EO	CVV2 MISMATCH	CVV2 MISMATCH
EP	TRAN NOT ALLOWED	TRAN NOT ALLOWED
EQ	SYSTEM ERROR	NETWORK GATEWAY NOT AVAILABLE
ES	DECLINE	Transaction not allowed due to failure of internal validations
ET	FORMAT ERROR	EMV data is required for card entry method
EU	NO REPLY	Network rejected the item
EV	NO ACTION TAKEN	ITEM ALREADY CAPTURED
EW	FORMAT ERROR	FAILED REGEX VALIDATION
EX	CHECK NBR REQUIR	CHECK NBR REQUIRED
EY	RETRY - DIP CARD	CONTACTLESS MSD NOT ALLOWED. DIP CARD

VISA		
N0	DECLINE	Force STIP
N3	CASHBACK NOT AVL	CASH SERVICE NOT AVAILABLE
N4	DECLINE	CASH REQUEST EXCEEDS ISSUER LIMIT
N6	DECLINE	DECLINE
N7	CVV2 MISMATCH	DECLINE FOR CVV2 FAILURE
NR	NO DEBIT ROUTE	No valid debit network available to route
P2	DECLINE	Invalid biller information
P5	DECLINE	PIN Change/Unblock request declined
P6	DECLINE	Unsafe PIN
Q1	DECLINE	CARD AUTHENTICATION FAILED
R0	DECLINE	Stop Payment Order
R1	DECLINE	REVOCATION OF AUTHORIZATION ORDER
R3	DECLINE	REVOCATION OF ALL AUTHORIZATIONS ORDER
RR	ERROR	Reference response tag AUTH_RESP_TEXT for details of the invalid data supplied in a request tag. If unable to determine the issue, contact the customer support team for further instructions.
S4	CRYPTO FAILURE	PIN BLOCK TRANSLATION ERROR
S5	UNABLE TO LOCATE	Unable to locate a matching original purchase transaction
S7	INVALID RETURN	Unable to locate a matching original purchase transaction
S8	NO AUTHORIZATION	Unable to locate a matching authorization
S9	TLV TAGS INVALID	TLV TAGS INVALID
SS	BRIC STORAGE EXPIRED	BRIC STORAGE ACCT VERIFY DATA HAS EXPIRED
ST	ACCOUNT VERIFY FAILED	BRIC STORAGE ACCT VERIFY DATA FAILED
SU	TOKEN DECRYPTION FAILED	APPLE TTP / VISA VAC TOKEN DECRYPTION FAILED
SV	CALL	MERCHANT HAS BEEN SUSPENDED BY RTF
SW	REQUIRED DETAIL NOT PROVIDED	REQUIRED TRANSACTION DETAIL WAS NOT PROVIDED
Z1	DECLINE	Offline declined
Z3	DECLINE	Unable to go online

MasterCard Response Codes

MASTERCARD		
CODE	**DISPLAY**	**DESCRIPTION**
00	APPROVAL	APPROVED
01	CALL	CALL
02	CALL	CALL
03	TERM ID ERROR	TERMINAL ID ERROR
04	HOLD-CALL	CAPTURE CARD

MASTERCARD		
05	DECLINE	DECLINE
06	ERROR	ERROR
07	HOLD-CALL	HOLD-CALL
08	HONOR WITH ID	HONOR WITH ID
10	PARTIAL APPROVED	APPROVED PARTIAL
12	INVALID TRANS	INVALID TRANSACTION
13	AMOUNT ERROR	AMOUNT ERROR
14	CARD NO. ERROR	CARD NUMBER ERROR
15	NO SUCH ISSUER	NO SUCH ISSUER
17	DECLINE	CUSTOMER CANCEL
19	RE ENTER	RE ENTER
21	NO ACTION TAKEN	NO ACTION TAKEN
25	UNABLE TO LOCATE	UNABLE TO LOCATE
28	NO REPLY	NO REPLY
30	CALL	FORMAT ERROR
39	NO CREDIT ACCT	NO CREDIT ACCOUNT
41	HOLD-CALL	LOST CARD
43	HOLD-CALL	STOLEN CARD
51	INSUFF FUNDS	INSUFFICIENT FUNDS
52	NO CHECK ACCOUNT	NO CHECKING ACCOUNT
53	NO SAVE ACCOUNT	NO SAVINGS ACCOUNT
54	EXPIRED CARD	EXPIRED CARD
55	WRONG PIN	WRONG PIN
57	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ISSUER/CARDHOLDER
58	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ACQUIRER/TERMINAL
61	DECLINE	EXCEEDS WITHDRAWAL AMOUNT LIMIT
62	DECLINE	RESTRICTED CARD
63	SEC VIOLATION	SECURITY VIOLATION
65	DECLINE DIP CARD	EXCEEDS WITHDRAWAL COUNT LIMIT
70	CALL	CONTACT CARD ISSUER
75	PIN EXCEEDED	NUMBER PIN TRIES EXCEEDED
76	NO ACTION TAKEN	UNABLE TO LOCATE PREVIOUS MESSAGE
77	NO ACTION TAKEN	NO MATCH ON ORIGINAL MESSAGE
78	NO ACCOUNT	NO ACCOUNT
79	DECLINE	LIFE CYCLE (NEW ABU AVAIL)
80	DATE ERROR	DATE ERROR
81	SERV NOT ALLOWED	DEBIT TRANSACTION NOT ALLOWED
82	DECLINE	POLICY (NEW ABU AVAIL)
83	DECLINE	FRAUD/SECURITY
84	INVALID ALC	INVALID ALC

MASTERCARD		
85	NOT DECLINED	Issuer has no reason to decline the transaction (CCx0 Account Verification & CCx9/CCxA Return/Refund)
86	CANT VERIFY PIN	CAN NOT VERIFY PIN
87	CASHBACK NOT AVL	NO CASH BACK
88	CRYPTO FAILURE	CRYPTO FAILURE
89	PIN REQUIRED	PIN REQUIRED
91	NO REPLY	NO REPLY
92	INVALID ROUTING	INVALID ROUTING NUMBER
93	DECLINE	DECLINE
94	DUP TRANS	DUPLICATE TRANSMISSION DETECTED
96	SYSTEM ERROR	SYSTEM ERROR
1A	DECLINE	ADDITIONAL CUSTOMER AUTHENTICATION REQUIRED
DA	INVALID FLEET	Required fleet prompts invalid or missing
E2	AVS REQUIRED	AVS data required
E3	CVV2 REQUIRED	CVV2 data required
E4	SERV NOT ALLOWED	SERV NOT ALLOWED
E5	SERV NOT ALLOWED	SERV NOT ALLOWED
E6	SERV NOT ALLOWED	SERV NOT ALLOWED
E7	TERM ID ERROR	TERMINAL ID ERROR
E9	NO REPLY	NO REPLY NETWORK
EA	ACCT LENGTH ERR	ACCOUNT LENGTH ERROR
EB	CHK DIGIT ERROR	CHECK DIGIT ERROR
EC	CID FORMAT ERROR	CID FORMAT ERROR
ED	EXPIRED AUTH	AUTH IS TO OLD FOR CAPTURE
EE	RESTRICTED CARD	CARD PRODUCT BLOCKED
EF	INVALID TRANS	BRIC ON PIN TRAN NOT ALLOWED
EH	CEM INVALID	INVALID CARD ENTRY METHOD
EI	CARD_ID INVALID	INVALID CARD ID
EJ	NO PIN BLK	NO PIN BLK
EK	SERV NOT ALLOWED	PINLESS ROUTING NOT ALLOWED
EL	STORAGE FAILED	BRIC STORAGE FAILED
EM	DEBIT SWIPE ONLY	DEBIT SWIPE ONLY
EN	BRIC RESPONSE TO	BRIC RESPONSE TIMEOUT
EO	CVV2 MISMATCH	CVV2 MISMATCH
EP	TRAN NOT ALLOWED	TRAN NOT ALLOWED
EQ	SYSTEM ERROR	NETWORK GATEWAY NOT AVAILABLE
ES	DECLINE	Transaction not allowed due to failure of internal validations
ET	FORMAT ERROR	EMV data required
EU	NO REPLY	Network rejected the item
EV	NO ACTION TAKEN	ITEM ALREADY CAPTURED
EW	FORMAT ERROR	FAILED REGEX VALIDATION

