BANK OF AMERICA

Bank of America Gateway

Full Integration Developer Guide v2.0.4

October 2024

Table of Contents

1 Overview 12
1.1 Purpose 12
1.2 Scope 12
1.3 Definitions 12
2 Certification Process 14
2.1 Certification Overview 14
2.2 Solution consulting and discovery 14
2.3 Technical scope assessment 14
2.4 Documentation for EMV Level 3 Certification (Card Present Only) 14
2.5 Certification intake forms (Card Present Only) 14
2.6 Certification intake form validation 14
2.7 Test Tools / Self-Test Platform 14
2.8 Development 15
2.8.1 Use of Production Cardholder Data 15
2.8.2 Development Checklist 16
2.9 Pre-certification and validation 18
2.10 Certification 18
2.11 Launch and Delivery 18
2.12 Dormant Projects 18
2.13 Industry/Security Updates 18
2.14 Re-Certification 19
3 Integration Types 20
3.1 Card Not Present 20
3.1.1 Direct Integration to the Bank of America Gateway – REST API 21
3.1.2 Checkout API 22
3.1.3 Flex Microform Integration 23
3.1.4 Hosted Payment Page 24
3.1.5 Unified Checkout 25
3.2 Card Present 26
3.2.1 Payment Type field when initiating a Card Present transaction 26
4 Integration Methods 26
5 Sending Transaction Request 26

6 Authentication methods 27
7 Creating Security Keys 29
7.1 REST API Key 29
7.1.1 Creating a REST API Key 29
7.2 Secure Acceptance Keys 29
7.2.1 Creating a Secure Acceptance Key 29
7.3 Partner Solution Meta key Authentication 28
8 Certification Timelines 30
8.1 Card Not Present 30
8.1.1 Direct Integration to the Bank of America Gateway – REST API 30
8.1.2 Digital Payments 30
8.2 Card Present Integration – REST API 31
9 Development and Certification Requirements 32
9.1 PCI/PA-DSS and Card Data Security 32
9.2 Self-Assessment Questionnaire and Integration Type 32
9.3 Communication Protocols 32
10 Definitions - Best Practices - Features 33
10.1 Batch-less Environment 33
10.2 Track data Information 33
10.3 Transaction ID 33
10.4 Code 33
10.5 Payment ID or “ID” 34
10.6 Reconciliation ID /Retrieval Reference Number (RRN) 34
10.7 Merchant Solution Configuration Number or Solution ID 34
10.7.1 MSCN Submission for a Secure Acceptance and Hosted Payment Page 34
10.8 Point to Point Encryption 35
10.9 Tokenization 36
10.9.1 Merchant Token Hierarchy 36
10.9.2 Unsupported Token Features 37
11 Supported Transactions and Industry Types 38
11.1 Supported Transaction Types 38
11.1.1 Payment 38
11.1.2 Incremental Authorization – For future use 38

11.1.3 Capture 38
11.1.4 Void 39
11.1.5 Refund 39
11.1.6 Credit 39
11.1.7 Authorization Reversal 39
11.1.8 Duplicate Transaction Checking 39
11.1.9 Reversal vs Void 40
11.1.10 Timeout Reversal or Merchant Initiated Reversal 40
11.1.11 Timeout Void or Merchant Initiated Void 41
11.1.12 Transaction Matrix 43
11.2 Industry Types 45
11.2.1 Industry Data Type field 45
11.3 Balance Inquiry Transactions 45
11.4 Partial Authorization 45
11.5 How a Partial Authorization Works 46
11.6 Processing tip transactions 46
11.6.1 Inline tipping 47
11.6.2 Processing post tipping transaction 47
11.7 Processing Level II Transactions 48
11.7.1 Overview 48
11.7.2 Requirements 49
11.8 Store and Forward for Card-Present Transactions 50
11.9 Transaction Request Status/Reason Codes 50
11.9.1 Status/Reason Codes for REST API 50
12 EMV Implementation Considerations for direct integration to the Bank of America Gateway 52
12.1 EMV Transaction Initiation 52
12.2 Cardholder Prompts 52
12.3 Fallback Processing 52
12.4 Application Selection 53
12.4.1 Supported AIDs 54
12.4.2 Application Selection Process 54
12.5 Read Data Record and Processing Restrictions 55
12.6 Offline Card Authentication 55

12.7 Cardholder Verification 56
12.8 PIN Processing 57
12.8.1 PIN Entry Prompts 57
12.8.2 PIN Bypass 57
12.9 Terminal Risk Management 58
12.10 1st Generate Application Cryptogram 58
12.11 Online Processing and External Authenticate 59
12.12 Transaction Completion 59
12.13 EMV Credit and Debit Refund Transactions 60
12.14 AFD and EMV Consideration (For Future Use) 60
12.15 Contactless Payments 60
12.16 Contactless Magstripe vs Contactless EMV 61
12.16.1 Terminal Compliance 61
12.16.2 Cardholder Verification 61
12.17 Quick Chip 61
12.17.1 Contact Quick Chip 62
12.17.2 Contactless Quick Chip/Contactless Pre-Tap 62
12.17.3 Pre-Tap/Placeholder Requirements per brand 63
12.17.4 Device Type 65
12.18 EMV Tags 67
12.18.1 Sensitive EMV Tag 67
12.18.2 Transaction Request EMV Tags 67
12.18.3 Transaction Response EMV Tags 69
13 EMV Parameter Files and Keys 70
13.1 Test/Certification Configuration Parameters 70
13.1.1 American Express Credit 71
13.1.2 American Express U.S. Common Debit 73
13.1.3 UnionPay 74
13.1.4 Discover Credit 75
13.1.5 JCB 76
13.1.6 MasterCard Credit 77
13.1.7 MasterCard U.S. Maestro 78
13.1.8 MasterCard Maestro 79

13.1.9 Visa Credit 80
13.1.10 Visa Interlink 81
13.1.11 Visa U.S. Common Debit 82
14 Reporting Guidelines 83
14.1 EMV Parameter and Key Load Reports 83
14.1.1 EMV Parameter Report 83
14.1.2 EMV Key Load Report 84
14.2 EMV Transaction Reports 84
14.3 Fallback Reports 86
14.3.1 Clerk Technical Fallback Reports 86
14.3.2 PIN Pad Technical Fallback 86
14.4 POS Entry Mode Report 87
15 Card-On-File transaction Processing 88
A) Overview 88
B) Requirements 88
15.1 Initial Transactions (SALE/AUTH) 89
15.1.1 Sample initial transaction log for Card-On-File (SALE/AUTH) for Visa, MasterCard, Discover & Amex 90
15.1.2 Sample initial transaction log for Recurring & Instalment – Visa, Discover, Amex 91
15.1.3 Sample initial transaction log for Recurring, Subscription/Standing Order & Instalment for Mastercard 92
15.2 Subsequent Transactions (SALE/AUTH) 93
15.2.1 Sample subsequent transaction log for Card-On-File (SALE/AUTH) for Visa, MasterCard, Discover & Amex 94
15.2.2 Sample subsequent transaction log for Recurring & Installment for Visa 95
15.2.3 Sample subsequent transaction log for Subscription/Standing Order & Installment for Mastercard 96
15.2.4 Sample subsequent transaction log for Recurring - American Express 97
15.2.5 Sample subsequent transaction log for Installment - American Express 98
15.2.6 Sample subsequent transaction log for Recurring & Installment – Discover 100
16 Fraud Management with Device Fingerprinting 101
16.1 Fraud Management with Device Fingerprinting Workflow 101
16.1.1 Website Implementation 101
16.1.2 Adding the Fingerprinting Code to your website 102

16.1.3 Supported Tag Deployments 102
16.1.4 The Review Process 103
16.1.5 Required fields for CNP transactions: 104
16.1.6 Basic Ecommerce event: 105
16.1.7 Basic eCommerce sample including shipping and device information 106
16.1.8 Basic Response (no Reject / Review rules triggering) 107
16.1.9 Basic Response (Review outcome triggered) 109
16.2 Interpreting the Response 111
16.3 Fraud Management Review outcome 111
16.3.1 General Decline 111
16.3.2 Soft Decline 112
16.4 Additional Functionality 112
16.4.1 Device fingerprinting 112
16.4.2 EMV 3DSecure 112
16.5 Order conversion Report 112
16.5.1 Order Conversion Detail Report (On-Demand) 112
16.5.2 View the Conversion Detail Report (On-Demand) 113
16.5.3 JSON Example of Conversion Detail Report (On-Demand) 114
16.6 Receipt Requirements and Receipt Generation 117
16.7 Retail/Restaurant Card Present Receipt Requirements – Cardholder/Merchant template 119
16.7.1 Receipt Examples 122
16.8 Retail/Restaurant Card Present Receipt Requirements – Single template 127
16.8.1 Receipt Examples single template 129
16.9 Retail/Restaurant Card Not Present/Electronic Commerce Receipt Requirements 135
16.9.1 Retail/Restaurant - Card Not Present Receipt Sample 136
16.10 Card Not Present / Bill Pay Receipt Requirements 137
C) Healthcare Receipt Requirements 138
16.10.1 Healthcare Card Present - Cardholder/Merchant template 138
16.10.2 Healthcare Receipt Samples 140
16.10.3 Healthcare Hosted Payment Page / Electronic Commerce Receipt Requirements 143
17 Appendix A - Token 145
18 Appendix B 146
18.1 AVS Codes 146

18.2 CVN Codes 148
19 Appendix C 149
19.1 CA public key load file format 149
19.2 CAPK load Example 149
20 Appendix D - Device Type 150
21 Appendix E – Transaction Endpoints 151
A. Sandbox Transaction Endpoints 151
B. DCE Transaction Endpoints 152
C. Production Transaction Endpoints 153
22 Appendix F – Sample Transaction Requests and Responses Using REST API 154
22.1 EMV Contact Payment with an Online PIN 154
22.2 EMV Fallback Payment Using the REST API 156

Revision History

Version	Date	Description	Section	Author
2.0.4	10/1/24	• Added instructions on how to create security keys. • Added a note regarding blocking at the device/application level captured transactions amount that are higher than partially approved transactions. • Added a note about always sending the "Exemption Code" field for Level II card transaction. • Updated COF Overview section • Added EMV parameters values for American Express U.S. Common Debit AID • Added information on how to submit a capture request for partially approved transactions. • Added a Visa requirement not to support offline plaintext PIN for Unattended Cardholder Activated Terminal (UCAT).		
2.0.3	10/1/23	• Added a language not to use live PAN in the development and testing environments. • Made printing "duplicate" on a reprinted receipt an optional requirement. • Made displaying "demo" on the terminal when it is used in demo mode an optional requirement		
2.0.2	4/30/23	• Added Card-On-File Transaction Processing requirements. • Added Level II Transaction Processing requirements. • Added Fraud Management and device fingerprinting implementation. Added SIT, DCE, and Production URLs		
2.0.1	2/21/2022	• Added a Partner Development Checklist. • Added Track Data information. • Added Point to Point Encryption device list. • Added a paragraph about when to submit a Reversal request vs a Void request. • Updated Cardholder Verification Method table for online PIN support and removed CDCVM as Contactless CVM (CDCVM is still supported) • Added EMV Pre-Tap/Placeholder Requirements for each brand. • Added EMV tag 9F03 requirements for AMEX.		

