# BANK OF AMERICA

# Hosted Payments Page Integration Guide

V2.0 September 2023

# Contents

# 1 Recent Revisions to This Document

| Release | Changes |
|---------|---------|
| December 2020 | Initial release. |
| September 2023 | |

# 2   About This Guide

## 2.1   Audience and Purpose

This guide is written for merchants who want to accept payments using Hosted Payments Page and who do not want to handle or store sensitive payment information on their own servers.

Using 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 the Merchant Portal to review and manage orders.

# 3   Web Site Requirements

Your web site must meet the following requirements:

- It must have a shopping-cart, customer order creation software, or an application for initiating disbursements to send funds to payment accounts.

- 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 Hosted Payments Page.

# 4   Conventions

## 4.1   Important and Warning Statements

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

 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.

## 4.2   Text and Command Conventions

| Convention | Usage |
|---|---|
| Bold | • Field and service names in text; for example: Include the transaction_type field. |
|  | • Items that you are instructed to act upon; for example: Click **Save**. |
| Screen text | • Code examples and samples. |
|  | • Text that you enter in an API environment, for example:  Set the **transaction_type** field to `create_payment_token`. |

# 5 Hosted Payments Page

Bank of America Hosted Payments Page is your secure hosted customer checkout experience. It consists of securely managed payment forms or as a single page payment form for capturing payment card data, processing transactions, enabling you to simplify your Payment Card Industry Data Security Standard (PCI DSS) compliance and reduce risks associated with handling and/or storing sensitive payment card information. You, the merchant, out-source capturing and managing sensitive payment card data to Secure Acceptance, which is designed to accept card payments.

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 profiles.

2. Update the code on your web site to render the Hosted Payments Page and immediately process card transactions (see "Samples in Scripting Languages" ). Sensitive card data bypasses your network and is accepted by Secure Acceptance directly from the customer. 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 reply information to display an appropriate transaction response page to the customer. You can view and manage all orders in the Merchant Portal (see "Viewing Transactions in the Merchant Portal").

# 6 Required Browers

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

Desktop browsers:

- IE 10 or later

- Edge 13 or later

- Firefox 42 or later

- Chrome 48 or later

- Safari 7.1 or later

- Opera 37 or later

Mobile browsers:

- iOS Safari 7.1 or later

- Android Browser 4.4 or later

- Chrome Mobile 48 or later

# 7 Secure Acceptance Profile

Please note, throughout this document, you will see references to "Secure Acceptance." Secure Acceptance is the umbrella term for our Hosted Payments Page and Checkout API integration methods. Information about Secure Acceptance applies to Hosted Payments Page.

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 (see "Custom Checkout Appearance"). For example, you might need multiple profiles for localized branding of your web sites.You can display a multi-step checkout process or a single page checkout (see "Checkout Configuration") to the customer as well as configure the appearance and branding, payment options, languages, and customer notifications.

**Secure Acceptance Transaction Flow**

The Hosted Payments Page transaction flow is illustrated described below.
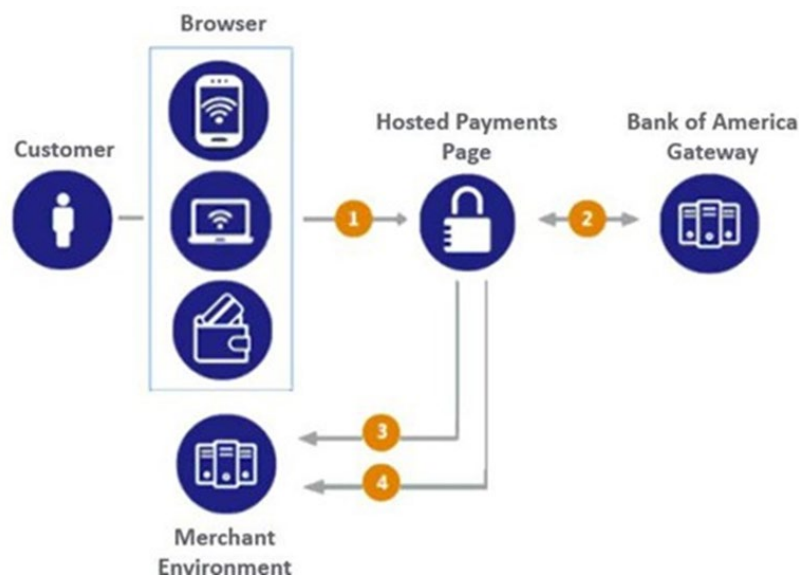


1.  The customer clicks the "checkout now" button on your web site, which triggers an HTTPS POST that directs the customer to the Hosted Payments Page that you configured in your Merchant Services account in Business Advantage 360 (BA 360.). The HTTPS POST includes the signature and signed data fields containing the order information.

    Hosted Payments Page works best with JavaScript and cookies enabled in the customer browser.

    Your system should sign only Secure Acceptance request fields. To prevent malicious actors from impersonating Bank of America, do not allow unauthorized access to the signing function.

2.  Secure Acceptance verifies the signature to ensure that the order details were not amended or tampered with and displays the Hosted Payments Page. The customer enters and submits payment details and/or their billing and shipping information. The customer confirms the payment, and the transaction is processed.

3. Bank of America recommends that you configure a custom receipt page in your Merchant Services account in BA 360 (see "Merchant Notifications") so that the signed transaction response is sent back to your merchant server through the browser. You must validate the reply signature to confirm that the reply data was not amended or tampered with. Secure Acceptance can also display a standard receipt page to your customer, and you can verify the result of the transaction in your account in BA 360 search or the standard Bank of America reports.

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

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

4. Bank of America recommends implementing the merchant POST URL notification (see "Merchant Notifications") 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.

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

# 8 Payment Tokens

Payment tokens represent the customer token in the Token Management Service. 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.

The payment token replaces the card or electronic check bank account number, and optionally the associated billing, shipping, and card information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

## 8.1 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.

# 9 One-click Checkout

With *One-click Checkout*, customers can buy products with a single click. Secure Acceptance is integrated to Bank of America Tokenization, so returning customers are not required to enter their payment details. Before a customer can use One-click Checkout, they must create a payment token during the first transaction on the merchant web

site. See "Payment Token Transactions". The payment token is an identifier for the payment details; therefore, no further purchases require that you enter any information. When the payment token is included in a payment request, it retrieves the card, billing, and shipping information related to the original payment request from the payment repository.

To use one-click Checkout, you must include the One-click Checkout endpoint to process the transaction. See "Endpoints and Transaction Types".

# 10 Payment Configuration

## 10.1 Creating a Hosted Payments Page Profile

⚠️ Contact Bank of America Customer Support to enable your account for Secure Acceptance. You must activate a profile in order 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 Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

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

4. Enter or verify the following 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 **Hosted Payments Page** |
| 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 phone number |
| Payment Tokenization | Check **Payment Tokenization**. For more information. See "Payment Transactions". |
| Fraud Management | Check **Custom Fraud Management**. For more information, please refer to the Guides section under Fraud Management. |
| Verbose Data | Check **Verbose Data**. (Not required.) |
| Generate Device Fingerprint | Check **Generate Device Fingerprint**. For more information, please refer to the Guides section under Fraud Management. |

## 10.2 Payment Method Configuration

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

A payment method selection page is displayed as part of the checkout process for any of the following scenarios:

- Multiple payment methods are enabled for the profile, and no **payment_method** field is included in the request.

- **payment_method=**visacheckout is included in the request.

- Visa Checkout or Visa Secure Remote Commerce (SRC) is the only enabled payment method for the profile (see "Enabling the Payment Method for Visa Checkout or Visa SRC").

⚠️ Visa SRC uses Visa Checkout services, Merchant Portal labels, and API fields.

You can skip displaying the payment method selection page by specifying card as the only available payment method.

Customers can change the payment method during the checkout process.

## 10.3 Adding Card Types and Currencies

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

The card verification number (CVN) is a three- or four-digit number that helps ensure that the customer possess the card at the time of the transaction.

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

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

3. Click **Payment Settings**. The Payment Settings page appears.

4. Click **Add Card Types**. The list of card types appear.

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

6. Click the settings icon for each card type. The card settings and currencies lists appear.

7. Check **CVN Display** to display the CVN field on Secure Acceptance. The customer decides whether to enter the CVN. Bank of America recommends displaying the CVN to reduce fraud.

8. Check **CVN Required**. The CVN Display option must also be checked. If this option is checked, the customer is required to enter the CVN. Bank of America recommends requiring the CVN to reduce fraud.

9. Check **Payer Authentication**.

10. 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. If you select the Elo or Hipercard card type, only the Brazilian Real currency is supported.

11. Click **Submit**. The card types are added as an accepted payment type.

12. Click **Save**.

## 10.4 Configuring Payer Authentication

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

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

3. Click **Payment Settings**. The Payment Settings page appears.

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

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

   - Amex

   - Cartes Bancaires

   - Diners Club

   - Discover

   - JCB

   - Mastercard

   - Maestro (UK Domestic or International)

   - Visa

## 10.5 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 Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

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

3. Click **Payment Settings**. The Payment Settings page appears.

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

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

6. Click **Save**.

⚠️ 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".

## 10.6 Visa Checkout or Visa SRC Configuration

Please note: Visa Checkout and Visa SRC are forms of Digital Payments, which are not available in production for Bank of America merchants at this time.

You must enroll in Visa Checkout or Visa SRC and create a Visa Checkout profile before you can enable it as a payment method. See the Visa Checkout or Visa SRC guide. Only the authorization and sale transaction types are supported for Visa Checkout and Visa SRC transactions.

⚠️ Visa SRC uses Visa Checkout services, Merchant Portal labels, and API fields.

The payment methods selection page is displayed as part of the checkout process for the following scenarios:

- Multiple payment methods are enabled for the profile, and no **payment_method** field is included in the request.
- Visa Checkout is the only enabled payment method for the profile.
- **payment_method=**`visacheckout` is included in the request.

Visa Checkout and Visa SRC require the customer to enter only a username and password to pay for goods. It eliminates the need to enter account, shipping, and billing information. The customer logs in to their Visa Checkout or Visa SRC account and chooses the card with which they would like to pay. If the Secure Acceptance profile is enabled to request the payer authentication service for a specific card type, the customer is redirected to the relevant payer authentication screen before Secure Acceptance processes the transaction and redirects the customer to your web site.

## 10.7 Configuring Visa Checkout or Visa SRC

1. In the left navigation panel, choose **Payment Configuration > Digital Payment Solutions**. The Digital Payment Solutions page appears.

