BANK OF AMERICA

CHECKOUT API Developer's Guide

V1.1.0 - February 2024

Contents

1 Recent Revisions to This Document

V1.1.0
New Guide

2 About This Guide

This section describes how to use this guide and where to find further information.

2.1 Audience and Purpose

Using Secure Acceptance Hosted Payments Page requires minimal scripting skills. You must create a security script and modify your HTML form to invoke Secure Acceptance. You will also use your merchant services account to review and manage orders.

This guide is written for merchants who want to customize and control their own customer checkout experience, including receipt and response pages. After the customization, you will have full control to store and control customer information before sending it to Bank of America to process transactions, and to use Business Advantage 360 online banking to review and manage all your orders.

Using the Secure Acceptance Checkout API requires moderate scripting skills. You must create a security script and modify your HTML form to pass order information to Bank of America.

2.2 Conventions

These special statements are used in this document:

IMPORTANT: An Important statement contains information essential to successfully completing a task or learning a concept.

WARNING! A Warning contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.

3 Website Requirements

Your website must meet these requirements:

- It must have a shopping-cart or customer order creation software.

- It must contain product pages in one of the supported scripting languages. See Sample Transaction Process Using JSP.

- The IT infrastructure must be Public Key Infrastructure (PKI) enabled to use SSL-based form POST submissions.

- The IT infrastructure must be capable of digitally signing customer data prior to submission to Secure Acceptance.

4 Secure Acceptance Checkout API Overview

Bank of America Secure Acceptance Checkout API provides a seamless customer checkout experience that keeps your branding consistent. You can create a Secure Acceptance Checkout API profile and configure the required settings to set up your customer checkout experience.

Secure Acceptance Checkout API can significantly simplify your Payment Card Industry Security Standard (PCI DSS) compliance by sending sensitive payment card data directly from your customer's browser to Bank of America servers. Your web application infrastructure does not come in contact with the sensitive payment data and the transition is silent.

> ⚠️ IMPORTANT: Secure Acceptance is designed to process transaction requests directly from the customer browser so that sensitive payment data does not pass through your servers. Sending server-side payments using Secure Acceptance incurs unnecessary overhead and could result in the suspension of your merchant account and subsequent failure of transactions.

To create your customer's Secure Acceptance experience, you take these steps:

1. Create and configure Secure Acceptance Checkout API profiles.

2. Update the code on your web site to POST payment data directly to Bank of America from your secure payment form. See Sample Transaction Process Using JSP. Bank of America processes the transaction on your behalf by sending an approval request to your payment processor in real time. See Secure Acceptance Transaction Flow.

3. Use the response information to generate an appropriate transaction response page to display to the customer. You can view and manage all orders in the Business Center. You can configure the payment options, response pages, and customer notifications. See Creating a Secure Acceptance Profile.

4.1 Required Browsers

You must use one of these browsers to ensure that the Secure Acceptance checkout flow is fast and secure.

| Desktop browser	Mobile browser
IE 10 or later	iOS Safari 7.1 or later
Edge 13 or later	Android Browser 4.4 or later
Firefox 42 or later	Chrome Mobile 48 or later
Chrome 48 or later	
Safari 7.1 or later	
Opera7 or later	

4.2 Secure Acceptance Profile

A Secure Acceptance profile consists of settings that you configure to create a customer checkout experience. You can create and edit multiple profiles, each offering a custom checkout experience. For example, you might want to offer different payment options for different geographic locations.

4.3 Secure Acceptance Transaction Flow

Secure Acceptance Checkout API Transaction Flow
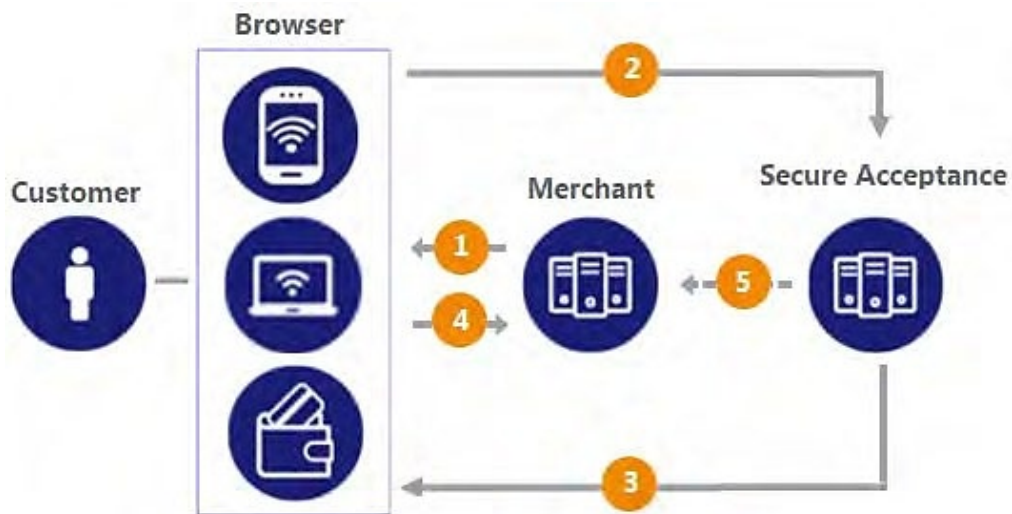
1. Display the checkout page on your customer's browser with a form to collect their payment information and include a signature to validate their order information (signed data fields).

    ⚠️ WARNING: Your system should sign all request fields except for fields that contain data the customer is entering. To prevent malicious actors from impersonating Bank of America, do not allow unauthorized access to the signing function.

2. The customer enters and submits their payment details (the unsigned data fields). The transaction request message, the signature, and the signed and unsigned data fields are sent directly from your customer's browser to the Bank of America servers. The unsigned data fields do not pass through your network.

    Bank of America reviews and validates the transaction request data to confirm it has not been amended or tampered with and that it contains valid authentication credentials. Bank of America processes the transaction and creates and signs the response message. The response message is sent to the customer's browser as an automated HTTPS form POST.

    ⚠️ WARNING: If the response signature in the response field does not match the signature calculated based on the response data, treat the POST as malicious and disregard it.

    Secure Acceptance signs every response field. Ignore any response fields in the POST that are not in the signed_fields field.

3. The response HTTPS POST data contains the transaction result in addition to the masked payment data that was collected outside of your domain. Validate the response signature to confirm that the response data has not been amended or tampered with.

   If the transaction type is sale, it is immediately submitted for settlement. If the transaction type is authorization, use the Simple Order API to submit a capture request when goods are shipped.

4. Bank of America recommends that you implement the merchant POST URL notification as a backup means of determining the transaction result. This method does not rely on your customer's browser. You receive the transaction result even if your customer lost connection after confirming the payment. See Merchant Notifications.

4.4 Payment Tokens

Payment tokens represent the customer token in the Token Management Service (TMS). They are unique identifiers for sensitive customer and payment data that cannot be mathematically reversed. The payment token replaces the payment card, and optionally the associated billing and shipping information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

Secure Acceptance offers limited support for TMS, providing the ability to create and update a customer's default payment and shipping information. In the Secure Acceptance API, the payment_token field identifies the TMS customer token.

4.4.1 Tokens That Represent a Card or Bank Account Only

Instrument identifier tokens represent a payment card number or bank account number. The same card number or bank account number sent in multiple token creation calls results in the same payment token being returned.

When using Secure Acceptance with tokens that represent only the card number or bank account, you must include associated data, such as expiration dates and billing address data, in your transaction request.

4.5 Level II Data

Secure Acceptance supports Level II data. Level II cards, also known as Type II cards, provide customers with additional information on their payment card statements. Business and corporate cards along with purchase and procurement cards are considered Level II cards.

For detailed descriptions of each Level II field, see the Bank of America Integration Guide that also describes how to request sale and capture transactions.

5 Payment Acceptance Configuration

5.1 Creating a Secure Acceptance Profile

Contact Bank of America Customer Support to enable your account for Secure Acceptance. You must activate a profile to use it. See Activating a Profile.

1. Log in to Merchant Services inside Business Advantage 360.

2. In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

3. Click New Profile. The Create Profile page appears.

4. Enter or verify these profile details.

   Profile Details

Profile detail	Description
Profile Name	The Secure Acceptance profile name is required and cannot exceed 40 alphanumeric characters.
Profile Description	The profile description cannot exceed 255 characters.
Integration Method	Check Checkout API.
Company Name	The company name is required and cannot exceed 40 alphanumeric characters.
Company Contact Name	Enter company contact name.
Company Contact Email	Enter company contact email.
Company Phone Number	Enter company contact phone number.
Payment Tokenization	Check Payment Tokenization. For more information, see Payment Transactions.
Fraud Management	Check Fraud Management. For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.
Verbose Data	Check Verbose Data. For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.

5. Click Submit.

5.2 Payment Method Configuration

You must configure at least one payment method before you can activate a profile.

5.2.1 Adding Card Types and Currencies

For each card type you choose, you can also manage currencies. Choose only the types of payment cards and currencies that your merchant account provider authorizes.

1. In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2. Find the profile and click the more options ellipsis (...).

3. Select Edit Profile. The General Settings page appears.

4. Click Payment Settings. The Payment Settings page appears.

5. Click Add Card Types. The list of card types appears.

6. Check each card type that you want to offer to the customer as a payment method. Your payment processor must support the card types.

7. Click the settings icon for each card type. The card settings and currencies list appear.

8. Check the currencies for each card. By default, all currencies are listed as disabled. You must select at least one currency. Contact your merchant account provider for a list of supported currencies.

9. Click Save.

5.2.2 3-D Secure Configuration (Future Use)

3-D Secure is the Bank of America implementation of Payer Authentication. It prevents unauthorized card use and provides added protection from fraudulent chargeback activity. 3-D Secure is not available to Bank of America merchants in production currently. You will see a Payer Authentication section within the Payment Acceptance Configuration tab in the Demonstration and Certification Environment (DCE) if you choose to use the DCE.

Before you can use Bank of America 3-D Secure, you must contact Bank of America Technical Support to configure your account. Your merchant ID must be enabled for 3D Secure.

Secure Acceptance supports 3-D Secure 1.0 and 2.0.

For Secure Acceptance, Bank of America supports these kinds of payer authentication:

- American Express SafeKey
- China UnionPay (3-D Secure 2.0 only)
- Diners ProtectBuy
- J/Secure by JCB
- Mastercard Identity Check
- Visa Secure

For each transaction, you receive detailed information in the replies and in the transaction details page of your Merchant Services account. You can store this information for 12 months. Bank of America recommends that you store the payer authentication data because you can be required to display this information as enrollment verification for any payer authentication transaction that you re-present because of a chargeback.

Your merchant account provider can require that you provide all data in human-readable format.

