Bank of America Gateway

Integration Guide

Date	09/14/2023
Version	2.1.0

BANK OF AMERICA

Table of Contents

BANK OF AMERICA

1 Overview

1.1 Purpose

This document provides guidelines for integrating with the Bank of America (BAC) Merchant Services platform; it supports the following:

- Demonstration and Certification Environment (DCE)
- Card Not Present processing

1.2 Scope

This guide covers the following:

- Integration Types
- Development and Certification Requirements
- Definitions, Best Practices, and Features
- Supported Transactions
- Receipt Requirements
- DCE Self-Test Validation

Supporting documents, specifications, APIs and SDKs card not present integrations are available on the Developer Portal

1.3 Definitions

The following terms are used in this document:

Term	Definition
Integrator	The merchant that is integrating its shopping cart solution into the Bank of America Gateway
Solution	Integrator's custom shopping cart
Bank of America Gateway	Bank of America's Gateway for Card Not Present processing, fraud management and payment security

2 Integration Types

2.1 Card Not Present

Bank of America offers 4 types of Card Not Present integrations through the Bank of America Gateway. They are all supported by:

- Robust and intuitive APIs for all payment types and solutions
- Client libraries for the leading developer platforms
- SDKs in six of the most popular coding languages (PHP, C#, Java, Ruby, Python, Node)
- Comprehensive sandbox testing
- Sample code for hundreds of payment use cases

Please refer to section 4.1 for Card Not Present PCI requirements.

3 Integrations Methods

All new integrations should adopt the CNP Integration Tool kit (also known as the Direct REST API) for follow-on transactions; it provides functionalities for processing payment (sale), authorization, capture, reversal, refund, void, token management etc.

The bank still supports the existing SOAP API, SOAP Toolkit and SCMP implementations, but will not be adding new functionalities or features to these 3 integration methods.

4 Sending Transaction Request

All requests to the Bank of America Gateway must be authenticated. In addition to the appropriate end point for the request type being sent, you will need three pieces of credentials from your Merchant Services account in Business Advantage 360 (BA360). These credentials are sent in the transaction request header message.

- Merchant ID (MID)
- Terminal ID (TID)
- Authentication key

5 Authentication methods

The following authentication methods are supported:

- HTTP Signature – Shared Secret Key
- JSON Web Token – P12 Certificate key

5.1 HTTP Signature – Shared Secret Key Authentication

The HTTP signature authentication is provided by a base-64 encoded transaction key, represented in a string format. The shared secret key is created at a merchant account level; it is used to authenticate the transaction source belonging to the Bank of America Gateway Merchant ID (MID) that generated the key; the key is valid for 3 years. The merchant will generate the shared secret key via BA360.

Note: Once a key is generated, it is the merchant's responsibility to include the key in all transaction header messages.

5.2 JSON Web Token Authentication

A JSON Web Token (JWT) is a standardized/encrypted container format that is used to securely transfer information between two parties. The Certificate authentication uses a PKCS 12 key file with the .p12 extension to digitally sign the API request message before transmitting it to Bank of America Gateway. Click here for more information about JSON Web Token (JWT) authentication.

Note: Once a key is generated, it is the merchant's responsibility to include the key in all transaction header messages.

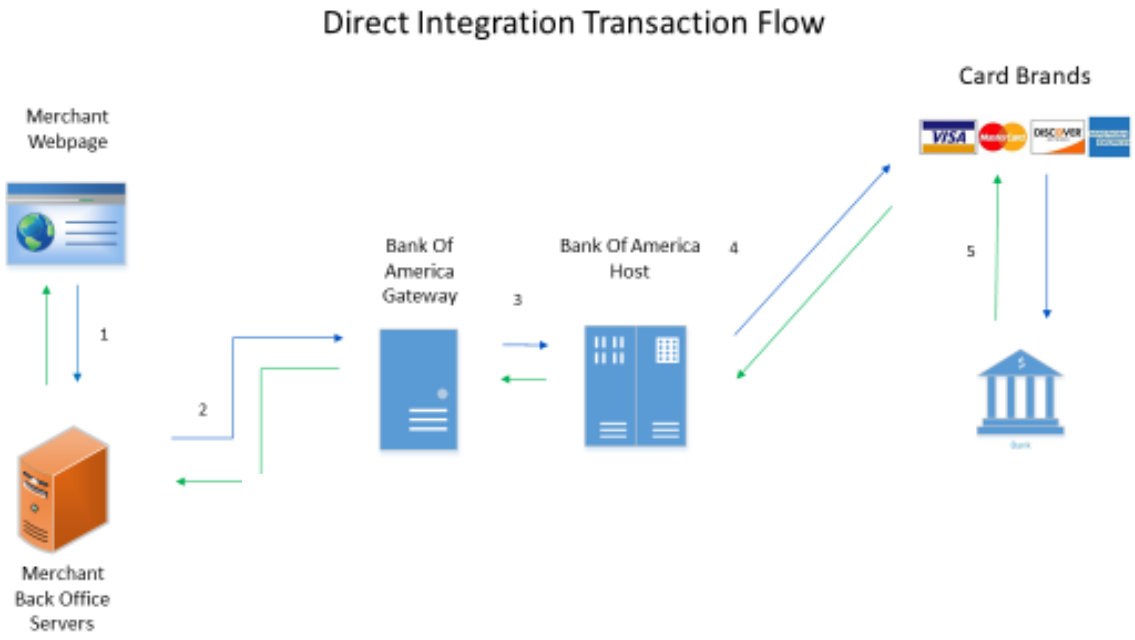
6 Integration Types

6.1 Direct Integration to the Bank of America Gateway – CNP Integration Toolkit

A *CNP Integration Toolkit* – integration is ideal for an Integrator that wants to control the entire customer checkout experience, including the payment form, response pages, and receipt.