2. Click **Configure**. The Visa Merchant Services Agreement appears.

3. Review the Visa Checkout Services Agreement, then click **Agree and Create Account**. The Visa Checkout Configuration panel opens to the Merchant Configuration section.

4. Enter your payment details.

5. Click Submit.

## 10.8 Enabling the Payment Method for Visa Checkout or Visa SRC

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

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

3. Click **Payment Settings**. The Payment Settings page appears.

4. Check Enable Visa Checkout.

5. Enter the name of the Visa Checkout profile to be used. If no profile name is entered, the default Visa Checkout profile is used.

6. Check the card types to request the payer authentication service for:

   - Visa—the Visa Secure service is requested.
   - Mastercard—the Mastercard Identity Check service is requested.
   - American Express—the American Express SafeKey service is requested. See "Payer Authentication Configuration".

7. Indicate when to reject transactions based on a certain criterion:

   - Billing address details are incorrect (AVS fail).
   - Security code is incorrect (CVV/CVN fail).
   - The Visa Checkout risk score is above your specified score. Select the risk score to use with your fraud model. A value of 0 indicates that a risk score will not be taken into account, and a higher risk score indicates a higher perceived fraud risk.

8. Click **Save**.

# 11 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 live 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.

## 11.1 Creating Security Keys

1. Log in to the Merchant Portal.

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

3. Select a profile. The General Settings page appears.

4. Click **Security.** The security keys page appears.

5. Click the Create Key plus sign (+).

6. Enter a key name (required).

7. Choose signature version **1** (default).

8. Choose signature method **HMAC-SHA256** (default).

9. Click Create.

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

11. 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 "Samples in Scripting Languages".

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

   ⚠ 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.

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.

# 12 Checkout Configuration

The payment form is the customer's checkout experience. It consists of either a series of pages or as a single checkout page in which the customer enters or reviews information before submitting a transaction. Select the fields that you want displayed on the single checkout page or on each page of the multi-step checkout process: billing, shipping, payment, and order review.

## 12.1 Configuring the Payment Form

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 **Payment Form**. The Payment Form page appears.

4. Choose the payment form flow:

   - **Multi-step payment form**—the checkout process consists of a sequence of pages on which the customer enters or reviews information before submitting a transaction. The default sequence is payment selection (if multiple payment methods are enabled), billing, shipping, payment, review, and receipt.
   - **Single page form**—the checkout process consists of one page on which the customer enters or reviews information before submitting a transaction.

   Do not click **Save** until you have selected the billing or shipping fields, or both.

5. Check Display the total tax amount in each step of the checkout process.

   The total tax amount must be included in each transaction. Calculate and include the total tax amount in the **tax_amount** field.

   Do not click **Save** until you have selected the billing or shipping fields, or both.

6. Click **Save**.

## 12.2 Configuring Billing Information Fields

⚠ Select the billing information fields that your Bank of America requires.

If the billing country is U.S. or Canada, you can select the state code field as a required field. Bank of America recommends that if the billing country is U.S. or Canada, the state code and the postal code fields be selected as required. If the billing country is located in the rest of the world, you can also select the state code field as a required field.

Select the customer billing information fields that you want displayed on Secure Acceptance. If these fields are captured at an earlier stage of the order process (for example on your web site), they can be passed into Secure Acceptance as hidden form fields (see "Request Fields"). You can shorten the checkout process by not selecting billing information.

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 **Payment Form**. The Payment Form page appears.

4. Check **Billing Information**. The billing information fields appear.

5. Check the billing information fields that your merchant provider requires. The options for each field are:

   - Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the billing information fields when Hosted Payments Page is rendered—these fields must be passed into Secure Acceptance as hidden form fields.

   - Edit: the customer can view and edit the billing information on the Hosted Payments Page. When you select this option, the display option is automatically selected.

   - Require: the customer is required to enter the billing information on the Hosted Payments Page before they submit the transaction. When you select this option, all other options are automatically selected.

   Do not click **Save** until you have selected the billing and order review fields.

6. Indicate whether to mask sensitive fields.

7. Click **Save**.

## 12.3 Configuring Shipping Information Fields

Select the shipping information fields that your merchant provider requires.

Select the customer shipping information fields that you want displayed on Secure Acceptance. These fields are optional. If you do not add these fields, the shipping information step is removed from Secure Acceptance. If these fields are captured at an earlier stage of the order process (for example, on your web site), they can be passed into Secure Acceptance as hidden form fields (see "Request Fields"). You can shorten the checkout

process by not selecting shipping information.

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 **Payment Form**. The Payment Form page appears.

4. Check **Shipping Information**.

5. Check the shipping information fields that your merchant provider requires. The options for each field are:

   • Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the shipping information fields when Hosted Payments Page is rendered—these fields must be passed into Secure Acceptance as hidden form fields.

   • Edit: the customer can view and edit the shipping information on the Hosted Payments Page. When you select this option, the display option is automatically selected.

   • Require: the customer is required to enter the shipping information on the Hosted Payments Page before they submit the transaction. When you select this option, all other options are automatically selected.

     Do not click **Save** until you have selected the shipping and order review fields.

6. Indicate whether to mask sensitive fields.

7. Click **Save**.

## 12.4 Configuring Order Review Details

Select the fields that you want displayed on the Order Review page of Hosted Payments Page. The customer reviews this information before submitting a transaction.

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 **Payment Form**. The Payment Form page appears.

4. Check the fields that you want displayed on the Order Review page of Hosted Payments Page. The options for each field are:

   • Display: the customer can view the information contained in this field. Available only for billing and shipping information.

   • Edit: the customer can view and edit the information contained in this field.

5. Click **Save**.

# 13 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.

⚠ It is recommended 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.

## 13.1 Configuring Merchant Notifications

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 **Notifications**. The Notifications page appears.

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

   - Check **Merchant POST URL**. Enter the HTTPS URL. Bank of America sends transaction information to this URL. For more information, see "Reply 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.

   - 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 "Reply Fields".

5. 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 six digits of the card number. All other digits are masked: 123456xxxxxxxxxx

   - 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: 123456xxxxxx1234

6. Continue to configure the customer notifications (see "Customer Receipts") or click **Save**.

# 14 Customer Receipts

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers can reply with questions regarding their purchases, so use an active email account. The email format is HTML unless your customer email is rich text format (RTF).

## 14.1 Configuring Customer Notifications

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 **Notifications**. The Notifications page appears.

4. Check **Email Receipt to Customer**.

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

6. Enter the sender name of your business. It is displayed on the customer receipt.

7. Check **Send a copy to**. This setting is optional.

8. 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.

# 15 Customer Response Page

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

You can choose to have a transaction response page displayed to the customer at the end of the checkout process, and a cancel response page displayed during the checkout process. Enter a URL for your own customer response page, or use the Bank of America hosted response pages. Depending upon the transaction result, the Bank of America hosted response pages are Accept, Decline, or Error. 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.

## 15.1 Configuring a Bank of America Hosted 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. Under the Transaction Response Page heading, check **Hosted by Bank of America**.

5. Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is five.

6. Under the Customer Redirect after Checkout heading, enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.

7. Click **Save**. The Profile Settings page appears.

## 15.2 Configuring a Custom Hosted 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. Under the Transaction Response Page heading, check **Hosted by You**.

5. Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL.

   Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code (), and redirect your customer to the appropriate response page. See "Reason Codes".

6. Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is 5.

7. Under the Customer Redirect after Checkout heading, enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.

8. Click **Save**.

## 15.3 Configuring a Custom Bank of America Hosted 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. Under the Custom Cancel Response Page heading, check **Hosted by Bank of America**.

5. Click **Save**.

## 15.4 Configuring a Custom Cancel 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. Under the Custom Cancel Response Page heading, check **Hosted by You**.

5. Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL.

   Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code (), and redirect your customer to the appropriate response page. See "Reason Codes".

6. Click **Save**.

# 16 Custom Checkout Appearance

Customize the appearance and branding of the Secure Acceptance checkout pages by choosing a background color, font, and text color. Upload a logo or image, and align it within the header or footer.

Bank of America recommends that you preview your changes in the Image Preview window.

To display an image as the header banner of the payment form, the image dimensions must not exceed 840 (w) x 60 (h) pixels and the image size must not exceed 100 kB. To display a small logo within the header banner, the logo height must not exceed 60 pixels. The image file must be GIF, JPEG, or PNG.

## 16.1 Changing Header Content

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 **Branding**. The Branding page appears.

4. Check **Display Header**. **Step 5**      Click the header color icon.

5. Choose a color in one of two ways:

   • Enter a hexadecimal value for the header color of the payment form.

   • Click within the header color palette to choose a color. Click the color icon to confirm your selection.

7. Click **Browse** to upload the image to display as the header banner or as a logo within the header banner.

8. Choose the alignment option for the image or logo: left-aligned, centered, or right-aligned.

9. Click **Save**.

## 16.2 Changing Body Color and Font Settings

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 **Branding**. The Branding page appears.

4. Choose a background color for the main body in one of two ways:

   - Enter a hexadecimal value for the background color.

   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.

5. Select a text font from the drop-down list.

6. Choose a text color in one of two ways:

   - Enter a hexadecimal value for the background color.

   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.

7. Click **Save**.

8. Click **Set to Default** to restore all the default settings on this page.

## 16.3 Changing Background and Text Color of the Total Amount

⚠️ If you are implementing the iframe embedded version of Hosted Payments Page, the total amount figure is not displayed within the iframe. Any settings you select below are ignored.

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 **Branding**. The Branding page appears.

4. Choose a background color in one of two ways:

   - Enter a hexadecimal value for the background color.

   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.

5. Choose a text color in one of two ways:

   - Enter a hexadecimal value for the text color of the total amount.

   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.

6. Click **Save**.

7. Click **Set to Default** to restore all the default settings on this page.

## 16.4 Changing the Progress Bar Color

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 **Branding**. The Branding page appears.

4. Choose a color in one of two ways:

   • Enter a hexadecimal value for the color of the progress bar.

   • Click within the header color palette to choose a color. Click the color icon to confirm your selection.

5. Click **Save**.

6. Click **Set to Default** to restore all the default settings on this page.

## 16.5 Changing Color and Text on Pay or Finish Button

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 **Branding**. The Branding page appears.

4. Choose a background color of the pay or the finish button in one of two ways:

   • Enter a hexadecimal value for the background color.

   • Click within the header color palette to choose a color. Click the color icon to confirm your selection.

5. Choose a color of the pay or the finish button text in one of two ways:

   • Enter a hexadecimal value for the text.

   • Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

6. Check **Change Button text.** A text box appears for the pay button.

7. Enter the text you want displayed on the pay button. This button text is required.

8. Enter the text you want displayed on the finish button. This button text is required.

9. Click **Save**.

10. Click **Set to Default** to restore all the default settings on this page.

## 16.6 Changing Footer Color and Uploading a SmallLogo or Image

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 **Branding**. The Branding page appears.

4. Check **Display Footer**.

5. Choose a color in one of two ways:

    • Enter a hexadecimal value for the footer color of the payment form.

    • Click within the header color palette to choose a color. Click the color icon to confirm your selection.

6. Click **Browse** to upload a footer logo. Upload the image that you want displayed within the footer of the payment form.

   To display a small logo or image in the footer of the payment form, the file must not exceed 840 (w) x 60 (h) pixels. The image file must be GIF, JPEG, or PNG.

7. Choose the alignment option for the image: left-aligned, centered, or right-aligned.

8. Click **Save**.

9. Click **Set to Default** to restore all the default settings on this page.

# 17 Checkout Language Localization

Secure Acceptance supports multiple languages. The Locale Codes table lists all the supported languages and the locale code that you must include in your payment form.

From the list, include the locale code in the **locale** request field on your payment form. See "Sample Transaction Process Using JSP".

**Example** American English

<input type="hidden" name="locale" value="en-us">

**Locale Codes**

| Language | Locale Code |
|---|---|
| Arabic | ar-xn |
| Catalan | ca-es |
| Chinese—Hong Kong | zh-hk |
| Chinese—Macau | zh-mo |

| Language | Locale Code |
|---|---|
| Chinese—Mainland | zh-cn |
| Chinese—Singapore | zh-sg |
| Chinese—Taiwan | zh-tw |
| Croatian | hr-hr |
| Czech | cz-cz |
| Danish | da-dk |
| Dutch | nl-nl |
| English—United States of America | en-us |
| English—Australia | en-au |
| English—Great Britain | en-gb |
| English—Canada | en-ca |
| English—Ireland | en-ie |
| English—New Zealand | en-nz |
| Finnish | fi-fi |
| French | fr-fr |
| French—Canada | fr-ca |
| German | de-de |
| German—Austria | de-at |
| Greek | el-gr |
| Hebrew | he-il |
| Hungary | hu-hu |
| Indonesian | id-id |
| Italian | it-it |
| Japanese | ja-jp |
| Korean | ko-kr |
| Lao People's Democratic Republic | lo-la |
| Malaysian Bahasa | ms-my |
| Norwegian (Bokmal) | nb-no |
| Philippines Tagalog | tl-ph |
| Polish | pl-pl |
| Portuguese—Brazil | pt-br |
| Russian | ru-ru |

| Language | Locale Code |
| --- | --- |
| Slovakian | sk-sk |
| Spanish | es-es |
| Spanish—Argentina | es-ar |
| Spanish—Chile | es-cl |
| Spanish—Colombia | es-co |
| Spanish—Mexico | es-mx |
| Spanish—Peru | es-pe |
| Spanish—United States of America | es-us |
| Swedish | sv-se |
| Thai | th-th |
| Turkish | tr-tr |
| Vietnamese | vi-vn |

# 18 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"

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

2. Perform one of the following steps:

   - On the Active Profiles tab, select the profile that you want to activate, and click the **Promote Profile** icon.

   - On the Edit Profile page, click the **Promote Profile** icon.

3. Click **Confirm**.

# 19 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.

# 20 Samples in Scripting Languages

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

Select to download the sample script for the scripting language that you use:

JSP

ASP.NET (C#)

Ruby

PHP

Perl

VB

## 20.1 Sample Transaction Process Using JSP

1. ***payment_form.jsp*** file—represents the customer's product selection on a web site. Enter your access key and profile ID into their respective fields. POST the fields to your server to sign and create the signature. All the fields must be included in the **signed_field_names** field as a CSV list.

2. ***security.jsp*** file—security algorithm signs fields 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. ***payment_confirmation.jsp*** file—represents the customer order review page on a web site, before the customer makes a payment. POST transaction to the Secure Acceptance endpoint () and render the Hosted Payments Page. See "Payment Transactions".

# 21 Payment Transactions

## 21.1 Endpoints and Transaction Types

Table 4        Endpoints

**Create Payment Token Endpoints**

| Endpoint | URL | Supported Transaction Type |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/token/ create | create_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/token/create | create_payment_token |

**Iframe Create Payment Token Endpoints** (see "Iframe Implementation".)

| Endpoint | URL | Supported Transaction Type |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/token/ create | create_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/token/create | create_payment_token |

**Iframe Transaction Endpoints** (see "Iframe Implementation".)

| Endpoint | URL | Supported Transaction Types |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/pay | • authorization<br>• authorization,create_payment_token<br>• authorization,update_payment_token<br>• sale<br>• sale,create_payment_token<br>• sale,update_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/embedded/ pay | • authorization<br>• authorization,create_payment_token<br>• authorization,update_payment_token<br>• sale<br>• sale,create_payment_token<br>• sale,update_payment_token |

**Iframe Update Payment Token Endpoints** (see "Iframe Implementation".)

| Endpoint | URL | Supported Transaction Type |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/token/update | update_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/embedded/token/update | update_payment_token |

**One-Click Endpoints**

| Endpoint | URL | Supported Transaction Types |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/pay | • authorization<br>• authorization,update_payment_token<br>• sale<br>• sale,update_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/embedded/ pay | • authorization<br>• authorization,update_payment_token<br>• sale<br>• sale,update_payment_token |

**Process Payment Token Endpoints**

| Endpoint | URL | Supported Transaction Types |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/pay | • authorization<br>• authorization,create_payment_token<br>• authorization,update_payment_token<br>• sale<br>• sale,create_payment_token<br>• sale,update_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/pay | • authorization<br>• authorization,create_payment_token<br>• authorization,update_payment_token<br>• sale<br>• sale,create_payment_token<br>• sale,update_payment_token |

**Update Payment Token Endpoints**

| Endpoint | URL | Supported Transaction Type |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/token/update | update_payment_token |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/embedded/token/update | update_payment_token |

**Visa Checkout and Visa SRC Endpoints**

| Endpoint | URL | Supported Transaction Types |
|---|---|---|
| Test Transactions | https://testsecureacceptance.merchant-services.bankofamerica.com/pay | • authorization<br>• sale |
| Live Transactions | https://secureacceptance.merchant-services.bankofamerica.com/pay | • authorization<br>• sale |

# 22 Required Signed Fields

The following signed fields are required in all Secure Acceptance requests:

- access_key
- amount
- currency
- locale
- reference_number
- signed_date_time
- signed_field_names
- transaction_type
- transaction_uuid

For descriptions of signed request fields, see "Request Fields".

# 23 Payment Tokens

## 23.1 Creating a Payment Card Token

⚠️ Include the appropriate endpoint that supports the **create_payment_token** transaction type (see "Endpoints and Transaction Types"). For descriptions of all request and reply fields, see "API Fields".

Include all request fields in the **signed_field_names** field with the exception of the **card_ number** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction in order to prevent data tampering.

**Example Request:** Create a Standalone Payment Token

```
reference_number=123456789
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z signed_field_names=comma
separated list of signed 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
```

**Example Reply:** Create a Standalone Payment Token

```
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_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=3529893314302230706689
```

# 24 Payment Token Transactions

## 24.1 One-Click

The customer is directed to the Order Review page. Depending on the settings you configured for Hosted Payments Page (see "Checkout Configuration"), the customer can view or update billing, shipping, and payment details before confirming to pay.

⚠ Include the appropriate endpoint that supports the **authorization** or **sale** transaction types (see "Endpoints and Transaction Types"). For descriptions of all request and reply fields, see "API Fields".