The language used on each payer authentication page is determined by your issuing bank and overrides the locale you have specified. If you use the test card numbers for testing purposes the default language used on the payer authentication page is English and overrides the locale you have specified. See Test and View Transactions.

5.2.2.1   Configuring Payer Authentication

1. In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2. Find the profile and click the more options ellipsis (...).

3. Select Edit Profile. The General Settings page appears.

4. Click Payment Settings. The Payment Settings page appears.

5. Choose a 3-D Secure version. If you choose 3-D Secure 2.0 and the card issuer is not 3-D Secure 2.0 ready, some transactions might still authenticate over 3-D Secure 1.0. The payer_authentication_specification_version response field indicates which version was used.

6. Click Save. The card types that support payer authentication are:

   - Amex
   - China UnionPay
   - Diners Club
   - JCB
   - Mastercard
   - Maestro (UK Domestic or International)
   - Visa

5.2.3   Enabling Automatic Authorization Reversals

For transactions that fail to return an Address Verification System (AVS) or a Card Verification Number (CVN) match, you can enable Secure Acceptance to perform an automatic authorization reversal. An automatic reversal releases the reserved funds held against a customer's card.

1.   In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2.   Find the profile and click the more options ellipsis (…).

3.   Select Edit Profile. The General Settings page appears.

4.   Click Payment Settings. The Payment Settings page appears.

5.   Check Fails AVS check. Authorization is automatically reversed on a transaction that fails an AVS check.

6.   Check Fails CVN check. Authorization is automatically reversed on a transaction that fails a CVN check.

7.   Click Save.

> ⚠️ IMPORTANT: When the AVS and CVN options are disabled and the transaction fails an AVS or CVN check, the customer is notified that the transaction was accepted. You are notified to review the transaction details. See Types of Notifications.

5.3   Security Keys

You must create a security key before you can activate a profile.

You cannot use the same security key for both test and production transactions. You must download a security key for each version of Secure Acceptance for test and production.

On the Profile Settings page, click Security. The Security Keys page appears. The security script signs the request fields using the secret key and the HMAC SHA256 algorithm. To verify data, the security script generates a signature to compare with the signature returned from the Secure Acceptance server. A security key expires in two years and protects each transaction from data tampering.

5.3.1 Creating Security Keys

1. Log in to your Merchant Services account.

2. In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

3. Find the profile and click the more options ellipsis (…).

4. Select Edit Profile. The General Settings page appears.

5. Click Security. The security keys page appears.

6. Click Create Key.

7. Enter a key name (required).

8. Choose signature version 1 (default).

9. Choose signature method HMAC-SHA256 (default).

10. Click Create.

11. Click Confirm. The Create New Key window expands and displays the new access key and secret key. This panel closes after 30 seconds.

12. Copy and save or download the access key and secret key.

   - Access key: Secure Sockets Layer (SSL) authentication with Secure Acceptance. You can have many access keys per profile. See Scripting Language Samples.

   - Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See Scripting Language Samples.

   IMPORTANT: Remember to delete the copied keys from your clipboard or cached memory.

   By default, the new security key is active. The other options for each security key are:

   - Deactivate: deactivates the security key. The security key is inactive.

   - Activate: activates an inactive security key.

   - View: displays the access key and security key.

13. When you create a security key, it is displayed in the security keys table. You can select a table row to display the access key and the secret key for that specific security key.

5.4 Merchant Notifications

Secure Acceptance sends merchant and customer notifications in response to transactions. You can receive a merchant notification by email or as an HTTPS POST to a URL for each transaction processed. Both notifications contain the same transaction result data.

Ensure that your system acknowledges POST notifications (even when under load) as quickly as possible. Delays of more than 10 seconds might result in delays to future POST notifications.

⚠️ IMPORTANT: Bank of America recommends that you implement the merchant POST URL to receive notification of each transaction. Parse the transaction response sent to the merchant POST URL and store the data within your order management system. This ensures the accuracy of the transactions and informs you when the transaction was successfully processed.

5.4.1 Configuring Merchant Notifications

1. In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2. Find the profile and click the more options ellipsis (...).

3. Select Edit Profile. The General Settings page appears.

4. Click Notifications. The Notifications page appears.

5. Choose a merchant notification in one of two ways:

    A. Check Merchant POST URL. Enter the HTTPS URL.

    Bank of America sends transaction information to this URL. For more information, see Response Fields. Only an HTTPS URL supporting TLS 1.2 or higher should be used for the merchant POST URL. If you encounter any problems, contact Bank of America Customer Support.

    B. Check Merchant POST Email. Enter your email address.

    Bank of America sends transaction response information to this email address including payment information, return codes, and all relevant order information. See Response Fields.

6. Choose the card number digits that you want displayed in the merchant or customer receipt:

    - Return payment card BIN: displays the card's Bank Identification Number (BIN), which is the first eight digits of the card number. All other digits are masked: 12345678xxxxxxxx

    - Return last four digits of payment card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxxx1234

    - Return BIN and last four digits of payment card number: displays the BIN and the last four digits of the card number. All other digits are masked: 12345678xxxx1234

7. Click Save.

5.5 Customer Receipts

You must send a purchase receipt email to your customer, and you may send a copy to your own email address. The email format is HTML unless your customer email is rich text format (RTF).

5.5.1 Configuring Customer Notifications

1. In the left navigation panel, choose Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2. Find the profile and click the more options ellipsis (...).

3. Select Edit Profile. The General Settings page appears.

4. Click Notifications. The Notifications page appears.

5. Check Email Receipt to Customer.

6. Enter the sender email address to be displayed on the customer receipt. The customer will reply to this email with any queries.

7. Enter the sender's name of your business. It is displayed on the customer receipt.

8. Check Send a copy to. This setting is optional.

9. Enter your email address to receive a copy of the customer's receipt. Your copy of the customer receipt will contain additional transaction response information.

5.6 Customer Response Page

You must configure the customer response page before you can activate a profile.

You must choose to display a response page to the customer at the end of the checkout process. Enter a URL for your own customer response page. This page is displayed to the customer after the transaction is processed. Review declined orders as soon as possible because you might be able.

to correct problems related to address or card verification, or you might be able to obtain a verbal authorization. You can also choose to display a web page to the customer after the checkout process is completed.

5.6.1 Configuring a Transaction Response Page

1. In the left navigation panel, choose Payment Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2. Choose a profile. The General Settings page appears.

3. Click Customer Response. The Customer Response page appears.

4. Enter the URL for your customer response page. Use port 80, 443, or 8080 in the URL. Only port 443 should be used with an HTTPS URL.

   A POST request with the transaction data is provided to this URL after the customer completes checkout.

   The POST request contains the reason code value of the transaction, which helps you determine possible actions to take on the transaction.

   See Reason Codes.

5. Click Save.

5.7 Activating a Profile

You must complete the required settings described in each of these sections before you can activate a profile:

- Payment Method Configuration

- Security Keys

- Customer Response Page

To activate a profile

1. On the left navigation pane, click the Payment Acceptance Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.

2. Find the inactive profile and click the Promote Profile button.

3. Click Confirm.

5.7.1 Additional Profile Options

- Deactivate: Deactivates the active profile. The profile is now listed in the inactive profile list. This option is available only for an active profile.

- Create Editable Version: Duplicates the active profile and creates an editable version. The editable version is listed in the inactive profile list. This option is available only for an active profile.

- Promote to Active: Activates the inactive profile. This option is available only for an inactive profile.

6   Scripting Language Samples

Secure Acceptance can support any dynamic scripting language that supports HMAC256 hashing algorithms.

Select the scripting language you use to download a sample script:

- JSP

- ASP.NET (C#)

- Ruby

- PHP

- Perl

- VB

6.1   Sample Transaction Process Using JSP

1. signedatafields.jsp file—paste your access key and profile ID into their respective fields. The customer enters billing, shipping, and other information. POST the fields to your server to sign and create the signature. The fields must be included in the signed_field_names field as a CSV list.

2. security.jsp file—security algorithm signs field and creates a signature using the signed_field_names field. Enter your security key in the SECRET_KEY field. Modify the security script to include the Secret Key that you generated in Security Keys.

   The security algorithm in each security script sample is responsible for:

   - Request authentication—the signature is generated on the merchant server by the keyed- hash message authentication code (HMAC) signing the request parameters using the shared secret key. This process is also carried out on the Secure Acceptance server, and the two signatures are compared for authenticity.

   - Response authentication—the signature is generated on the Secure Acceptance server by HMAC signing the response parameters, using the shared secret key. This process is also carried out on the merchant server, and the two signatures are compared for authenticity.

3. unsigneddatafields.jsp file—customer enters their payment information: card type, card number, and card expiry date. Include these fields in the unsigned_field_names field. POST the transaction to the Secure Acceptance endpoint.

7 Payment Transactions

This section provides endpoints and transaction use cases.

7.1 Endpoints and Transaction Types

Create Payment Token Endpoints See Creating a Payment Card Token.

Endpoint	URL	Supported transaction type
Test	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/token/create	create_payment_token
Production	https://secureacceptance.merchant-services.bankofamerica.com/silent/token/create	create_payment_token

Iframe Create Payment Token Endpoints See Iframe Implementation.

Endpoint	URL	Supported transaction type
Test	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/create	create_payment_token
Production	https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/create	create_payment_token

Iframe Transaction Endpoints See Iframe Implementation.

Endpoint	URL	Supported transaction type
Test	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/pay	- authorization - authorization, create_payment_token - authorization, update_payment_token - sale - sale, create_payment_token - sale, update_payment_token - create_payment_token
Production	https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/pay	- authorization - authorization, create_payment_token - authorization, update_payment_token - sale - sale, create_payment_token - sale, update_payment_token - create_payment_token

Iframe Update Payment Token Endpoints See Iframe Implementation.

Endpoint	URL	Supported transaction type
Test	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/update	update_payment_token
Production	https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/update	update_payment_token

Endpoint	URL	Supported transaction type
Test	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/pay	- authorization - authorization, create_payment_token - authorization, update_payment_token - sale - sale, create_payment_token - sale, update_payment_token
Production	https://secureacceptance.merchant-services.bankofamerica.com/silent/pay	- authorization - authorization, create_payment_token - authorization, update_payment_token - sale - sale, create_payment_token - sale, update_payment_token

Update Payment Token Endpoints See Payment Token Updates.

Endpoint	URL	Supported transaction type
Test	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/token/update	update_payment_token
Production	https://secureacceptance.merchant-services.bankofamerica.com/silent/token/update	update_payment_token

7.2   Required Signed Fields

Signing fields protects them from malicious actors adding or changing transaction data during transmission. To sign fields, include them in a comma-separated string in the signed_field_names field in your request.

⚠️   IMPORTANT: To prevent data tampering, sign all request fields except for fields that contain data the customer is entering.