In this integration type, the card data flow is as follows:

1. Cardholder enters card data into the merchant's website.
2. Back-office servers capture the complete card data and submit the transaction to the Bank of America Gateway
3. Bank of America Gateway submits the transaction to Bank of America Host for processing.
4. Bank of America Host submits the transactions to Card Brands for processing.
5. Approval and or decline is provided back in the response. (Bank of America provides a PAN token in every Authorization Response)



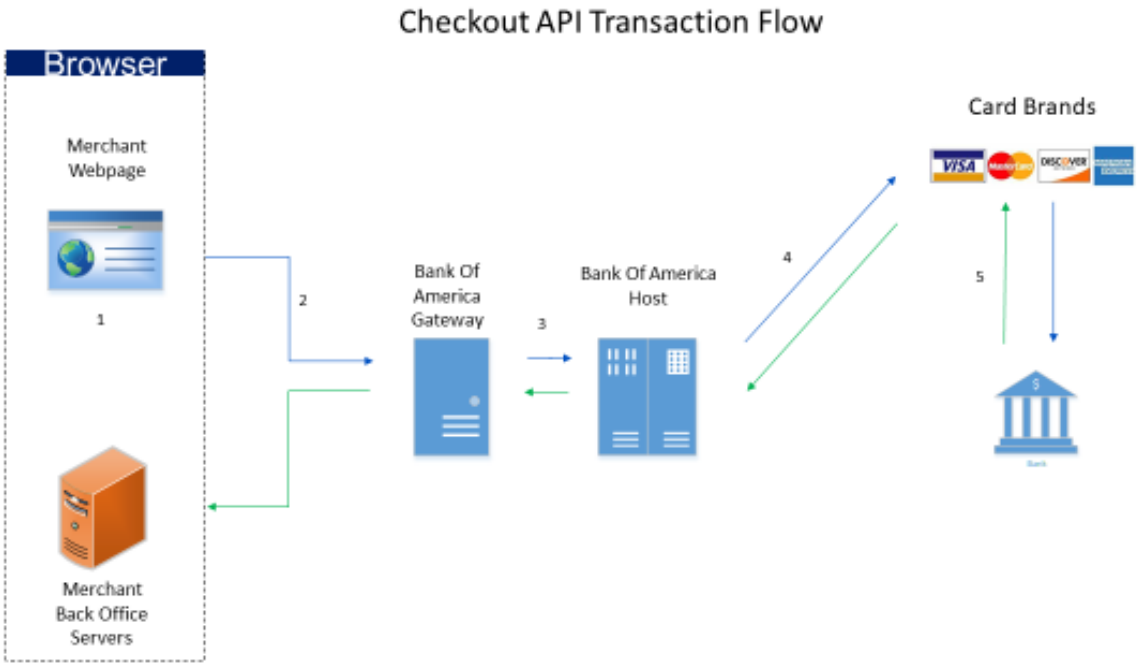
Click here for more information on REST API

6.2 Checkout API

With the Checkout API, the Integrator submits the card data directly from the customer's web browser to the Bank of America Gateway. The Integrator controls the receipt.

In this integration type, the card data flow is as follows:

1. The Cardholder enters card data into the cardholder's browser; the payment page is rendered by the Merchant.
2. The transaction is submitted directly from the cardholder's browser to the Bank of America Gateway for processing.
3. Bank of America Gateway submits the transaction to Bank of America Host for processing.
4. Bank of America Host submits the transaction to the Card Brands for processing.
5. Approval and or decline is provided back in the response. (Bank of America provides a PAN token in every Authorization Response)