MASTERCARD		
EX	CHECK NBR REQUIR	CHECK NBR REQUIRED
EY	RETRY - DIP CARD	CONTACTLESS MSD NOT ALLOWED. DIP CARD
N3	CASHBACK NOT AVL	CASHBACK NOT AVAILABLE
N4	DECLINE	DECLINE
N6	DECLINE	DECLINE
N7	CVV2 MISMATCH	DECLINE FOR CVV2 FAILURE
NR	NO DEBIT ROUTE	No valid debit network available to route
RR	ERROR	Reference response tag AUTH_RESP_TEXT for details of the invalid data supplied in a request tag. If you are unable to determine the issue, contact the customer support team for further instructions.
S4	CRYPTO FAILURE	PIN BLOCK TRANSLATION ERROR
S5	UNABLE TO LOCATE	Unable to locate a matching original purchase transaction
S7	INVALID RETURN	Unable to locate a matching original purchase transaction
S8	NO AUTHORIZATION	Unable to locate a matching authorization
S9	TLV TAGS INVALID	TLV TAGS INVALID
SA	DECLINED	Life Cycle - NEW ACCOUNT INFORMATION AVAILABLE
SB	DECLINED	Life Cycle - CANNOT APPROVE AT THIS TIME, TRY AGAIN LATER
SC	DECLINED	Life Cycle - DO NOT TRY AGAIN
SD	DECLINED	Life Cycle - TOKEN REQUIREMENTS NOT FULFILLED FOR THIS TOKEN TYPE
SE	DECLINED	Life Cycle - PAYMENT CANCELLATION
SF	DECLINED	Life Cycle - MERCHANT DOES NOT QUALIFY FOR PRODUCT CODE
SG	DECLINED	Policy - NEW ACCOUNT INFORMATION AVAILABLE
SH	DECLINED	Policy - CANNOT APPROVE AT THIS TIME, TRY AGAIN LATER
SI	DECLINED	Policy - DO NOT TRY AGAIN
SJ	DECLINED	Policy - TOKEN REQUIREMENTS NOT FULFILLED FOR THIS TOKEN TYPE
SK	DECLINED	Policy - PAYMENT CANCELLATION
SL	DECLINED	Policy - MERCHANT DOES NOT QUALIFY FOR PRODUCT CODE
SM	DECLINED	FRAUD/SECURITY - NEW ACCOUNT INFORMATION AVAILABLE
SN	DECLINED	FRAUD/SECURITY - CANNOT APPROVE AT THIS TIME, TRY AGAIN LATER
SO	DECLINED	FRAUD/SECURITY - DO NOT TRY AGAIN
SP	DECLINED	FRAUD/SECURITY - TOKEN REQUIREMENTS NOT FULFILLED FOR THIS TOKEN TYPE
SQ	DECLINED	FRAUD/SECURITY - PAYMENT CANCELLATION

MASTERCARD		
SR	DECLINED	FRAUD/SECURITY - MERCHANT DOES NOT QUALIFY FOR PRODUCT CODE
SS	BRIC STORAGE EXPIRED	BRIC STORAGE ACCT VERIFY DATA HAS EXPIRED
ST	ACCOUNT VERIFY FAILED	BRIC STORAGE ACCT VERIFY DATA FAILED
SU	TOKEN DECRYPTION FAILED	APPLE TTP / VISA VAC TOKEN DECRYPTION FAILED
SV	CALL	MERCHANT HAS BEEN SUSPENDED BY RTF
SW	REQUIRED DETAIL NOT PROVIDED	REQUIRED TRANSACTION DETAIL WAS NOT PROVIDED

Discover Response Codes

DISCOVER		
CODE	**DISPLAY**	**DESCRIPTION**
00	APPROVAL	APPROVED
01	CALL	REFER TO CARD ISSUER
03	TERM ID ERROR	INVALID MERCHANT
04	HOLD-CALL	CAPTURE CARD
05	DECLINE	DO NO HONOR
06	ERROR	ERROR
07	HOLD-CALL	PICK-UP CARD SPECIAL CONDITION
08	HONOR WITH ID	HONOR WITH ID
10	PARTIAL APPROVED	APPROVED PARTIAL
12	INVALID TRANS	INVALID TRANSACTION
13	AMOUNT ERROR	INVALID AMOUNT
14	CARD NO. ERROR	INVALID CARD MEMBER
15	NO SUCH ISSUER	INVALID ISSUER
19	RE ENTER	RE-ENTER TRANSACTION
21	NO ACTION TAKEN	NO ACTION TAKEN
30	CALL	FORMAT ERROR
31	CALL	BANK NOT SUPORTED BY SWITCH
33	EXPIRED CARD	EXPIRED CARD
34	CALL	SUSPECTED FRAUD
35	CALL	CARD ACCEPTOR CONTACT ACQUIRER
36	CALL	RESTRICTED CARD
37	CALL	CALL - SECURITY
38	PIN EXCEEDED	ALLOWABLE PIN TRIES EXCEEDED
39	NO CREDIT ACCT	NO CREDIT ACCOUNT
40	CALL	REQUESTED FUNCTION NOT SUPPORTED
41	HOLD-CALL	LOST CARD
43	HOLD-CALL	STOLEN CARD
51	DECLINE	DECLINE

DISCOVER		
53	NO SAVE ACCOUNT	NO SAVINGS ACCOUNT
54	EXPIRED CARD	EXPIRED CARD
55	WRONG PIN	INVALID PIN
56	NO CARD RECORD	NO CARD RECORD
57	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ISSUER/CARDHOLDER
58	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ACQUIRER/TERMINAL
59	DECLINE	SUSPECTED FRAUD
60	CALL	CARD ACCEPTOR ERROR
61	DECLINE	EXCEEDS WITHDRAWAL AMOUNT LIMIT
62	DECLINE	RESTRICTED CARD
63	SEC VIOLATION	SECURITY VIOLATION
64	CALL	ORIGINAL AMOUNT INCORRECT
65	DECLINE	EXCEEDS WITHDRAWAL COUNT LIMIT
66	CALL	CARD ACCEPTOR ERROR
67	HOLD-CALL	HARD CAPTURE - CALL
68	CALL	RESPONSE RECEIVED TO LATE
75	PIN EXCEEDED	ALLOWABLE NUMBER OF PIN TRIES EXCEEDED
76	CALL	UNABLE TO LOCATE PREVIOUS MESSAGE
77	CALL	INVALID/NONEXISTENT FROM ACCOUNT SPECIFIED
78	NO ACCOUNT	INVALID/NONEXISTENT ACCOUNT SPECIFIED (GENERAL)
83	DECLINE	DOMAIN RESTRICTION CONTROLS FAILURE
85	NOT DECLINED	Issuer has no reason to decline the transaction (CCx0 Account Verification & CCx9/CCxA Return/Refund)
87	NO REPLY	NETWORK UNAVAILABLE
91	NO REPLY	AUTHORIZATION SYSTEM OR ISSUER SYSTEM INOPERATIVE
92	INVALID ROUTING	UNABLE TO ROUTE TRANSACTION
93	DECLINE	DECLINE
94	CALL	DUPLICATE TRANSMISSION DETECTED
96	SYSTEM ERROR	SYSTEM ERROR
1A	DECLINE	ADDITIONAL CUSTOMER AUTHENTICATION REQUIRED
DA	INVALID FLEET	Required fleet prompts invalid or missing
E2	AVS REQUIRED	AVS data required
E3	CVV2 REQUIRED	CVV2 data required
E4	SERV NOT ALLOWED	SERV NOT ALLOWED
E5	SERV NOT ALLOWED	SERV NOT ALLOWED
E6	SERV NOT ALLOWED	SERV NOT ALLOWED
E7	TERM ID ERROR	TERMINAL ID ERROR
E9	NO REPLY	NO REPLY NETWORK
EA	ACCNT LEN ERROR	CHECK DIGIT ERROR
EB	CHK DIGIT ERROR	CHECK DIGIT ERROR
EC	CID FORMAT ERROR	CID FORMAT ERROR