		• Added a section for Receipt Requirements and Generation . • Removed CVM printing on the receipt as a requirement. • Added a note regarding circumstances when MID/TID can be printed on the merchant's and customer's receipt. • Receipt - renamed Card Present Receipt Requirement to Retail/Restaurant Card Present Receipt Requirements. • Receipt – updated Card Type to Card Network Name . • Receipt – Added Truncated Card Number to the receipt requirements table. • Removed shipping method and billing information for eCommerce receipt. • Added Healthcare receipt requirements and receipt samples. • Added REST API transaction trace Samples. • Re-formatted Receipt Samples • Updated "Bank of America's Merchant Services to Bank of America's Payment Platform • Removed printing AVS/CVV result code for manual transactions on the receipt requirement.		
2.0.0	2/12/2021	• Added a section for Timeout Void • Added a section for Incremental Authorization • Added single template receipt. • Added a section for Balance Inquiry transaction. • Added a section for In Industry Data Type • Added a section partial approval. • Added a section for Pay at the Table. • Added EMV implementation information. • Added store and forward processing information. • Added duplicate checking processing information. • Added receipt template for bill payment. • Removed Pax Semi-Integrated information. • Removed MID from receipt requirement table and receipt samples. • Added authentication methods information. Added information regarding credit and debit EMV refund be Full EMV ONLINE transaction.		
1.0.3	6/5/2020	• Removed Single Use Token API section. • Initiating a Card Present transaction. Added a SubTypeName value for tender types.		
1.0.2	5/20/2020	• MSCN or Solution ID.		

		- Clarified MSCN handling. • Timeout Reversal or Merchant Initiated Reversal. Added use cases for Timeout Reversal scenario.		
1.0.1	4/20/2020	• Updated legal disclaimer. • Certification Timelines. - Update certification timelines. Updated MSCN handling information.		
1.0.0	4/2/2020	Initial Draft		

1 Overview

1.1 Purpose

This document provides guidelines for integrating with the Bank of America's payment platform; it supports the following:

- Card Present processing (full integration to the Bank of America gateway)
- Card Not Present processing

Contact your Solutions Engineer to obtain credentials to connect to the Bank of America Gateway Developer Portal and any additional development information.

1.2 Scope

This guide covers the following:

- Certification Process
- Integration Types
- Development and Certification Requirements
- Definitions, Best Practices, and Features
- Supported Transactions and Industry Types
- EMV Implementation
- Receipt Requirements
- Sample Transaction Traces

Supporting documents, specifications, APIs and SDKs for card present and 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 entity that is integrating its solution into the Bank of America's payment platform
Solution	A point-of-sale (POS)/electronic cash register (ECR)/Gateway application
Certified Solution	A solution that Bank of America has certified for use with the Bank of America's payment Platform
Bank of America Gateway	Bank of America's Gateway for Card Present and Card Not Present processing, fraud management and payment security
MSCN	MSCN is an eight bytes alphanumeric Bank of America unique ID assigned to a Gateway, ISV or POS. This number will be provided at the beginning or during the certification process. It tracks features and functionalities certified for the software application or ISV on the bank side. It is sent in every transaction request to the host
STP	Self-Test Platform
UL BTT	UL Brand Test Tool
AID	Application Identifier

Term	Definition
RID	Registered Application Identifier
PIX	Proprietary Application Identifier Extension
GAID	Global AID
CAID	Common AID or Common Debit AID
PSE	Payment Selection Environment
CDCVM	Consumer Device Cardholder Verification Method
MDES	MasterCard Digital Enablement Service
MIT	Merchant Initiated Transaction
COF	Card on File
ODCV	On-Device Cardholder Verification
SIT	System Integration Testing
DCE	Demonstration and Certification Environment

2 Certification Process

2.1 Certification Overview

The certification process requires an Integrator to demonstrate that its solution adheres to the payment networks and Bank of America's payment platform requirements.

2.2 Solution consulting and discovery

When an Integrator is ready to begin discussing the technical aspects of the certification process, Bank of America will assign a Solutions Engineer to the effort.

The goal of the Solutions Engineer is to bridge the gap between business development conversations and the certification itself, whether it is an EMV Level 3 certification to the Bank of America Gateway or a card not present certification.

To achieve this goal, the Solutions Engineer will work with the Integrator to gather the necessary documentation for the solution, provide the Integrator the brand certification intake forms for EMV Level 3 certification, and finalize the features and functionalities that the integrator intends to certify.

2.3 Technical scope assessment

The technical scope assessment is provided to card present and card not present integrators to capture the certification scope. This document defines the project outputs and will impact the development and certification processes as outlined in the document.

2.4 Documentation for EMV Level 3 Certification (Card Present Only)

The following documents are required for the brand L3 certification:

- EMVCO EMV Level 1 and EMV Level 2 Letters of Approval for EMV contact
- Product bulletin for device family using the same smart card Interface Module
- MasterCard TQM
- EMVCO Contactless Level 1 Letter of Approval
- Brand Contactless Level 2 Letters of Approval for each supported brand
- PCI PTS documents

2.5 Certification intake forms (Card Present Only)

The Solution Engineering team will provide the integrator the following brand intake forms to complete

- Visa CCRT
- Discover CRF
- American Express (ATS)
- MasterCard TSE (Bank of America will generate the TSE for the Partner)

2.6 Certification intake form validation

The Solutions Engineer engages third party certification resource to: validate the collected forms and request new L3 projects for the integrator with Visa, MasterCard, Discover and Amex.

2.7 Test Tools / Self-Test Platform

Bank of America recommends UL test tool which contains the required card brands test cases to complete the EMV certification. Bank of America certification analyst creates test plan based on the

intake forms and setup access for the integrators in the self-test platform; the certification analyst will export test plan and provide it to the integrator for BTT import.

2.8 Development

Bank of America certification analyst provides development support by answering questions and assisting with unit testing.

- Bank's certification analyst provisions the integrator access for Self-Test Platform
- Bank's certification analyst generates test plan based on brand L3 intake forms and provides a copy of the test plan to the integrator.
- The integrator utilizes BTT and STP tools to complete EMV development.

2.8.1 Use of Production Cardholder Data

Production cardholder data (primary account number - PAN) should not be used for the development, the testing, or the certification. The use of production data in the development or the testing environments provides malicious individuals with the opportunity to gain unauthorized access to live cardholder data. If realistic PANs are needed to test a system functionality, payment card brands or other suppliers can often provide appropriate account numbers for this purpose.

2.8.2 Development Checklist

This section outlines the steps needed for an Independent Software Vendor (ISV) to complete before being assigned a Certification Analyst.

- Confirm the development is at least 100% complete, the ISV partner to provide their development status.

  - ☐ If Development is less than 100% complete, Bank of America will not begin the certification process.
  - ☐ Tested all applicable transaction types per the Development test script:
    - Sale (Auth + Capture)
    - Pre-Auth
    - Capture (Post-Auth)
    - Refund
    - Void
    - Reversal
    - Credit
    - Tip Adjust
    - Inline Tipping
  - ☐ Tested all industry types in scope:
    - Retail
    - Restaurant/Quick Service Restaurant (QSR)
    - Personal Services
    - Professional Services
    - Healthcare
    - Ecommerce/MOTO
  - ☐ Tested all applicable ancillary features and functionality based on the agreed upon project scope. Refer to Technical Scope Assessment.

- Confirm implementation of the Bank of America Gateway Integration Developer Guide's Receipt requirements:

Off-Site Gateway

- ☐ Receipt Requirement:
  - Produce an actual or a mock-up receipt that displays all the payment transaction information as outlined in the Developer Guide, no product or service description related information is required to be printed on the receipt.

Hybrid Gateway

- ☐ Receipt Requirement:
  - Provide a sample of the payload returned to a payment application needed to generate a receipt and any additional receipt configuration information provided to the merchant or the ISV partner.
  - Produce a mock-up receipt that displays all receipt requirements as outlined in the Developer Guide.

On-site Gateway

- ☐ Receipt Requirement:
  - Provide full receipt samples as outlined in the Developer Guide.

- ☐ If Receipt development is not complete, Bank of America will not begin the certification process.
- ☐ Verify decline receipts are printing as part of negative testing.

- Confirm implementation of the Bank of America Gateway Integration Developer Guide's Merchant Solution Configuration Number (MSCN) requirements:
  - ☐ If MSCN is not complete, Bank of America will not begin the certification process.
  - ☐ Validate MSCN value is being transmitted in the transaction request to the Host as part of the certification test script**.**
- Confirm API Payload logs are available for certification including the below details:
  - ☐ Services and endpoint that are being called.
  - ☐ Content Body
  - ☐ Complete set of request headers
  - ☐ Full response being received.
  - ☐ Response headers including correlation.
- Confirm merchant plug-in integration with Fraud Management. FME is a required feature for all E-commerce /Card Not Present (CNP) Native Solutions**.**
  - ☐ Device fingerprinting – Fraud Management supports end point device data collection for the purpose of device ID generation by Threatmetrix. All ISV partners are <u>required</u> to implement the Threatmetrix SDK to enable this functionality as part of their Fraud Management integration. The TM SDK is only for mobile devices, iOS & Android. The only required implementation is running the java collectors on the ISV'HPP.
  - ☐ IF the bank's FME integration is not coded to and tested: A certification letter will not be issued**.**

2.9 Pre-certification and validation

During the pre-certification and validation phase, the following will happen:

- Once the development is completed, the certification analyst will transition the project to pre-certification/validation in STP.
- The integrator will execute all use cases for each brand, import BTT results and receipts.
- The third-party certification resource will assist with the validation of card and host logs, ensuring all test cases pass validation before final certification run.

2.10 Certification

Once the solution is ready for the card brands run certification, the following steps happen:

- The certification analyst will transition the project from pre-certification to certification in STP.
- Bank's certification analyst and the third-party certification resource team collaborate to validate card logs, host logs, and receipts.
- The third-party certification team aggregates final certification test run results and submits them to the brands for approval.
- Bank's certification analyst provides EMV letters of approval to ISV.

2.11 Launch and Delivery

Before releasing a certified solution for General Availability, Bank of America requires each certified solution to complete a beta period of at least 2 weeks to ensure the solution is working as designed. If Bank of America identifies a defect, the Integrator must remediate it to move the solution to General Availability.

At the end of the beta period, Bank of America issues an official certification letter which details the certified features and functionalities.

2.12 Dormant Projects

If at any time while in testing with the Bank of America Certification Management Team, the project is dormant for a period of 30 calendar days, they will be re-assigned and must start over at the Validation Phase with Bank of America Solutions Engineering.

2.13 Industry/Security Updates

It is important to demonstrate an ongoing business-as-usual (BAU) approach to application and network security so merchants can stay protected; this includes staying current on PCI compliance mandates, required critical software/OS updates and changes in Internet encryption protocols.

2.14 Re-Certification

There are several reasons a Card Present or Card Not Present certified solution may need to be updated or recertified. The following section lists some of the reasons an integrator may need to recertify a solution.

<u>For Card present solutions (EMV level 3 certification)</u>

A. A partner making changes to a payment module or to an EMV parameter configuration of an already certified solution such as:
    - Supporting a new operating system or new functionalities that alter payment processing performance.
    - A firmware changes impacting L1 performance.
    - Any change to the Cardholder Verification methods (Bypass PIN Entry, Get Data for PIN Try Counter, Fail CVM, Amount known before CVM processing)
B. Production support challenges or continuous system improvement. (An example would be the Bank making changes to enhance its processing platform or to comply with a network regulatory requirement.

For a complete list of EMVCo recommended recertification considerations please see EMVCo's *EMV® Terminal Type Approval Bulletin No. 11 Ninth Edition April 2019* document

Notes:
Existing EMV certified solutions with expired Level 2 kernel can remain in production beyond the kernel approval expiration date as long as there are no changes to the kernel, or payment module processing logic.