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

**Example Request:** One-Click Transaction

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p
2 reference_number=1350029885978
payment_token=3427075830000181552556
consumer_id=1239874561
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M
```

**Example Reply:** One-Click Transaction

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
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
payment_token_instrument_identifier_id=0000111122225555
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==2012-08-14T134608Z
req_payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
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==2012-08-14T134608Z
payment_token=3427075830000181552556 signed_field_names=comma
separated list of signed fields signed_date_time=2012-10-
12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

# 25 Payment Token Updates

## 25.1 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.

You must configure the billing, shipping, and payment details so that a customer can edit their details on the Order Review page. See "Configuring Order Review Details".

⚠️  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 Request:** Updating a Payment Token for a Card

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
reference_number=1350029885978
payment_token=3427075830000181552556
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=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

**Example Reply:** Updating a Payment Token for a Card

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
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==2012-08-14T134608Z
payment_token=3427075830000181552556
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

# 26 TEST and View Transactions

⚠️ 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.

## 26.1 Testing Transactions

1. Log in to the Merchant Portal test environment.

2. Create a Secure Acceptance profile. See "Creating a Hosted Payments Page Profile".

3. Integrate with Secure Acceptance. See "Samples in Scripting Languages".

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

4. You can use the following test payment card numbers for transactions. Remove spaces when sending 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 |

## 26.2 Viewing Transactions in Business Advantage 360 (BA360)

1. Log in to your Merchant Services account in Business Advantage 360.

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.

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

# 27 Appendix A: API Fields

## 27.1 Data Type Definitions

⚠ 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 | 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) |

## 27.2 Request Fields

⚠️ To prevent data tampering, sign all request fields with the exception of the **card_number** field, the **card_cvn** field, and the **signature** field.

**Request Fields**

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| access_key | Required for authentication with Secure Acceptance. See <u>"Security Keys"</u>.<br><br>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.<br><br>Possible values:<br><br>• `true`: Customer can update details.<br>• `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. | • create_payment_token (R)<br>• authorization or sale (R)<br>• authorization,create_ payment_token (R)<br>• sale,create_payment_ token (R)<br>• update_payment_token (O) | Amount String (15) |
| auth_indicator | Flag that specifies the purpose of the authorization. Possible values:<br><br>• 0: Preauthorization<br>• 1: Final authorization<br><br>Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization.<br><br>To set the default for this field, contact customer support. | authorization (See description) | String (1) |

© Bank of America Corporation. All rights reserved.

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| auth_type | Authorization type. Possible values:<br><br>• AUTOCAPTURE: Automatic capture.<br>• STANDARDCAPTURE: Standard capture.<br>• verbal: Forced capture. | authorization (See description.)<br><br>capture (Required for a verbal authorization; otherwise, not used.) | String (11) |
| bill_payment | Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values:<br><br>• true: Bill payment or loan payment.<br>• false (default): Not a bill payment or loan payment. | This field is optional. | Enumerated String (5) |
| bill_to_address_city | City in the billing address.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | • create_payment_token (R)<br>• authorization or sale (R)<br>• authorization,create_payment_token (R)<br>• sale,create_payment_token (R)<br>• update_payment_token (O) | AlphaNumeric Punctuation<br><br>String (50) |
| bill_to_address_ country | Country code for the billing address. Use the two-character ISO country codes.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | • create_payment_token (R)<br>• authorization or sale (R)<br>• authorization,create_payment_token (R)<br>• sale,create_payment_token (R)<br>• update_payment_token (O) | Alpha String (2) |
| bill_to_address_line1 | First line of the billing address.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | • create_payment_token (R)<br>• authorization or sale (R)<br>• authorization, create_payment_token (R)<br>• sale,create_payment_token (R) | AlphaNumeric Punctuation<br><br>String (60) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | | • update_payment_token (O) | |
| bill_to_address_ line2 | Second line of the billing address.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | This field is optional | AlphaNumeric Punctuation<br><br>String (60) |
| bill_to_address_ postal_code | Postal code for the billing address.<br><br>This field is required if **bill_to_address_ country** is U.S. or Canada.<br><br>When the billing country is the U.S., the 9- digit postal code must follow this format: [5 digits][dash][4 digits]<br><br>**Example** 12345-6789<br><br>When the billing country is Canada, the 6- digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]<br><br>**Example** A1B 2C3<br><br>For the rest of the world countries, the maximum length is 10.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | See description. | AlphaNumeric Punctuation<br><br>See description. |
| bill_to_address_state | State or province in the billing address. Use the two-character ISO state and province code.<br><br>This field is required if **bill_to_address_ country** is U.S. or Canada.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | See description | AlphaNumeric Punctuation String (2) |
| bill_to_company_ name | Name of the customer's company.<br><br>This value can be entered by your customer during the checkout process, or you can | This field is optional | AlphaNumeric Punctuation String (40) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | include this field in your request to Secure Acceptance. "Configuring Billing Information Fields". | | |
| bill_to_email | Customer email address, including the full domain name.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,create_payment_token (R)<br><br>• sale,create_payment_token (R)<br><br>• 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.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,create_payment_token (R)<br><br>• sale,create_payment_token (R)<br><br>• update_payment_token (O) | AlphaNumeric Punctuation<br><br>String (60) |
| bill_to_phone | Customer phone number. It is recommended that you include the country code if the order is from outside the U.S.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields".<br><br>This field is optional for card payments. | See description. | Phone<br><br>String (6 to 15) |
| bill_to_surname | Customer last name. This name must be the same as the name on the card.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Billing Information Fields". | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,create_payment_token (R)<br><br>• sale,create_payment_ | AlphaNumeric Punctuation<br><br>String (60) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | | token (R)<br><br>• update_payment_token (O) | |
| card_cvn | Card verification number.<br><br>For American Express card types, the CVN must be 4 digits.<br><br>This field can be configured as required or optional. See "Payment Method Configuration". | See description | Numeric String (4) |
| card_expiry_date | Card expiration date.<br><br>Format: MM-YYYY | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,creat e_ payment_token (R)<br><br>• sale,create_paymen t_ token (R)<br><br>• update_payment_tok en (O) | Date (a) String (7) |
| card_number | Card number.<br><br>Use only numeric values. Be sure to include valid and well-formed data for this field. | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,create_ payment_token (R)<br><br>• sale,create_payment_ token (R)<br><br>• update_payment_token (O) | Numeric String (20) |
| card_type | • Type of card to authorize. Use one of these values:<br><br>• 001: Visa<br><br>• 002: Mastercard<br><br>• 003: American Express<br><br>• 004: Discover<br><br>• 005: Diners Club: cards starting with 54 or | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,create_ payment_token (R)<br><br>• sale,create_payment_ token (R)<br><br>• ⬜update_payment_token | Enumerated String<br><br>String (3) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | 55 are rejected.<br><br>• 006: Carte Blanche<br><br>• 007: JCB<br><br>• 014: EnRoute<br><br>• 021: JAL<br><br>• 024: Maestro UK Domestic<br><br>• 031: Delta<br><br>• 033: Visa Electron<br><br>• 034: Dankort<br><br>• 036: Carte Bancaire<br><br>• 037: Carta Si<br><br>• 042: Maestro International<br><br>• 043: GE Money UK card<br><br>• 050: Hipercard (sale only)<br><br>• 054: Elo | (O) | |
| complete_route | Concatenation of individual travel legs in the format for example:<br><br>SFO-JFK:JFK-LHR:LHR-CDG.<br><br>For a complete list of airport codes, see IATA's City Code Directory.<br><br>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. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management | AlphaNumeric Punctuation<br><br>String (255) |
| currency | Currency used for the order. For the possible values, see the ISO currency codes.<br><br>**Important!** To prevent data tampering, sign this field. | • create_payment_token (R)<br><br>• authorization or sale (R)<br><br>• authorization,create_ payment_token (R)<br><br>• sale,create_payment_ token (R)<br><br>• update_payment_token | Alpha String (3) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | | (O) | |
| customer_browser_ color_depth | Indicates the bit depth of the color palette for displaying images, in bits per pixel.<br><br>Secure Acceptance automatically populates this field, but you can override it.<br><br>For more information, see https://en.wikipedia.org/wiki/Color_depth. | This field is 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:<br><br>• `true`<br><br>• `false` | This field is optional. | String (5) |
| 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:<br><br>• `true`<br><br>• `false` | This field is 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.<br><br>For more information, see https://en.wikipedia.org/wiki/IETF_language_tag. | This field is optional. | String (8) |
| customer_browser_ screen_height | Total height of the cardholder's screen in pixels. Secure Acceptance automatically populates this field, but you can override it.<br><br>**Example** 864 | This field is optional. | String (6) |
| customer_browser_ screen_width | Total width of the cardholder's screen in pixels. Secure Acceptance automatically populates this field, but you can override it. | This field is optional. | String (6) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|-------|-------------|--------------------------------------|--------------------|
| 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 | This field is optional. | String (5) |
| customer_cookies_ accepted | Indicates whether the customer's browser accepts cookies. This field can contain one of the following values:<br><br>• `true`: Customer browser accepts cookies.<br><br>• `false`: Customer browser does not accept cookies | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | Enumerated String<br><br>String (5) |
| customer_gift_wrap | Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values:<br><br>• `true`: Customer requested gift wrapping.<br><br>• `false`: Customer did not request gift wrapping. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | Enumerated String<br><br>String (5) |
| customer_ip_address | Customer's IP address reported by your web server using socket information. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | IP<br><br>IPv4: String (15)<br><br>IPv6: String (39) |
| departure_time | Departure date and time of the first leg of the trip. Use one of the following formats:<br><br>• yyyy-MM-dd HH:mm z<br><br>• yyyy-MM-dd hh:mm a z<br><br>• yyyy-MM-dd hh:mma z<br><br>• HH = 24-hour format<br><br>• hh = 12-hour format<br><br>• a = am or pm (case insensitive)<br><br>• z = time zone of the departing flight.<br><br>**Examples**<br><br>• 2020-01-20 23:30 GMT<br><br>• 2020-01-20 11:30 PM GMT | This field is optional.<br><br>Please refer to the Guides section under Fraud Management | Date (c) DateTime (29) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | • 2020-01-20 11:30pm GMT | | |
| 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 (_)<br><br>However, do not use the same uppercase and lowercase letters to indicate different session IDs.<br><br>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.<br><br>**Important** The Bank of America- generated device fingerprint ID overrides the merchant-generated device fingerprint ID | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | AlphaNumeric Punctuation<br><br>String (88) |
| health_care_#_ amount | See **skip_decision_manager**. Amount of the healthcare payment can range from `0` to `4`. Send this field with a corresponding **health_care_#_amount_ type** field. | | |