DISCOVER		
ED	EXPIRED AUTH	AUTH IS TO OLD FOR CAPTURE
EE	RESTRICTED CARD	CARD PRODUCT BLOCKED
EF	INVALID TRANS	BRIC ON PIN TRAN NOT ALLOWED
EH	CEM INVALID	INVALID CARD ENTRY METHOD
EI	CARD_ID INVALID	INVALID CARD ID
EJ	NO PIN BLK	NO PIN BLK
EK	SERV NOT ALLOWED	PINLESS ROUTING NOT ALLOWED
EL	STORAGE FAILED	BRIC STORAGE FAILED
EM	DEBIT SWIPE ONLY	DEBIT SWIPE ONLY
EN	BRIC RESPONSE TO	BRIC RESPONSE TIMEOUT
EO	CVV2 MISMATCH	CVV2 MISMATCH
EP	TRAN NOT ALLOWED	TRAN NOT ALLOWED
EQ	SYSTEM ERROR	NETWORK GATEWAY NOT AVAILABLE
ES	DECLINE	Transaction not allowed due to failure of internal validations
ET	FORMAT ERROR	EMV data required
EU	NO REPLY	The network rejected the item
EV	NO ACTION TAKEN	ITEM ALREADY CAPTURED
EW	FORMAT ERROR	FAILED REGEX VALIDATION
EX	CHECK NBR REQUIR	CHECK NBR REQUIRED
EY	RETRY - DIP CARD	CONTACTLESS MSD NOT ALLOWED. DIP CARD
N6	DECLINE	DECLINE
N7	CVV AVS MISMATCH	CVV2 / AVS FAILURE
NR	NO DEBIT ROUTE	No valid debit network available to route
RR	ERROR	Reference response tag AUTH_RESP_TEXT for details of the invalid data supplied in a request tag. If you are unable to determine the issue, contact the customer support team for further instructions.
S4	CRYPTO FAILURE	PIN BLOCK TRANSLATION ERROR
S5	UNABLE TO LOCATE	Unable to locate a matching original purchase transaction
S7	INVALID RETURN	Unable to locate a matching original purchase transaction
S8	NO AUTHORIZATION	Unable to locate a matching authorization
S9	TLV TAGS INVALID	TLV TAGS INVALID
SS	BRIC STORAGE EXPIRED	BRIC STORAGE ACCT VERIFY DATA HAS EXPIRED
ST	ACCOUNT VERIFY FAILED	BRIC STORAGE ACCT VERIFY DATA FAILED
SU	TOKEN DECRYPTION FAILED	APPLE TTP / VISA VAC TOKEN DECRYPTION FAILED
SV	CALL	MERCHANT HAS BEEN SUSPENDED BY RTF
SW	REQUIRED DETAIL NOT PROVIDED	REQUIRED TRANSACTION DETAIL WAS NOT PROVIDED

American Express Response Codes

AMERICAN EXPRESS		
CODE	**DISPLAY**	**DESCRIPTION**
00	APPROVAL	APPROVED
01	PLEASE CALL	Refer to card issuer
03	TERM ID ERROR	INVALID MERCHANT
04	HOLD-CALL	DENY-PICK UP CARD
05	DECLINE	DENY
06	ERROR	ERROR
10	PARTIAL APPROVAL	PARTIAL APPROVAL
13	AMOUNT ERROR	INVALID AMOUNT
14	INVALID ACCT NBR	INVALID ACCOUNT NUMBER
25	UNABLE TO LOCATE	UNABLE TO LOCATE
30	FORMAT ERROR	FORMAT ERROR
38	PIN EXCEEDED	PIN EXCEEDED
54	EXPIRED CARD	EXPIRED CARD
55	WRONG PIN	INVALID PIN
56	NO CARD RECORD	NO CARD RECORD
57	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ISSUER/CARDHOLDER
58	SERV NOT ALLOWED	TRANSACTION NOT PERMITTED TO ACQUIRER/TERMINAL
78	NO ACCOUNT	INVALID ACCOUNT
85	NOT DECLINED	Issuer has no reason to decline the transaction (CCx0 Account Verification & CCx9/CCxA Return/Refund)
91	NO REPLY	ISSUER NOT AVAILABLE
96	SYSTEM ERROR	SYSTEM ERROR
1A	DECLINE	ADDITIONAL CUSTOMER AUTHENTICATION REQUIRED
DA	INVALID FLEET	Required fleet prompts invalid or missing
E2	AVS REQUIRED	AVS data required
E3	CVV2 REQUIRED	CVV2 data required
E4	SERV NOT ALLOWED	SERV NOT ALLOWED
E5	SERV NOT ALLOWED	SERV NOT ALLOWED
E6	SERV NOT ALLOWED	SERV NOT ALLOWED
E7	TERM ID ERROR	TERMINAL ID ERROR
E9	NO REPLY	NO REPLY NETWORK
EA	ACCT LENGTH ERR	ACCOUNT LENGTH ERROR
EB	CHK DIGIT ERROR	CHECK DIGIT ERROR
EC	CID FORMAT ERROR	CID FORMAT ERROR
ED	EXPIRED AUTH	AUTH IS TO OLD FOR CAPTURE
EE	RESTRICTED CARD	CARD PRODUCT BLOCKED
EF	INVALID TRANS	BRIC ON PIN TRAN NOT ALLOWED
EH	CEM INVALID	INVALID CARD ENTRY METHOD
EI	CARD_ID INVALID	INVALID CARD ID