Example of minor changes that will not result in a re-certification project:

- Update to Application Version Number
- Adding, removing, or changing printer or a display hardware

<u>For Card not present solutions</u>

- A partner making changes to a payment module (ex: API)
- Production support challenges or continuous system improvement. (An example would be the Bank making changes to enhance its processing platform or to comply with a network regulatory requirements)

If the bank initiates the changes (Card present and card not present solutions), the partner will be notified to discuss the re-certification efforts. The partner can also initiate the changes by contacting the Solutions Engineering team or their Account Representative. The bank requires to be notified before any changes that affect the payment module is made to a certified solution.

3 Integration Types

Integration types are considered either Card Not Present or Card Present.

3.1 Card Not Present

Bank of America offers Card Not Present digital payment integrations using the latest technology that are fast, smart, and secure through the Bank of America Gateway. They are supported by:

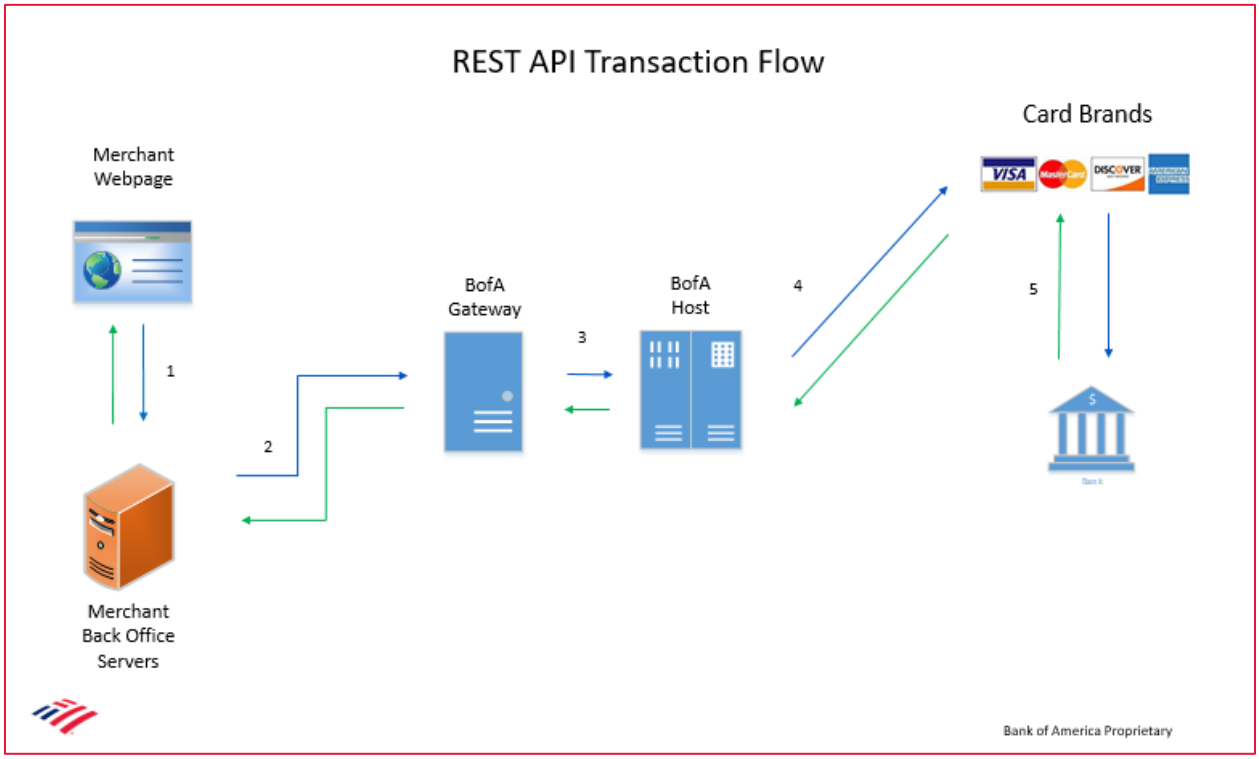
- Robust and intuitive APIs for all payment types and solutions.
- Client libraries for the leading developer platforms.
- SDKs (SDK Link) in six of the most popular coding languages (PHP, C#, Java, Ruby, Python, Node).
- Comprehensive sandbox testing.
- Sample code of payment use cases .

3.1.1 Direct Integration to the Bank of America Gateway – REST API

A *Direct API – REST* integration is ideal for an Integrator that wants to control the entire customer checkout experience, including the payment form, response pages, and receipts. This integration type requires the Integrator to connect to the Bank of America Gateway via its REST API.

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 submits the transaction to the BofA Gateway.
3. BofA gateway submits the transaction to BofA host for processing.
4. BofA host submits the transaction to the Card Brands for processing.
5. Approval and or decline is provided back in the response. (BAC provides a PAN token in every Authorization Response)



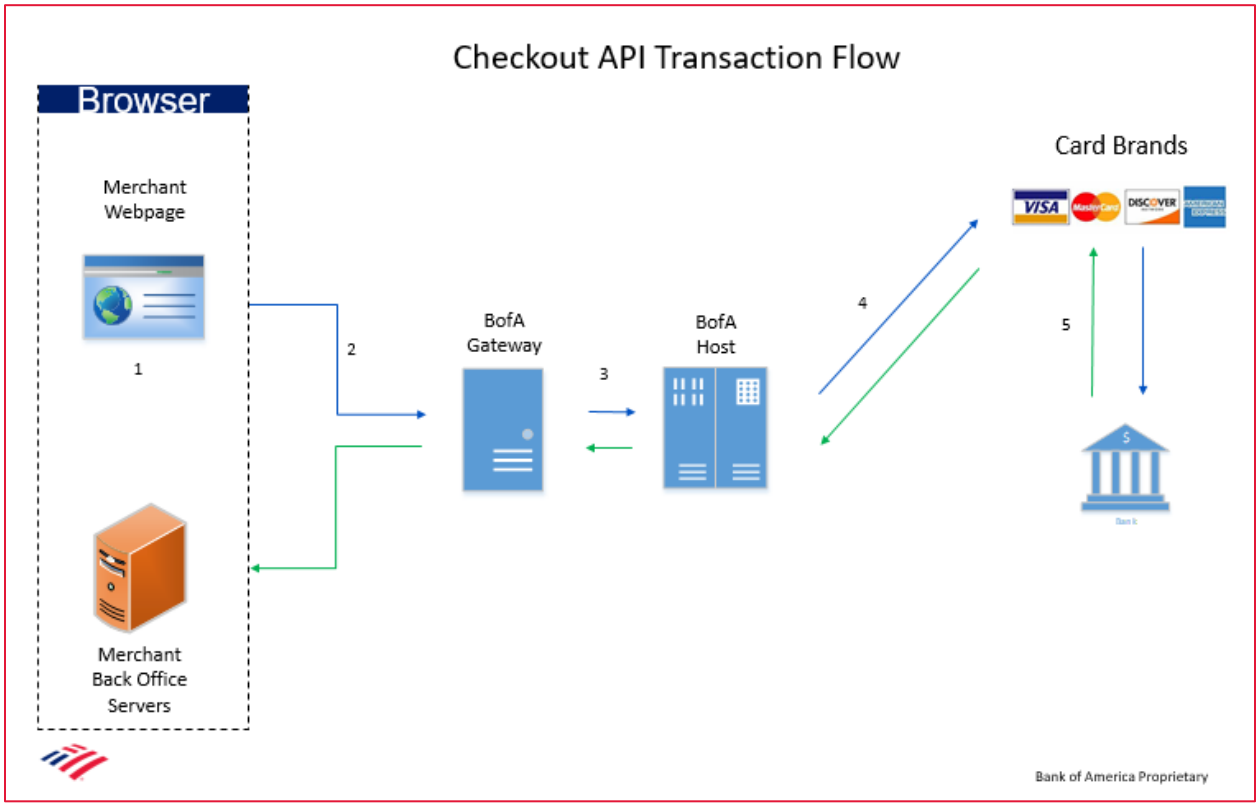
Click here for more information on REST API

3.1.2 Checkout API

With the Secure Acceptance 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 merchant's website.
   The payment page is rendered by the Merchant.
1. The transaction is submitted directly from the Merchant webpage to BofA Host for processing.
2. BofA gateway submits the transaction to BofA Host for processing.
3. BofA Host submits the transactions to Card Brands for processing.
4. Approval and or decline is provided back in the response. (BofA provides a PAN token in every Authorization Response)



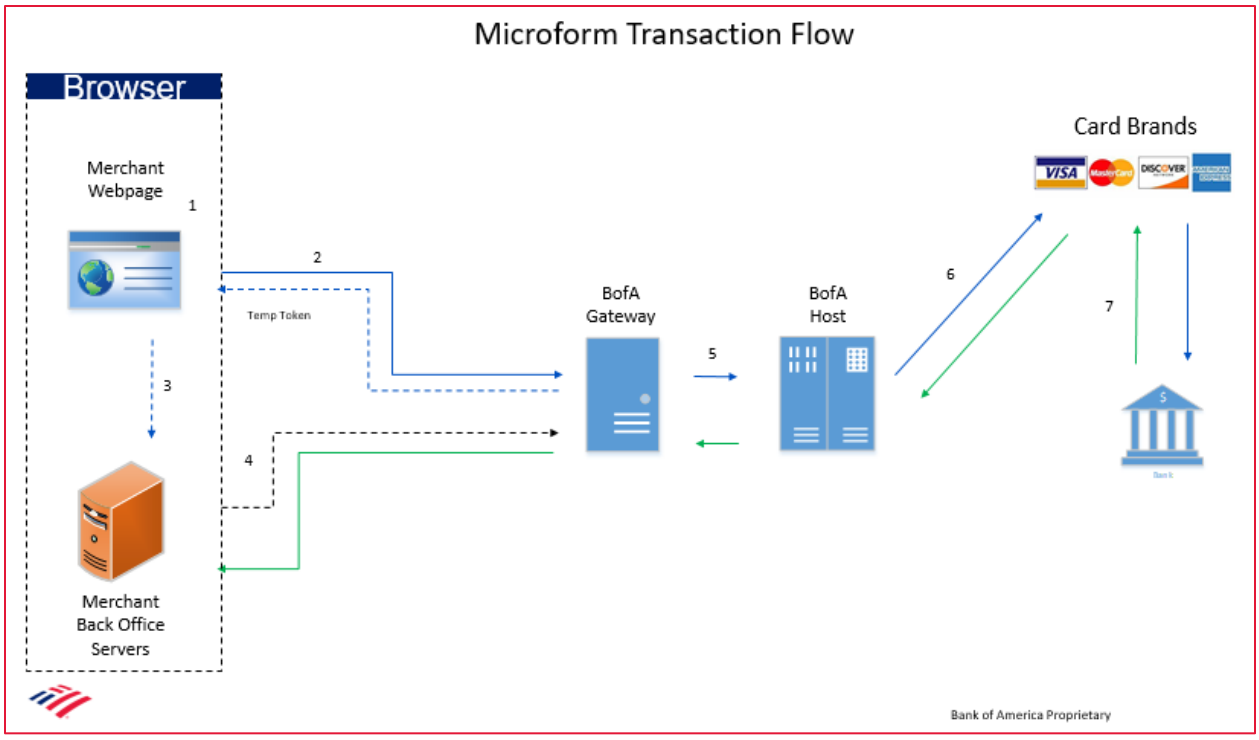
Click here for more information on Secure Acceptance Checkout API:

3.1.3 Flex Microform Integration

The Flex *Microform Integration* provides the most secure method for tokenizing card data. 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 PCI scope, a solution using Flex *Microform Integration* will likely qualify for SAQ A.