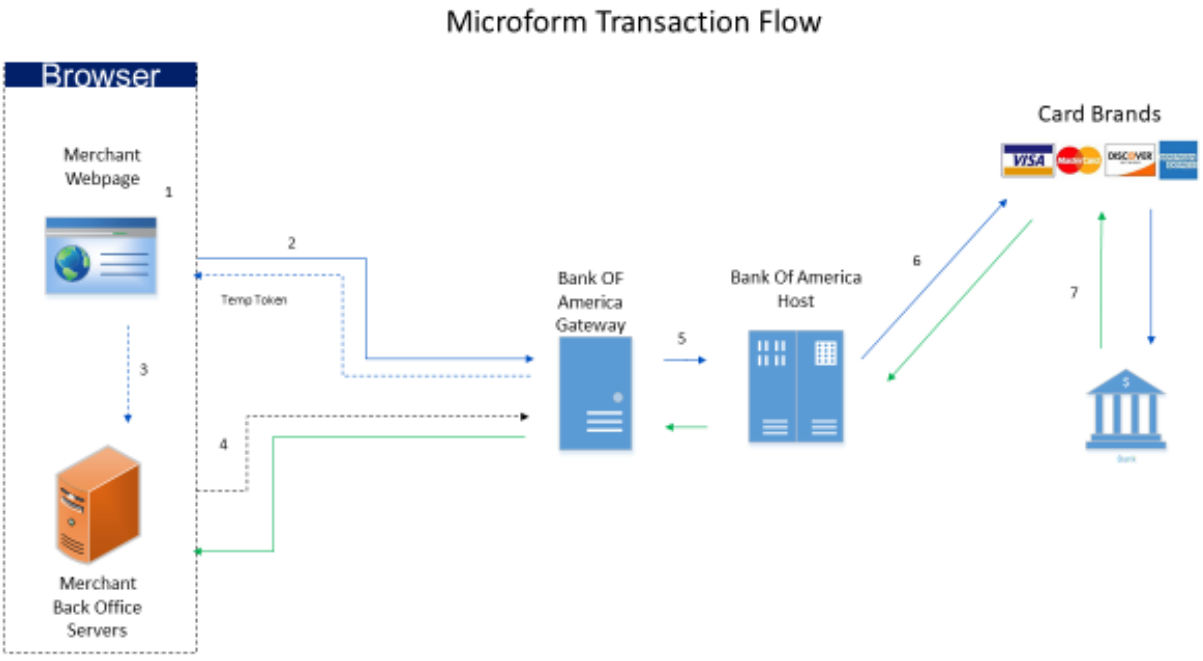
Click here for more information on Secure Acceptance Checkout API:

6.3 Microform Integration

The *Microform Integration* provides the most secure method for tokenizing card data that Bank of America offers. The Bank of America Gateway renders a secure iFrame to collect the customer's card data. The Bank of America Gateway hosts the iFrame and transmits the card data via the secure *Single Use Token API*. This integration type reduces the risk of a man-in-the-middle attack compromising the HTTPS connection. In regard to Payment Card Industry (PCI) scope, a solution using *Microform Integration* will likely qualify for Self-Assessment Questionnaire (SAQ) A.

In this integration type, the card data flow is as follows:

1. Cardholder enters card data into the cardholder's browser.
   - The payment page is rendered by the Merchant.
   - The PAN Data Field and CVV on the payment page is replaced with a secure iframe hosted by the Bank of America gateway.
2. An asynchronous request is made to the Bank of America Gateway which will return a temporary token to the merchant back-office server.
3. The merchant back-office server will then initiate a REST API call using the temporary token to initiate a payment.
4. Bank of America gateway submits the transaction to Bank of America Host for processing.
5. Bank of America Host submits the transactions to Card Brands for processing.
6. Approval and or decline is provided back in the response. (Bank of America provides a PAN token in every Authorization Response)



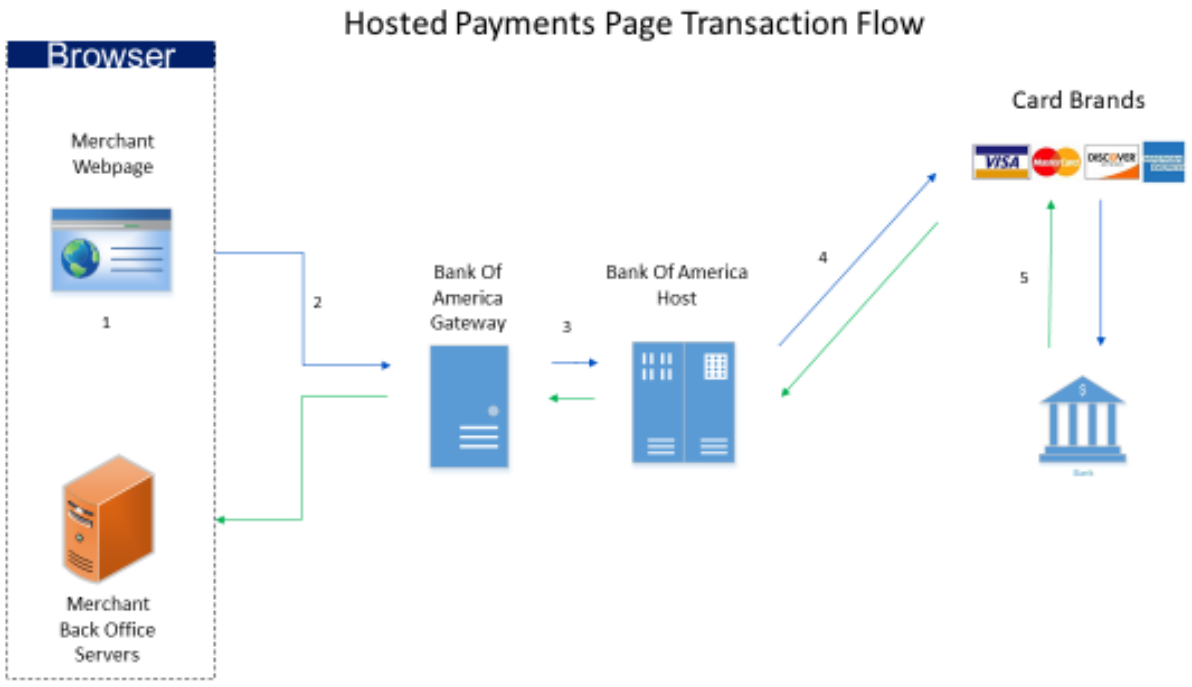
Click here for more information on the Flex Microform Integration:

6.4 Hosted Payment Page

With a *Hosted Payment Page* (HPP) integration, the Bank of America Gateway hosts and renders the solution's entire payment details page. The Bank of America Gateway will control the user experience of the payment details page. The solution is responsible for displaying the receipt page.