These signed fields are required in all Secure Acceptance requests:

- access_key

- amount

- currency

- locale

- payment_method

- profile_id

- reference_number

- signed_date_time

- signed_field_names

- transaction_type

- transaction_uuid

- unsigned_field_names

For descriptions of these fields, see Request Fields.

7.3   Payment Tokens

7.3.1   Creating a Payment Card Token

⚠️   IMPORTANT: Include the appropriate endpoint that supports the create_payment_token transaction type. See Endpoints and Transaction Types. For descriptions of all request and response fields. See Checkout API Fields.

Include all request fields in the signed_field_names field except for the card_number, card_cvn, and signature fields. The signed_field_names field is used to generate a signature that is used to verify the content of the transaction to prevent data tampering.

7.3.1.1 Example: Creating a Standalone Payment Card Token

Request

```
reference_number=123456789
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_city=Mountain View
bill_to_address_postal_code=94043
bill_to_address_state=CA
bill_to_address_country=US
```

Response

```
req_reference_number=123456789
req_transaction_type=create_payment_token
req_locale=en
req_amount=100.00
req_payment_method=card
req_card_type=001
req_card_number=xxxxxxxxxxxx1111
req_card_expiry_date=12-2022
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_city=Mountain View
req_bill_to_address_postal_code=94043
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
```

```
req_reference_number=123456789
req_transaction_type=create_payment_token
req_locale=en
req_amount=100.00  req_payment_method=card
req_card_type=001
req_card_number=xxxxxxxxxxxx1111
req_card_expiry_date=12-2022
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_city=Mountain View
req_bill_to_address_postal_code=94043
req_bill_to_address_state=CA
```

```
req_bill_to_address_country=US
payment_token_instrument_identifier_id=0000111122225555
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,access
_key,profile_id,transaction_uuid,signed_date_time,signed_field_names,etc...
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
```

7.4   Payment Token Transactions

To create a single-click checkout experience for returning customers, send the payment token instead of the payment data to the transaction endpoints. See Endpoints and Transaction Types.

7.4.1   Requesting a Payment Card Transaction with a Token

IMPORTANT: Include the appropriate endpoint that supports the authorization or sale transaction types. See Endpoints and Transaction Types. For descriptions of all request and response fields, see Checkout API Fields.

The payment_token field identifies the card and retrieves the associated billing, shipping, and payment information.

Payment Card Transaction with a Token

Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-
1CD38A28A384
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
consumer_id=1239874561
transaction_type=authorization
```

```
currency=USD
payment_method=card
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Response

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-
1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My
Apartment req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2022-08-
14T134608Z
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

```
payment_token_latest_card_suffix=1717
payment_token_latest_card_expiry_date=11-2024
payment_solution=015
```

7.5 Payment Token Updates

7.5.1 Updating a Payment Card Token

The payment_token field identifies the TMS customer token and its default payment instrument and shipping address. The customer is directed to the Order Review page and clicks Edit Address or Edit Details to return to the relevant checkout page. The customer clicks Pay to confirm the transaction.

⚠️ IMPORTANT: Include the endpoint that supports update_payment_token or the endpoint that supports authorization,update_payment_token (updates the token and authorizes the transaction) or sale,update_payment_token(updates the token and processes the transaction). See Sample Transaction Process Using JSP. You must include the allow_payment_token_update field and set it to true.

Example: Updating a Payment Card Token

Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
transaction_type=update_payment_token
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
amount=100.00
currency=USD
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
locale=en
```

```
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
consumer_id=1239874561
signed_field_names=reference_number,transaction_type,currency,amount,locale,paymen
t_method,access_key,profile_id,transaction_uuid,signed_date_time,signed_field_name
s,unsigned_field_names,etc...
unsigned_field_names=comma separated list of unsigned fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Response

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,update_payment_token
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
payment_token_instrument_identifier_id=0000111122225555
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time=2022-08-14T134608Z
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

8 Test and View Transactions

⚠ IMPORTANT: You must create a profile in both the test and live versions of Secure Acceptance. You cannot copy a profile from the test version to the live version but must recreate the profile.

8.1 Testing Transactions

1. Log in to the Demonstration and Certification Environment (DCE).

2. Create a Secure Acceptance profile. See Creating a Secure Acceptance Profile.

3. Integrate with Secure Acceptance. See Scripting Language Samples.

⚠ IMPORTANT: Include the test transactions endpoint in your HTML form. See Sample Transaction Process Using JSP.

4. You can use these test payment card numbers for transactions. Remove spaces when sending the request to Bank of America.

Test Credit Card Numbers

Payment card type	Test account number
Visa	4111 1111 1111 1111
Mastercard	5555 5555 5555 4444
American Express	3782 8224 6310 005
Discover	6011 1111 1111 1117
JCB	3566 1111 1111 1113
Diners Club	3800 0000 0000 0006
Maestro International (16 digits)	6000 3400 0000 9859
Maestro Domestic (16 digits)	6759 1800 0000 5546

8.2   Viewing Transactions in Your Merchant Services Account

Use the transaction request ID to search for transactions received from your customer's browser and see full transaction details, including the transaction response that was provided to your customer's browser. This is helpful for troubleshooting issues.

1. Log in to your Merchant Services account.

2. In the left navigation panel, choose Transaction Management > Secure Acceptance. The Secure Acceptance Search page appears.

3. Search transactions search using your preferred methods.

4. Click the Request ID link of the transaction that you want to view. The Details page opens.

⚠️   IMPORTANT: If a transaction has missing or invalid data, it is displayed in the Secure Acceptance Transaction Search Results page without a request ID link.

9 Checkout API Fields

9.1 Data Type Definitions

⚠️ IMPORTANT: Unless otherwise noted, all fields are order and case sensitive. It is recommended that you not include URL-encoded characters in any request field prior to generating a signature.

Data Type Definitions

Data type	Permitted characters and formats
Alpha	Any letter from any language
AlphaNumeric	Alpha with any numeric character in any script
AlphaNumericPunctuation	Alphanumeric including ! "#$%&'()*+,-./:;=?@^_~
Amount	0123456789 including a decimal point (.)
ASCIIAlphaNumericPunctuation	Any ASCII alphanumeric character including !&'()+,-./:@
Date (a)	MM-yyyy
Date (b)	yyyyMMDD
Date (c)	yyyy-MM-dd HH:mm z yyyy-MM-dd hh:mm a z yyyy-MM-dd hh:mma z
Email	Valid email address.
Enumerated String	Comma-separated alphanumeric string
IP	Valid IP address
ISO 8601 Date	yyyy-MM-DDThh:mm:ssZ
Locale	[a-z] including a hyphen (-)
Numeric	0123456789
Phone	( ),+-.*#xX1234567890
URL	Valid URL (http or https)

9.2 Request Fields

> **!** IMPORTANT: To prevent data tampering, sign all request fields except for fields that contain data the customer is entering.

> **!** **IMPORTANT:**
>
> When signing fields in the request, create a comma-separated list of the fields. The sequence of the fields in the string is critical to the signature generation process. For example:
>
> ```
> bill_to_forename=john
> bill_to_surname=doe
> bill_to_email=jdoe@example.com
> signed_field_names=bill_to_forename,bill_to_email,bill_to_surname
> ```
>
> When generating the security signature, create a comma-separated name=value string of the POST fields that are included in the **signed_field_names** field. The sequence of the fields in the string is critical to the signature generation process. For example:
>
> - bill_to_forename=john
>
> - bill_to_surname=doe
>
> - bill_to_email=jdoe@example.com
>
> The string to sign is
>
> bill_to_forename=john,bill_to_email=jdoe@example.com,bill_to_surname=doe
>
> For information on the signature generation process, see the security script of the sample code for the scripting language you are using. See Scripting Language Samples

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
access_key	Required for authentication with Secure Acceptance. See Security Keys. ⚠ IMPORTANT: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Alphanumeric String (32)
allow_payment_ token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. Possible values: • true: Customer can update details. • false: Customer cannot update details.	update_payment_token (R)	Enumerated String (5)
amount	Total amount for the order. Must be greater than or equal to zero and must equal the total amount of each line item including the tax amount. ⚠ IMPORTANT: To prevent data tampering, sign this field.	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_to ken (R) • sale,create_payment_t oken (R) • update_payment_toke n (O)	Amount String (15)
auth_indicator	Flag that specifies the purpose of the authorization. Possible values: • 0: Preauthorization • 1: Final authorization Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization. To set the default for this field, contact customer support.	authorization (See description)	String (1)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
auth_type	Authorization type. Possible values: • AUTOCAPTURE: Automatic capture. • STANDARDCAPTURE: Standard capture. • verbal: Forced capture.	• authorization (See description.) • capture (Required for a verbal authorization; otherwise, not used.)	String (11)
bill_to_address_ city	City in the billing address.	• create_payment_token (R) • authorization or sale (R) • authorization,create_p ayment_token (R) • sale,create_payment_t oken (R) • update_payment_toke n (O)	AlphaNumericP unctuation String (50)
bill_to_address_ country	Country code for the billing address. Use the two-character ISO country codes.	• create_payment_token (R) • authorization or sale (R) • authorization,create_p ayment_to ken (R) • sale,create_payment_t oken (R) • update_payment_toke n (O)	Alpha String (2)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
bill_to_address_ line1	First line of the billing address.	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_to ken (R) • sale,create_payment_t oken (R) • update_payment_toke n (O)	AlphaNumericP unctuation String (60)
bill_to_address_ line2	Second line of the billing address.	Optional	AlphaNumericP unctuation String (60)
bill_to_address_ postal_code	Postal code for the billing address. This field is required if bill_to_address_country is U.S. or Canada. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example: 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example: A1B2C3 For the rest of the world countries, the maximum length is 10.	See description.	AlphaNumericP unctuation See description.