AMERICAN EXPRESS		
EJ	NO PIN BLK	NO PIN BLK
EK	SERV NOT ALLOWED	PINLESS ROUTING NOT ALLOWED
EL	STORAGE FAILED	BRIC STORAGE FAILED
EM	DEBIT SWIPE ONLY	DEBIT SWIPE ONLY
EN	BRIC RESPONSE TO	BRIC RESPONSE TIMEOUT
EO	CVV2 MISMATCH	CVV2 MISMATCH
EP	TRAN NOT ALLOWED	TRAN NOT ALLOWED
EQ	SYSTEM ERROR	NETWORK GATEWAY NOT AVAILABLE
ES	DECLINE	Transaction not allowed due to failure of internal validations
ET	FORMAT ERROR	EMV data is required for card entry method
EU	NO REPLY	The network rejected the item
EV	NO ACTION TAKEN	ITEM ALREADY CAPTURED
EW	FORMAT ERROR	FAILED REGEX VALIDATION
EX	CHECK NBR REQUIR	CHECK NBR REQUIRED
EY	RETRY - DIP CARD	CONTACTLESS MSD NOT ALLOWED. DIP CARD
N6	DECLINE	DECLINE
N7	CID MISMATCH	INVALID CARD (CID) SECURITY CODE
NR	NO DEBIT ROUTE	No valid debit network available to route
RR	ERROR	Reference response tag AUTH_RESP_TEXT for details of the invalid data supplied in a request tag. If you are unable to determine the issue, contact the customer support team for further instructions.
S4	CRYPTO FAILURE	PIN BLOCK TRANSLATION ERROR
S5	UNABLE TO LOCATE	Unable to locate a matching original purchase transaction
S7	INVALID RETURN	Unable to locate a matching original purchase transaction
S8	NO AUTHORIZATION	Unable to locate a matching authorization
S9	TLV TAGS INVALID	TLV TAGS INVALID
SS	BRIC STORAGE EXPIRED	BRIC STORAGE ACCT VERIFY DATA HAS EXPIRED
ST	ACCOUNT VERIFY FAILED	BRIC STORAGE ACCT VERIFY DATA FAILED
SU	TOKEN DECRYPTION FAILED	APPLE TTP / VISA VAC TOKEN DECRYPTION FAILED
SV	CALL	MERCHANT HAS BEEN SUSPENDED BY RTF
SW	REQUIRED DETAIL NOT PROVIDED	REQUIRED TRANSACTION DETAIL WAS NOT PROVIDED
Amex Specific Codes – Will only map to NETWORK_RESPONSE		
CODE	**DISPLAY**	**DESCRIPTION**
000	APPROVAL	APPROVED
001	APPROVE WITH ID	APPROVE WITH ID
002	PARTIAL APPROVAL	PARTIAL APPROVAL

AMERICAN EXPRESS		
100	DECLINE	DENY
101	EXPIRED CARD	EXPIRED CARD
106	PIN EXCEEDED	PIN EXCEEDED
107	PLEASE CALL	PLEASE CALL ISSUER
109	TERM ID ERROR	INVALID MERCHANT
110	AMOUNT ERROR	INVALID AMOUNT
111	NO ACCOUNT	INVALID ACCOUNT
115	SERV NOT ALLOWED	SERVICE NOT PERMITTED
116	DECLINE	INSUFFICIENT FUNDS
117	WRONG PIN	INVALID PIN
119	NO CARD RECORD	NO CARD RECORD
121	DECLINE	LIMIT EXCEEDED
125	EXPIRED CARD	INVALID EFFECTIVE DATE
181	FORMAT ERROR	FORMAT ERROR
183	DECLINE	INVALID CURRENCY CODE
187	INVALID ACCT NBR	DENY-NEW CARD ISSUED
189	TERM ID ERROR	DENY-CANCELED OR CLOSED MERCHANT
200	HOLD-CALL	DENY-PICK UP CARD
900	SYSTEM ERROR	ATC SYNCHRONIZATOIN
909	SYSTEM ERROR	SYSTEM MALFUNCTION (CRYPTO ERROR)
912	NO REPLY	ISSUER NOT AVAILABLE

PINless Debit Response Codes

PINless Debit Response Codes

Code	Display
00	Approved
01	Call
02	Call
03	Term Id Error
04	Hold-Call
05	Decline
06	Error
08	Honor With Id
10	Approved
11	Approved
12	Invalid Trans

Code	Display
13	Amount Error
14	Card No. Error
15	No Such Issuer
19	Re Enter
21	No Action Taken
22	No Action Taken
25	Unable To Locate
30	Format Error
33	Hold-Call
34	Hold-Call
36	Hold-Call
40	Totals Avail
41	Hold-Call
43	Hold-Call
51	Decline
52	No Check Account
53	No Save Account
54	Expired Card
55	Wrong PIN
57	Serv Not Allowed
61	Decline
62	Decline
63	Key Sync Error
65	Decline
66	Hold-Call
67	Hold-Call
75	PIN Exceeded
76	No Action Taken
82	Cashback Not App
86	Cant Verify PIN
90	System Error
91	No Reply

Code	Display
92	Invalid Routing
93	Decline
94	Dup Trans
96	System Error
E2	AVS Required
E3	CVV2 Required
EA	Account Length Error
EB	Check Digit Error
ES	Decline

AUTH_RESP_DETAIL

The AUTH_RESP_DETAIL field contains additional information for declined transactions. This information can change at any time and should not be used in code to validate the response of a transaction. The field is used to provide more information about the transaction when there is a decline. This field is not returned for all transaction and card types. A response version of Dynamic XML or 9 and higher is required.

NOTE: The EPX terminal profile must be set with minimum Response Version of 9 or to Dynamic XML.

- Variable Type: Alphanumeric
- Max Length: 1024

Example:

```
<FIELD KEY="AUTH_RESP_DETAIL">INVALID OR MISSING FLEET TAGS: 04 06</FIELD>
```

AUTH_RESP_TEXT

The AUTH_RESP_TEXT field contains additional information for the transaction requested. This information can change at any time and should not be used in code to validate the response of a transaction (except for a limited case with Account Updater, for MasterCard only). The field is used to provide more information about the transaction when there is a decline, or a transaction with insufficient information to process.

- Variable Type: Alphanumeric
- Max Length: 80

Example:

```
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
```

AUTH_RESP_TEXT_ENHANCED

The AUTH_RESP_TEXT_ENHANCED field contains additional information for declined transactions. This information can change at any time and should not be used in code to validate the response of a transaction. The field is used to provide more information about the transaction when there is a layered decline. This field is not returned for all transaction and card types. A response version of 10 and higher is required or can be set to "999" which will inherit new response versions as they are made available.

NOTE: The EPX terminal profile must be set with minimum Response Version of 10 or above.

- Variable Type: Alphanumeric
- Max Length: 512

Example:

```
<FIELD KEY="AUTH_RESP_TEXT_ENHANCED">DECLINED - CANNOT APPROVE AT THIS TIME, TRY
AGAIN LATER</FIELD>
```

AUTH_SPECIAL_1

The AUTH_SPECIAL_1 field contains the Purchase APR for a Citi Bank Private Label Auth or Sale transaction.

- Variable Type: Numeric
- Max Length: 25

Example:

```
<FIELD KEY="AUTH_SPECIAL_1">29.5</FIELD>
```

AUTH_SPECIAL_2

The AUTH_SPECIAL_2 field contains the APR Type for a Citi Bank Private Label Auth or Sale transaction.

- Variable Type: Alpha
- Max Length: 25

Example:

```
<FIELD KEY="AUTH_SPECIAL_2">V</FIELD>
```

AUTH_SPECIAL_3

The AUTH_SPECIAL_3 field contains the Status Flag for a Citi Bank Private Label Auth or Sale transaction.

- Variable Type: Alpha
- Max Length: 25

Example:

```
<FIELD KEY="AUTH_SPECIAL_3">A</FIELD>
```

AUTH_TRAN_DATE_GMT

The AUTH_TRAN_DATE_GMT field contains the date and time in GMT of when the transaction was processed.

- Variable Type: Alphanumeric
- Max Length: 22

Example:

```
<FIELD KEY="AUTH_TRAN_DATE_GMT">06/19/2009 05:31:40 PM</FIELD>
```

AUTH_TRAN_IDENT

The AUTH_TRAN_IDENT response tag contains the NTID (Network Transaction ID) value that is returned by the Networks only for approved transactions.

Note: This value is specifically used to support PAN based COF / MIT transactions, and is non-applicable to EPX BRIC / GUID based COF / MIT transactions.

- Variable Type: Alphanumeric
- Max Length: 20
- REGEX: ^([A-Z0-9]){0,20}$

Example:

```
<AUTH_TRAN_IDENT>210817175754976</AUTH_TRAN_IDENT>
```

BATCH_ID

The BATCH_ID field contains the Batch ID sent in during the transaction request. This field is defined in the Transaction Request Fields.