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

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



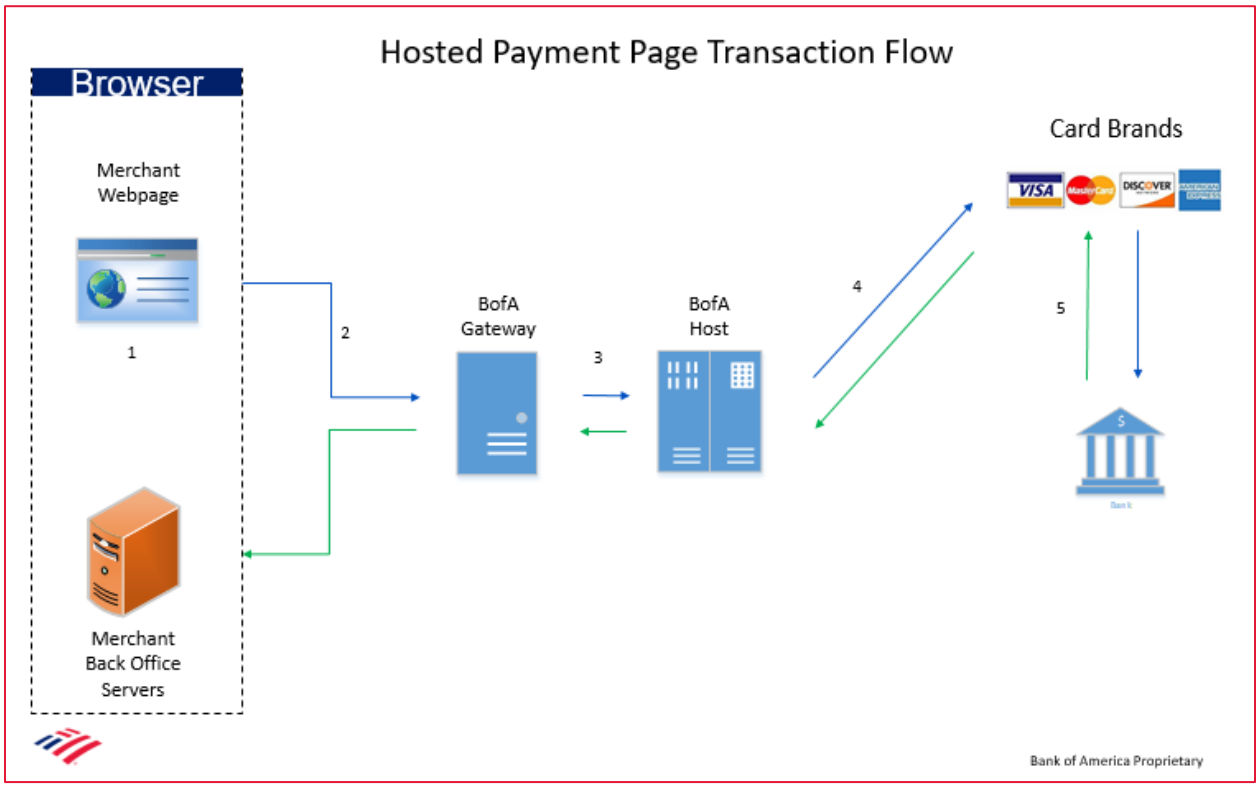
Click here for more information on the Flex Microform Integration:

3.1.4 Hosted Payment Page

With the *Hosted Payment Page* 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/printing the receipt page.

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

1. The Cardholder enters their card data on a checkout page that is hosted and rendered by BofA.
2. The transaction is submitted directly from the Merchant webpage to BofA for processing.
3. BofA gateway submits the transaction to BofA Host for processing.
4. BofA Host submits the transactions to Card Brands for processing.
5. Approval and or decline is provided back in the response. (BofA provides a PAN token in every Authorization Response)



Click here for more information on Hosted Payment Page

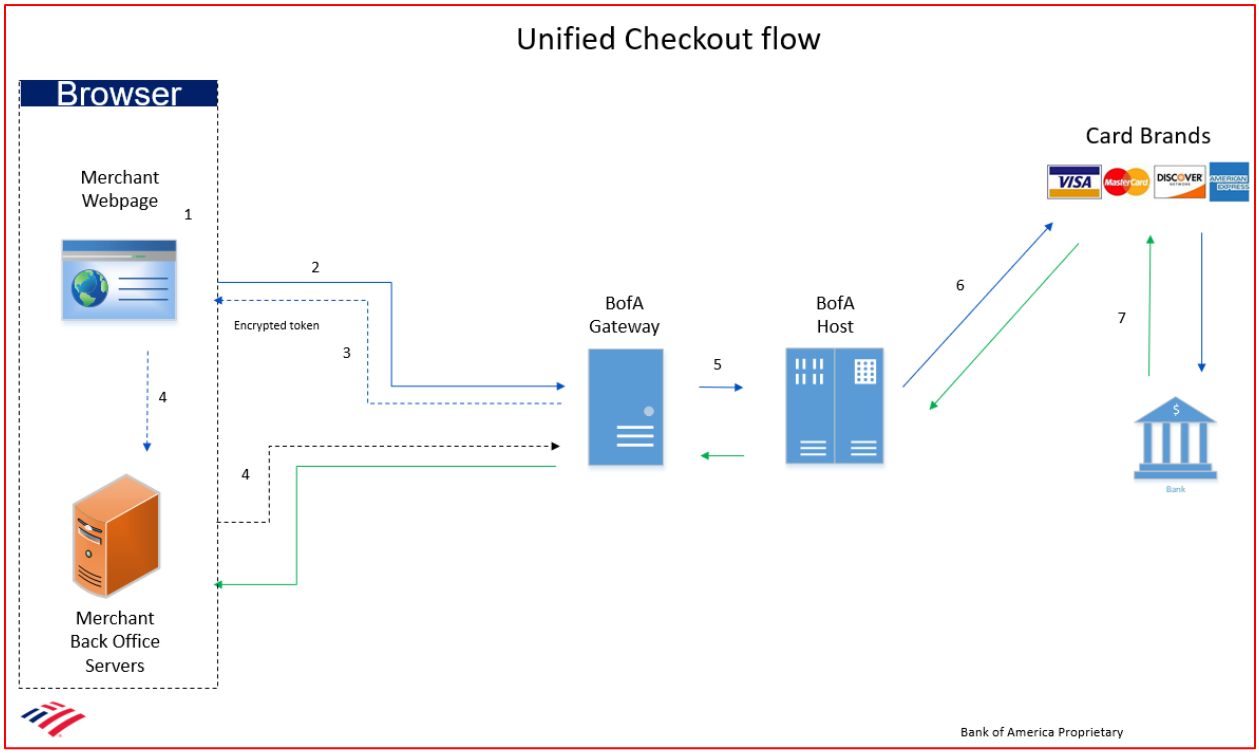
3.1.5 Unified Checkout

Unified Checkout provides a single interface that accepts numerous types of digital payments; this includes Apple Pay, Google Wallet, Samsung Pay and Paze.

With a *Unified Checkout* integration, the merchant hosts and renders the solution's entire payment details page. The Bank of America Gateway will control the user experience via iframe from the time the payment option is selected, and the encrypted payload is returned to the merchant. The integration then requires the merchant to pass the encrypted payload via its REST API.

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

1. Cardholder selects a digital payment on merchant's website (Paze, Apple Pay, Google Pay, Click to Pay or manual entry). The payment page is rendered by the Merchant.
2. Customer selects a digital payment on Merchant site.
3. Depending on which digital payment is selected by the consumer Unified Checkout will provide the encrypted payload to the merchant to process the payment.
4. The merchant back-office server will then initiate a REST API call using the payload to initiate a payment.
5. BofA Gateway submits the transaction to BofA Host for processing.
6. BofA Host submits the transactions to Card Brands for processing.
7. Approval and or decline is provided back in the response. (BofA provides a PAN token in every Authorization Response)



Click here for more information on Unified Checkout

3.2 Card Present

Bank of America card present integration supports EMV acceptance, point-to-point encryption (P2PE), and tokenization.

Click here for information on integrating with the Bank of America Gateway for Card Present transactions; the link provides detailed requirements related to API request format for a card present integration to the Bank of America Gateway; it is used in conjunction with the Payment Swagger Specification and other addendum documents. The integrator must ensure that the API requests comply with the requirements listed on the portal and in the Payment Swagger Spec. The transaction response format is also detailed in the specification documents.

3.2.1 Payment Type field when initiating a Card Present transaction

To initiate a Card Present transaction, set the PaymentType -> SubTypeName to the following value in the message request for all the transaction types.

Tender Type	SubTypeName Value
Debit	Debit
EBT	Debit
Credit	Credit
Prepaid	Credit

Example for SubTypeName Value for a Debit transaction

```
"paymentInformation": {
  "paymentType": {
    "subTypeName": "DEBIT"
  }
}
```

4 Integration Methods

All new integrations should adopt the REST API implementation; it provides functionalities for processing payment (sale), authorization, capture, reversal, refund, credit, 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.

5 Sending Transaction Request

All requests to the Bank of America gateway must be authenticated. In addition to the appropriate endpoint for the request type being sent, you will need three pieces of credentials that can be retrieved from the Bank of America Business Center Portal or provided by your certification or your account representative; these credentials are sent in the transaction request header message.

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

6 Authentication methods

The following authentication methods are supported for REST API and Secure Acceptance:

- HTTP Signature – Shared Secret Key
- JSON Web Token – P12 Certificate key
- Partner Solution Meta-keys

6.1 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. It is retrieved from the Business Center Portal or provided by your Certification Analyst or Account Representative.

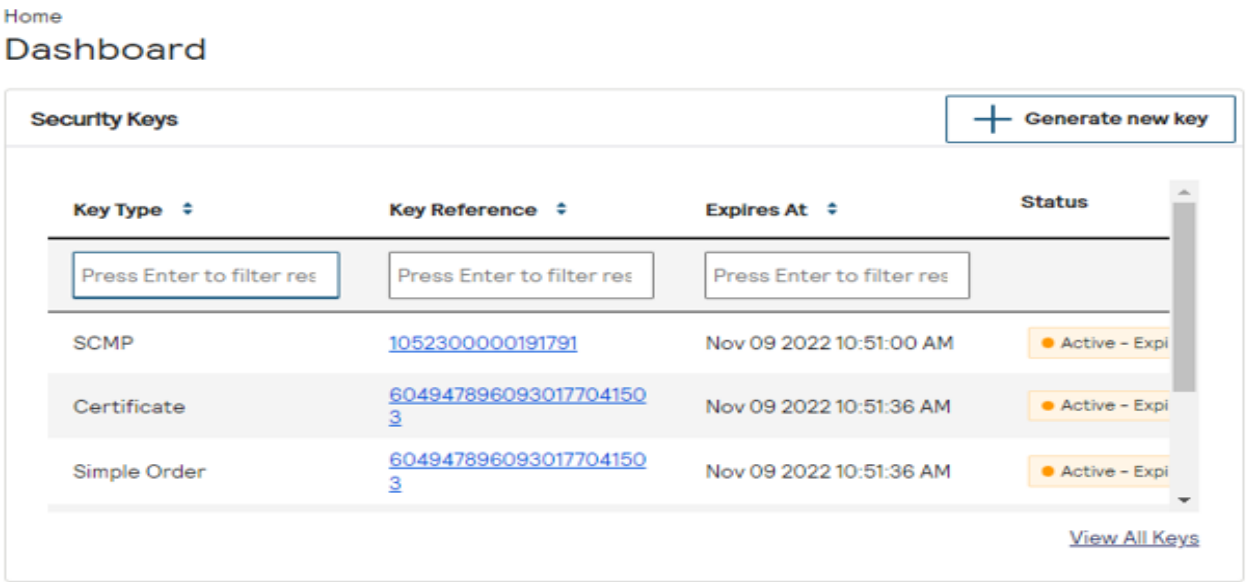
Note: Once a key is provided, it is the ISV/merchant's responsibility to enter the key in their system so the information is sent in the transaction request.