In this integration type, the card data flow is as follows:

1. While on the merchant's website, customer enters card data into *Hosted Payment Page*.
2. *Hosted Payment Page* captures and submits card data directly to the Bank of America Gateway.
3. Bank of America Gateway responds to the merchant back-office servers with payment results and Merchant/PAN Token generated by the bank.



Click here for more information on Hosted Payment Page

7 Definitions, Best Practices, and Features

7.1 Batch-less Environment

Bank of America host operates in a batch-less environment. The Bank processes and clears all transactions in a host capture mode environment but does not maintain any transaction specific information on the host. All transaction types but AUTH are processed and sent out for settlement every hour at the half hour.

Sale (Payment + Capture) transactions are cleared and sent out for settlement every hour at the half hour. A sale transaction is a bundle of an authorization and capture. Typical business situations where sale transactions can be used include:

- When there is no delay between taking a customer's order and shipping the goods
- To process a Sale transaction, send a "Payment" request with a capture flag under "Processinginformation" object set to "true". The sale message causes the cardholder account to be debited immediately.

Authorization (Payment) transactions pre-authorized the purchase, allowing flexibility to change the final transaction amount when closing the transaction by sending a Capture request. This is a two-step process to allow a merchant to capture an authorization when there is a delay in shipping the goods.

- First, "**Payment**" message type is sent to authorize the transaction
- Then, "**Capture**" message type is sent with the final transaction amount

7.2 Transaction ID

It is a unique identifier generated by the merchant shopping cart for each transaction and should be sent in all transaction requests to the Bank of America Gateway.
The transaction ID is required for a timeout or a merchant-initiated reversal, void, and duplicate checking requests.

7.3 Code

It is a unique identifier generated by the merchant shopping cart for each transaction if supporting a duplicate checking using this field; It is also referred to as order reference number or tracking number.

7.4 Payment ID or "ID"

It is a unique transaction reference number returned by the Bank of America Gateway for every approved transaction. The Payment ID or "ID" must be included in any subsequent transaction such as capture, void, reversal, refund (linked to a previous transaction).

7.5 Reconciliation ID /Retrieval Reference Number (RRN)

This is a unique reference number returned on all approved transactions by the Bank of America Gateway. This number must be printed on the receipt.

7.6 Tokenization

7.6.1 Merchant Token Hierarchy

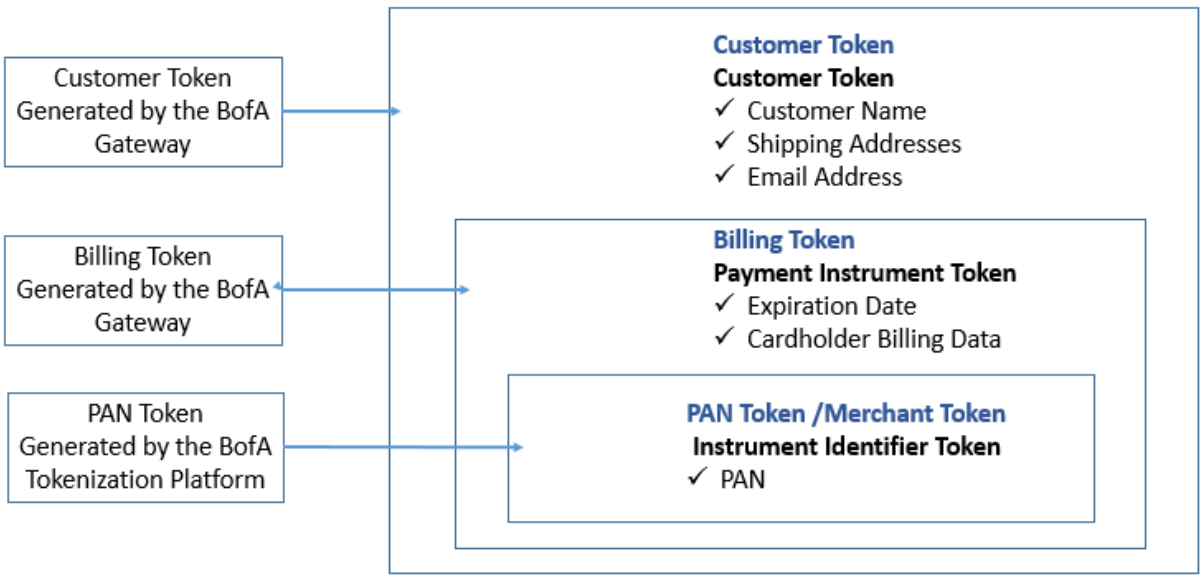
Tokenization is the process of replacing sensitive payment and customer data, such as Personal Account Number (PAN), with a non-sensitive and unique identifier called a *token*.