- Variable Type: Numeric
- Max Length: 10

Example:

```
<FIELD KEY="BATCH_ID">20090315</FIELD>
```

LOCAL_DATE

The LOCAL_DATE field contains the local date the transaction request was sent relative to the time zone setting on the terminal that was used during the request.

- Variable Type: Numeric
- Format: MMDDYY
- Max Length: 6

The following example represents April 10, 2017:

```
<LOCAL_DATE>041017</LOCAL_DATE>
```

NETWORK_RESPONSE

The NETWORK_RESPONSE field includes additional information on the result of the transaction from the issuing bank. Refer to the response code tables for information on ACH, CC, and PIN-less Debit. The AUTH_RESP field should be used as the primary determination for the result of the transaction, and the NETWORK_RESPONSE used as a secondary source containing additional information usually for the declined reasoning.

- Variable Type: Alphanumeric
- Max Length: 3

Example:

```
<FIELD KEY="NETWORK_RESPONSE">05</FIELD>
```

LOCAL_TIME

The LOCAL_TIME field contains the local time the transaction request was sent relative to the time zone setting on the terminal that was used during the request.

- Variable Type: Numeric
- Format: HHMMSS (24hr)
- Max Length: 6

Example:

```
<LOCAL_TIME>100205</LOCAL_TIME>
```

ORIG_TRAN_TYPE

The ORIG_TRAN_TYPE field contains the TRAN_TYPE sent in the original transaction request from the client application. In some scenarios, and based on certain processing rules, the EPX platform may automatically change the TRAN_TYPE value before sending the transaction to the Card Networks for approval. The ORIG_TRAN_TYPE field will contain the original TRAN_TYPE value from the client request and can be used for matching purposes. The newly returned value in the TRAN_TYPE field will contain the transaction type that the transaction was processed as (after potentially being changed by EPX).

NOTE: The EPX terminal profile must be set with minimum Response Version of 8 or to Dynamic XML.

- Variable Type: Alphanumeric
- Max Length: 4

Example:

```
<ORIG_TRAN_TYPE>CCR9</ORIG_TRAN_TYPE>
```

TRAN_NBR

The TRAN_NBR field contains the transaction number sent in during the transaction request. This field is defined in the Transaction Request Fields.

- Variable Type: Numeric
- Max Length: 10

Example:

```
<FIELD KEY="TRAN_NBR">123</FIELD>
```

TRAN_TYPE

The TRAN_TYPE field contains the transaction type code sent in during the transaction request. This information identifies the nature, purpose, and/or reason for an individual transaction, primarily used for regulatory reporting requirements.

- Variable Type: Alphanumeric
- Max Length: 4

Example:

```
<FIELD KEY="TRAN_TYPE">CCE1</FIELD>
```

PayPage and Browser Post API Request Fields

This chapter describes the fields that can be used in a transaction request to the EPX PayPage or Browser Post API.

CANCEL_URL

The CANCEL_URL field contains the URL that the customer will be redirected to when the **Cancel** button is selected by the user from the PayPage. During this process the session will be destroyed and then the redirection will occur. If no redirect URL is provided, the default redirection is to an epx webpage.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
CANCEL_URL=www.merchantswebsite.com/cancel.htm
```

CUSTOM_CSS_URL

The CUSTOM_CSS_URL field and the CUSTOM_JAVASCRIPT_URL field are used together to allow development of the PayPage customization. This field would contain the URL of the CSS file that the merchant would host locally in their environment. When sent in the PayPage POST, the browser will use the local file to customize the PayPage allowing an easier development process. This field will only work in the test environment and will be ignored if sent in Production.

- Variable Type: Alphanumeric
- Max Length: N/A

NOTE: If you experience errors calling your locally hosted CSS scripts with http://, try using https:// instead.

Key Value Pair Example:

```
CUSTOM_CSS_URL=http://localhost/9001-900300-1.css
```

CUSTOM_JAVASCRIPT_URL

The CUSTOM_JAVASCRIPT_URL field and the CUSTOM_CSS_URL field are used together to allow development of the PayPage customization. This field would contain the URL of the JavaScript PHP file that the merchant would host locally in their environment. When sent in the PayPage POST, the browser will use the local file to customize the PayPage allowing an easier development process. This field will only work in the test environment and will be ignored if sent in Production.

NOTE: If you experience errors calling your locally hosted js scripts with http://, try using https:// instead.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
CUSTOM_JAVASCRIPT_URL=http://localhost/9001-900300-1.php
```

FORCE_CREDIT

The FORCE_CREDIT field contains a value which will determine if the PayPage will require the use of a credit card transaction rather than giving the option of various transaction types on the page, such as PIN-less debit or ACH. This field is used when a PayPage is set up for both credit card and PIN-less debit transactions.

- Variable Type: Alpha
- Max Length: 1

Key Value Pair Example:

```
FORCE_CREDIT=Y
```

FORCE_CREDIT Values

- Y—Sending a tag with a value of Y will allow only credit card transactions. All PIN-less debit options that would otherwise be available on the page will not be available.
- N—When this field is not sent, the default value is N.

INVALID_REDIRECT_URL

The INVALID_REDIRECT_URL field contains the URL the user will be redirected to when there is an issue with the TAC during a PayPage or Browser Post API request.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
INVALID_REDIRECT_URL=www.merchantswebsite.com/tac_invalid.html
```

INVALID_REDIRECT_URL Error Cases

- Post no parameters in the post
- Empty TAC value on initial post
- TAC decryption error
- Expired TAC—A TAC is good for 2 hours after generation
- Invalid TAC—Failed 4-part Key match
- Invalid TAC—TRAN_NBR doesn't match value supplied in TAC
- Invalid TAC—Invalid 4-part Key
- Multiple TAC Use

RECEIPT

The RECEIPT field contains a value which will determine if the receipt is shown after a PayPage transaction prior to redirecting the user to the URL sent in the REDIRECT_URL field.

- Variable Type: Alpha
- Max Length: 1

Key Value Pair Example:

```
RECEIPT=N
```

NOTE: When this field is not sent, the default value is Y.

RECEIPT Values

- Y—The PayPage will show the receipt before redirecting the user.
- N—This value will redirect without first showing the receipt.

REDIRECT_ECHO

The REDIRECT_ECHO field contains a value which will determine how much of the transaction response will be posted to the URL sent in the REDIRECT_URL. The values used with the REDIRECT_ECHO field are below.

- Variable Type: Alpha
- Max Length: 1

Key Value Pair Example:

```
REDIRECT_ECHO=V
```

NOTE: When this field is not sent, the default value is R.

REDIRECT_ECHO Values

- N—No response will be sent to the REDIRECT_URL.
- R—The default response fields will be sent to the REDIRECT_URL.
- V—A verbose response will be sent to the REDIRECT_URL. The verbose response contains the default response files as well as the additional fields submitted with the transaction request.

REDIRECT_NON_APPROVALS

The REDIRECT_NON_APPROVALS field contains a value that determines if the user will be redirected on a decline to the URL sent in the REDIRECT_URL field during a PayPage transaction. The values used with the REDIRECT_NON_APPROVALS field are below.

- Variable Type: Alpha
- Max Length: 1

Key Value Pair Example:

```
REDIRECT_NON_APPROVALS=N
```

NOTE: When this field is not sent, the default value is N.

REDIRECT_NON_APPROVALS Values

- Y—The PayPage redirects the user.
- N—This value will not redirect the user, but allows him to resubmit the transaction using the same BATCH_ ID/TRAN_NBR combination as the original transaction attempt.

REDIRECT_URL

The REDIRECT_URL field contains the URL the user will be redirected to once the transaction has been completed during a PayPage or Browser Post transaction. This URL can also be made to accept the post of response values during the redirection.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
REDIRECT_URL=www.merchantswebsite.com/transaction_complete.php
```

RESPONSE_ECHO

The RESPONSE_ECHO field contains a value to determine how much of the transaction response will be posted to the URL sent in the RESPONSE_URL. The values used with the RESPONSE_ECHO field are below.