6.2 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.

Note: Once a key is provided, it is the ISV/merchant's responsibility to enter the key in their system, so the information is sent in the transaction request.

REST API keys expire after 3 years. You can use the Expiring Keys dashboard to view any keys that will expire soon. You can click **View All Keys** to go directly to the Key Management page or click **Generate new key** to create a new key.



6.3 Partner Solution Meta key Authentication

This solution is applicable for partners of the bank that have large number of merchants. The partner's meta key will allow partners to submit transactions on behalf of merchants. Partners will have the power to perform any functions that are supported via API using the meta key.

Meta Keys are available for the following APIs:

- REST
- Simple Order API
- SOAP
- SCMP

Contact your Solutions Engineer or your Account Representative on how to get set up for the Partner Solution Key

7 Creating Security Keys

7.1 REST API Key

The Bank of America REST API uses public key cryptography to securely exchange information over the Internet. Before you can send requests for Bank of America services using the REST API, you must create a security key for your Bank of America merchant account.

7.1.1 Creating a REST API Key

1. Log in to your Merchant Services Account.
2. On the left navigation panel, click the **Payment Acceptance Configuration** icon.
3. Click **Key Management**.
   The Key Management page appears.
4. Click + Generate Key.
   The Create Key page appears.
5. Select the type of REST key you want and click **Generate Key.**
6. Follow the sub-step below that corresponds to the key you selected.
   REST Shared Secret: Copy the generate key to your clipboard by clicking the clipboard icon or click **Download Key** to download the shared secret Key. The first value is the key and the second value is the shared secret.
   REST Certificate: Click **Download Key** to download the certificate.

7.2 Secure Acceptance Keys

The Bank of America Secure Acceptance API uses public key cryptography to securely exchange information over the Internet. Before you can send requests for Bank of America services using the Secure Acceptance, you must go to the Business Center and create a security key for your Bank of America merchant account.

Secure Acceptance keys expire after 2 years.

7.2.1 Creating a Secure Acceptance Key

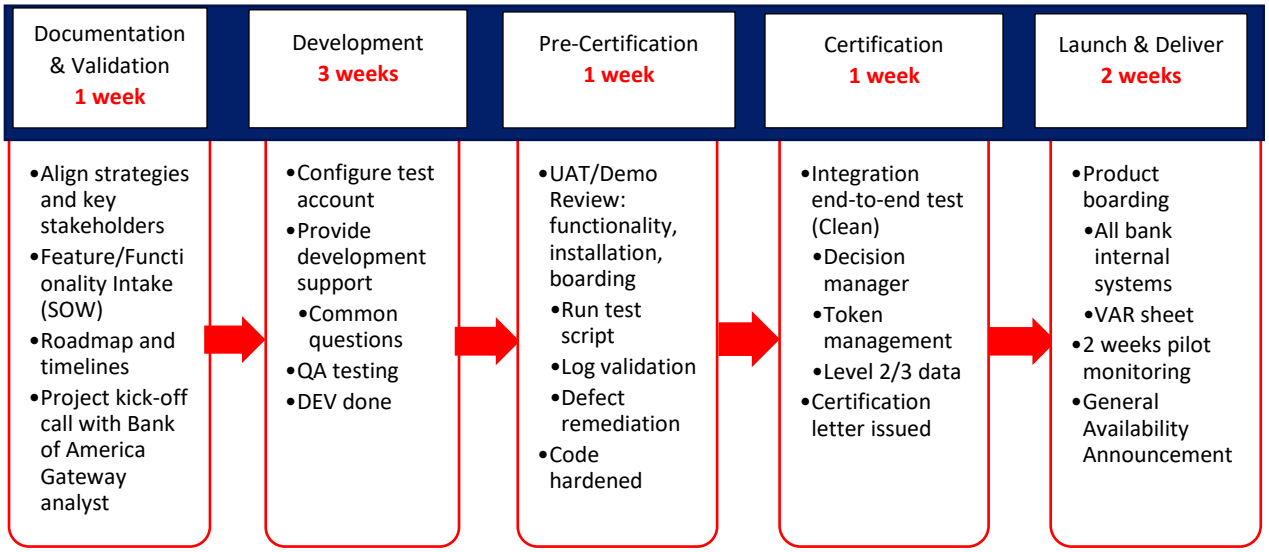
1. Log in to your Merchant Services Account.
2. On the left navigation panel, click the **Payment Configuration** icon.
3. Click **Key Management**.
   The Key Management page appears.
4. Click + Generate Key
5. Select **Secure Acceptance** and click **Generate Key**.
6. Enter the required information:
   - Key Name: enter a name for this key.
   - Signature version: select **1** from the drop-down menu.
   - Signature Method: select **HMAC-SHA256** from the drop-down menu.
   - Security Profile: select a security profile from the drop-down menu.
7. Click **Generate Key**. You can copy the access key and secret key by clicking the clipboard icons or click **Download key** to download a text file containing both keys.

8 Certification Timelines

The following section contains diagrams explaining the integration timeline for each integration type that Bank of America supports. Code development and defect remediation timelines for both Card Present and Card not Present are estimated and may be adjusted.

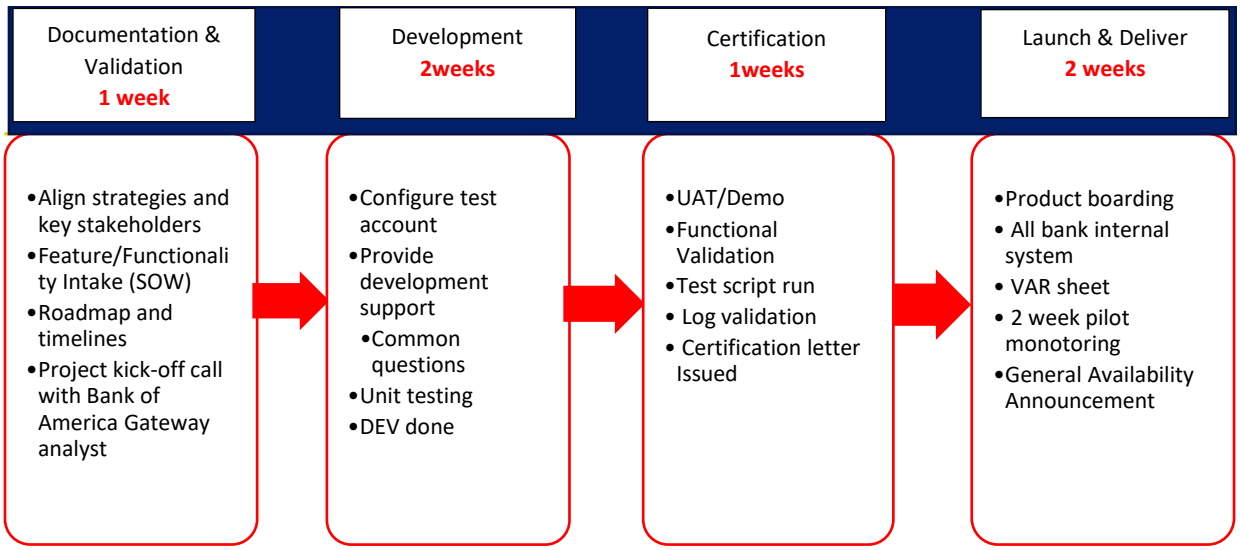
8.1 Card Not Present

8.1.1 Direct Integration to the Bank of America Gateway – REST API

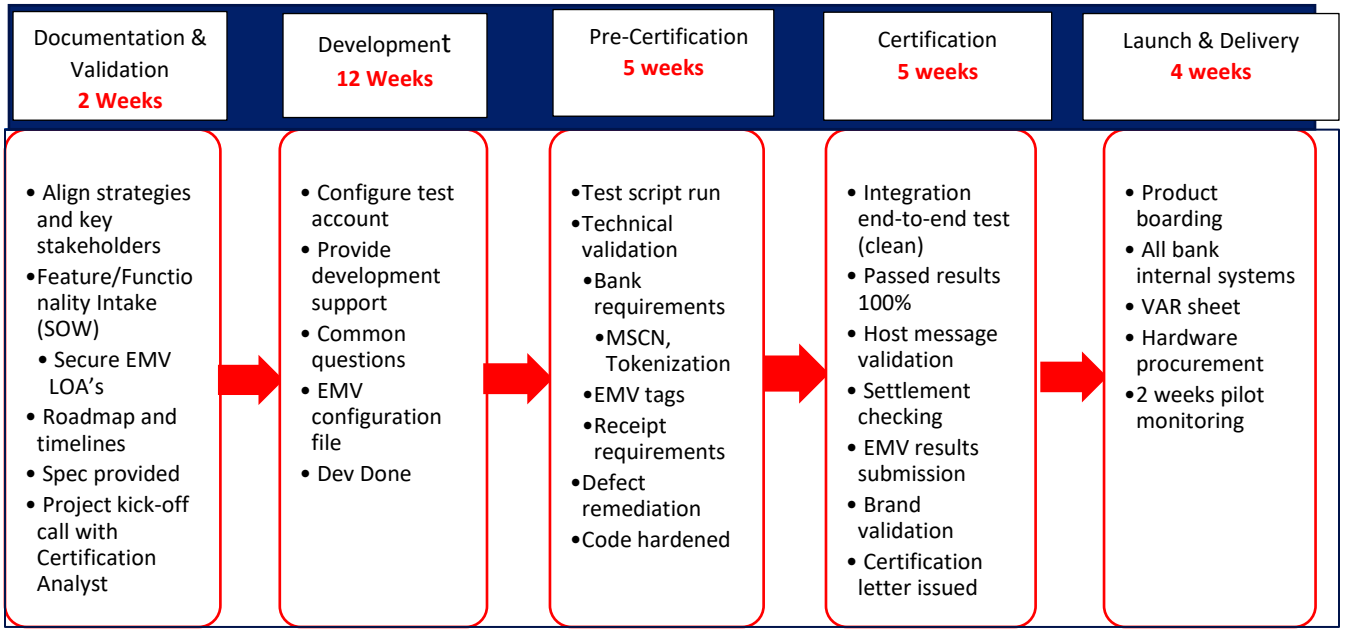


8.1.2 Digital Payments

(Checkout API, Flex Microform, Hosted Payment Page, Unified Checkout)



8.2 Card Present Integration – REST API



9 Development and Certification Requirements

9.1 PCI/PA-DSS and Card Data Security

All certified solutions must adhere to PA-DSS and PCI-DSS compliance standards. These standards apply to all entities that store, process, or transmit cardholder data.

9.2 Self-Assessment Questionnaire and Integration Type

The PCI DSS utilizes Self-Assessment Questionnaires (SAQ) as a tool to validate compliance. Refer to the table below to see the probable SAQ qualification for each integration type:

Integration Type	**SAQ Qualifications**
Direct Integration to the Bank of America Gateway – REST API	D
Checkout API	A-EP
Flex Microform Integration	A
Hosted Payment Page	A

9.3 Communication Protocols

Bank of America Gateway supports IP connection into the Bank of America Gateway.

Minimum requirements for a connection include HTTPS URL supporting Transport Layer Security (TLS) with cryptographic protocol version 1.2 or higher and Secure Hashing Algorithm (SHA) 256.

The Bank of America gateway also supports MPLS connection for partners who process high volume transactions and who want to control the network traffic flow, please contact your Solutions Engineer for implementation information.

10 Definitions - Best Practices - Features

10.1 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 AUTHORIZATION are processed and sent out for settlement every hour at the half hour; transactions that include tip adjustment must be managed on the terminal/POS batch.