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
bill_to_address_ state	State or province in the billing address. For the U.S. and Canada, use the standard state, province, and territory codes. This field is required if bill_to_address_country is U.S. or Canada.	See description.	AlphaNumeric Punctuation String (2)
bill_to_company_ name	Name of the customer's company.	Optional	AlphaNumericP unctuation String (40)
bill_to_email	Customer email address, including the full domain name.	• create_payment_t oken (R) • authorization or sale (R) • authorization,cre ate_payment_to ken (R) • sale,create_paym ent_token (R) • update_payment_ token (O)	Email String (255)
bill_to_forename	Customer first name. This name must be the same as the name on the card.	• create_payment_t oken (R) • authorization or sale (R) • authorization,cre ate_payment_to ken (R) • sale,create_paym ent_token (R) • update_payment_ token (O)	AlphaNumericP unctuation String (60)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
bill_to_phone	Customer phone number. Bank of America recommends that you include the country code if the order is from outside the U.S. This field is optional for card payments.	See description.	Phone String (6 to 15)
bill_to_surname	Customer last name. This name must be the same as the name on the card.	• create_payment_t oken (R) • authorization or sale (R) • authorization,cre ate_payment_to ken (R) • sale,create_paym ent_token (R) • update_payment_ token (O)	AlphaNumericP unctuation String (60)
card_cvn	Card verification number. For American Express card types, the CVN must be 4 digits. This field can be configured as required or optional. See Payment Method Configuration.	See description.	Numeric String (4)
card_expiry_date	Card expiration date. Format: MM-yyyy	• create_payment_token (R) • authorization or sale (R) • authorization,create_p ayment_token (R) • sale,create_payment_t oken (R) • update_payment_toke n (O)	Date (a) String (7)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
card_number	Card number. Use only numeric values. Be sure to include valid and well-formed data for this field.	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Numeric String (20)
card_type	Type of card to authorize. Possible values: • 001: Visa • 002: Mastercard • 003: American Express • 004: Discover • 005: Diners Club: cards starting with 54 or 55 are rejected. • 006: Carte Blanche • 007: JCB • 014: EnRoute • 024: Maestro UK Domestic • 033: Visa Electron • 034: Dankort • 036: Carte Bancaire • 042: Maestro International • 043: GE Money UK card • 050: Hipercard (sale only) • 062: China UnionPay	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Enumerated String (3)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
complete_route	Concatenation of individual travel legs in the format for example: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete route or the individual legs (journey_leg#_orig and journey_leg#_dest). If you send all the fields, the value of complete_route takes precedence over that of the journey_leg# fields.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking	AlphaNumericPunctuation String (255)
credential_stored _on_file	Indicates whether to associate the new network transaction ID with the payment token for future merchant-initiated transactions (MITs). Set this field to true when you use a payment token for a cardholder-initiated transaction (CIT) and you plan to set up a new schedule of MITs using an existing payment token. This will ensure that the new network transaction ID is associated with the token. Possible values: • true • false ⚠️ IMPORTANT: In Europe, enable Payer Authentication on Secure Acceptance and set the payer_authentication_ch	Optional	String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
	⚠️ IMPORTANT: allenge_code field to 04 on the initial cardholder-initiated transaction (CIT) to ensure compliance with Strong Customer Authentication (SCA) rules.		
currency	Currency used for the order. For the possible values, see the ISO currency codes. ⚠️ IMPORTANT: To prevent data tampering, sign this field.	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Alpha String (3)
customer_ browser_color_ depth	Indicates the bit depth of the color palette for displaying images, in bits per pixel. Secure Acceptance automatically populates this field, but you can override it. For more information, see https://en.wikipedia.org/wiki/Color_depth.	Optional	String (2)
customer_ browser_java_ enabled	Indicates the ability of the cardholder browser to execute Java. The value is returned from the navigator.javaEnabled property. Secure Acceptance automatically populates this field, but you can override it. Possible values: • true • false	Optional	String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
customer_ browser_ javascript_ enabled	Indicates the ability of the cardholder browser to execute JavaScript. This value is available from the fingerprint details of the cardholder's browser. Secure Acceptance automatically populates this field, but you can override it. Possible values: • true • false	Optional	String (5)
customer_ browser_ language	Indicates the browser language as defined in IETF BCP47. Secure Acceptance automatically populates this field, but you can override it. For more information, see https://en.wikipedia.org/wiki/IETF_language_tag.	Optional	String (8)
customer_ browser_screen_ height	Total height of the customer's screen in pixels. Secure Acceptance automatically populates this field, but you can override it. Example: 864	Optional	String (6)
customer_ browser_screen_ width	Total width of the customer's screen in pixels. Secure Acceptance automatically populates this field, but you can override it.	Optional	String (6)
customer_ browser_time_ difference	Difference between UTC time and the cardholder browser local time, in minutes. Secure Acceptance automatically populates this field, but you can override it.	Optional	String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
customer_ cookies_accepted	Indicates whether the customer's browser accepts cookies. Possible values: • true: Customer browser accepts cookies. • false: Customer browser does not accept cookies.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	Enumerated String (5)
customer_gift_ wrap	Indicates whether the customer requested gift wrapping for this purchase. Possible values: • true: Customer requested gift wrapping. • false: Customer did not request gift wrapping.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	Enumerated String (5)
customer_ip_ address	Customer's IP address reported by your web server using socket information.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking	IP IPv4: String (15) IPv6: String (39)
departure_time	Departure date and time of the first leg of the trip. Use one of these formats: • yyyy-MM-dd HH:mm z • yyyy-MM-dd hh:mm a z • yyyy-MM-dd hh:mma z • HH = 24-hour format • hh = 12-hour format • a = am or pm (case insensitive) • z = time zone of the departing flight. Examples • 2023-01-20 23:30 GMT • 2023-01-20 11:30 PM GMT • 2023-01-20 11:30pm GMT	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services Account through your online banking.	Date (c) DateTime (29)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
device_ fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_) However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID. ⚠️ IMPORTANT: The Bank of America-generated device fingerprint ID overrides the merchant-generated device fingerprint ID.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	AlphaNumericPunctuation String (88)
health_care_#_ amount	Amount of the healthcare payment. # can range from 0 to 4. Send this field with a corresponding health_care_#_amount_type field.	authorization (O)	String (13)
health_care_#_ amount_type	Type of healthcare payment. # can range from 0 to 4. Mastercard possible values: • eligible-total: total amount of healthcare. • prescription Visa possible values: • clinic • dental • healthcare: total amount of healthcare. • healthcare-transit • prescription • vision Send this field with a corresponding health_care_#_amount field.	authorization (O)	String (35)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
ignore_avs	Ignore the results of AVS verification. Possible values: • true • false ⚠ IMPORTANT: To prevent data tampering, sign this field.	Optional	Enumerated String (5)
ignore_cvn	Ignore the results of CVN verification. Possible values: • true • false ⚠ IMPORTANT: To prevent data tampering, sign this field.	Optional	Enumerated String (5)
industry_datatype	Indicates whether the transaction includes industry data. For certain industries, you must set this field to an industry data value to be sent to the processor. When this field is not set to an industry value or is not included in the request, industry data does not go to the processor. Possible values: • healthcare_medical • healthcare_transit	authorization (O)	String (20)
item_#_code	Type of product. # can range from 0 to 199.	Optional If you include this field, you must also include the line_item_count field.	AlphaNumericPunctuation String (255)
item_#_name	Name of the item. # can range from 0 to 199. This field is required when the item_#_code value is not default nor related to shipping or handling.	See description. If you include this field, you must also include the line_item_count field.	AlphaNumericPunctuation String (255)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
item_#_passenger _email	Passenger's email address.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (255)
item_#_passenger _forename	Passenger's first name.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	String (60)
item_#_passenger _id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	String (32)
item_#_passenger _phone	Passenger's phone number. If the order is from outside the U.S., include the country code.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	String (15)
item_#_passenger _status	Your company's passenger classification, such as with a frequent flyer number. In this case, you might use values such as standard, gold, or platinum.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	String (32)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
item_#_passenger _surname	Passenger's last name.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	String (60)
item_#_passenger _type	Passenger classification associated with the price of the ticket. Possible values: • ADT: Adult • CNN: Child • INF: Infant • YTH: Youth • STU: Student • SCR: Senior Citizen • MIL: Military	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	String (32)
item_#_quantity	Quantity of line items. The default value is 1. Required field when one of these product codes is used: • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription # can range from 1to 199. This field is required when the item_#_code value is not default nor related to shipping or handling.	See description. If you include this field, you must also include the line_item_count field.	Numeric String (10)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
item_#_sku	Identification code for the product. Required field when one of these product codes is used: • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription # can range from 0 to 199.	See description. If you include this field, you must also include the line_item_count field.	AlphaNumericPunctuation String (255)
item_#_tax_ amount	Tax amount to apply to the line item. # can range from 0to 199. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	Optional If you include this field, you must also include the line_item_count field.	Amount String (15)
item_#_unit_price	Price of the line item. # can range from 0 to 199. This value cannot be negative. ⚠ IMPORTANT: You must include either this field or the amount field in the request.	See description. If you include this field, you must also include the line_item_count field.	Amount String (15)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
journey_leg#_dest	Airport code for the destination leg of the trip, designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete_route field or the individual legs (journey_leg#_orig and journey_leg#_dest). If you send all the fields, the complete route takes precedence over the individual legs.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	Alpha String (3)
journey_leg#_orig	Airport code for the origin leg of the trip, designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete_route field or the individual legs (journey_leg#_orig and journey_leg#_dest). If you send all the fields, the complete route takes precedence over the individual legs.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	Alpha String (3)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
journey_type	Type of travel, such as one way or round trip.	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	AlphaNumericPunctuation String (32)
line_item_count	Total number of line items. Maximum number is 200.	This field is required when you include any item fields in the request.	Numeric String (2)
locale	Indicates the language to use for customer-facing content. Possible value: en-us. See Activating a Profile. ⚠ IMPORTANT: To data tampering, sign this prevent field.	Required by the Secure Acceptance application.	Locale String (5)
merchant_defined _data#	Optional fields that you can use to store information (see Configuring Customer Notifications (page 15)). # can range from 1 to 100. Merchant-defined data fields 1 to 4 are associated with the payment token and are used for subsequent token-based transactions. Merchant defined data fields 5 to 100 are passed through to Fraud Management as part of the initial payment request and are not associated with the payment token. ⚠ IMPORTANT: Merchant-defined data fields are not intended to and MUST NOT be used to capture personally	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account through your online banking.	AlphaNumericPunctuation String (100)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
	identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields and any Secure Acceptance field that is not specifically designed to capture personally identifying information. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, card verification numbers (CVV, CVC2, CVV2, CID, CVN). If it is discovered that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, the merchant's account WILL immediately be suspended, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.		

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
merchant_ descriptor	Your business name. This name appears on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed. ⚠ IMPORTANT: This value must consist of English characters.	authorization (O)	String (23)
merchant_ descriptor_ alternate	Alternate contact information for your business, such as an email address or URL. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant URL in your account is sent. ⚠ IMPORTANT: This value must consist of English characters.	authorization (O)	String (13)
merchant_ descriptor_city	City for your business location. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant city in your account is sent. ⚠ IMPORTANT: This value must consist of English characters.	authorization (O)	String (13)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
merchant_ descriptor_ contact	Telephone number for your business. This value might appear on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed. When you do not include this value in your request, the merchant phone number in your account is sent. ⚠️ IMPORTANT: This value must consist of English characters.	authorization (O)	String (14)
merchant_ descriptor_ country	Country code for your business location. Use the standard ISO Standard Country Codes. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant country in your account is sent. ⚠️ IMPORTANT: This value must consist of English characters.	authorization (O)	String (2)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
merchant_ descriptor_post al_ code	Postal code for your business location. This value might appear on the cardholder's statement.	authorization (O)	String (14)
	If your business is domiciled in the U.S., you can use a 5-digit or 9-digit postal code. A 9-digit postal code must follow this		
	format: [5 digits][dash][4 digits]		
	Example: 12345-6789		
	If your business is domiciled in Canada, you can use a		
	6-digit or 9-digit postal code. A 6-digit postal code must follow this format:		
	[alpha][numeric][alpha][space] [numeric][alpha][numeric]		
	Example: A1B 2C3		
	When you do not include this value in your request, the merchant postal code in your account is sent.		
	⚠ IMPORTANT: This value must consist of English characters.		
	⚠ IMPORTANT: Mastercard requires a postal code for any country that uses postal codes. You can provide the postal code in your account, or you can include this field in your request.		