- Variable Type: Alpha
- Max Length: 1

Key Value Pair Example:

```
RESPONSE_ECHO=V
```

NOTE: When this field is not sent, the default value is R.

RESPONSE_ECHO Values

- R—The default response fields will be sent to the RESPONSE_URL.
- V—A verbose response will be sent to the RESPONSE_URL. The verbose response contains the default response fields as well as the additional fields submitted with the transaction request.

RESPONSE_FORMAT

The RESPONSE_FORMAT field contains the value XML which will instruct the PostMaster to post the transaction response in XML format to the URL sent in the RESPONSE_URL. When this field is not sent, the default format of the response will be key value pairs.

- Variable Type: Alpha
- Max Length: 1

Key Value Pair Example:

```
RESPONSE_FORMAT=XML
```

RESPONSE_URL

The RESPONSE_URL field contains the URL of an HTTP server in the merchant domain that will receive the transaction results via HTTP post from the EPX Postmaster application.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
RESPONSE_URL=www.merchantswebsite.com/accept_response.php
```

TAC

The TAC field contains the Terminal Authentication Code generated by the EPX Key Exchange service. The TAC is a required field when calling the PayPage or Browser Post API.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
TAC=FEU86Eo5/S1jfob4gVaDPP7w1IpJSFIiehqsHymY7dltXrJmcRNMAw==
```

TIMEOUT_REDIRECT_URL

The TIMEOUT_REDIRECT_URL field contains the URL the user will be redirected to when the PayPage session times out (default of 15 minutes).

NOTE: To change the session timeout minutes, contact your EPX Integration specialist.

- Variable Type: Alphanumeric
- Max Length: N/A

Key Value Pair Example:

```
TIMEOUT_REDIRECT_URL=www.merchantswebsite.com/session_timeout.html
```

TRAN_CODE

The TRAN_CODE field contains the transaction code that loosely corresponds to the EPX TRAN_TYPE field. This field can be configured in the custom JavaScript that is used to customize the PayPage API and will dictate the transaction performed on the PayPage during submission. This field is also required when using a web form to send a transaction to the Browser Post API. Refer to the TRAN_GROUP field definition for more information on the possible values for this field.

TRAN_GROUP

The payment page may offer an end user a choice of payment methods, which would then determine the TRAN_ CODE tag that is submitted by the PayPage API, or to the Browser Post API by the merchant payment page. The TRAN_GROUP field is used during the KeyExchange request to validate that the TRAN_CODE submitted during the transaction corresponds to a general category of payment types, since the merchant may not know which payment option the customer will choose on the payment page at the time of serving the page. The following table shows the available values for TRAN_GROUP and the corresponding TRAN_CODE values that must match for successful validation. Refer to the TRAN_TYPE field definition for more information on the corresponding TRAN_TYPEs listed.

- Variable Type: Alpha
- Max Length: N/A

Key Value Pair Example:

```
TRAN_GROUP=SALE
```

Specified Groups

TRAN_ GROUP Values

TRAN_GROUP	TRAN_CODE	TRAN_TYPE
SALE	SALE	CCX1
	DBSALE	DB00
	PLDBSALE	DB0P
	ACHSALE_C	CKC2
	ACHSALE_S	CKS2
AUTH	AUTH	CCX2
CAPTURE	CAPT	CCX4
REFUND	REFUND	CCX9
	DBREFUND	DB01
	ACHCREDIT_C	CKC3
	ACHCREDIT_S	CKS3
AVS	AVS	CCX0
PRENOTE	ACHPNDEBIT_C	CKC0
	ACHPNDEBIT_S	CKS0
	ACHPNCREDIT_C	CKC1
	ACHPNCREDIT_S	CKS1
STORAGE	STORAGE	CCX8
	ACHSTORAGE_C	CKC8
	ACHSTORAGE_S	CKS8

Browser Post Validation Response Fields

BP_FIELD_ERRORS

The BP_FIELD_ERRORS field will contain a pipe/caret-delimited list of the fields that failed and the reason code for the failure, during a request to the Browser Post API. In the example below, the ACCOUNT_NBR and EXP_DATE fields were missing and the FIRST_NAME field failed the regular expression validation. All other POSTed fields were accepted by the Browser Post system. The possible field error reason codes are listed in the following table.

Example:

```
BP_FIELD_ERRORS = 'first_name^FE_002|account_nbr^FE_001|exp_date^FE_001'
```

BP_FIELD Error Codes

Code	Description
FE_001	Required Field Missing
FE_002	Field failed RegEx Validation
FE_003	ACCOUNT_NBR failed MOD-10 check

BP_RESP_CODE and BP_RESP_TEXT

The BP_RESP_CODE field contains a code value that corresponds with one of the specific validation events that can occur when processing using the Browser Post API. The table below outlines the possible codes that may be received. Contact the EPX Integration team for assistance in troubleshooting error messages received while implementing the Browser Post API.

BP_RESP_CODE

BP_RESP_CODE	BP_RESP_TEXT
BP_000	Success

Merchant Configuration Errors

These errors are a result of instances where the Merchant configuration file cannot be loaded. Without this file we cannot access the merchant's stored value for INVALID_REDIRECT_URL, so the client browser will be redirected to a generic EPX error page.

NOTE: Due to the nature of the issue, these errors cannot be returned; however, they will be logged and for assistance in troubleshooting contact the Integration team at EPX.

Merchant Configuration Errors

BP_RESP_CODE	BP_RESP_TEXT
BP_100	Missing TAC
BP_101	TAC decryption error
BP_102	Invalid TAC parameter
BP_103	TAC validation – 4-part key mismatch
BP_104	Merchant configuration not found
BP_105	Merchant configuration decryption error
BP_106	Merchant configuration parse error
BP_110	Merchant REDIRECT_URL not configured

REDIRECT_URL Validation Errors

These errors are a result of instances where the REDIRECT_URL cannot be validated. If a merchant provides a value for INVALID_REDIRECT_URL, the browser will be redirected there with error codes, response variables, etc. If INVALID_REDIRECT_URL is not configured, the browser will be redirected to the EPX generic error page.

REDIRECT_URL Validation Errors

BP_RESP_CODE	BP_RESP_TEXT	Additional Detail
BP_111	TAC validation – REDIRECT_URL missing	This response occurs when a redirect URL was not sent.
BP_112	TAC validation – Invalid REDIRECT_URL	If this error occurs the system will append the value for REDIRECT_URL contained in the TAC to the response output, using the tag: REDIRECT_URL
BP_113	Merchant REDIRECT_URL mismatch	If this error occurs the RTBP system will append the value for REDIRECT_URL contained in the TAC to the response output, using the tag: REDIRECT_URL. In addition, the system will also echo back the stored (configured URL, sans query string) value for REDIRECT_URL, using the tag: MERCH_REDIRECT_URL

Basic Validation Errors

These errors are a result of instances where the REDIRECT_URL has been validated, but there is an additional validation issue. The code will be returned to the REDIRECT_URL address if they occur. The BP_140 code is used for any field mismatch validation failures.