Sale (Payment + Capture) transactions are cleared and sent out for settlement every hour at the half hour. A sale transaction is a bundled of payment 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
- For in-line tipping
- For PIN based transactions i.e. Debit, EBT.
- 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 restaurants to process tip transactions without regard for the host batch-less environment. Tip adjustment transactions are processed as dual message transactions.

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

PIN Debit transactions are processed as single message or Sale (Payment + Capture) transaction.

10.2 Track data Information

The Bank of America gateway supports both Track 1 and Track 2 data. The integrator must demonstrate during the certification their application can populate and transmit Track 1 and Track 2 data for card present transactions; If Tracks 1 and 2 are both captured, both should be forwarded.

10.3 Transaction ID

It is a unique identifier generated by the POS 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.

10.4 Code

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

10.5 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)

10.6 Reconciliation ID /Retrieval Reference Number (RRN)

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

10.7 Merchant Solution Configuration Number or Solution ID

The Merchant Solution Configuration Number (*MSCN*) is a unique ID that Bank of America assigns to each **certified version** of a solution. **Documentation for the Bank of America Gateway references the *MSCN* as *Solution ID***. The Bank provides the *MSCN* during the certification process. The *MSCN* consists of 8 alphanumeric characters. The Bank requires integrators to include the Solution ID (*MSCN)* in each transaction request to the host. When a change is made to the payment processing functionality in a previously certified solution, the Bank will issue a new *MSCN*. The integrator needs to replace the previous MSCN with the new one so that the latest MSCN is included with each transaction.

The steps that an integrator needs to follow to submit the *MSCN* vary by the integration type that the solution uses:

- MSCN Submission for a Secure Acceptance and Hosted Payment Page
- MSCN Submission for a REST API integration

10.7.1 MSCN Submission for a Secure Acceptance and Hosted Payment Page

If a solution utilizes Secure Acceptance Checkout API, Flex Microform, or the Hosted Payment Page, the integrator is responsible for submitting the *MSCN* with each transaction request.

The integrator includes the *MSCN (SolutionID)* in the *HTTP Post* request in the *signed_field_names* Partner_Solution_id field as shown below:

signed_field_names= **partner_solution_id**,
partner_solution_id=MSCN Value

10.7.1.1 MSCN Submission for a REST API integration

The MSCN (referenced as SolutionID) is submitted as part of the transaction request fields.

For example, if the *MSCN* for a solution is CCCCCCCC, then the integrator will submit the following:

"clientReferenceInformation":
"partner": {

"solutionId": "CCCCCCCC"

}

10.8 Point to Point Encryption

Bank of America Point to Point Encryption (P2PE) provides field-level encryption services to protect the primary account number (PAN) and other sensitive cardholder data from the point of interaction (POI) through the merchant's environment until it reaches the Bank of America Gateway.

For card present transactions, the field-level encryption will occur within a Secure Cryptographic Device (SCD) that is tamper resistant referred to as "hardware" encryption solution.

Bank of America supports Standard Encryption Method that uses Triple-DES DUKPT encryption algorithm.

Using Point to Point Encryption may lower merchant PCI compliance scope and cost and reduce compromise risk for merchants.

The following devices support the bank's Point to Point Encryption and require the device serial number to the sent in the payment request.

MAKE	**TYPE**	**MODEL**
INGENICO	TERMINAL	LINK 2500
INGENICO	TERMINAL	LANE 3000
INGENICO	TERMINAL	LANE 5000
MIURA	TERMINAL	M010
MIURA	TERMINAL	M021
PAX	TERMINAL	Q20
PAX	TERMINAL	A920
PAX	TERMINAL	S80
PAX	TERMINAL	D135
PAX	TERMINAL	SP30
PAX	TERMINAL	S300
PAX	TERMINAL	A80

MAKE	TYPE	MODEL
PAX	TERMINAL	ARIES 6
PAX	TERMINAL	ARIES 8
PAX	TERMINAL	E600
PAX	TERMINAL	E700
PAX	TERMINAL	E800
PAX	TERMINAL	E800 LITE
PAX	TERMINAL	A60
PAX	TERMINAL	A800
VERIFONE	TERMINAL	E355
VERIFONE	TERMINAL	P400
VERIFONE	TERMINAL	M400

10.9 Tokenization

10.9.1 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*.

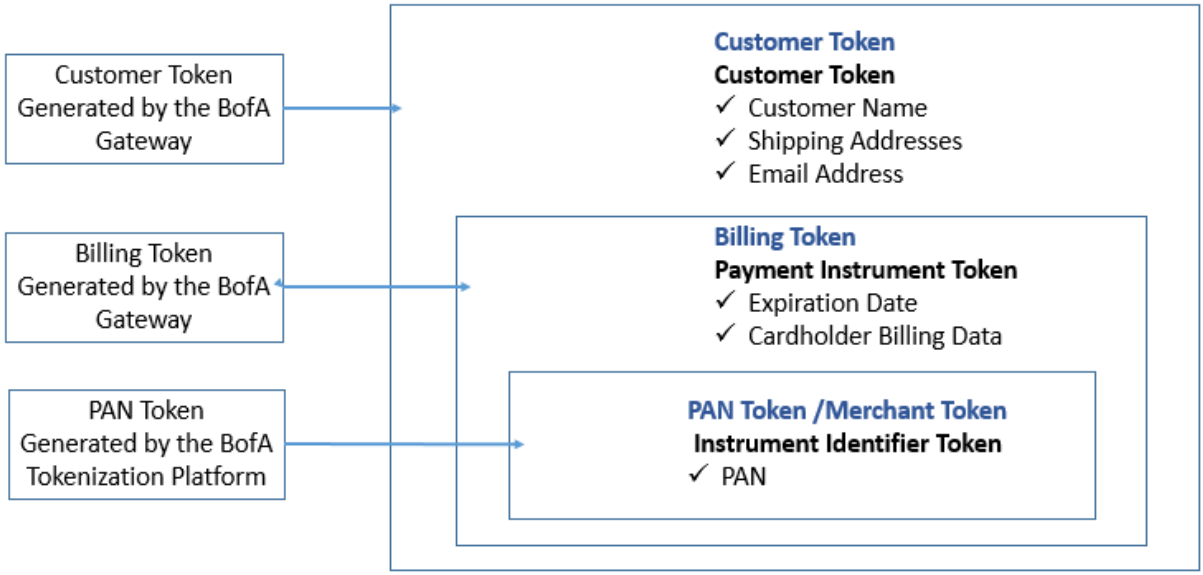
See below for the types of tokens involved in the Bank of America platform:

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. Bank of America's tokenization platform generates this token, and it is 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 POS 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



10.9.2 Unsupported Token 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).
3. Token for Account Updater request.
4. Network Tokens (e.g., Visa, MasterCard, etc.)

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

11 Supported Transactions and Industry Types

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

11.1 Supported Transaction Types

11.1.1 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. This is ideal for merchants that **do not** know the final transaction amount at the time of authorization, for example full-service restaurants.

11.1.1.1 Payment – Bar Tab transaction processing on the Bank of America Gateway

Bank of America recommends processing bar tab transactions where multiple rounds of orders a placed as follow:

1) Send an initial authorization (Payment) for the estimated amount.
2) Send an authorization reversal for the initial authorized amount if additional charges accrued.
3) Submit a new authorization (Payment) for the new estimated amount.
4) Submit a completion (Capture) for the final amount.

The merchant must disclose to the cardholder the amount of the authorization request and the cardholder must insert the EMV card for each Payment (authorization) transaction.

11.1.2 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; examples of industry types where an incremental authorization is used are restaurant, bar, auto rental, lodging etc.

11.1.3 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.

Notes:

- A transaction with $$0.00 tip amount requires a capture request in order to be settled, if no capture is received, the transaction will not be settled nor funded to the merchant account.
- 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. Debit transactions tend to have lesser capture time limit (generally between one to seven business days) while credit transactions may have as long as thirty business days capture time limit.

Captured transactions with amounts higher than the partially approved amount should be blocked by the device/application; these transactions should never be sent to the gateway.

11.1.4 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.

11.1.5 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.

11.1.6 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.

11.1.7 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).

11.1.8 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.

11.1.8.1 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 contains invalid data"
}
```

11.1.8.2 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. This is more applicable for card not present transactions but if this configuration if set, the same rules apply for card present transactions. 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 this authorization requ
               est matches the merchantReferenceCode of another authorization request
               that you sent in the last 15 minutes."
}
```

11.1.9 Reversal vs Void

When using the Bank of America REST API there are nuances to how Reversals and Voids are initiated. This also varies based on the type of transaction, whether it is a credit card SALE, or a signature debit card transaction using the credit rail.

On the Bank of America processing platform, REVERSAL is only used for:

1. Pre-Authorization (Payment)
2. SALE (Payment with "capture" :true) credit card or signature debit card transactions **prior to the host initiating a capture**.

All PIN Debit transactions and Sale credit transactions that are already captured will only use VOID; VOID is also used for Refund, Credit and settled transactions.

11.1.10 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/POS 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/POS did not get the response.

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

11.1.11 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
- PIN Debit Sale

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

Below are Timeout Reversal and Timeout Void use cases and the response returned by the Bank of America Gateway (BofA 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
BofA Gateway approved the transaction	- POS sends a transaction - BofA Gateway approved the transaction - POS did not get the response - POS sends a reversal request - Reversal is processed successfully	Status: "REVERSED", Reason: N/A", Message: "Successful transaction.	N/A
- BofA Gateway did not receive the original transaction	- POS sends a transaction - BofA Gateway did not receive the original transaction - POS did not get a response - POS sends a reversal - BofA 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
- BofA Gateway declined the transaction	- POS sends a transaction - BofA Gateway declined the transaction - POS did not get the response - POS 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	Request a new authorization

Use Case	Scenario	Transaction Response	Action
		there was not a previously successful authorization request or if the previously successful authorization has already been used in another capture request	
- BofA Gateway already sent the transaction for settlement	- POS sends a transaction - BofA Gateway approved the transaction and sent it out for settlement - POS send a reversal request late	Status:"INVALID_REQUEST", Reason:"NOT_VOIDABLE", Message:"The capture or credit is not voidable because the capture or credit Information has already been submitted for settlement. Or you requested a void for a type of transaction that cannot be voided	Proceed with a refund

11.1.12 Transaction Matrix

Transaction Type	Definition	Card Present	Card Not Present	Credit	Debit	EBT	FSA/ HSA
Payment	**Authorization**	Yes	Yes	Yes	No	No	Yes
	Incremental Authorization (future use)	Yes	Yes	Yes	No	No	Yes
	Sale (Authorization + Capture) • *Processinginformation.capture=true*	Yes	Yes	Yes	Yes	Yes	Yes
Capture	**Capture (**Completion for authorized transaction) • *Must include the Payment ID from the authorization request*	Yes	Yes	Yes	No	No	Yes
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	Yes	Yes	Yes
	Credit (Standalone) – Refund a standalone authorization/capture or a sale transaction. • Must include PIN Block for Debit transactions	Yes	Yes	Yes	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 BofA Gateway • If the settlement is already processed, a Refund must be submitted instead	Yes	Yes	Yes	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	Yes	Yes	Yes
	Void a Credit – Void of a standalone Refund transaction	Yes	Yes	Yes	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	Yes	Yes	Yes
Timeout Void	**Timeout Void or Merchant Initiated Void:** Void the following transactions in case no response is received from the BofA Gateway due to communication issue. Payment (Authorization + Capture) Refund Credit • **Must Include "transactionID"**	Yes	Yes	Yes	Yes	Yes	Yes

Transaction Type	Definition	Card Present	Card Not Present	Credit	Debit	EBT	FSA/ HSA
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	Yes	Yes	Yes

Bank of America supports retail FSA only at this time, 90% rule with the MCC codes, no SIGIS validation at the POS.