See below for the types of tokens involved in the Bank of America Gateway:

1. **Merchant/PAN Token** - Referenced in the Bank of America Gateway documentation as an *instrument identifier token*. It consists of the Payment Account Number (PAN) being replaced with a series of randomly generated numbers. The Bank of America Gateway tokenization generates this token and it's returned in the transaction response. The token is format preserving, passes Luhn check, and displays the trailing 4 digits of the card.
2. **Billing Token** - Referenced in Bank of America Gateway documentation as a *payment instrument token*, it includes: PAN token, expiration date, card type, and cardholder billing data. It is generated by the Bank of America Gateway.
3. **Customer Token** – Referenced in Bank of America Gateway documentation as a *customer token*. It includes: PAN token, cardholder name, date of birth, phone number, shipping address, loyalty number, and *payment account reference number*. The *payment account reference number* links the cardholder account to all transactions for the account. It is generated by the Bank of America Gateway.

The merchant can store these tokens (if applicable) and use them to refund or void a previous transaction and to perform a new transaction.

See Appendix A for more information about billing and customer tokens



7.6.2 Unsupported Features

Bank of America currently **does not** support the following:

1. Tokens for closed-loop gift card numbers (i.e., ValueLink)
2. Tokens for Alternative Payment Method (APM) usernames
3. Account Updater
4. Network Tokens (e.g., Visa, MasterCard, etc.)

For more information on how to code and implement tokens in your payment application using the CNP Integration Toolkit, see *Bank of America Gateway Developer Center* > *TMS RESTful services*.

8 Supported Transactions and Industry Types

The following section details the transaction and industry types that Bank of America Gateway currently supports.

8.1 Supported Transaction Types

8.1.1 Payment

A Payment – (Authorization) transaction puts a temporary hold on the customer's credit card. The Bank of America Gateway **will not** submit an approved authorization for settlement until it receives a corresponding capture transaction. Once the Bank of America Gateway receives the capture transaction, it submits the transaction for settlement at the next batch interval.

8.1.2 Incremental Authorization – For future use

Incremental authorization can be used to request additional amount if the original authorized amount is insufficient; it gives merchants the flexibility to increase the authorized amount as additional charges accrue. Multiple incremental authorizations can be requested as long as the capture is not submitted.

8.1.3 Capture

A capture transaction signals to the Bank of America Gateway to send a previously authorized transaction (payment) for settlement; the capture amount may be different from the authorized amount. Bank of America requires a capture for each authorization (payment) transaction prior to sending the transaction to the card networks for settlement. Only after Bank of America receives the capture request, does Bank of America consider the transaction complete.

Note: The card networks/issuers may limit the time during which an authorized transaction can be captured. This time limit depends on the industry type, the card network or the card type.

8.1.4 Void

A void transaction prevents the Bank of America Gateway from submitting a previous sale (payment + capture), capture, refund, or credit transaction for settlement. A void transaction will only be successful if received before the next batch interval time. Due to the Bank of America Gateway host capture environment, it is recommended to process void transactions as follow:

- Void request can be submitted to cancel previous Sale, Capture, Refund, or Credit transactions if the original transaction hasn't already been submitted for settlement yet by the Bank of America Gateway. If the original transaction is already settled, an error message will be returned with a reason code "NOT_VOIDABLE". In this case a refund request should be submitted.

8.1.5 Refund

A refund is a follow-on transaction that uses the ID returned from either a payment or capture request. The money is debited from the merchant's account and returns to the customer's card.

8.1.6 Credit

A credit is a stand-alone transaction that is not linked to any previous transactions. It takes money from the merchant's account and returns it to the customer's card

8.1.7 Authorization Reversal

An authorization reversal releases the hold the Payment placed on the cardholder's fund; it must be submitted prior to initiating a capture. Once a capture has been submitted the transaction must be voided if it needs to be cancelled.

The Authorization Reversal also complies with the Visa requirements to settle authorized transactions. Visa will assess a fee for all transactions that are authorized, but not settled. (Visa misuse of authorization fee, aka "ghost authorization" of $.09 per item).

8.1.8 Duplicate Transaction Checking

Duplicate transaction checking helps prevent the same transaction being processed more than once. There are two approaches of processing duplicate transaction checking for a direct integration to the Bank of America Gateway: using the "TransactionID" and "Code" fields.

8.1.8.1 Duplicate Transaction Checking using TransactionID

In order to use the "TransactionID" field for duplicate checking, the "TransactionID" value needs to be unique for 60 days. In the event of communication issues, the payment application re-submits the transaction with the original "TransactionID". If the original transaction was successfully processed, the Bank of America Gateway returns an error response code, any subsequent transaction with the same "TransactionID" will be rejected by the Bank of America Gateway for 60 days.

The following response is received by the API request with a duplicate TransactionID:


```
{
    "submitTimeUtc": "2020-05-26T20:34:22Z",
    "status": "INVALID_REQUEST",
    "reason": "INVALID_DATA",
    "message": "Declined - One or more fields in the request conta
ins invalid data"
}
```

8.1.8.2 *Duplicate Transaction Checking using Code*

"Code" is also referred to as the "Merchant Reference Number". This is often the merchants order number. For this to be included in duplicate checking requires a merchant configuration. Merchants can be configured to allow or not allow duplicate "code" or merchant reference number. If the merchant is configured to not allow duplicates, the field is required to be unique for only 15 minutes. The default configuration for the Bank of America Gateway is to not allow duplicates for this field.