Basic Validation Errors

BP_RESP_CODE	BP_RESP_TEXT
BP_120	Multiple TAC use
BP_121	Expired TAC
BP_122	TAC validation - TRAN_NBR missing
BP_123	TAC validation - TRAN_GROUP missing
BP_124	TAC validation - AMOUNT missing
BP_125	TAC validation - POST value mismatch
BP_126	TAC validation - Invalid merchant validation code (MVC)
BP_127	TAC validation - Invalid RESPONSE_URL
BP_128	TAC validation - TRAN_GROUP mismatch
BP_129	TAC validation - Unknown TRAN_GROUP
BP_130	Unknown tran_code
BP_131	System Error
BP_132	3-D Secure authentication failure
BP_133	3-D Secure system error
BP_140	Field error

Verified by Visa and MasterCard SecureCode Request Fields

CAVV_RESP

The CAVV_RESP field contains the response returned by the authentication agent. Refer to the table below for additional information about possible values for this field.

- Variable Type: Numeric
- Max Length: 1

Example:

```
<CAVV_RESP>5</CAVV_RESP>
```

CAVV_RESP Values

CAVV_RESP Values

CAVV_ RESP	Request Card Type	Condition
0	MasterCard	Used when UCAF data collection is not supported by the merchant.
1	MasterCard	Used when UCAF data collection is supported by the merchant, but was not populated.
2	MasterCard	Used when UCAF data collection is supported by the merchant and the CAVV_UCAF field is populated.
5	Visa	Used when submitting a secure ecommerce transaction.
6	Visa	Used when submitting a non-authenticated security transaction at a 3-D Secure-capable merchant, and the merchant attempted to authenticate the cardholder data using 3-D Secure.
7	Visa	Used when submitting a non-authenticated security transaction.
8	Visa	Used when submitting a non-secure transaction.
9	Visa	For optional regional use only.

CAVV_UCAF

The CAVV_UCAF field contains the UCAF string returned by the authentication agent and can contain up to 81 characters.

When sending a MasterCard request, if the values of 0 or 1 are submitted in the CAVV_RESP field, the CAVV_UCAF field is not required; however if the value of CAVV_RESP is 2, the UCAF data string is required in Base64 format.

When sending a Visa request, if the string length is 28 it will be considered to be in Base64 format; if the string length is 40 it will be considered to be in HEX format; if its length is not equal to 28 or 40 it will not be included in the authorization request.

The optional XID can be in BASE64 or HEX (40) representation. If present, place a "|" (vertical bar) after the CAVV_UCAF and then append the XID value.

- Variable Type: Alphanumeric
- Max Length:81

Example (HEX):

```
<CAVV_UCAF>00000107327993123456789012799300000000000</CAVV_UCAF>
```

Example (Base64):

```
<CAVV_UCAF>jCgfkf1O8LnoCBEAAAAbBQQAAAA=</CAVV_UCAF>
```

DIRECTORY_SERVER_TRAN_ID

The DIRECTORY_SERVER_TRAN_ID field contains the MasterCard Directory Server Transaction ID and can contain up to 36 characters. This is required for MasterCard 3DS version 2 transctions.

The Directory Server Transaction ID is a Universally Unique Transaction ID which can be provided by the processors/acquirers as part of the authentication transaction and is required to be sent with the transaction if the authentication agent provides it in the response.

- Variable Type: Alphanumeric
- Max Length:36

Example:

```
<DIRECTORY_SERVER_TRAN_ID>f38e6948-5388-41a6-bca4-
b49723c19437</DIRECTORY_SERVER_TRAN_ID>
```

TDS_VER

The TDS_VER field contains the 3DS version of the authentication agent. This field is required for the use of 3DS version 2. The table below contains the possible values for this field.

- Variable Type: Numeric
- Max Length: 2

Example:

```
<TDS_VER>1</TDS_VER>
```

TDS_VER Values

TDS_VER	Condition
2	3DS Version 2

TOKEN_TRAN_IDENT

The TOKEN_TRAN_IDENT is the Token Transaction Identifier and is required to be sent with the transaction if returned by the authentication agent or token provider.

A 44-byte base64 value will be sent for MasterCard BIN ranges.

A 64-byte base64 value will be sent for Visa BIN ranges, Hex is 128

- Variable Type: Alphanumeric
- Max Length: 128

Example (Base64):

```
<TOKEN_TRAN_IDENT>
e220aa1707zz15987a375f9f8359e27dcbc1abz1f959a379d1308dd8731c9371</TOKEN_TRAN_IDENT
>
```

Visa Money Transfer (VMT) Request & Response Fields

This section outlines the request and response fields specific to VMT transactions, Account Funding Transaction (AFT), Watch List Screening (WLS), and Original Credit Transaction (OCT).

Request Fields

The request fields are organized into tag-length-value (TLV) fields, which in turn consist of multiple tags. Accordingly, this section is organized by TLV field and tag.

NOTE: This section provides a summary of the important transaction fields. For comprehensive information about all VMT fields, refer to the *Transaction Specs - Visa Money Transfer* guide.

TLV tags

Visa requires Money Transfer data to be presented in type-length-value (TLV) format, which is a method of encoding information in a single string, versus multiple EPX tags.

TLV data is grouped into a TLV_SETS tag, which is a set of two or more TLV elements. Various types of TLV sets exist, as described in the *Transaction Specs - Visa Money Transfer* guide.

TLV tag 007 from TLV set "SENDER"

Within the TLV set "SENDER," TLV tag 007 contains the Sender Country Code. The originator must provide the sender's country in this field on cross-border transactions and U.S. domestic transactions. This will use the 3-digit ISO numeric country code.

This is for the TLV set "SENDER"

- Mandatory: OCT and WLS Transactions
- Length: 3
- Format: Alphanumeric

TLV tag 011 from TLV set "SENDER"

Within the TLV set "SENDER," TLV tag 011 contains the Sender Account Number. If the sender's account number is available, the originator must provide it in this field. If the sender's account number is not available, the originator must provide the Sender Reference Number in the SPECIAL_3 field.

- Mandatory: OCT and WLS Transactions
- Length: 34
- Format: Alphanumeric

TLV tag 012 from TLV set “SENDER”

Within the TLV set “SENDER,” TLV tag 012 contains the Sender Reference Number. If the sender’s account number is not available, the originator must provide the Sender Reference Number in this field. Even when the Sender Account Number is available, it is strongly recommended that the originator provides the Sender Reference Number in addition to the Sender Account Number.

- Mandatory: OCT and WLS Transactions
- Length: 16
- Format: Alpha-Numeric

TLV tag 001 from TLV set “TRAN_DATA”

Within the TLV set “TRAN_DATA,” TLV tag 001contains a numeric code that indicates the funding source. The possible values are provided in the table below.

Funding Source Code Values

Value	Definition
04	Cash
05	DDA Account
06	Mobil Money Account
V1	Visa Credit
V2	Visa Debit
V3	Visa Prepaid

- Mandatory: OCT transactions
- Length: 2
- Format: Alphanumeric

TLV tag 005 from TLV set “TRAN_DATA”

Within the TLV set “TRAN_DATA,” TLV tag 005 contains the Business Application identifier. The table below provides the values for OCT and AFT transactions.

NOTE: Additional business application identifiers may be supported by the EPX platform, please confirm with your relationship manager or integration specialist.

Applicable OCT Business Application Identifier Values

Value	Definition
AA	Account to Account / Sender and Recipient are the same person
BA	I Value Description
BB	Business to Business
BI	Money transfer—bank-initiated
BP	Non-card bill payment
CP	Card bill payment*
FD	Funds disbursement*
GD	Government disbursement
GP	Gambling payout (other than online gambling)
LO	Loyalty and offers
MD	Merchant disbursement*
MI	Money transfer—merchant-initiated
OG	Online gambling payout
PD	Payroll/pension disbursement
PP	Person to Person / Sender and Recipient are not the same person
TU	Top-Up for enhanced prepaid loads*
WT	Wallet transfer (digital wallet)

*U.S. domestic enhanced OCTs with the additional BAI values will be subject to the same conversion logic to merchandise returns, and network processing on both network 0002 and network 0003, as enhanced money transfer OCTs with a BAI value of AA or PP.