11.2 Industry Types

The Bank of America Gateway supports the following industry types:

- Retail
- Restaurant
- Ecommerce
- MOTO
- Healthcare
- Auto Rental (Future Use)
- Airline (Future Use)

11.2.1 Industry Data Type field

For Card Present transactions, this field is used to carry additional data in the transaction request for the following industries:

- Restaurant
- Healthcare
- Airline
- Auto Rental
- Transit

When this field is not set to the appropriate industry or it is not included in the transaction request, the additional required data will not be submitted to the host. For example, “Gratuity or tip amount for restaurants when the card is present is allowed only when `industryDatatype=restaurant

Example for “IndustryDataType” Value for a Restaurant industry type

```
“industryDataType”: {
 “type”: “restaurant”,
 }
```

11.3 Balance Inquiry Transactions

Balance inquiry transactions ideally should be performed when using prepaid or EBT cards. For EMV prepaid card, balance inquiry transactions are full EMV transactions. Because balance inquiry transaction does not transfer fund, they should not be reversed when they are declined or timed out.

11.4 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 in card present environment. Bank of America requires partial authorization be supported for all card types for card present transactions. 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.

In Card present environment, Bank of America requires to enable the Partial Authorization Indicator flag (partialAuthIndicator) in the transaction request. In the event the issuer partially approved the transaction, and the cardholder does not have another form of payment for the remaining balance, a reversal (for authorization) or void (for sale) message should be sent to the Bank of America Gateway to reverse the partially approved amount.

11.5 How a Partial Authorization Works

When the balance is less than the requested authorized amount, the issuing bank can approve a partial amount. When this happens, you can accept multiple forms of payment for the order starting with some or all the approved amount followed by one or more different payment methods. When a transaction is partially approved, the capture of the partially approved is not automatic. *The merchant must **submit** a capture request for the partially approved amount for settlement.*

1. If your account is not configured for partial authorization, you must enable partial authorization for the transaction by setting "processinginformation.authorization.partialAuthIndicator to "true" in the request.
2. You must submit an authorization request or a sale request.
3. The transaction response message includes:
    a. Orderinformation.amountDetails.totalAmount (amount you requested)
    b. Processinginformation.amountDetails.authorizeAmount (amount that was authorized)
4. You submit a capture request for the partial authorization.
5. When you capture only part of the approved amount, Bank of America gateway might be able to perform an automatic partial authorization reversal for you.
6. If you do not capture the partial authorization, you must request a full authorization reversal if this service is supported for your Bank of America Gateway and card type.
7. You use one or more different payment methods for the rest of the order amount.

11.6 Processing tip transactions

Bank of America host operates in a batch-less environment. Transactions that include tip adjustment or incremental authorization must be managed on the terminal/POS batch. Transaction requests are authorized at the host but stored in the terminal/POS. After the tip is adjusted, a capture (completion) request is sent to the host for settlement.
Tip adjusted transactions requests can be submitted to the host in two ways:

1) In a single transaction upload: Each pre-authorized transaction can be adjusted for the tip amount in the terminal/POS one at a time, and then a completion submitted to the host one at a time.
2) In multiple transactions: Pre-authorized transactions can be adjusted in the terminal/POS in groups and the corresponding completions are submitted to the host at once via a single socket connection.

Below are recommendations to manage the batch on the terminal/POS side for tip adjusted completion transactions:

- The terminal/POS batch will contain pre-authorization and incremental authorization transactions only.
- The terminal/POS batch may not contain sales, voids refunds, captured or voice authorization transactions.
- A Payment transaction in the terminal/POS batch will not be settled or paid until a "Capture" is sent to the host.

11.6.1 Inline tipping

Inline tipping requires to send SALE (Payment + Capture) transaction type. Bank of America recommends a wireless EMV terminal to process inline tipping EMV transactions. The process goes as follows.

1) The waiter brings a portable terminal to the table and rings up the transaction with the tipping options directly on the machine.
2) The customer adds the tip amount (the terminal must give an option to the cardholder not to add tip).
3) The terminal displays the tip amount and the total transaction amount.
4) The cardholder confirms the total transaction amount.
5) A receipt must print (email or text) showing the original transaction amount, the tip amount and the total transaction amount.

11.6.2 Processing post tipping transaction

A pair of PAYMENT/CAPTURE transaction type is required to process EMV post tipping or tip adjustment, the transaction is authorized for the original transaction amount only excluding tip; the terminal must support signature CVM and no CVM.

A receipt is printed with a tip line or a space for the cardholder to optionally add tip and another line or a space for signature. The cardholder adds tip and signs the pre-authorization slip.

The capture request may be submitted to include the tip amount the cardholder indicated on the Payment sale slip.

Note:

- A “Capture” should be sent for the total amount (original transaction plus tip amount)
- Authorization with $0 tip will still need to send a “Capture” request in order to settle

Below are tip processing transaction flow scenarios

Set-up Scenarios	Transaction Type	Transaction Amount	Tip Amount	Total Amount	Trans Type: Sale	Trans Type: Payment	Trans Type: Capture
Merchant supporting Inline Sale or Pay at the table only	Inline Tipping	$1$0.00	$2.50	$12.50	$12.50	n/a	n/a
	Post Tipping	n/a	n/a	n/a	n/a	n/a	n/a
Merchant supporting Post-sale tipping or tip adjustment only	Inline Tipping	n/a	n/a	n/a	n/a	n/a	n/a
	Post Tipping	$1$0.00	$2.50	$12.50	n/a	$1$0.00	$ 12.50
Merchant supporting both inline and tip adjustment	Inline Tipping	$1$0.00	$2.50	$12.50	$12.50	n/a	n/a
	Post Tipping	$1$0.00	$2.50	$12.50	n/a	$1$0.00	$ 12.50
	Post Tipping (No tip on Transaction)	$1$0.00	$0	$1$0.00	n/a	$1$0.00	$1$0.00
Merchant not supporting tipping	No tipping	$1$0.00	$0	$1$0.00	$1$0.00	n/a	n/a

11.7 Processing Level II Transactions

11.7.1 Overview

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.

11.7.2 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 = “N/Y” (orderInformation.amountDetails.taxDetails.exemptioncode)

11.8 Store and Forward for Card-Present Transactions

Bank of America is an Online Only Acquirer. It is recommended to set the floor limit to zero dollar for all card schemes for transactions to go online for issuer authorization. Merchants may decide to process Store and Forward transactions at their own risk. The transactions may be approved and stored locally following PCI requirements with the EMV data from the first generate AC command when their solution cannot communicate with the Bank of America gateway; once the communication is restored the transactions can be forwarded to the host as regular transactions; they may be approved or declined by the issuer. The merchant will not get paid for the declined store and forward transactions.

The Integrators who wish to support store and forward should proceed as follows:

- Card data and transaction information should be stored in a PCI compliant manner
- Store and Forward may be allowed for domestic cards only
- Ensure a positive TVR result (00 00 00 00 00)
- Bank of America suggests supporting store and forward for signature and no CVM only
- Generate a local approval code starting with SFXXXX when the transaction is approved offline
- when the transaction is sent to host and approved online, the payment application should add the host approval code returned in the response to the receipt for chargeback purposes
- Set "DeferredAuthIndicator" flag to true when submitting the store and forward transactions

```
"processingInformation": {
  "authorizationOptions": {
   "deferredAuthIndicator": true
  }
 }
```

11.9 Transaction Request Status/Reason Codes

11.9.1 Status/Reason Codes for REST API

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

- You must parse the response data according to the names of the fields instead of the field order in the response 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.

12 EMV Implementation Considerations for direct integration to the Bank of America Gateway

The following section provides an overview of EMV payment processing requirements and recommendations. Bank of America recommends all EMV solutions certification support both contact and contactless transactions.

12.1 EMV Transaction Initiation

Once the transaction is initiated by the clerk, the terminal should display a prompt to the cardholder to insert or tap (in the case of a contactless transaction) their card.

There are two ways an EMV transaction can be initiated:

1. The card insertion/card tap where the cardholder inserts/taps the card.
2. Service Code interrogation where the terminal reads the service code within the track data if the cardholder swipes the card. If the service code indicates the card is a chip card, the terminal should prompt the user to insert or tap their card. In case of fallback, the card may be swiped.

Requirements:

- If a card contains a **Service Code** beginning with 2xx or 6xx, the terminal must prompt for card insertion or tap.
- Only one card interface can be used at a time (swipe, contact or contactless). Once the card read begins on one interface, all other interfaces should be deactivated.
- In case of blocked application or blocked card, the terminal should terminate the transaction and it should not allow a fallback or magstripe transaction.

12.2 Cardholder Prompts

The terminal should display prompts to aid the cardholder through the transaction process. Below are recommendations for Card Prompting. Prompts should be clear and concise to avoid confusion.

- Card presentation required → "Insert, Tap or Swipe Card".
- Inform cardholder not to remove the card → "Leave Card Inserted".
- Transaction is completed and card should be removed → "Remove Card".
- Chip Card is swiped with a service code indicating card is a chip card → "Use Chip Reader".
- Fallback is initiated → "Use Magstripe".

12.3 Fallback Processing

A fallback occurs when the magstripe on a chip card is swiped to run a transaction on a chip enabled terminal. Bank of America recommends allowing your solution to perform fallback only when a chip enable terminal malfunctions or unable to read the chip card due to technical issue with the chip on the card or if there is an empty candidate list meaning there are no mutually supported AIDs between the card and the terminal.

An EMV fallback transaction occurs when an EMV transaction fails for one of these reasons:

A. **Technical Fallback:** the EMV terminal or EMV card cannot read and process chip data.
B. **Empty Candidate List/Business Fallback:** the EMV terminal does not have any applications in common with the EMV card.

The integrator should include the fallback field and set it to “true” to indicate fallback was used. The entry mode should be set to either “swiped” or “keyed”.

Requirements/Recommendations:

- In case of empty candidate list or unknown AID, the transaction should be processed as magstripe transaction.
- Only one card interface can be used at a time (swipe, contact or contactless). Once the card read begins on one interface all other interfaces should be deactivated.
- In case of blocked application or blocked card, the terminal should terminate the transaction and it should not allow a fallback or magstripe transaction.

12.4 Application Selection

The terminal performs Application Selection to identify which card application to use for the transaction. The terminal must be configured with all supported AIDs. If the card presented includes an **Application Identifier (AID**) that is not supported, a chip transaction cannot be performed; the terminal will initiate fallback where the cardholder should be prompted to swipe their card.

An AID consists of three components:

1. **Registered Application Identifier (RID)** – indicates the payment scheme, i.e., Visa, MasterCard, etc.
2. **Proprietary Application Identifier Extension (PIX**) – Indicates the payment brand, i.e., credit, debit, ATM-only, etc.
3. **Issuer Suffix** – optional field added by the issuer.

The Application Selection Indicator associated with each AID designates how application match is performed. There is Full Selection and Partial Selection.

- **Full Selection** is when the terminal AID list matches exactly to the card AID, including any issuer suffix assigned to the card.
- **Partial Selection** is when the terminal can select an AID based on only its AID matching the card AID, excluding the issuer assigned suffix.

It is recommended that EMV enabled terminals only accept AIDs supported based on the merchant agreement and those that were included in the EMV certification. An AID that has not been approved during certification must be ignored by the terminal without being sent to the host for authorization.