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
merchant_ descriptor_state	State code or region code for your business location. This value might appear on the cardholder's statement. For the U.S. and Canada, use the standard state, province, and territory codes. When you do not include this value in your request, the merchant state in your account is sent. ⚠ IMPORTANT: This value must consist of English characters.	authorization (O)	String (3)
merchant_ descriptor_street	Street address for your business location. This value might appear on the cardholder's statement. When you do not include this value in your request, the merchant street in your account is sent. ⚠ IMPORTANT: This value must consist of English characters.	authorization (O)	String (60)
merchant_secure_ data4	Optional field that you can use to store information. The data is encrypted before it is stored in the payment repository.	Optional	AlphaNumericP unctuation String (2000)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
merchant_secure_ data1 merchant_secure_ data2 merchant_secure_ data3	Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository.	Optional	AlphaNumericP unctuation String (100)
override_ backoffice_post_ url	Overrides the backoffice post URL profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later.	Optional	URL String (255)
override_custom_ cancel_page	Overrides the custom cancel page profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later.	Optional	URL String (255)
override_custom_ receipt_page	Overrides the custom receipt profile setting with your URL. URL must be HTTPS and support TLS or later. ⚠ IMPORTANT: To prevent data tampering, sign this field.	Optional	URL String (255)
override_ customer_ utc_offset	Overrides the transaction date and time with the number of minutes the customer is ahead of or behind UTC. Use this field to override the local browser time detected by Secure Acceptance. This time determines the date on receipt pages and emails. For example, if the customer is 2 hours ahead, the value is 120; if 2 hours behind, then -120; if UTC, the value is 0.	Optional	Integer (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
payer_ authentication_ acquirer_country	Send this to tell issuers that the acquirer's country differs • from the merchant country, and the acquirer is in the European Economic Area (EEA) and UK and Gibraltar.	Optional	String (2)
payer_ authentication_ acs_window_size	Sets the challenge window size that displays to the cardholder. The Access Control Server (ACS) replies with content that is formatted appropriately for this window size. The sizes are width x height in pixels. Secure Acceptance calculates this value based on the size of the window in which Secure Acceptance is displayed, but you can override it. Possible values: • 01: 250 x 400 • : 390 x 400 • 03: 500 x 600 • 0204: 600 x 400 • 05: Full page	Optional	Integer (2)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
payer_ authentication_ challenge_code	Possible values: • 01: No preference • 02: No challenge request • 03: Challenge requested (3-D Secure requestor preference) • 04: Challenge requested (mandate)	Optional	Integer (2)
payer_ authentication_ customer_annual_ transaction_ count	Number of transactions (successful and abandoned) for this cardholder account within the past year.	Optional	Integer (3)
payer_ authentication_ customer_daily_ transaction_ count	Number of transaction (successful or abandoned) for this cardholder account within the past 24 hours.	Optional	Integer (3)
payer_ authentication_ indicator	Indicates the type of authentication request. Secure Acceptance automatically populates this field, but you can override it. Possible values: • 01: Payment transaction • 04: Add card • 05: Maintain card • 06: Cardholder verification as part of EMV token identity and verification (ID&V)	Optional	Integer (2)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
payer_ authentication_ marketing_source	Indicates origin of the marketing offer.	Optional	String (40)
payer_ authentication_ merchant_fraud_ rate	Possible values: • 1: Represents fraud rate ≤1 • 2: Represents fraud rate >1 and ≤6 • 3: Represents fraud rate >6 and ≤13 • 4: Represents fraud rate >13 and ≤25 • 5: Represents fraud rate >25	Optional	Integer (2)
payer_ authentication_ merchant_name	Your company's name as you want it to appear to the customer in the issuing bank's authentication form. This value overrides the value specified by your merchant bank.	Optional	String (25)
payer_ authentication_ merchant_score	Risk score provided by merchants. Used for Cartes Bancaires transactions.	Optional	String (20)
payer_ authentication_ message_category	Identifies the category of the message for a specific use case 3-D Secure Server. Possible values: • 01: PA (payment authentication). • 02: NPA (non-payment authentication). • 03-71: Reserved for EMVCo future use (values invalid until defined by EMVCo). • 80-99: Reserved for directory server use.	Optional	String (2)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
payer_ authentication_ mobile_phone	Cardholder's mobile phone number.	Optional	Integer (25)
payer_ authentication_ new_customer	Indicates whether the customer is a new or existing customer with the merchant. Possible values: • true • false	Optional	String (5)
payer_ authentication_ pre_order	Indicates whether cardholder is placing an order with a future availability or release date. Possible values: • 01: Merchandise available • 02: Future availability	Optional	Integer (2)
payer_ authentication_ pre_order_date	Expected date that a pre-ordered purchase will be available. Format: yyyyMMDD	Optional	Integer (8)
payer_ authentication_ prior_ authentication_ data	Data that the ACS can use to verify the authentication process.	Optional	String (2048)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
payer_ authentication_ prior_ authentication_ method	Method that the cardholder used previously to authenticate to the 3-D Secure requester. Possible values: • 01: Frictionless authentication through the ACS • 02: Cardholder challenge through the ACS • 03: AVS verified • 04: Other issuer methods • 05-79: Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80-99: Reserved for directory server use	Optional	Integer (2)
payer_ authentication_ prior_ authentication_ time	Date and time in UTC of the previous cardholder authentication. Format: yyyyMMDDHHMM	Optional	Integer (12)
payer_ authentication_ product_code	Specifies the product code, which designates the type of transaction. Possible values:	Optional	String (3)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
	• AIR: Airline purchase ⚠ IMPORTANT: To prevent data tampering, sign this field. • ACC: Accommodation Rental • ACF: Account funding • CHA: Check acceptance • DIG: Digital Goods • DSP: Cash Dispensing • GAS: Fuel • GEN: General Retail • LUX: Luxury Retail • PAL: Prepaid activation and load • PHY: Goods or services purchase • QCT: Quasi-cash transaction • REN: Car Rental • RES: Restaurant • SVC: Services • TBD: Other • TRA: Travel		
payer_ authentication_ transaction_ mode	Transaction mode identifier. Identifies the channel from which the transaction originates. Possible values: • M: MOTO (Mail Order Telephone Order) • R: Retail • S: E-commerce • P: Mobile Device • T: Tablet	Required by the Secure Acceptance application.	String (1)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
payer_ authentication_ whitelisted	Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3-D Secure requester. Possible values: • true: 3-D Secure requester is whitelisted by cardholder • false: 3-D Secure requester is not whitelisted by cardholder	Optional	String (5)
payment_method	Method of payment. Possible values: • card	Required by the Secure Acceptance application.	Enumerated String (30)
payment_token	Identifier for the TMS customer token or the instrument identifier token. Populates the request with the information associated with the token.	• authorization or sale (R) • authorization,update _payment_token (R) • sale,update_pay ment_token (R) • update_payment_ token (R)	Numeric String (32)
payment_token_ comments	Optional comments you can add for the customer token.	Optional	AlphaNumericP unctuation String (255)
payment_token_ title	Name or title for the customer token.	Optional	AlphaNumericP unctuation String (60)
profile_id	Identifies the profile to use with each transaction.	Assigned by the Secure Acceptance application.	ASCIIAlphaNum ericPun ctuation String (36)
promotion_code	Promotion code for a transaction.	Optional	String (100)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
recipient_ account_id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	authorization (R for recipient transactions, otherwise not used)	Numeric String (10)
recipient_ date_of_birth	Recipient's date of birth. Format: yyyyMMDD.	authorization (R for recipient transactions, otherwise not used)	Date (b) String (8)
recipient_ postal_code	Partial postal code for the recipient's address. For example, if the postal code is NN5 7SG, the value for this field should be the first part of the postal code: NN5.	authorization (R for recipient transactions, otherwise not used)	Alphanumeric String (6)
recipient_ surname	Recipient's last name.	authorization (R for recipient transactions, otherwise not used)	Alpha String (6)
reference_ number	Unique merchant-generated order reference or tracking number for each transaction. ⚠ IMPORTANT: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	AlphaNumericPunctuation String (50)
returns_accepted	Indicates whether product returns are accepted. This field can contain one of these values: • true • false	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Enumerated String (5)
ship_to_address_ city	City of shipping address.	Optional	AlphaNumericPunctuation String (50)
ship_to_address_ country	Country code for the shipping address. Use the two-character ISO country codes.	Optional	Alpha String (2)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
ship_to_address_line1	First line of shipping address.	Optional	AlphaNumericPunctuation String (60)
ship_to_address_line2	Second line of shipping address.	Optional	AlphaNumericPunctuation String (60)
ship_to_address_postal_code	Postal code for the shipping address. This field is required if bill_to_address_country is U.S. or Canada. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example: 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric] Example: A1B 2C3 For the rest of the world countries, the maximum length is 10.	Optional	AlphaNumericPunctuation See description.
ship_to_address_state	State or province of shipping address. For the U.S. and Canada, use the standard state, province, and territory codes. This field is required if shipping address is U.S. or Canada.	Optional	AlphaNumericPunctuation String (2)
ship_to_company_name	Name of the company receiving the product.	Optional	AlphaNumericPunctuation String (40)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
ship_to_forename	First name of the person receiving the product.	Optional	AlphaNumericPunctuation String (60)
ship_to_phone	Phone number of the shipping address.	Optional	Phone String (6 to 15)
ship_to_surname	Last name of the person receiving the product.	Optional	AlphaNumericPunctuation String (60)
ship_to_type	Shipping destination. Example: Commercial, residential, store	Optional	String (25)
shipping_method	Shipping method for the product. Possible values: - sameday: Courier or same-day service - oneday: Next day or overnight service - twoday: Two-day service - threeday: Three-day service - lowcost: Lowest-cost service - pickup: Store pickup - other: Other shipping method - none: No shipping method	Optional	Enumerated String (10)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
signature	Merchant-generated Base64 signature. This is generated using the signing method for the access_key field supplied.	Required by the Secure Acceptance application.	AlphaNumeric Punctuation
signed_date_time	Date and time that the signature was generated. Must be in UTC Date & Time format. This field is used to check for duplicate transaction attempts. Format: yyyy-MM-DDThh:mm:ssZ Example: 2020-08-11T22:47:57Z equals August 11, 2020, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC. Your system time must be accurate to avoid payment processing errors related to the signed_date_time field. ⚠ IMPORTANT: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	ISO 8601 Date String (20)
signed_field_ names	A comma-separated list of request fields that are signed. This field is used to generate a signature that is used to verify the content of the transaction to protect it from tampering. ⚠ IMPORTANT: All request fields should be signed to prevent data tampering, with the exception of the card_number, card_cvn, and signature fields.	Required by the Secure Acceptance application.	AlphaNumericP unctuation Variable