| health_care_#_ amount_type | Type of healthcare payment. # can range from 0 to 4.<br><br>Mastercard possible values:<br><br>• `eligible-total`: total amount of healthcare.<br>• `prescription`<br>Visa possible values:<br><br>• `clinic`<br>• `dental`<br>• `healthcare`: total amount of healthcare<br>• `healthcare-transit`<br>• `prescription`<br>• `vision`<br><br>Send this field with a corresponding **health_care_#_amount** field. | authorization (O) | String (35) |
| ignore_avs | Ignore the results of AVS verification.<br><br>Possible values:<br><br>• `true`<br>• `false`<br><br>**Important** To prevent data tampering, sign this | This field is optional. | Enumerated String<br><br>String (5) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | field. | | |
| ignore_cvn | Ignore the results of CVN verification.<br><br>Possible values:<br><br>• `true`<br><br>• `false`<br><br>**Important** To prevent data tampering, sign this field. | This field is optional. | Enumerated String<br><br>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.<br><br>Possible values:<br><br>• `healthcare_medical`<br><br>• `healthcare_transit` | authorization (O) | String (20) |
| item_#_code | Type of product. # can range from 0 to 199. | This field is optional.<br><br>If you include this field, you must also include the **line_item_count** field. | AlphaNumeric Punctuation String (255) |
| item_#_name | Name of the item. # can range from 0 to 199.<br><br>This field is required when the **item_#_ code** value is not default nor related to shipping or handling. | See description.<br><br>If you include this field, you must also include the **line_item_count** field. | AlphaNumeric Punctuation String (255) |
| item_#_passenger_ email | Passenger's email address. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | String (255) |
| item_#_passenger_ forename | Passenger's first name. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | 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. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | String (32) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| item_#_passenger_ phone | Passenger's phone number. If the order is from outside the U.S., include the country code. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | 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. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | String (32) |
| item_#_passenger_ surname | Passenger's last name. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | String (60) |
| item_#_passenger_ type | Passenger classification associated with the price of the ticket. You can use one of the following values:<br><br>• `ADT`: Adult<br>• `CNN`: Child<br>• `INF`: Infant<br>• `YTH`: Youth<br>• STU: Student<br>• SCR: Senior Citizen<br>• MIL: Military | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | String (32) |
| item_#_quantity | Quantity of line items. The default value is `1`.<br><br>Required field when one of the following product codes is used:<br><br>• adult_content<br>• coupon<br>• electronic_good<br>• electronic_software<br>• gift_certificate<br>• service<br>• subscription<br><br># can range from `1` to `199`.<br><br>This field is required when the **item_#_ code** value is not default nor related to shipping or handling. | See description.<br><br>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.<br><br>Required field when one of the following product codes is used:<br><br>• adult_content<br><br>• coupon<br><br>• electronic_good<br><br>• electronic_software<br><br>• gift_certificate<br><br>• service<br><br>• subscription<br><br># can range from 0 to 199. | See description.<br><br>If you include this field, you must also include the **line_item_count** field. | AlphaNumeric Punctuation<br><br>String (255) |
| item_#_tax_amount | Tax amount to apply to the line item. # can range from 0 to **199.** This value cannot be negative. The tax amount and the offer amount must be in the same currency. | This field is optional.<br><br>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.<br><br>**Important** You must include either this field or the amount field in the request. | See description.<br><br>If you include this field, you must also include the **line_item_count** field. | Amount String (15) |
| 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<br><br>= San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory.<br><br>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. | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | Alpha String (3) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| journey_leg#_orig | Airport code for the origin leg of the trip, | This field is optional. | Alpha String (3) |
| | 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, IATA's City Code Directory. | Please refer to the Guides section under Fraud Management. | |
| | 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. | | |
| journey_type | Type of travel, such as one way or round trip. | This field is optional. | AlphaNumeric Punctuation |
| | | Please refer to the Guides section under Fraud Management. | String (32) |
| line_item_count | Total number of line items. Maximum number is 200. | This field is required if 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," page 35. | Required by the Secure Acceptance application. | Locale String (5) |
| | **Important** To prevent data tampering, sign this field. | | |
| merchant_defined_ data# | Optional fields that you can use to store information (see "Configuring Customer Notifications"). # can range from 1 to 100. | This field is optional. | AlphaNumeric Punctuation |
| | | Please refer to the Guides section under Fraud Management. | String (100) |
| | Merchant-defined data fields 1 to 4 are stored against the payment token and are used for subsequent token based transactions. Merchant defined data fields 5 to 100 are passed trough to Custom Fraud Management as part of the initial payment request and are not stored against the payment token. | | |
| | **Important** 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 | | |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | 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. | | |
| 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.<br><br>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.<br><br>When you do not include this value in your request, the merchant URL in your account is sent.<br><br>**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.<br><br>When you do not include this value in your request, the merchant city in your account is sent.<br><br>**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.<br><br>When you do not include this value in your request, the merchant phone number in your account is sent.<br><br>**Important** This value must consist of English characters. | authorization (O) | String (14) |
| merchant_descriptor_ country | Country code for your business location.<br><br>Use the standard ISO Standard Country Codes. This value might appear on the cardholder's statement.<br><br>When you do not include this value in your request, the merchant country in your account is sent.<br><br>**Important** This value must consist of English characters. | authorization (O) | String (2) |
| merchant_descriptor_ postal_code | Postal code for your business location. This value might appear on the cardholder's statement.<br><br>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:<br><br>[5 digits][dash][4 digits]<br><br>Example 12345-6789<br><br>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]<br><br>**Example** A1B 2C3<br><br>When you do not include this value in your request, the merchant postal code in your account is sent.<br><br>**Important** This value must consist of English characters. | authorization (O) | String (14) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | **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. | | |
| merchant_descriptor_ state | State code or region code for your business location. This value might appear on the cardholder's statement.<br><br>For the U.S. and Canada, use the standard State, Province, and Territory Codes for the United States and Canada.<br><br>When you do not include this value in your request, the merchant state in your account is sent.<br><br>Important This value must consist of English characters. | authorization (O) | String (3) |
| merchant_descriptor_ street | Street address for your business location.<br><br>This value might appear on the cardholder's statement.<br><br>When you do not include this value in your request, the merchant street in your account is sent.<br><br>**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. | This field is optional. | AlphaNumeric Punctuation<br><br>String (2000) |
| merchant_secure_ data1<br><br>merchant_secure_ data2<br><br>merchant_secure_ data3 | Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository. | This field is optional. | AlphaNumeric Punctuation<br><br>String (100) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| 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. | This field is 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. | This field is optional. | URL String (255) |
| override_custom_ receipt_page | Overrides the custom receipt profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later. Important To prevent data tampering, sign this field. | This field is 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`. | This field is optional. | Integer (5) |
| override_paypal_ order_setup | Overrides the PayPal order setup profile setting. Possible values: <br> • `include_authorization`: The PayPal order is created and authorized. <br> • `exclude_authorization`: The PayPal order is created but not authorized. | This field is optional. See "Enabling PayPal Express Checkout," page 20 | String (21) |
| 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. | This field is optional. | String (2) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| 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.<br><br>Possible values:<br><br>• 01: 250 x 400<br><br>• 02: 390 x 400<br><br>• 03: 500 x 600<br><br>• 04: 600 x 400<br><br>• 05: Full page | This field is optional. | Integer (2) |
| payer_authentication_ challenge_code | Possible values:<br><br>• 01: No preference<br><br>• 02: No challenge request<br><br>• 03: Challenge requested (3D Secure requestor preference)<br><br>• 04: Challenge requested (mandate) | This field is optional. | Integer (2) |
| payer_authentication_ customer_annual_ transaction_count | Number of transactions (successful and abandoned) for this cardholder account within the past year.<br><br>Recommended for Discover ProtectBuy. | This field is optional. | Integer (3) |
| payer_authentication_customer_ daily_transaction_count | Number of transaction (successful or abandoned) for this cardholder account within the past 24 hours.<br><br>Recommended for Discover ProtectBuy. | This field is optional. | Integer (3) |
| payer_authentication_indicator | Indicates the type of authentication request. Secure Acceptance automatically populates this field, but you can override it.<br><br>Possible values:<br><br>• 01: Payment transaction | This field is optional. | Integer (2) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | • 04: Add card | | |
| | • 05: Maintain card | | |
| | • 06: Cardholder verification as part of EMV token identity and verification (ID&V) | | |
| payer_authentication_marketing_source | Indicates origin of the marketing offer. Recommended for Discover ProtectBuy | This field is optional. | String (40) |
| payer_authentication_merchant_fraud_rate | Calculated by merchants according to Payment Service Directive 2 (PSD2) and Regulatory Technical Standards (RTS). European Economic Area (EEA) and UK and Gibraltar card fraud divided by all EEA and UK and Gibraltar card volumes. 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 | This field is 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. | This field is optional. | String (25) |
| payer_authentication_merchant_score | Risk score provided by merchants. Used for Cartes Bancaires transactions. | This field is optional | String (20) |
| payer_authentication_mobile_phone | Cardholder's mobile phone number. **Important** Required for Visa Secure transactions in Brazil. Do not use this request field for any other types of transactions. | This field is optional | Integer (25) |
| payer_authentication_new_customer | Indicates whether the customer is a new or existing customer with the merchant. Possible values: • true • false | This field is optional | String (5) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| payer_authentication_ pre_order | Indicates whether cardholder is placing an order with a future availability or release date. <br><br> Possible values: <br><br> • 01: Merchandise available <br><br> • 02: Future availability | This field is optional | Integer (2) |
| payer_authentication_ pre_order_date | Expected date that a pre-ordered purchase will be available. <br><br> Format: <br><br> YYYYMMDD | This field is optional. | Integer (8) |
| payer_authentication_ prior_authentication_data | Data that the ACS can use to verify the authentication process. | This field is optional. | String (2048) |
| payer_authentication_ prior_authentication_method | Method the cardholder used previously to authenticate to the 3D Secure requester. <br><br> Possible values: <br><br> • 01: Frictionless authentication through the ACS <br><br> • 02: Cardholder challenge through the ACS <br><br> • 03: AVS verified <br><br> • 04: Other issuer methods <br><br> • 05-79: Reserved for EMVCo future use (values invalid until defined by EMVCo) <br><br> • 80-99: Reserved for directory server use | This field is optional. | Integer (2) |
| payer_authentication_ prior_authentication_time | Date and time in UTC of the previous cardholder authentication. <br><br> Format: YYYYMMDDHHMM | This field is optional. | Integer (12) |
| payer_authentication_ product_code | Specifies the product code, which designates the type of transaction. Specify one of the following values for this field: <br><br> • AIR: Airline purchase <br><br> **Important** Required for American Express SafeKey (U.S.). <br><br> • ACC: Accommodation Rental | This field is optional | String (3) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | • `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 | | |