- Mandatory: OCT and AFT transactions
- Length: 2
- Format: Alpha

Applicable AFT Business Application Identifier Values

Value	Definition
AA	Account to Account / Sender and Recipient are the same person
BI	Money transfer—bank-initiated (MCC 6012 - Only)
PP	Person to Person / Sender and Recipient are not the same person
TU	Top-up for enhanced prepaid loads
WT	Wallet transfer (digital wallet)

- Mandatory: OCT and AFT transactions

- Length: 2
- Format: Alpha

REFERENCE_NBR

The REFERENCE_NBR field contains the Transaction Identifier from the WLS or AFT response. Having the transaction identifier from the WLS transaction is preferred over having it from an AFT transaction. The value is taken from the AUTH_SPECIAL_1 field in the response from the AFT or WLS request.

Optional: OCT Transactions

Response Fields

AUTH_SPECIAL_1

The AUTH_SPECIAL_1 field contains the Transaction Identifier. When a WLS is done, the transaction identifier from the response must be provided in the REFERENCE_NBR field of the OCT transaction request. When an AFT is done and there is no WLS transaction, the transaction identifier from the AFT must be provided in the REFERENCE_NBR field of the OCT request.

AUTH_SPECIAL_10

The AUTH_SPECIAL_10 field contains the WLS Data. When available this data would need to be sent in the SPECIAL_10 field during an OCT request.

MasterCard Money Transfer Request Fields

This section outlines the request fields specific to MasterCard Money Transfer SMS Funding and Payment transactions.

NOTE: This section provides a summary of the important transaction fields. For comprehensive information about all MasterCard Money Transfer fields, refer to the Transaction Specs - MasterCard Money Transfer guide.

Request Fields

ACI_EXT

The ACI_EXT field is fully defined in the ACI_EXT section, page 5. The table below provides the additional values that would be used to define the payment type when submitting MasterCard Money Transfer transactions.

ACI_EXT values for MasterCard Money Transfer

Value	Description
C02	MasterCard Rebate
C03	rePower Load Value
C04	Gaming Re-pay
C07	General Person-to-Person
C51	MoneySend Funding/Payment Indicator (Reserved for Future Use)
C52	General Transfer to Own Account
C53	Agent Cash Out
C54	Payment of Own Credit Card Bill
C55	Business Disbursement
C56	Government/Non-Profit Disbursement
C57	Rapid Merchant Settlement
C58	MoneySend Cash2ATM (Usage limited to specific countries)
C59	MoneySend Cash2Card (Usage limited to specific countries)
C65	General Business to Business Transfer
C67	MasterCard Merchant Presented QR
C68	MasterCard Merchant Presented QR Refund Payment
C91	Utility Payments (for Brazil domestic use only)
C92	Government Services (for Brazil domestic use only)
C93	Mobile phone top-ups (for Brazil domestic use only)
C94	Coupon booklet payments (for Brazil domestic use only)
F07	General Person-to-Person Transfer

Value	Description
F08	Person-to-Person Transfer to Card Account
F52	General Transfer to Own Account
F53	Agent Cash Out
F54	Payment of Own Credit Card Bill
F55	Business Disbursement
F61	Transfer to Own Staged Digital Wallet Account
F64	Transfer to Own Debit or Prepaid Account
F65	General Business-to-Business Transfer
P01	MasterCard ATM Cash Pick-Up Transaction
P10	Installment-based repayment
P70	Cryptocurrency
P71	High-risk Securities

- Length: 2
- Format: Numeric

TLV tag 001 from TLV set "TRAN_DATA"

MasterCard requires Money Transfer data to be presented in type-length-value (TLV) format, which is a method of encoding information in a single string, versus multiple EPX tags.

TLV data is grouped into a TLV_SETS tag, which is a set of TLV elements. Various types of TLV sets exist, as described in the *Transaction Specs - MasterCard Money Transfer* guide.

Within the TLV set "TRAN_DATA," TLV tag 001 contains a numeric code that indicates the funding source. The possible values are shown in the table below.

Funding Source Code values for TLV tag 001

Value	Definition
01	Credit (Non Visa)
02	Debit (Non Visa)
03	Prepaid (Non Visa)
04	Cash
05	DDA Account
06	Mobil Money Account

- Length: 2
- Format: Alphanumeric

Transaction fees

Overview

Platform Support:

Transaction fees can be applied as a percentage or as a flat fee to a Sale (CCx1) or an Auth Only (CCx2) transaction.

With the percentage option, a Minimum Fee and Maximum Fee amount can be configured in the merchant profile at the terminal level.

When enabled, EPX will perform the fee calculation on the back end, apply it to the total amount (AUTH_AMOUNT_REQUESTED) in the transaction request, and return specific details in the response message via the AUTH_FEE and AUTH_FEE_TEXT tags. To enable this feature in the Production environment, the client must submit a request directly through EPX Client Services or their relationship manager.

Flat Fee

EPX will add the fee to the total amount of the sale/authorization request and the response will contain tags AUTH_FEE and AUTH_FEE_TEXT that reflect the flat fee amount set in the terminal profile.

Example:

```
<FIELD KEY="AUTH_FEE">10.00</FIELD>
<FIELD KEY="AUTH_FEE_TEXT">10.00</FIELD>
```

Percentage

EPX will calculate the percentage amount into the total amount of the sale/authorization request; the response will contain tags AUTH_FEE reflecting the percentage amount and AUTH_FEE_TEXT reflecting the percentage rate with the maximum amount in parenthesis set in the terminal profile.

Example:

```
<FIELD KEY="AUTH_FEE">5.00</FIELD>
<FIELD KEY="AUTH_FEE_TEXT">5.00% (Max 25.00)</FIELD>
```

Transaction Response Fields

AUTH_FEE

The AUTH_FEE field contains the actual surcharge fee amount that was added and applied to the total AMOUNT in the transaction request.

- Variable Type: Numeric
- Max Length: 19
- Format: *N.NN*

Example:

```
<FIELD KEY="AUTH_FEE">5.00</FIELD>
```

AUTH_FEE_TEXT

The AUTH_FEE_TEXT field reflects the transaction (surcharge) percentage rate or flat fee amount that was used during the EPX platform's transaction fee calculation.

- Variable Type: Numeric
- Max Length: Var

Example:

```
<FIELD KEY="AUTH_FEE_TEXT">5.00% (Max 25.00)</FIELD>
```

Client Application Management / Support:

The client application has the ability to manage the transaction fee calculation on their end.

- For convenience fees, the amount would be indicated in the CONVENIENCE_FEE tag as a reference field for reporting purposes. The client application would be responsible for adding the convenience fee amount into the total AMOUNT prior to initiating the transaction request. Please reference the CONVENIENCE_FEE field definition for additional information.
- For surcharge fees, the amount would be indicated in the TRAN_FEE tag and the EPX platform will add that to the total transaction AMOUNT prior to going out to the Networks for authorization. Please reference the TRAN_FEE field definition for additional information.

Visa Debt Repayment Program

This section outlines the request fields specific to Visa Debt Repayment transactions.

NOTE: This section provides a summary of the important transaction fields. For comprehensive information about all Visa Debt Repayment fields and requirements, refer to the *Transaction Specs – Visa Debt Repayment* guide.

Request Fields

ACI

The ACI field is fully defined in the *ACI* section, page *4* provides the value that would be used to define the payment type when submitting Visa Debt Repayment transactions.

Table 23: ACI value for Visa Debt Repayment

Value	Description
D	Debt Repayment / Consumer Loan

- Length: 2
- Format: Alphanumeric