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
skip_auto_auth	Indicates whether to skip or perform the preauthorization check when creating this token. Possible values: • true (skip the preauthorization check) • false (perform the preauthorization check)	Optional	Enumerated String (5)
skip_decision_ manager	Indicates whether to skip Fraud Management. This field can contain one of these values: • true: Fraud Management is not enabled for this transaction, and the device fingerprint ID will not be displayed. • false	Optional For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	Enumerated String (5)
tax_amount	Total tax amount to apply to the order. This value cannot be negative. ⚠️ IMPORTANT: To prevent data tampering, sign this field.:	Optional	Amount String (15)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & (Length)
transaction_type	The type of transaction. Possible values: • authorization • authorization,create_payment_token • authorization,update_payment_token • sale • sale,create_payment_token • sale,update_payment_token • create_payment_token • update_payment_token ⚠️ IMPORTANT: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Enumerated String (60)
transaction_uuid	Unique merchant-generated identifier. Include with the access_key field for each transaction. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts. ⚠️ IMPORTANT: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	ASCIIAlphaNumericPunctuation String (50)
unsigned_field_names	A comma-separated list of request fields that are not signed.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable

9.3 Response Fields

Response fields are sent using these notification methods:

- Merchant POST URL. See Merchant Notifications.

- Merchant POST Email. See Merchant Notifications.

- POST to the URL specified in the Transaction or Custom Cancel Response page. See Customer Response Page.

Notification methods are enabled on the Notifications and Customer Response pages of your Secure Acceptance profile.

To ensure the integrity of the response fields, a signature is included in the response. This signature is generated using the same secret_key value that was used to generate the request signature.

To verify that the response fields have not been tampered with, create a signature using the fields listed in the signed_field_names response field. This signature must be the same value that is included in the signature response field. Refer to the receipt page that is included in the sample scripts. See Samples in Scripting Languages.

IMPORTANT: Because response fields and reason codes can be added at any time, proceed as follows:

- Parse the response data according to the names of the fields instead of their order in the response. For more information on parsing response fields, see the documentation for your scripting language.

- The signature that you generate must be the same value that is included in the signature response field.

- Your error handler should use the decision field to determine the transaction result if it receives a reason code that it does not recognize.

If configured, these response fields are sent back to your Merchant POST URL or email. See Merchant Notifications. Your handler should use the decision field to obtain the transaction result if it receives a reason code that it does not recognize.

Response Fields

Field	Description	Data Type & Length
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See AVS Codes.	String (1)
auth_avs_code_raw	AVS result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_cavv_result	Mapped response code for the Visa Secure and American Express SafeKey: • See Visa Secure Response Codes. • See American Express SafeKey Response Codes.	String (3)
auth_cavv_result_raw	Raw response code sent directly from the processor for Visa Secure and American Express SafeKey.	String (3)
auth_code	Authorization code. Returned only if a value is returned by the processor.	String (7)
auth_cv_result	CVN result code. See CVN Codes.	String (1)
auth_cv_result_raw	CVN result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_reconciliation_ reference_number	Unique number that Bank of America generates to identify the transaction. You can use this value to identify transactions in the Ingenico ePayments Collections Report, which provides settlement information. Contact customer support for information about the report.	String (20)
auth_response	For most processors, this is the error message sent directly from the bank. Returned only if a value is returned by the processor.	String (10)
auth_time	Time of authorization in UTC.	String (20)
auth_trans_ref_no	Reference number that you use to reconcile your transaction reports with your processor reports.	AlphaNumeric (60)

Field	Description	Data Type & Length
bill_trans_ref_no	Reference number that you use to reconcile your transaction reports with your processor reports.	AlphaNumeric (60)
card_type_name	Name of the card type. For security reasons, this field is returned only in the merchant POST URL and email notifications (not in the receipt POST through the browser).	String (50)
decision	The result of your request. Possible values: • ACCEPT • DECLINE • REVIEW • ERROR • CANCEL	String (7)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Response message from the payment gateway.	String (255)
payer_authentication_acs_transaction_id	Unique transaction identifier assigned by the ACS to identify a single transaction.	String (36)
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank. This field is used by the payer authentication validation service.	String (50)

Field	Description	Data Type & Length
payer_authentication_ challenge_type	The type of 3-D Secure transaction flow that occurred. Possible values: • CH: Challenge • FR: Frictionless • FD: Frictionless with delegation (challenge not generated by the issuer but by the scheme on behalf of the issuer). Used for Cartes Bancaires transactions.	String (2)
payer_authentication_eci	Electronic commerce indicator (ECI). This field is used by payer authentication validation and enrollment services. Possible values for Visa, American Express, and JCB: • 05: Successful authentication. • 06: Authentication attempted. • 07: Failed authentication. Possible values for Mastercard: • 01: Merchant is liable. • 02: Card issuer is liable.	String (3)

Field	Description	Data Type & Length
payer_authentication_enroll_e_commerce_indicator	Commerce indicator for cards not enrolled. Possible values: • internet: Card not enrolled or card type not supported by payer authentication. No liability shift. • js_attempted: JCB card not enrolled, but attempt to authenticate is recorded. Liability shift. • js_failure: J/Secure directory service is not available. No liability shift. • spa: Mastercard card not enrolled in the Identity Check program. No liability shift. • vbv_attempted: Visa card not enrolled, but attempt to authenticate is recorded. Liability shift.	String (255)
payer_authentication_pares_status	Raw result of the authentication check. Possible values: • A: Proof of authentication attempt was generated. • N: Customer failed or cancelled authentication. Transaction denied. • U: Authentication not completed regardless of the reason. • Y: Customer was successfully authenticated.	String (255)
payer_authentication_pares_status_reason	Provides additional information about the PARes status value.	Integer (2)

Field	Description	Data Type & Length
payer_authentication_proof_ xml	XML element containing proof of enrollment verification. For cards not issued in the U.S. or Canada, your bank can require this data as proof of enrollment verification for any payer authentication transaction that you re-submit because of a chargeback. For cards issued in the U.S. or Canada, Visa can require this data for specific merchant category codes. This field is HTML encoded. This field is not returned for 3-D Secure 2.0 transactions.	String (1024)
payer_authentication_ reason_code	Numeric value corresponding to the result of the payer authentication request. See Reason Codes.	String (5)
payer_authentication_ specification_version	This field contains the 3-D Secure version that was used to process the transaction. For example, 1.0.2 or 2.0.0.	String (20)
payer_authentication_ transaction_id	Payer authentication transaction identifier used by Secure Acceptance to link the enrollment check and validate authentication messages.	String (20)
payer_authentication_type	Indicates the type of authentication that is used to challenge the card holder. Possible values: • 01: Static • 02: Dynamic • 03: OOB (Out of Band)	Integer (2)

Field	Description	Data Type & Length
payer_authentication_uad	Mastercard Identity Check UCAF authentication data. Returned only for Mastercard Identity Check transactions.	String (32)
payer_authentication_uci	Mastercard Identity Check UCAF collection indicator. This field indicates whether authentication data is collected at your website. Possible values: • 0: Authentication data was not collected and customer authentication not completed. • 1: Authentication data was not collected because customer authentication not completed. • 2: Authentication data was collected. Customer completed authentication.	String (1)

Field	Description	Data Type & Length
payer_authentication_ validate_e_commerce_ indicator	Indicator that distinguishes Internet transactions from other types. The authentication failed if this field is not returned. The value of this field is passed automatically to the authorization service if you request the services together. Possible values: • aesk: American Express SafeKey authentication verified successfully. • aesk_attempted: Card not enrolled in American Express SafeKey, but the attempt to authenticate was recorded. • internet: Authentication was not verified successfully. • js: J/Secure authentication verified successfully. • js_attempted: JCB card not enrolled in J/Secure, but the attempt to authenticate was recorded. • spa: Mastercard Identity Check authentication verified successfully. • spa_failure: Mastercard Identity Check failed authentication. • vbv: Visa Secure authentication verified successfully. • vbv_attempted: Card not enrolled in Visa Secure, but the attempt to authenticate was recorded. • vbv_failure: Visa Secure authentication unavailable.	String (255)

Field	Description	Data Type & Length
payer_authentication_ validate_result	Raw authentication data that comes from the card-issuing bank that indicates whether authentication was successful and whether liability shift occurred. Possible values: • -1: Invalid PARes. • 0: Successful validation. • 1: Cardholder is not participating, but the attempt to authenticate was recorded. • 6: Issuer unable to perform authentication. • 9: Cardholder did not complete authentication.	String (255)
payer_authentication_white_ list_status	Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3-D Secure requester. Possible Values: • Y: 3-D Secure requester is whitelisted by cardholder • N: 3-D Secure requester is not whitelisted by cardholder	String (1)
payer_authentication_white_ list_status_source	This field is populated by the system setting whitelist status. Possible Values: • 01: 3-D Secure Server • 02: Directory server • 03: ACS	Integer (2)

Field	Description	Data Type & Length
payer_authentication_xid	Transaction identifier generated by payer authentication. Used to match an outgoing payer authentication request with an incoming payer authentication response.	String (28)
payment_account_reference	Reference number serves as a link to the cardholder account and to all transactions for that account. The same value is returned whether the account is represented by a PAN or a network token.	String (32)
payment_solution	Type of credential-on-file (COF) payment network token. Returned in authorizations that use a payment network token associated with a TMS token. Possible values: • 014: Mastercard • 015: Visa • 016: American Express	String (3)
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. This payment token supersedes the previous payment token and is returned if: • The merchant is configured for a 16-digit payment token that displays the last four digits of the primary account number (PAN) and passes Luhn mod-10 check. See Payment Tokens (page 8). • The customer has updated the card number on their payment token. This payment token supersedes the previous payment token and should be used for subsequent transactions. You must be using Token Management Services.	String (32)