Duplicate checking using "Code" provides more leeway, successfully authorized transactions will prevent duplicate transactions using the "code" field; if a transaction is declined or rejected, the merchant can resend a transaction with the same "Code", and it will not be considered a duplicate. Since this field is often the merchants order number which may not change, it allows for the consumer to use another card if necessary for the same order.

If the merchant configuration does not allow duplicate merchant reference numbers, and a transaction is successfully authorized, any subsequent transaction with same "code" will be rejected by Bank of America Gateway for 15 minutes.

The following response is received to the API request with a duplicate "code":


```
{
    "submitTimeUtc": "2020-05-26T20:32:44Z",
    "status": "INVALID_REQUEST",
    "reason": "DUPLICATE_REQUEST",
    "message": "Declined - The merchantReferenceCode sent with thi
               s authorization request matches the merchantReferen
               ceCode of another authorization request that you se
               nt in the last 15 minutes."
}
```


8.1.9 Timeout Reversal or Merchant Initiated Reversal

In the event a "Payment" (Authorization) request is sent to the Bank of America Gateway and no response is received by the terminal or the network connection is lost before the specified timeout setting, the Gateway should initiate a Timeout Reversal or Merchant Initiated Reversal using the **Transaction ID** sent in the original payment request.

The Timeout Reversal or the Merchant Initiated Reversal request should be sent immediately.

The Timeout Reversal or the Merchant Initiated Reversal enables the cancelation of the original "Payment" (authorization) transaction in case it was approved by the host, but the gateway did not get the response.

Bank of America recommends setting the timeout value **to 23 seconds** for gateway connected directly to the Bank of America Gateway

8.1.10 Timeout Void or Merchant Initiated Void

Timeout Void or Merchant Initiated Void is used to cancel the following transaction types in case no response is received from the Bank of America Gateway.

- Sale (Payment + Capture)
- Capture
- Refund
- Credit

Similar to Timeout Reversal, Bank of America recommends setting the timeout value to 23 seconds for IP gateway connected directly to the Bank of America Gateway.

8.1.11 Timeout Reversal and Timeout Void use cases

Below are Timeout Reversal and Timeout Void use cases and the response returned by the Bank of America Gateway (Bank of America Gateway) when a Timeout Reversal or Timeout Void request is sent; the integrator uses the error reason and the associated message to determine the next action.

Use Case	Scenario	Transaction Response	Action
Bank of America Gateway approved the transaction	- Merchant sends a transaction - Bank of America Gateway approved the transaction - Merchant did not get the response - Merchant sends a reversal request - Reversal is processed successfully	Status: “REVERSED", Reason: N/A", Message: “Successful transaction.	N/A
- Bank of America Gateway did not receive the original transaction	- Merchant sends a transaction - Bank of America Gateway did not receive the original transaction - Merchant did not get a response - Merchant sends a reversal - Bank of America Gateway responds with error message	Status:"INVALID_REQUEST" Reason:"INVALID_DATA", Message:"One or more fields in the request contains invalid data	- See the reply fields status Information.details for which fields are invalid - Resend the request with the correct information
- Bank of America Gateway declined the transaction	- Merchant sends a transaction - Bank of America Gateway declined the transaction - Merchant did not get the response - Merchant sends a reversal request	Status: "INVALID_REQUEST", Reason:"MISSING_AUTH", Message: "You requested a capture, but there is no corresponding, unused authorization record. Occurs if there was not a previously successful authorization request or if the previously successful authorization has already been used in another capture request.”	Request a new authorization
- Bank of America Gateway already sent	- Merchant sends a transaction - Bank of America Gateway approved the transaction and sent it out for settlement	Status: "INVALID_REQUEST", Reason: "NOT_VOIDABLE", Message: "The capture or credit is not voidable because the capture or credit	Proceed with a refund

Use Case	Scenario	Transaction Response	Action
the transaction for settlement	- Merchant send a reversal request late	information has already been submitted for settlement. Or you requested a void for a type of transaction that cannot be voided.”	

8.2 Transaction Matrix

Transaction Type	Definition	Card Not Present	Credit	Debit
Payment	**Authorization**	Yes	Yes	No
	Incremental Authorization (future use)	Yes	Yes	No
	Sale (Authorization + Capture) • *Processinginformation.capture=true*	Yes	Yes	Yes
Capture	**Capture (**Completion for authorized transaction) • *Must include the Payment ID from the authorization request*	Yes	Yes	No
Refund	**Refund** (**Linked to a previous transaction**) for a pair of authorization/capture or sale transaction • *Must include the Payment ID from the previous transaction* • Must include PIN Block for Debit Transactions	Yes	Yes	Yes
	Credit (Standalone) – Refund a standalone authorization/capture or a sale transaction • Must include PIN Block for Debit transactions	Yes	Yes	Yes
Void	**Void a Payment–** Void of previously Sale (Authorization + Capture), transaction • Must include the Payment ID • Void will not be successful if the Capture is already submitted for settlement by the Bank of America Gateway • If the settlement is already processed, a Refund must be submitted instead	Yes	Yes	Yes
	Void Refund – Void of a Refund for a pair of Authorize/Capture or Sale linked to a previous transaction • Must include the Refund ID	Yes	Yes	Yes
	Void a Credit – Void of a standalone Refund transaction	Yes	Yes	Yes
Reversal	**Reversal –** Releases the hold placed on the customer's fund by the authorization request (Payment) • Must include the Payment ID	Yes	Yes	Yes
Timeout Void	**Timeout Void or Merchant Initiated Void:** Void the following transactions in case no response is received from the Bank of America Gateway due to communication issue Payment (Authorization + Capture) Refund Credit	Yes	Yes	Yes