| | **Important** Required for Visa Secure transactions in Brazil. Do not use this request field for any other types of transactions. | | |
| payer_authentication_ reorder | Indicates whether the cardholder is reordering previously purchased merchandise. Possible values: • `01`: First time ordered • `02`: Reordered | This field is optional. | Integer (2) |
| payer_authentication_secure_ corporate_payment | Indicates that dedicated payment processes and procedures were used. Potential secure corporate payment exemption applies. Possible Values: • `0` • `1` | This field is optional. | String (1) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| payer_authentication_ship_ to_address_first_used | Date on which this shipping address was first used.<br><br>Possible values:<br><br>• −1: Guest account<br><br>• 0: First used during this transaction<br><br>If neither value applies, enter the date in YYYYMMDD format.<br><br>Recommended for Discover ProtectBuy. | This field is optional. | Integer (8) |
| payer_authentication_ transaction_mode | Transaction mode identifier. Identifies the channel from which the transaction originates.<br><br>Possible values:<br><br>• M: MOTO (Mail Order Telephone Order)<br><br>• R: Retail<br><br>• S: E-commerce<br><br>• P: Mobile Device<br><br>• T: Tablet | This field is optional. | String (1) |
| • payer_authentication_ whitelisted | Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3D Secure requester.<br><br>• Possible Values:<br><br>• true: 3D Secure requester is whitelisted by cardholder<br><br>• false: 3D Secure requester is not whitelisted by cardholder | This field is optional. | String (5) |
| payment_method | Method of payment. Possible values<br><br>• card<br><br>• paypal<br><br>• visacheckout | This field is optional. | Enumerated String String (30) |
| payment_token | Identifier for the TMS customer token or the instrument identifier token. Populates the request with the information stored against the token. | • authorization or sale (R)<br><br>• authorization,update_ payment_token (R)<br><br>• sale,update_payment_ | Numeric String (26) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | | token (R) <br> • update_payment_token (R) | |
| payment_token_ comments | Optional comments you can add for the customer token. | This field is optional. | AlphaNumeric Punctuation String (255) |
| payment_token_title | Name or title for the customer token. | This field is optional. | AlphaNumeric Punctuation String (60) |
| promotion_code | Promotion code for a transaction. | This field is optional. | String (100) |
| 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. <br><br> 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. <br><br> **Important** To prevent data tampering, sign this field. | Required by the Secure Acceptance application. | AlphaNumeric Punctuation <br><br> Asia, Middle East, and Africa Gateway: String (40) <br><br> String (50) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| returns_accepted | Indicates whether product returns are accepted. This field can contain one of the following values:<br>• true<br>• false | This field is optional.<br><br>Please refer to the Guides section under Fraud Management. | Enumerated String (5) |
| ship_to_address_city | City of shipping address.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | AlphaNumeric Punctuation String (50) |
| ship_to_address_ country | Country code for the shipping address. Use the two-character ISO country codes.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | Alpha String (2) |
| ship_to_address_ line1 | First line of shipping address.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | AlphaNumeric Punctuation<br><br>String (60) |
| ship_to_address_ line2 | Second line of shipping address.<br><br>This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | AlphaNumeric Punctuation<br><br>String (60) |
| ship_to_address_ postal_code | Postal code for the shipping address.<br><br>This field is required if **bill_to_address_ country** is U.S. or Canada.<br><br>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]<br><br>**Example** 12345-6789<br><br>When the billing country is Canada, the 6- digit postal code must follow this format: [alpha][numeric][alpha][space] | This field is optional. | AlphaNumeric Punctuation See description. |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | [numeric][alpha][numeric] Example A1B 2C3 For the rest of the world countries, the maximum length is 10. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | | |
| ship_to_address_ state | State or province of shipping address. Use the two-character ISO state and province codes. This field is required if shipping address is U.S. or Canada. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | AlphaNumeric Punctuation String (2) |
| ship_to_company_ name | Name of the company receiving the product. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | AlphaNumeric Punctuation String (40) |
| ship_to_forename | First name of the person receiving the product. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional | AlphaNumeric Punctuation String (60) |
| ship_to_phone | Phone number of the shipping address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | Phone String (6 to 15) |
| ship_to_surname | Last name of the person receiving the product. This can be entered by your customer during the checkout process, or you can include this in your request to Secure Acceptance. See "Configuring Shipping Information Fields". | This field is optional. | AlphaNumeric Punctuation String (60) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| ship_to_type | Shipping destination.<br><br>Example Commercial, residential, store | This field is optional. | String (25) |
| shipping_method | Shipping method for the product. Possible values:<br><br>• sameday: Courier or same-day service<br><br>• oneday: Next day or overnight service<br><br>• twoday: Two-day service<br><br>• threeday: Three-day service<br><br>• lowcost: Lowest-cost service<br><br>• pickup: Store pick-up<br><br>• other: Other shipping method<br><br>• none: No shipping method | This field is optional. | Enumerated String String (10) |
| signature | Merchant-generated Base64 signature.<br><br>This is generated using the signing method for the **access_key** field supplied. | Required by the Secure Acceptance application. | AlphaNumeric Punctuation |
| signed_date_time | The 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.<br><br>Format: YYYY-MM-DDThh:mm:ssZ<br><br>**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.<br><br>Your system time must be accurate to avoid payment processing errors related to the **signed_date_time** field.<br><br>**Important** To prevent data tampering, sign this field. | Required by the Secure Acceptance application. | ISO 8601 Date String (20) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| 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.<br><br>**Important** All request fields should be signed to prevent data tampering, with the exception of the **card_number** field and the signature field. | Required by the Secure Acceptance application. | AlphaNumeric Punctuation Variable |
| skip_auto_auth | Indicates whether to skip or perform the preauthorization check when creating this token.<br><br>Possible values:<br><br>• `true` (skip the preauthorization check)<br><br>• `false` (perform the preauthorization check) | This field is optional. | Enumerated String String (5) |
| skip_decision_ manager | Indicates whether to skip Fraud Management. Please refer to the Guides section under Fraud Management. This field can contain one of the following values:<br><br>• `true` (Fraud Management is not enabled for this transaction, and the device fingerprint ID will not be displayed)<br><br>• `false` | This field is optional. | Enumerated String String (5) |
| tax_amount | Total tax amount to apply to the order. This value cannot be negative.<br><br>**Important** To prevent data tampering, sign this field. | This field is optional. | Amount String (15) |
| transaction_type | The type of transaction. Possible values:<br><br>• `authorization`<br><br>• `authorization,create_ payment_token`<br><br>• `authorization,update_ payment_token`<br><br>• `sale`<br><br>• `sale,create_payment_token`<br><br>• `sale,update_payment_token` | Required by the Secure Acceptance application | Enumerated String String (60) |

| Field | Description | Used By: Required (R) or Optional (O) | Data Type & Length |
|---|---|---|---|
| | • `create_payment_token` | | |
| | • `update_payment_token` | | |
| | Only authorization and sale are supported for Visa Checkout and Visa SRC transactions. | | |
| | **Important** To prevent data tampering, sign this field. | | |
| transaction_uuid | Unique merchant-generated identifier.<br><br>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.<br><br>**Important** To prevent data tampering, sign this field. | Required by the Secure Acceptance application. | ASCIIAlphaNu mericPunctuation String (50) |

## 27.3 Reply Fields

Reply fields are sent using the following 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 reply 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 reply fields have not been tampered with, create a signature using the fields listed in the **signed_field_names** reply 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").

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

- Parse the reply data according to the names of the fields instead of their order in the reply. For more information on parsing reply 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 reply fields are sent back to your Merchant POST URL or email. (See "Merchant Notifications".) Your error handler should use the **decision** field to obtain the transaction result if it receives a reason code that it does not recognize.

**Reply 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:<br><br>• See Appendix D, "Visa Secure Response Codes," on page 112.<br><br>• See Appendix B, "American Express SafeKey Response Codes," on page 109. | 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_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) |
| 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.<br><br>For security reasons, this field is returned only in merchant POST URL and email notifications (not in the receipt POST through the browser). | String (50) |
| decision | The result of your request. Possible values:<br><br>• ACCEPT<br><br>• DECLINE<br><br>• REVIEW | String (7) |

| Field | Description | Data Type & Length |
|---|---|---|
| | • `ERROR`<br>• `CANCEL`<br>See ["Types of Notifications"](). | |
| exchange_rate | Exchange rate if a currency conversion occurred.<br><br>The 17 characters include the decimal point. | Decimal (17) |
| invalid_fields | Indicates which request fields were invalid. | Variable |
| message | Reply 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).<br><br>Transaction identifier generated by the issuing bank, Visa Checkout, or Visa SRC. This field is used by the payer authentication validation service. | String (50) |
| payer_authentication_challenge_ type | The type of 3D Secure transaction flow that occurred. It can be one of the following:<br><br>• `CH`: Challenge<br>• `FR`: Frictionless<br>• `FD`: Frictionless with delegation (challenge not generated by the issuer but by the scheme on behalf of the issuer).<br><br>Used for Cartes Bancaires transactions. | String (2) |
| payer_authentication_eci | Electronic commerce indicator (ECI). This field is used<br><br>by payer authentication validation and enrollment services. Possible values for Visa, American Express, and JCB:<br><br>• `05`: Successful authentication.<br>• `06`: Authentication attempted.<br>• `07`: Failed authentication.<br>Possible values for Mastercard:<br>• `01`: Merchant is liable.<br>• `02`: Card issuer is liable | String (3) |
| payer_authentication_enroll_e_ commerce_indicator | Commerce indicator for cards not enrolled. This field contains one of these values:<br><br>• `internet`: Card not enrolled or card type not supported by payer authentication. No liability shift. | String (255 |

| Field | Description | Data Type & Length |
|---|---|---|
| | • `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. | |
| payer_authentication_enroll_veres_enrolled | Result of the enrollment check. This field can contain one of these values:<br><br>• `Y`: Card enrolled or can be enrolled; you must authenticate. Liability shift.<br><br>• `N`: Card not enrolled; proceed with authorization. Liability shift.<br><br>• `U`: Unable to authenticate regardless of the reason. No liability shift.<br><br>This field applies only to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request.<br><br>The following value can be returned if you are using rules-based payer authentication:<br><br>• `B`: Indicates that authentication was bypassed.<br><br>For rules-based payer authentication information see the [Payer Authentication Guide](#). | String (255) |
| payer_authentication_network_score | The global score calculated by the Cartes Bancaires scoring platform and returned to the merchant. | Integer (2) |
| payer_authentication_pares_status | Raw result of the authentication check. This field can contain one of these values:<br><br>• `A`: Proof of authentication attempt was generated.<br><br>• `N`: Customer failed or cancelled authentication. Transaction denied.<br><br>• `U`: Authentication not completed regardless of the reason.<br><br>• `Y`: Customer was successfully authenticated. | String (255) |
| payer_authentication_pares_status_reason | Provides additional information about the PARes status value. | Integer (2) |
| payer_authentication_pares_timestamp | Decrypted time stamp for the payer authentication result. Visa Checkout and Visa SRC generate this value. Format: Unix time, which is also called epoch time. | String |

| Field | Description | Data Type & Length |
|---|---|---|