Field	Description	Data Type & Length
payment_token_latest_card_ expiry_date	Card expiration date of the latest card issued to the cardholder. Returned when Network Tokenization is enabled, and a payment_token with an associated Network Token is used in a transaction. Network Tokens can continue to be used even if the original card has expired. Format: MM-yyyy	Date (a) (7)
payment_token_latest_card_ suffix	Last four digits of the latest card issued to the cardholder. Returned when Network Tokenization is enabled, and a payment_token with an associated Network Token is used in a transaction. Network Tokens can continue to be used even if the original card number has changed due to a new card being issued. Use the last four digits in payment confirmation messages to cardholders, for example: "Thank you for your payment using your Visa card ending [payment_token_latest_card_suffix]".	String (4)
req_auth_type	Authorization type. Possible values: • AUTOCAPTURE: Automatic capture. • STANDARDCAPTURE: Standard capture. • verbal: Forced capture. Forced Capture Set this field to verbal and include it in the authorization request to indicate that you are performing a forced capture; therefore, you receive the authorization code outside the transaction processing system. Verbal Authorization Set this field to verbal and include it in the capture request to indicate that the request is for a verbal authorization.	String (11)

Field	Description	Data Type & Length
req_bill_to_address_city	City in the billing address.	String (50)
req_bill_to_address_country	ISO country code for the billing address.	String (2)
req_bill_to_address_line1	First line of the street address in the billing address.	String (60)
req_bill_to_address_line2	Second line of the street address in the billing address.	String (60)
req_bill_to_address_postal_ code	Postal code for the billing address. This field is returned if bill_to_address_country is U.S. or Canada.	String (10)
req_bill_to_address_state	State or province in the billing address. The two-character ISO state and province code. This field is returned for U.S and Canada.	String (2)
req_bill_to_company_name	Name of the customer's company.	String (40)
req_bill_to_email	Customer email address.	String (255)
req_bill_to_forename	Customer first name.	String (60)
req_bill_to_phone	Customer phone number.	String (15)
req_bill_to_surname	Customer last name.	String (60)
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number.	String (20)
req_card_type	Type of card.	String (3)
req_company_tax_id	Company's tax identifier. The last four digits are not masked.	String (9)

Field	Description	Data Type & Length
req_complete_route	Concatenation of individual travel legs in the format: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the complete route field or the individual legs (journey_leg#_orig and journey_ leg#_dest). If you send all the fields, the value of complete_route takes precedence over that of the journey_leg# fields.	String (255)
req_currency	Currency used for the order. See ISO currency codes.	String (3)
req_customer_cookies_ accepted	Indicates whether the customer's browser accepts cookies. Possible values: • true: Customer browser accepts cookies. • false: Customer browser does not accept cookies.	String (5)
req_customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. Possible values: • true: Customer requested gift wrapping. • false: Customer did not request gift wrapping.	String (5)
req_customer_ip_address	Customer IP address reported by your web server using socket information.	

Field	Description	Data Type & Length
req_departure_time	Departure date and time of the first leg of the trip. Use one of these formats: • yyyy-MM-dd HH:mm z • yyyy-MM-dd hh:mm a z • yyyy-MM-dd hh:mma z • HH = 24-hour format • hh = 12-hour format • a = am or pm (case insensitive) • z = time zone of the departing flight.	String (29)
req_device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different sessions IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	String (88)
req_ignore_avs	Ignore the results of AVS verification. Possible values: • true • false	String (5)
req_ignore_cvn	Ignore the results of CVN verification. Possible values: • true • false	String (5)
req_item_#_code	Type of product. # can range from 0 to 199.	String (255)

Field	Description	Data Type & Length
req_item_#_description	Description of the item. # can range from 0 to 199.	String (255)
req_item_#_name	Name of the item. # can range from 0to 199.	String (255)
req_item_#_passenger_email	Passenger's email address.	String (255)
req_item_#_passenger_ forename	Passenger's first name.	String (60)
req_item_#_passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	String (32)
req_item_#_passenger_ phone	Passenger's phone number. If the order is from outside the U.S., it is recommended that you include the country code.	String (15)
req_item_#_passenger_ status	Your company's passenger classification, such as with a frequent flyer classification. In this case, you might use values such as standard, gold, or platinum.	String (32)
req_item_#_passenger_ surname	Passenger's last name.	String (60)
req_item_#_passenger_type	Passenger classification associated with the price of the ticket. Possible values: • ADT: Adult • CNN: Child • INF: Infant • YTH: Youth • STU: Student • SCR: Senior Citizen • MIL: Military	String (32)

Field	Description	Data Type & Length
req_item_#_quantity	Quantity of line items. # can range from 0to 199.	String (10)
req_item_#_sku	Identification code for the product. # can range from 0 to 199.	String (255)
req_item_#_tax_amount	Tax amount to apply to the line item. # can range from 0to 199. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	String (15)
req_item_#_unit_price	Price of the line item. # can range from 0to 199. This value cannot be negative.	String (15)
req_journey_leg#_dest	Airport code for the origin of the leg of the trip, designated by the pound (#) symbol in the field name. For a complete list of airport codes, see IATA's City Code Directory.	String (3)
req_journey_leg#_orig	Airport code for the origin of the leg of the trip, designated by the pound (#) symbol in the field name. This code is usually three digits long; for example: SFO = San Francisco. For a complete list of airport codes, see IATA's City Code Directory.	String (3)
req_journey_type	Type of travel, such as one way or round trip.	String (32)
req_line_item_count	Total number of line items. Maximum amount is 200.	String (2)
req_locale	Indicates the language to use for customer content. See Activating a Profile.	String (5)

Field	Description	Data Type & Length
req_merchant_defined_data#	Optional fields that you can use to store information. # can range from 1 to 100.	String (100)
	Merchant-defined data fields 1 to 4 are associated with the payment token and are used for subsequent token-based transactions. Merchant-defined data fields 5 to 100 are passed through to Fraud	
	Management as part of the initial payment request and are not associated with the payment token.	
	⚠ WARNING! Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields and any Secure Acceptance field that is not specifically designed to capture personally identifying information.	
	Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, card verification numbers (CVV, CVC2, CVV2, CID, CVN). If it	
	is discovered that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, the merchant's account WILL immediately be suspended, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	

Field	Description	Data Type & Length
req_merchant_descriptor	Your business name. This name appears on the cardholder's statement.	String (23)
req_merchant_descriptor_ alternate	Alternate contact information for your business, such as an email address or URL. This value might appear on the cardholder's statement.	String (13)
req_merchant_descriptor_ city	City for your business location. This value might appear on the cardholder's statement.	String (13)
req_merchant_descriptor_ contact	Telephone number for your business. This value might appear on the cardholder's statement.	String (14)
req_merchant_descriptor_ country	Country code for your business location. This value might appear on the cardholder's statement.	String (2)
req_merchant_descriptor_ postal_code	Postal code for your business location. This value might appear on the cardholder's statement.	String (14)
req_merchant_descriptor_ state	State code or region code for your business location. This value might appear on the cardholder's statement.	String (3)
req_merchant_descriptor_ street	Street address for your business location. This value might appear on the cardholder's statement.	String (60)
req_merchant_secure_data1 req_merchant_secure_data2 req_merchant_secure_data3	Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository.	String (100)
req_merchant_secure_data4	Optional field that you can use to store information. The data is encrypted before it is stored in the payment repository.	String (2000)
req_override_backoffice_ post_url	Overrides the backoffice post URL profile setting with your own URL.	URL (255)
req_override_custom_ cancel_page	Overrides the custom cancel page profile setting with your own URL.	URL (255)
req_override_custom_ receipt_page	Overrides the custom receipt profile setting with your own URL.	URL (255)

Field	Description	Data Type & Length
req_payment_method	Method of payment. Possible values: • card	String (30)
req_payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. When this field is included in the request, the card data and billing and shipping information are optional. You must be currently using Token Management Services.	String (32)
req_payment_token_ comments	Optional comments about the customer token.	String (255)
req_payment_token_title	Name of the customer token.	String (60)
req_profile_id	Identifies the profile to use with each transaction.	String (36)
req_promotion_code	Promotion code included in the transaction.	String (100)
req_recipient_account_id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	Numeric String (10)
req_recipient_date_of_birth	Recipient's date of birth. Format: yyyyMMDD.	Date (b) String (8)
req_recipient_postal_code	Partial postal code for the recipient's address.	Alphanumeric String (6)
req_recipient_surname	Recipient's last name.	Alpha String (6)
req_reference_number	Unique merchant-generated order reference or tracking number for each transaction.	String (50)
req_returns_accepted	Indicates whether product returns are accepted. Possible values: • true • false	String (5)

Field	Description	Data Type & Length
req_ship_to_address_city	City of shipping address.	String (50)
req_ship_to_address_country	The two-character ISO country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60)
req_ship_to_address_line2	Second line of shipping address.	String (60)
req_ship_to_address_postal_code	Postal code for the shipping address.	String (10)
req_ship_to_address_state	The two-character ISO state and province code.	String (2)
req_ship_to_company_name	Name of the company receiving the product.	String (40)
req_ship_to_forename	First name of person receiving the product.	String (60)
req_ship_to_phone	Phone number for the shipping address.	String (15)
req_ship_to_surname	Last name of person receiving the product.	String (60)
req_shipping_method	Shipping method for the product. Possible values: • sameday: Courier or same-day service • oneday: Next day or overnight service • twoday: Two-day service • threeday: Three-day service • lowcost: Lowest-cost service • pickup: Store pick-up • other: Other shipping method • none: No shipping method	String (10)
req_skip_decision_manager	Indicates whether to skip Fraud Management. Possible values: • true • false For more information, refer to the guides in the Fraud Management section in your Merchant Services account.	String (5)

Field	Description	Data Type & Length
req_tax_amount	Total tax to apply to the product.	String (15)
req_transaction_type	The type of transaction requested.	String (60)
req_transaction_uuid	Unique merchant-generated identifier. Include with the access_key field for each transaction.	String (50)
request_token	Request token data created for each response. This field is an encoded string that contains no confidential information.	String (256)
required_fields	Indicates which of the request fields were required but not provided.	Variable
service_fee_amount	The service fee amount for the order.	String (15)
signature	The Base64 signature returned by the server.	String (44)
signed_date_time	The date and time of when the signature was generated by the server. Format: yyyy-MM-DDThh:mm:ssZ Example 2020-08-11T22:47:57Z equals August 11, 2020, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.	String (20)
signed_field_names	A comma-separated list of response data that was signed by the server. All fields within this list should be used to generate a signature that can then be compared to the response signature to verify the response.	Variable
transaction_id	The transaction identifier returned from the payment gateway.	String (26)
utf8	Indicates whether the unicode characters are encoded. Possible value: √	String (3)

10 Reason Codes

The reason_code field contains additional data regarding the decision response of the transaction.

Depending on the decision of a transaction request, the default receipt page or your receipt page is displayed to the customer. Both you and your customer can also receive an email receipt. See Merchant Notifications.