Transaction Type	Definition	Card Not Present	Credit	Debit
	• **Must Include "TransactionID"**			
Timeout Reversal	**Timeout Reversal Merchant Initiated Reversal** This to reverse a previous payment (authorization) that merchant does not receive a reply due to timeout • **Must include "TransactionID"[1]**	Yes	Yes	Yes

8.3 Partial Authorization

Issuers may approve a transaction for an amount that is less than the requested amount. Partial authorization support is mandated by MasterCard and Discover. Bank of America requires partial authorization be supported for all card types. Partial authorization support is optional in Ecommerce environment, Bank of America strongly recommends its support in Ecommerce environment if the partner application can handle it.

8.4 Processing Level II Transactions

For business-to-business customers, Level II processing can provide lower interchange rates in exchange for providing more information during a transaction. Level II processing includes additional customer and tax information for the transaction. Currently, American Express, Mastercard, and Visa support Level II processing.

Level II cards, which are also called Type II cards or Purchase card Type II, provide customers with additional information on their credit card statements about their purchases. Level II cards enable customers to easily track the amount of sales tax they pay and to reconcile transactions with a unique customer code. There are two categories of Level II cards:

- Business/corporate cards are given by businesses to employees for business-related expenses such as travel and entertainment or for corporate supplies and services.
- Purchase/procurement cards are used by businesses for expenses such as supplies and services. These cards are often used as replacements for purchase orders.

Level II data is not stored on the Omni-Channel Gateway; the data is passed through to the processor. Thus, if multiple partial captures or credits are required to complete a transaction, the Level II data is required in each request.

8.4.1 Requirements

The following fields are required for Level II card in addition to the standard card processing information for Capture & Credit.

- Purchase Order Number (orderInformation.invoiceDetails.PurchaseOrderNumber)
- Tax Amount (orderInformation.amountDetails.taxAmount)
- Exemption Code = "Y" if exempt from sales and use tax (orderInformation.amountDetails.taxDetails.exemptioncode)

8.5 Transaction Request Status/Reason Codes

8.5.1 Status/Reason Codes for CNP Integration Toolkit

The Bank of America Gateway responds with the standard HTTP status/message, which includes 201, 400 or 502.

- You must parse the reply data according to the names of the fields instead of the field order in the reply message
- Your error handler should be able to process new reason codes without problems.
- Your error handler should use the error reason and the associated message fields to determine the result if it receives a reason code that it does not recognize.

Click here for details about each status/reason code category.

Status/ Reason Code 201

The status code 201 indicates the Bank of America Gateway successfully creates a transaction resource ID and sends the transaction to the processor. A transaction response is returned indicating the request has been approved or declined.

Status/Reason Code 400

The status code 400 indicates something is wrong or missing in the request payload from the transaction request. Try to correct the request payload based on the error message to get a successful response.

Status/Reason Code 502

The status code 502 indicates either a server error or time-out. The transaction can be re-tried, or a timeout reversal request can be sent. You may also contact support for further investigation.

9 Receipt Requirements

This guide includes receipt requirements for the following scenarios:

9.1 Card Not Present / Electronic Commerce Receipt Requirements

Card Not Present Receipt Requirements	Cardholder	Merchant
Merchant DBA (the name used by the merchant to identify itself to its customers)	X	X
Merchant DBA Location	X	X
Merchant URL (Internet Address)	X	X
Transaction Date and Time	X	X
General description of goods or services	X	X
Transaction Amount Price of goods and services including taxes and any card discount	X	X
Transaction Currency Currency symbol	X	X
Authorization Code	X	X
Reconciliation ID/Retrieval Reference Number	X	X
Payment Method used/Network Name (Visa, MC, Amex, Discover etc.)	X	X
Last 4 digit of the PAN/token	X	X
Transaction Type Purchase or Credit	X	X
Ship to address (if shipped)	X	X
Shipping Method	X	X
Customer Billing Address if different from Ship to address	X	X
Fee Assessed (if any) Convenience or Service Fees must be shown separate and clearly on the receipt	X	X
Customer email address (optional)		
Customer Telephone Number (Optional)		
Merchant Customer Service contact information	X	
Cancellation policy if restricted Can be communicated on the merchant's website and provide a way for the cardholder to acknowledge the policy during the checkout process or sent in a supplemental email with the receipt	X	
Return/Refund Policy if restricted Can be communicated on the merchant's website and provide a way for the cardholder to acknowledge the policy during the checkout process or sent in a supplemental email with the receipt	X	

The following table outlines the receipt requirements for card not present transactions. The information can be printed in any order

9.1.1 Card Not Present Receipt Sample

Your company name — Your company Logo (Optional)