| payer_authentication_proof_xml | XML element containing proof of enrollment checking.<br><br>For cards not issued in the U.S. or Canada, your bank can require this data as proof of enrollment validation for any payer authentication transaction that you re- present because of a chargeback.<br><br>For cards issued in the U.S. or Canada, Visa can require this data for specific merchant category codes.<br><br>This field is not returned for 3D Secure 2.0 transactions. | String (1024 |
| payer_authentication_ reason_code | Numeric value corresponding to the result of the payer authentication request.<br><br>See "Reason Codes". | String (5) |
| payer_authentication_ specification_version | This field contains the 3D 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<br><br>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<br><br>challenge the card holder. Possible Values:<br><br>• 01: Static<br><br>• 02: Dynamic<br><br>• 03: OOB (Out of Band) | Integer (2) |
| payer_authentication_uad | Mastercard Identity Check UCAF authentication data.<br><br>Returned only for Mastercard Identity Check transactions. | String (32 |
| payer_authentication_uci | Mastercard Identity Check UCAF collection indicator.<br><br>This field indicates whether authentication data is collected at your web site. Possible values:<br><br>• 0: Authentication data was not collected and customer authentication not completed.<br><br>• 1: Authentication data was not collected because customer authentication not completed.<br><br>• 2: Authentication data was collected. Customer completed authentication. | String (1) |
| payer_authentication_validate_ e_commerce_indicator | Indicator that distinguishes Internet transactions from other types. The authentication failed if this field is not returned.<br><br>The value of this field is passed automatically to the authorization service if you request the services together. This field contains one of these values: | String (255) |

| Field | Description | Data Type & Length |
|---|---|---|
| | • `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. | |
| 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. This field contains one of these values: <br> • `-1`: Invalid PARes. <br> • `0`: Successful validation. <br> • `1`: Cardholder is not participating, but the attempt to authenticate was recorded. <br> • `6`: Issuer unable to perform authentication. <br> • `9`: Cardholder did not complete authentication | String (255) |
| payer_authentication_veres_ timestamp | Decrypted time stamp for the verification response. Visa Checkout and Visa SRC generate this value. Format: Unix time, which is also called *epoch time*. | String |
| payer_authentication_white_list_ status | Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3D Secure requester. <br> Possible Values: <br> • `Y`: 3D Secure requester is whitelisted by cardholder <br> • `N`: 3D 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. <br> Possible Values: <br> • `01`: 3D Secure Server | Integer (2) |

| Field | Description | Data Type & Length |
|---|---|---|
| | • `02`: Directory server<br><br>• `03`: ACS | |
| 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_token | Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository.<br><br>This payment token supersedes the previous payment token and is returned if:<br><br>• The merchant is configured for a 16 digit payment token which displays the last four digits of the primary account number (PAN) and passes Luhn mod-10 check. See "Payment Tokens".<br><br>• 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.<br><br>You must be currently using Token Management Services. | String (26) |
| paypal_address_status | Status of the street address on file with PayPal.<br><br>Possible values:<br><br>• `None`<br><br>• `Confirmed`<br><br>• `Unconfirmed` | String (12) |
| paypal_authorization_correlation_id | PayPal identifier that is used to investigate any issues. | String (20) |
| paypal_authorization_transaction_id | Unique identifier for the transaction. | String (17) |
| paypal_customer_email | Email address of the customer as entered during checkout. PayPal uses this value to pre-fill the PayPal membership sign-up portion of the PayPal login page. | String (127) |
| paypal_do_capture_correlation_id | PayPal identifier that is used to investigate any issues. | String (20) |
| paypal_do_capture_transaction_id | Unique identifier for the transaction. | String (17) |

| Field | Description | Data Type & Length |
|---|---|---|
| paypal_ec_get_details_ correlation_ id | PayPal identifier that is used to investigate any issues. | String (20) |
| paypal_ec_get_details_ request_id | Value of the request ID returned from a PayPal get details service request. | String (26) |
| paypal_ec_get_details_ transaction_ id | Unique identifier for the transaction. | String (17) |
| paypal_ec_order_setup_ correlation_id | PayPal identifier that is used to investigate any issues. | String (20) |
| paypal_ec_order_setup_ transaction_id | Unique identifier for the transaction. | String (17) |
| paypal_ec_set_request_id | Value of the request ID returned from a PayPal set service request. | String (26) |
| paypal_fee_amount | PayPal fee charged for the transaction. This value does not exceed the equivalent of 10,000 USD in any currency and does not include a currency symbol. The decimal separator is a period (.), and the optional thousands separator is a comma (,). | String (9) |
| paypal_order_request_id | Value of the request ID returned from a PayPal order setup service request | String (9) |
| paypal_payer_id | Customer's PayPal account identification number. | Alphanumeric String (13) |
| paypal_payer_status | Customer's status. Possible values:<br><br>• `verified`<br><br>• `unverified` | String (10) |
| paypal_pending_reason | Indicates the reason that payment is pending. Possible values:<br><br>• `address`: Your customer did not include a confirmed shipping address, and your Payment Receiving preferences are set to manually accept or deny such payments. To change your preferences, go to the Preferences section of your PayPal profile.<br><br>• `authorization`: The payment has been authorized but not settled. Capture the authorized amount.<br><br>• `echeck`: Payment was made by an echeck that has not yet cleared.<br><br>• `intl`: You have a non-U.S. account and do not have a withdrawal mechanism. You must manually accept or deny this payment in your PayPal Account Overview.<br><br>• `multi-currency`: You do not have a balance in the currency sent, and your Payment Receiving preferences are not set to | String (14) |

| Field | Description | Data Type & Length |
|---|---|---|

automatically convert and accept this payment. You must manually accept or deny this payment in your PayPal Account Overview.

- none: No pending reason.

- order: The payment is part of an order that has been authorized but not settled.

- paymentreview: The payment is being reviewed by PayPal for possible fraud.

- unilateral: The payment was made to an email address that is not registered or confirmed.

- verify: Your account is not yet verified. You must verify your account before you can accept this payment.

| Field | Description | Data Type & Length |
|---|---|---|
| paypal_pending_status | Status of the transaction. Possible values: | String (20) |

- Canceled-Reversal: PayPal canceled the reversal, which happens when you win a dispute, and the funds for the reversal are returned to you.

- Completed: PayPal completed the payment and added the funds to your account.

- Denied: You denied a payment, which happens only if the payment was pending for the reason indicated in the reason_**code** field.

- Expired: The authorization expired.

- Failed: The payment failed. This event can happen only when the payment is made from your customer's bank account.

- In-Progress: The transaction is not complete yet.

- None: No status.

- Partially-Refunded: The payment was partially refunded.

- Pending: The payment is pending for the reason indicated in the **paypal_pending_reason** field.

- Processed: PayPal accepted the payment.

- ReasonCode

- Refunded: You refunded the payment.

- Reversed: PayPal reversed the payment for the reason specified in the **reason_code** field. The funds were transferred from your account to the customer's account.

- Voided: The authorization was voided

| Field | Description | Data Type & Length |
|---|---|---|
| paypal_protection_eligibility | Seller protection in force for the transaction. Possible | String (17) |

| Field | Description | Data Type & Length |
|---|---|---|
| | values: | |
| | • `Eligible`: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. | |
| | • `PartiallyEligible:` You are protected by the PayPal Seller Protection Policy for item not received. | |
| | • `Ineligible`: You are not protected under the PayPal Seller Protection Policy. | |
| paypal_protection_ eligibility_type | Seller protection in force for the transaction. Possible values: | String (32) |
| | • `Eligible`: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. | |
| | • `ItemNotReceivedEligible`: You are protected by the PayPal Seller Protection Policy for item not received. | |
| | • `UnauthorizedPaymentEligible`: You are protected by the PayPal Seller Protection Policy for unauthorized payment. | |
| | • `Ineligible`: You are not protected under the PayPal Seller Protection Policy. | |
| | To enable the **paypal_protection_eligibility_type** field, contact customer support to have your account configured for this feature. | |
| paypal_request_id | Identifier for the request generated by the client. | String (26) |
| paypal_token | Timestamped PayPal token which identifies that PayPal Express Checkout is processing the transaction. Save this value to send in future request messages. | String (20) |
| paypal_transaction_type | Indicates the PayPal transaction type. Possible value: `expresscheckout` | String (16) |
| reason_code | Numeric value corresponding to the result of the payment card transaction request. See "Reason Codes". | String (5) |
| req_access_key | Authenticates the merchant with the application. | String (32) |
| req_allow_payment_ token_update | Indicates whether the customer can update the billing, shipping, and payment information on the order review page. This field can contain one of the following values: • `true`: Customer can update details. • `false`: Customer cannot update details. | String (5) |
| req_amount | Total amount for the order. Must be greater than or equal to zero. | String (15) |

| Field | Description | Data Type & Length |
|---|---|---|
| req_auth_indicator | Flag that specifies the purpose of the authorization.<br><br>Possible values:<br><br>• `0`: Preauthorization<br><br>• `1`: Final authorization<br><br>Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization.<br><br>To set the default for this field, contact customer support. | String (1) |
| req_auth_type | Authorization type. Possible values:<br><br>• `AUTOCAPTURE`: Automatic capture.<br><br>• `STANDARDCAPTURE`: Standard capture.<br><br>• `verbal`: Forced capture.<br><br>**Forced Capture**<br><br>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.<br><br>**Verbal Authorization**<br><br>Set this field to verbal and include it in the capture request to indicate that the request is for a verbal authorization. | String (11) |
| req_bill_payment | Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values:<br><br>• `true`: Bill payment or loan payment.<br><br>• `false` (default): Not a bill payment or loan payment. | String (1) |
| req_bill_to_address_city | City in the billing address. | String (50) Visa Checkout and Visa SRC: String (100) |
| req_bill_to_address_country | Country code for the billing address. Use the two character ISO country codes.- | String (2) |
| req_bill_to_address_line1 | First line of the street address in the billing address. | String (60) Visa Checkout and Visa SRC: String (100) |
| req_bill_to_address_line2 | Second line of the street address in the billing address. | String (60)<br><br>Visa Checkout and Visa SRC: String (100) |

| Field | Description | Data Type & Length |
|---|---|---|
| req_bill_to_address_postal_ code | Postal code for the billing address. | String (10) |
| | This field is returned if **bill_to_address_country** is U.S. or Canada. | Visa Checkout and Visa SRC: String (100) |
| req_bill_to_address_state | State or province in the billing address. The two- character ISO state and province code. | String (2) |
| | This field is returned for U.S and Canada. | |
| req_bill_to_company_name | Name of the customer's company. | String (40) |
| req_bill_to_email | Customer email address. | String (255) |
| | | Visa Checkout and Visa SRC: String (256) |
| req_bill_to_forename | Customer first name. | String (60) |
| | | Visa Checkout and Visa SRC: String (256) |
| req_bill_to_phone | Customer phone number. | String (15) |
| | | Visa Checkout and Visa SRC: String (30) |
| req_bill_to_surname | Customer last name. | String (60) |
| | | Visa Checkout and Visa SRC: String (265) |
| 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) |
| req_complete_route | Concatenation of individual travel legs in the format: | String (255) |
| | 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. | |

| Field | Description | Data Type & Length |
|---|---|---|
| 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. This field can contain one of the following values:<br><br>• true: Customer browser accepts cookies.<br><br>• false: Customer browser does not accept cookies. | String (5) |
| req_customer_gift_wrap | Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values:<br><br>• true: Customer requested gift wrapping.<br><br>• false: Customer did not request gift wrapping. | String (5) |
| req_customer_ip_address | Customer's IP address reported by your web server using socket information. | |
| req_date_of_birth | Date of birth of the customer.<br>Format: YYYYMMDD. | String (8) |
| req_departure_time | Departure date and time of the first leg of the trip. Use one of the following formats:<br><br>• yyyy-MM-dd HH:mm z<br><br>• yyyy-MM-dd hh:mm a z<br><br>• yyyy-MM-dd hh:mma z<br><br>• HH = 24-hour format<br><br>• hh = 12-hour format<br><br>• a = am or pm (case insensitive)<br><br>• 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 (_).<br><br>However, do not use the same uppercase and lowercase letters to indicate different sessions IDs.<br><br>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_driver_license_number | Driver's license number of the customer. The last four digits are not masked. | String (30) |