Reason Codes

Reason Code	Description
100	Successful transaction.
101	Request is missing one or more required fields. Examine the response fields missingField_0 through missingField_N to identify which fields are missing. Resend the request with all the required fields.
102	One or more fields in the request contain invalid data.
	Possible action: see the response field invalid_fields to ascertain which fields are invalid. Resend the request with the correct information.
104	The access_key and transaction_uuid fields for this authorization request match the access_key and transaction_uuid fields of another authorization request that you sent within the past 15 minutes.
	Possible action: resend the request with unique access_key and transaction_uuid fields.
	A duplicate transaction was detected. The transaction might have already been processed.
	Possible action: before resubmitting the transaction, use the single transaction query or search for the transaction using your Merchant Services account to confirm that the transaction has not yet been processed. See Viewing Transactions in Your Merchant Services Account (page 28).
110	Only a partial amount was approved.
150	General system failure.
	Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in your Merchant Services account or programmatically through the single transaction query.
151	The request was received but a server timeout occurred. This error does not include timeouts between the client and the server.
	Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in your Merchant Services account or programmatically through the single transaction query.

Reason Code	Description
152	The request was received, but a service timeout occurred. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in your Merchant Services account or programmatically through the single transaction query.
200	The authorization request was approved by the issuing bank but declined because it did not pass the Address Verification System (AVS) check. Possible action: you can capture the authorization but consider reviewing the order for fraud.
201	The issuing bank has questions about the request. You do not receive an authorization code programmatically, but you might receive one verbally by calling the processor. Possible action: call your processor to possibly receive a verbal authorization. For contact phone numbers, refer to your merchant bank information.
202	Expired card. You might also receive this value if the expiration date you provided does not match the date the issuing bank has on file. Possible action: request a different card or other form of payment.
203	General decline of the card. No other information was provided by the issuing bank. Possible action: request a different card or other form of payment.
204	Insufficient funds in the account. Possible action: request a different card or other form of payment.
205	Stolen or lost card. Possible action: review this transaction manually to ensure that you submitted the correct information.
207	Issuing bank unavailable. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in your Merchant Services account or programmatically through the single transaction query.
208	Inactive card or card not authorized for card-not-present transactions. Possible action: request a different card or other form of payment.

Reason Code	Description
210	The card has reached the credit limit.
	Possible action: request a different card or other form of payment.
211	Invalid CVN.
	Possible action: request a different card or other form of payment.
221	The customer matched an entry on the processor's negative file.
	Possible action: review the order and contact the payment processor.
222	Account frozen.
230	The authorization request was approved by the issuing bank but declined because it did not pass the CVN check.
	Possible action: you can capture the authorization but consider reviewing the order for the possibility of fraud.
231	Invalid account number.
	Possible action: request a different card or other form of payment.
232	The card type is not accepted by the payment processor.
	Possible action: contact your merchant bank to confirm that your account is set up to receive the card in question.
233	General decline by the processor.
	Possible action: request a different card or other form of payment.
234	There is a problem with the information in your account.
	Possible action: do not resend the request. Contact customer support to correct the information in your account.
236	Processor failure.
	Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in your Merchant Services account or programmatically through the single transaction query.
240	The card type sent is invalid or does not correlate with the payment card number.
	Possible action: confirm that the card type correlates with the payment card number specified in the request; then resend the request.

Reason Code	Description
475	The cardholder is enrolled for payer authentication.
	Possible action: authenticate cardholder before proceeding.
476	Payer authentication could not be authenticated.
478	Strong customer authentication (SCA) is required for this transaction.
481	Transaction declined based on your payment settings for the profile.
	Possible action: review the risk score settings for the profile.
520	The authorization request was approved by the issuing bank but declined based on your Custom Fraud Management settings.
	Possible action: review the authorization request.

11 Types of Notifications

Decision	Description	Type of Notification
ACCEPT	Successful transaction. See reason codes 100 and 110.	• Custom receipt page • Customer receipt email • Merchant POST URL • Merchant receipt email
REVIEW	Authorization was declined; however, a capture might still be possible. Review payment details. See reason codes 200, 201, 230, and 520.	• Custom receipt page • Customer receipt email • Merchant POST URL • Merchant receipt email
DECLINE	Transaction was declined. See reason codes 102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, 476, 478, and 481. If the retry limit is set to 0, the customer receives the decline message, Your order was declined. Please verify your information. before the merchant receives it. The decline message relates to either the processor declining the transaction or a payment processing error, or the customer entered their 3-D Secure credentials incorrectly.	• Custom receipt page • Merchant POST URL • Merchant receipt email
ERROR	Access denied, page not found, or internal server error. See reason codes 102, 104, 150, 151 and 152.	• Custom receipt page • Merchant POST URL
CANCEL	The customer did not accept the service fee conditions. The customer cancelled the transaction.	• Custom receipt page • Merchant POST URL

12 AVS Codes

An issuing bank uses the AVS code to confirm that your customer is providing the correct billing address. If the customer provides incorrect information, the transaction might be fraudulent. The international and U.S. domestic Address Verification Service (AVS) codes are the Visa standard AVS codes, except for codes 1 and 2, which are Bank of America AVS codes. The standard AVS return codes for other types of payment cards (including American Express cards) are mapped to the Visa standard codes. You receive the code in the auth_avs_code response field. See Response Fields.

> When you populate billing street address 1 and billing street address 2, Bank of America concatenates the two values. If the concatenated value exceeds 40 characters, Bank of America truncates the value at 40 characters before sending it to Visa and the issuing bank. Truncating this value affects AVS results and therefore might also affect risk decisions and chargebacks.

12.1 U.S. Domestic AVS Codes

Code	Response	Description
A	Partial match	Street address matches, but five-digit and nine-digit postal codes do not match.
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
E	Invalid	AVS data is invalid or AVS is not allowed for this card type.
F	Partial match	Card member's name does not match but billing postal code matches. Returned only for the American Express card type.
G		Not supported.
H	Partial match	Card member's name does not match, but street address and postal code match. Returned only for the American Express card type.
I	No match	Address not verified.
J	Match	Card member's name, billing address, and postal code match. Shipping information verified and chargeback protection guaranteed through the Fraud Protection Program. Returned only if you are signed up to use AAV+ with the American Express Phoenix processor.
K	Partial match	Card member's name matches but billing address and billing postal code do not match. Returned only for the American Express card type.
L	Partial match	Card member's name and billing postal code match, but billing address does not match. Returned only for the American Express card type.
M	Match	Street address and postal code match.
N	No match	One of these descriptions: • Street address and postal code do not match. • Card member's name, street address, and postal code do not match. Returned only for the American Express card type.
O	Partial match	Card member's name and billing address match but billing postal code does not match. Returned only for the American Express card type.
P	Partial match	Postal code matches, but street address not verified.

Code	Response	Description
Q	Match	Card member's name, billing address, and postal code match. Shipping information verified but chargeback protection not guaranteed (Standard program). Returned only if you are registered to use AAV+ with the American Express Phoenix processor.
R	System unavailable	System unavailable.
S	Not supported	U.S.-issuing bank does not support AVS.
T	Partial match	Card member's name does not match, but street address matches. Returned only for the American Express card type.
U	System unavailable	Address information unavailable for one of these reasons: • The U.S. bank does not support non-U.S. AVS. • The AVS in a U.S. bank is not functioning properly.
V	Match	Card member's name, billing address, and billing postal code match. Returned only for the American Express card type.
W	Partial match	Street address does not match, but nine-digit postal code matches.
X	Match	Street address and nine-digit postal code match.
Y	Match	Street address and five-digit postal code match.
Z	Partial match	Street address does not match, but 5-digit postal code matches.
1	Not supported	AVS is not supported for this processor or card type.
2	Unrecognized	The processor returned an unrecognized value for the AVS response.
3	Match	Address is confirmed. Returned only for PayPal Express Checkout.
4	No match	Address is not confirmed. Returned only for PayPal Express Checkout.

13 CVN Codes

Code	Description
D	The transaction was considered to be suspicious by the issuing bank.
I	The CVN failed the processor's data validation.
M	The CVN matched.
N	The CVN did not match.
P	The CVN was not processed by the processor for an unspecified reason.
S	The CVN is on the card but was not included in the request.
U	Card verification is not supported by the issuing bank.
X	Card verification is not supported by the card association.
1	Card verification is not supported for this processor or card type.
2	An unrecognized result code was returned by the processor for the card verification response.
3	No result code was returned by the processor.

14 American Express SafeKey Response Codes

The American Express SafeKey response code is returned in the auth_cavv_result field in the response message for an authorization request.

Response Code	Description
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
U	Issuer does not participate or 3-D Secure data was not used.
99	An unknown value was returned from the processor.

15 Iframe Implementation

⚠ IMPORTANT: If you plan to embed Secure Acceptance in an iframe, ensure that you follow the steps in this section. PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.

⚠ IMPORTANT: For the payer authentication 3-D Secure 2.x process, ensure that the iframe is large enough to display the issuer's access control server (ACS) challenge content (at least 390 x 400 pixels). For more information about ACS, see the Payer Authentication guide.

Clickjacking Prevention

Clickjacking (also known as user-interface redress attack and iframe overlay) is used by attackers to trick users into clicking on a transparent layer (with malicious code) above legitimate buttons or clickable content for a site. To prevent clickjacking, you must prevent third-party sites from including your website within an iframe.

While no security remediation can prevent every clickjacking, these are the minimum measures you must use for modern web browsers:

- Set HTTP response header X-FRAME_OPTIONS to either "DENY" or "SAMEORIGIN".

- Provide frame-busting scripts to ensure that your page is always the top-level window or disabling code for older browsers that do not support X-FRAME_OPTIONS.

You are required to implement the recommended prevention techniques in your website. See the OWASP Clickjacking Defense page and the Cross Site Scripting page for up-to-date information.

Web application protections for Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), etc. must also be incorporated.

- For XSS protection, you must implement comprehensive input validation and the OWASP-recommended security encoding library to do output encoding on your website.

- For CSRF protection, you are strongly encouraged to use a synchronized token pattern. This measure requires generating a randomized token associated with the user session. The token will be inserted whenever an HTTP request is sent to the server. Your server application will verify that the token from the request is the same as the one associated with the user session.

15.1 Iframe Transaction Endpoints

For iframe transaction endpoints and supported transaction types for each endpoint, see Endpoints and Transaction Types.

16 Visa Secure Response Codes

The Visa Secure response code is returned in the auth_cavv_result field in the response message for an authorization request.

Visa Secure Response Codes

Response Code	Description
0	CAVV not validated because erroneous data was submitted.
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
6	CAVV not validated because the issuer does not participate.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
B	CAVV passed the validation with information only; no liability shift.
C	CAVV attempted but not validated; issuer did not return CAVV code.
D	CAVV not validated or authenticated; issuer did not return CAVV code.
I	Invalid security data.
U	Issuer does not participate or 3-D Secure data was not used.
99	An unknown value was returned from the processor.