123 your street
City, State, zip
Phone Number
Your@emailaddress.com
Your Website

Transaction Date: MM/DD/YYYY

SHIPPING INFORMATION
(if shipped)

Shipping Address:	Shipping Method:
Client name Street address City, State, Zip	

ORDER # 123456789

Description	Unit Cost	QTY	Amount
You item name	$0	1	$0
Your item name	$0	1	$0

Item(s) Subtotal:	$0
Shipping & handling:	$0
Fee:	$0
Subtotal:	$0
Discount:	$0
Tax Rate:	$0
Tax:	$0
Grand Total:	**$0**

PAYMENT INFORMATION

Payment Method:	**Billing information**:
Transaction Type: Purchase Card Type: Visa Last 4 PAN/token digit: 1234 Authorization Code: 12345 Reconciliation ID/RRN: XXXXXXX	Client Name Street Address City, State, Zip

RETURN POLICY

If you are not completely satisfied, you may exchange or return your purchase within 90 days…….
Questions? 1800-800-8000 | Onlinecustomerservice@yourstore.com

9.2 Card Not Present / Bill Pay Receipt Requirements

The following table outlines the receipt requirements for bill payment. The information can be printed in any order

Card Not Present Receipt Requirements	Cardholder	Merchant
Pay To Account (Account nickname the payment is being made to)	X	X
Last 4 digit of the PAN/token	X	X
Payment Method used/Network Name (Visa, MC, Amex, Discover etc.)	X	X
Transaction Date and Time	X	X
Funding Source Status (Has been debited)	X	X
Transaction Description (Bill Pay)	X	X
Invoice Number	X	X
Payment Date	X	X
Transaction Amount and Currency Symbol	X	X
Authorization Code	X	X
Reconciliation ID/Retrieval Reference Number	X	X
Transaction Type (Sale, Credit etc.)	X	X
Fee Assessed (if any) Convenience or Service Fees must be shown separate and clearly on the receipt	X	X
Customer Name (Optional)		X
Customer email address (optional)		X
Customer Telephone Number (Optional)		X
Merchant Customer Service contact information	X	
Merchant DBA and Address (The name used by the merchant to identify itself to its customers)	X	X

10 Demonstration and Certification Environment (DCE) Self-Test Validation

10.1 Its highly recommend for merchants to use the (DCE) Self-Test prior to going live in production by using the test URL that is associated with the integration method that you developed your website to.

10.2 In order to configure you website to send transactions to the DCE environment, you must create a secure acceptance profile and security keys via the DCE Merchant Portal. Link to

10.3 The DCE Merchant Portal can be accessed by visiting https://ebc2test.cybersource.com/ebc2/

11 Appendix A:

Token type	Format	Description
Billing Token/ Payment Instrument Token	• 32 character Hexadecimal • 16 to 19 digit, (format preserving), Luhn check Passing •	***Payment Card Transactions and Payouts*** Represents the tokenized: • Payment card PAN • Card expiration date • Billing information
Customer Token	• 32 character hexadecimal • 16 to 19 digit, (format preserving), Luhn check Passing	***Payment Card Transactions and Payouts*** Represents the tokenized: • Payment card PAN • Card expiration date • Billing information • Shipping information • Customer name • Email address

12 Appendix B

12.1 AVS Codes

Code	Description
Processors AVS	
A	Partial match: street address matches, but 5-digit and 9-digit postal codes do not match
B	Partial match: street address matches, but postal code is not verified. Returned only for Visa cards not issued in the US
C	No match: street address and postal code do not match. Returned only for Visa cards not issued in the US
D	Match: street address and postal code match. Returned only for Visa cards not issued in the US
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
G	Not supported: issuing bank outside the U.S. does not support AVS
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. Returned only for Visa cards not issued in the U.S.
K	Partial match: card member's name matches, but billing address and billing postal code do not match. Returned only for the American Express card type
L	Partial match: card member's name and billing postal code match, but billing address does not match. Returned only for the American Express card type
M	Match: street address and postal code match
N	No match: one of the following: ▪ Street address and postal code do not match. ▪ Card member's name, street address, and postal code do not match. *Returned only for the American Express card type*
O	Partial match: card member's name and billing address match but billing postal code does not match. Returned only for the American Express card type.
P	Partial match: postal code matches, but street address not verified. Returned only for Visa cards not issued in the U.S.
R	System unavailable
S	Not supported: issuing bank in the U.S. does not support AVS
T	Partial match: card member's name does not match, but street address matches. Returned only for the American Express card type.
U	System unavailable: address information unavailable for one of these reasons: ▪ The U.S. bank does not support AVS outside the U.S. ▪ 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 9-digit postal code matches.
X	Match: street address and 9-digit postal code match
Z	Partial match: street address does not match, but 5-digit postal code matches
Bank of America Gateway AVS	

Code	Description
1	Not supported: one of the following: ▪ AVS is not supported for this processor or card type. ▪ AVS is disabled for your Bank of America Gateway account. To enable AVS, contact Customer Service
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
5	No match: no AVS code was returned by the processor

12.2 CVN Codes

Code	Description
Processors CVN	
D	The transaction was determined to be suspicious by the issuing bank.
I	The CVN failed the processor's data validation check
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 payment card company
Bank of America Gateway CVN	
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