| Field | Description | Data Type & Length |
|---|---|---|
| req_driver_license_state | State or province from which the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada*. | String (2) |
| req_ignore_avs | Ignore the results of AVS verification. Possible values:<br><br>• `true`<br><br>• `false` | String (5) |
| req_ignore_cvn | Ignore the results of CVN verification. Possible values:<br><br>• `true`<br><br>• `false` | String (5) |
| req_item_#_code | Type of product. # can range `from` 0 to 199. | String (255) |
| 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 0 to 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. You can use one of the following values:<br><br>• `ADT`: Adult<br><br>• `CNN`: Child<br><br>• `INF`: Infant | String (32) |

| Field | Description | Data Type & Length |
|---|---|---|
| | • YTH: Youth | |
| | • STU: Student | |
| | • SCR: Senior Citizen | |
| | • MIL: Military | |
| req_item_#_quantity | Quantity of line items. # can range from 0 to 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 0 to 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 0 to 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. A maximum of 30 legs can be included in the request.<br><br>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.<br><br>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. | String (3) |
| req_journey_leg#_orig | Airport code for the origin of the leg of the trip,<br><br>designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request.<br><br>This code is usually three digits long; for example: SFO<br><br>= San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory.<br><br>In your request, send 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. | 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.<br><br>Merchant-defined data fields 1 to 4 are stored against 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 stored against the payment token.<br><br>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,<br><br>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.<br><br>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. | String (100) |
| 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) |

| Field | Description | Data Type & Length |
|---|---|---|
| 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) |
| req_payment_method | Method of payment. Possible values:<br><br>• card<br><br>• paypal<br><br>• visacheckout | 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.<br><br>You must be currently using Token Management Services. Populate this field with the customer token ID | String (26) |
| req_payment_token_comments | Optional comments about the customer token | String (255) |
| req_payment_token_title | Name of the customer token. | String (60) |
| 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.<br>Format: YYYYMMDD | Date (b) String (8) |
| req_recipient_postal_code | Partial postal code for the recipient's address.<br><br>For example, if the postal code is NN5 7SG, the value for this field | Alphanumeric String (6) |

| Field | Description | Data Type & Length |
|---|---|---|
| | should be the first part of the postal code: NN5 | |
| 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. This field can contain one of the following values:<br><br>• `true`<br><br>• `false` | String (5) |
| req_ship_to_address_city | City of shipping address. | String (50) Visa Checkout and Visa SRC: String (100) |
| req_ship_to_address_country | The two-character country code. | String (2) |
| req_ship_to_address_line1 | First line of shipping address. | String (60) Visa Checkout and Visa SRC: String (100) |
| req_ship_to_ address_line2 | Second line of shipping address. | String (60) Visa Checkout and Visa SRC: String (100) |
| req_ship_to_address_ postal_code | Postal code for the shipping address. | String (10) Visa Checkout and Visa SRC: String (100) |
| 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) Visa Checkout and Visa SRC: String (256) |
| req_ship_to_phone | Phone number for the shipping address. | String (15) Visa Checkout and Visa SRC: String (30) |
| req_ship_to_surname | Last name of person receiving the product. | String (60) Visa Checkout and Visa SRC: String (256) |
| req_shipping_method | Shipping method for the product. Possible values:<br><br>• `sameday`: Courier or same-day service<br><br>• `oneday`: Next day or overnight service | String (10) |

| Field | Description | Data Type & Length |
|---|---|---|
| | • twoday: Two-day service | |
| | • threeday: Three-day service | |
| | • lowcost: Lowest-cost service | |
| | • pickup: Store pick-up | |
| | • other: Other shipping method | |
| | • none: No shipping method | |
| req_skip_decision_manager | Indicates whether to skip Fraud Management. Please refer to the Guides section under Fraud Management This field can contain one of the following values: <br><br> • true <br><br> • false | String (5) |
| 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_ke**y field for each transaction. | String (50) Visa Checkout and Visa SRC: String (100) |
| request_token | Request token data created for each reply. 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. | |
| 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 |

| Field | Description | Data Type & Length |
|---|---|---|
| transaction_id | The transaction identifier returned from the payment gateway. | String (26) |
| utf8 | Indicates whether the unicode characters are encoded.<br><br>Possible value: ✓ | String (3) |
| vc_avs_code_raw | Decrypted raw (unmapped) AVS code provided by Visa Checkout and Visa SRC. | String (10) |
| vc_risk_score | Decrypted risk score used with your fraud model. See "Configuring Visa Checkout or Visa SRC". | Positive Integer (2) |
| vc_wallet_reference_id | Decrypted order identifier generated by Visa Checkout and Visa SRC. | String (100) |

## 27.4 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," page 26.

**Reason Codes**

| Reason Code | Description |
|---|---|
| 100 | Successful transaction. |
| 102 | One or more fields in the request contain invalid data.<br><br>Possible action: see the reply 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<br><br>Possible action: resend the request with unique **access_key** and **transaction_ uuid** fields.<br><br>A duplicate transaction was detected. The transaction might have already been processed.<br><br>Possible action: before resubmitting the transaction, use the single transaction query or search for the transaction using the Merchant Portal (see "Viewing Transactions Business Advantage 360) to confirm that the transaction has not yet been processed. |
| 110 | Only a partial amount was approved. |

| Reason Code | Description |
| --- | --- |
| 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 the Merchant Portal 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 the Merchant Portal or programmatically through the single transaction query. |
| 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 the Merchant Portal 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 |

| Reason Code | Description |
| --- | --- |
| | have reviewed the transaction status either directly in the Merchant Portal or programmatically through the single transaction query. |
| 208 | Inactive card or card not authorized for card-not-present transactions.<br><br>Possible action: request a different card or other form of payment. |
| 210 | The card has reached the credit limit.<br><br>Possible action: request a different card or other form of payment. |
| 211 | Invalid CVN.<br><br>Possible action: request a different card or other form of payment. |
| 221 | The customer matched an entry on the processor's negative file.<br><br>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.<br><br>Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud. |
| 231 | Invalid account number.<br><br>Possible action: request a different card or other form of payment. |
| 232 | The card type is not accepted by the payment processor.<br><br>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.<br><br>Possible action: request a different card or other form of payment. |
| 234 | There is a problem with the information in your account.<br><br>Possible action: do not resend the request. Contact customer support to correct the information in your account. |
| 236 | Processor failure.<br><br>Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Merchant Portal or programmatically through the single transaction query |
| 240 | The card type sent is invalid or does not correlate with the payment card number. |

| Reason Code | Description |
|---|---|
| | Possible action: confirm that the card type correlates with the payment card number specified in the request; then resend the request. |
| 475 | The cardholder is enrolled for payer authentication. |
| | Possible action: authenticate cardholder before proceeding. |
| 476 | Payer authentication could not be authenticated. |
| 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 legacy Smart Authorization settings. |
| | Possible action: review the authorization request. |

## 27.5 Types of Notifications

| Decision | Description | Type of Notification | Hosted Page |
|---|---|---|---|
| ACCEPT | Successful transaction. Reason codes 100 and 110. | • Custom receipt page<br>• Customer receipt email<br>• Merchant POST URL<br>• Merchant receipt email | Accept |
| REVIEW | Authorization was declined; however, a capture might still be possible. Review payment details.<br><br>See reason codes 200, 201, 230, and 520. | • Custom receipt page<br>• Customer receipt email<br>• Merchant POST URL<br>• Merchant receipt email | Accept |
| DECLINE | Transaction was declined.<br><br>See reason codes 102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, 476, and 481. | • Custom receipt page[1]<br>• Merchant POST URL[1]<br>• Merchant receipt email[1] | Decline |
| ERROR | Access denied, page not found, or internal server error.<br><br>See reason codes 102, 104, 150, 151 and 152 | • Custom receipt page<br>• Merchant POST URL | Error |
| CANCEL | • The customer did not accept the service fee conditions.<br>• The customer cancelled the transaction. | • Custom receipt page<br>• Merchant POST URL | Cancel |

[1] 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 3D Secure credentials incorrectly.

## 27.6 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 data, 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** reply field (see "Reply Fields").

⚠️ When you populate billing street address 1 and billing street address 2, Visa Platform Connect concatenates the two values. If the concatenated value exceeds 40 characters, Visa Platform Connect 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.

### 27.6.1 International AVS Codes

These codes are returned only for Visa cards issued outside the U.S.

| Code | Response | Description |
| --- | --- | --- |
| 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. |
| I | No match | Address not verified. |
| P | Partial match | Postal code matches, but street address not verified. |

## 27.6.2 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. |
| 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. |

| Code | Response | Description |
| --- | --- | --- |
| N | No match | One of the following:<br>• Street address and postal code do not match.<br>• Card member's name, street address, and postal code do not |
| 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. |
| Q | Match | Card member's name, billing address, and postal code match.<br>Shipping information verified but chargeback protection not guaranteed (Standard program). Returned only if you are signed 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:<br>• The U.S. bank does not support non-U.S. AVS.<br>• 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. |

| Code | Response | Description |
|------|----------|-------------|
| Y | Match | Street address and five-digit postal code match. |
| Z | Partial match | Street address does not match, but five-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. |

## 27.7 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. |

# 28 Appendix B: American Express SafeKey Response Codes

The American Express SafeKey response code is returned in **auth_cavv_result** in the reply 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 3D Secure data was not used. |
| 99 | An unknown value was returned from the processor |

# 29 Appendix C: Iframe Implementation

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

⚠ For the payer authentication 3D 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.

You must select the single page checkout option for the Hosted Payments Page iframe implementation (see "Checkout Configuration").

The total amount value and the transaction cancel button are not displayed within the iframe. Any settings that you configured for the total amount figure are ignored (see "Custom Checkout Appearance").

Bank of America recommends that you manage the total amount value on your web site containing the inline frame. You must also provide customers a cancel order functionality on your web site containing the inline frame.

## 29.1 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 web site 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.

🗏 Do not use double framing on the same page where the Hosted Payments Page iframe implementation is used.

You are required to implement the recommended prevention techniques in your web site. See the OWASP clickjacking 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.

## 29.2 Endpoints

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

# 30 Appendix D: Visa Secure Response Codes

The Visa Secure response code is returned in **auth_cavv_result** in the reply message for an authorization request.Response Code

| 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 3D Secure data was not used. |
| 99 | An unknown value was returned from the processor. |