Requirements/Recommendations:

- Partial Selection must be supported to ensure that all chip applications for a supported AID can be selected regardless of any issuer suffix. The exception is Union Pay where the unique suffixes differentiate between Union Pay Credit and Debit AIDs
- Each AID found on the card can be either a **Global AID (GAID**) or **Common Debit AID (Common AID or CAID)**. Cards can be personalized with multiple GAIDs and CAIDs. GAIDs allow cards to be used domestically and internationally. If a GAID is selected, the transaction is routed to the network that owns the AID. If a CAID is selected, the

transaction is routed to independent regional debit networks or brand networks. CAIDs are only supported domestically.

12.4.1 Supported AIDs

The following AIDs are supported on the Bank of America host. All the AIDs supported by the EMV solution being certified will be tested during the certification

Card Scheme	AID	Credit/Debit	RID	PIX
American Express	A00000002501	Credit	A000000025	01
American Express U.S Common Debit AID	A00000002504	Debit	A000000025	04
Discover	A0000001523010	Credit	A000000152	3010
Discover U.S. Common Debit	A0000001524010	Debit	A000000152	4010
JCB	A0000000651010	Credit	A000000065	1010
MasterCard Credit	A0000000041010	Credit	A000000004	1010
MasterCard International Maestro	A0000000043060	Debit	A000000004	3060
MasterCard U.S. Maestro	A0000000042203	Debit	A000000004	2203
UnionPay	A000000333010102	Credit	A000000333	010102
Visa Electron	A0000000032010	Credit	A000000003	2010
Visa Credit	A0000000031010	Credit	A000000003	1010
Visa Interlink	A0000000033010	Debit	A000000003	3010
Visa U.S. Common Debit	A0000000980840	Debit	A000000098	0840

12.4.2 Application Selection Process

The following section captures the Application Selection Process.

The first step of Application Selection is building the candidate list of AIDs supported by both the card and the terminal. After the application is selected, the terminal will proceed with the selected AID. There are two methods used for building the candidate list:

a) **Payment Selection Environment (PSE) -** This is a file that contains all the AIDs supported by the card.
b) **Explicit selection** - The terminal will go through the list of AIDs on the card and try to match all AIDs it is compatible with. This occurs when there is no PSE present.

12.4.2.1 Candidate List Filtering Implementation

A. If the candidate list only contains one AID then that AID will be selected.
B. If the candidate list contains two or more mutually supported AIDs then the application list will be presented to the cardholder for selection if there is no prioritization. The integrator determines how to prioritize.

Requirements/Recommendations:

- It is recommended to check Tag 42, Issuer Identification Number (IIN) for the list of U.S. Common Debit AIDs for debit preferred merchants.
- If there is a CAID present on the candidate list, it must be selected to ensure optimal network routing to the merchant. This is referred to CAID Auto Select.
- The applications should be displayed with the following format: Application Preferred Name (Tag 9F12), Application Label (Tag 50) if the Application is not present or cannot

be displayed, and if neither can be displayed then the terminal shall display a default application name assigned to the AID.
    - The transaction must be cancelled if the cardholder indicates the application during the Cardholder Application Confirmation should not be used.
    - There is no requirement to perform Cardholder Application Confirmation at unattended EMV implementations.

12.4.2.2 Durbin Amendment

The Durbin Amendment is a US federal regulation that limits the interchange fees placed on debit card processing. To comply with the Durbin amendment provision that mandates merchant acquirers provide a choice of networks for routing debit card transactions via at least two unaffiliated networks, Bank of America recommends the debit functionality is implemented in a way that provides choice and flexibility for routing debit transactions; Bank of America suggests selecting U.S. Common Debit AID over Global ID when both point to the same funding account.

12.5 Read Data Record and Processing Restrictions

Once the application is selected, the card data is read from the chip.

During this reading, several checks are performed to validate the card and to ensure the card data is formatted correctly.

The terminal will read through any Processing Restrictions that are present on the card to determine if a transaction should be allowed. The terminal reads through the following checklist:

- The expiration date of the card
- Whether the application versions of the EMV chip and terminal are matching
- If the issuer has listed any card specific restrictions such as, the card is not permissible for international cashback transactions, etc. These restrictions will be listed in Tag 9F07 Application Usage Control

12.6 Offline Card Authentication

Depending on the card and terminal capabilities, the terminal will perform Offline Card Authentication to authenticate the EMV chip. Offline Card Authentication uses Certificate of Authority Public Key (CAPK) to protect against card counterfeiting. Below are the three offline Card Authentication Methods (CAM).

- **Static Data Authentication (SDA)** – SDA detects alteration of selected static data elements after card personalization. It is the least secure as it only validates card authenticity using static data.
- **Dynamic Data Authentication (DDA)** – provides similar protection as SDA, but additionally protects against replication of chip data as it generates a dynamic signature for each transaction.
- **Combined DDA/Application Cryptogram Generation (CDA)** – CDA is the most secure method as it contains the same security features of DDA in addition to using an Authorization Request Cryptogram (ARQC) to ensure the dynamic signature has not been altered. CDA is mostly seen used for contactless transactions.

Requirements/Recommendations:

- For each of the Offline Card Authentication Method failure TVR bits, the TAC settings must ensure the transaction is selected for online authorization.
- If Offline Cardholder Authentication Method is not performed and there is no other reason to decline the transaction offline, the TAC value must ensure that the transaction is sent online for authorization.
- If any offline Cardholder Authentication Method is supported by the kernel, all three must be supported (SDA, DDA and CDA).
- CDA must be supported in a mode that performs the CDA process therefore only CDA Mode 1 is permitted.

12.7 Cardholder Verification

Cardholder Verification is used to ensure the authenticity of the cardholder. The terminal will use the Cardholder Verification Method (CVM) list from the card to decide which CVM will be used for the transaction i.e. Signature, PIN or NO CVM. The CVM list also indicates the priority of the CVM used.

Below is a list of Bank of America supported CVM for each card scheme.

CVM - Contact	American Express	UnionPay	Discover	JCB	MasterCard	MasterCard International Maestro	MasterCard U.S. Maestro	Visa	Visa Interlink	Visa U.S. Common Debit
Offline Plaintext PIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Offline Enciphered PIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Online PIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Signature	✓	✓	✓	✓	✓			✓		
NO CVM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

CVM - Contactless	American Express	UnionPay	Discover	JCB	MasterCard	MasterCard International Maestro	MasterCard U.S. Maestro	Visa	Visa Interlink	Visa U.S. Common Debit
Offline Plaintext PIN										
Offline Enciphered PIN										
Online PIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Signature	✓	✓	✓	✓	✓			✓		
No CVM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Requirements/Recommendations:

- If a POS device currently supports PIN for magnetic stripe swipe transactions, then it must support both online and offline PIN for any message type except for Visa Unattended Cardholder Activated Terminal (UCATs); Visa's new rules require the following:
  - Effective 1 January 2024, **newly deployed UCATs** must not support offline plaintext PIN.
  - Effective 1 January 2025, **all UCATs** must not support offline plaintext PIN
- Signature CVM must still be supported. Note: Effective April 2018, the card brands no longer require the capture or collection of signatures as they have outlived their usefulness. However, Signature CVM is NOT to be removed as a CVM.
- Integrators may choose to support the No Signature Required Program provided by the Payment Networks. Those participating in a No Signature Required Program merchants are not required to capture a signature (or PIN where applicable) for qualifying transactions except where required by law. If the integrator chooses not to participate or is not eligible in the No Signature Program, then a signature line should always be printed on the receipt.

12.8 PIN Processing

12.8.1 PIN Entry Prompts

The following list shows recommended prompts the terminal must display to aid the cardholder through the PIN entry process.

PIN entry required → "Enter PIN".

Incorrect PIN entered → "Invalid PIN".

Only one PIN try remaining before card is blocked → "Last PIN Try".

PIN tries exceeded and card may be blocked → "PIN Tried Exceeded".

Requirements/Recommendations:

- The maximum number of PIN try must not exceed the PIN Try Counter Tag 9F17.
- The cardholder must be notified of the last PIN attempt before the card is blocked.

12.8.2 PIN Bypass

For customer positive user experience, Bank of America recommends the support of PIN bypass functionality when supported by the interface in case the cardholder opts out of PIN entry.

Requirements/Recommendations:

CAID only supports online PIN and No CVM therefore PIN bypass functionality may be allowed at the merchants' discretion, bypassing the PIN will result in No CVM as the only option for cardholder verification when CAID is selected. Even though the merchant may allow PIN bypass, the issuer may decline transactions for consumers for whom they have issued a PIN preferring card.

- PIN Bypass is **not** allowed for the following Debit AIDs:
  - Maestro (A0000000043060)
  - Interlink (A0000000033010)

- PIN Bypass is **not** allowed on MasterCard CAT and Contactless transactions.

12.9 Terminal Risk Management

The terminal will always perform several risk management checks.

- **Floor Limit**: the maximum transaction amount that will keep a transaction offline; any amount above the floor limit will be sent online.
- **Random Selection**: the terminal may randomly select a transaction for online authorization.
- **Transaction Velocity Checking**: the terminal will check if the card's consecutive lower limit. consecutive offline limit has been exceeded. If so, the terminal will send a transaction online.
- **CVM limit:** the terminal will check the amount above which it will require the cardholder to enter a CVM.
- **New Card Verification:** checks to see if the card has been used in an online transaction since issuance.

Requirements/Recommendations:

- The US region is an online only market; thus, US integrators should always set the floor limit to $$0.00 to ensure online authorization .
- EMV Terminal Risk Management features must be supported regardless of the offline capabilities of the terminal.

12.10 1st Generate Application Cryptogram

The 1st Generate Application Cryptogram (1st GEN AC) consists of two steps: Terminal Action Analysis and the Card Action Analysis.

1. **Terminal Action Analysis:** the terminal will decide whether to request the card to decline the transaction, send the transaction online, or approve offline. This is done by comparing the Issuer Action Codes (IACs), Terminal Action Codes (TACs) and Terminal Verification Results (TVR). The terminal will request a GEN AC.

    a. **Issuer Action Codes (IACs)** – Rules set by the issuer in the card.
    b. **Terminal Action Codes (TACs)** – Rules set by the payment system in the POS solution.
    c. **Terminal Verification Results (TVR)** – Contains the current transaction results generated by the Processing Restrictions, Offline Data Authentication, Cardholder Verification and Terminal Risk Management steps.

    The results from the Terminal Action Analysis will determine the cryptogram requested to the card in the 1st GEN AC.

2. **Card Action Analysis:** the 1st GEN AC is the response from the card based on the terminal's request. The card can respond with one of the following decisions based on the cryptogram requested by the 1st GEN AC command by the terminal.

    a. **AAC (Decline)**, card will respond with:
        i. AAC - Decline
    b. **ARQC (Online authorization),** card can respond with:
        i. ARQC – Online Issuer Authorization Required

ii. AAC - Decline

c. **TC (Approval),** card can respond with:
   i. Approved
   ii. ARQC – Online Authorization Required

The card will always make the same or more restrictive decision than the terminal. The decision of the card is indicated in the Cryptogram Information Data (CID) (Tag 9F27).

Requirements/Recommendations:

- The terminal must not use the kernel force online feature to force transactions online. If this feature is used, the transaction will be set indicating it as a suspicious transaction

12.11 Online Processing and External Authenticate

If the card responds with an ARQC, then the transaction will be sent online to the issuer for authorization.

The issuer will send back an Authorization Response Code (ARPC) that determines the decision on whether to authorize or reject certain transactions based on the issuer defined limits.

If the ARPC and the Application Interchange Profile (AIP) indicate the chip supports issuer authentication, then the Issuer Authentication Data (Tag 91) will be sent to the chip in the **External Authenticate** command.

If the AIP indicates that chip does not support issuer authentication, and the Issuer Authentication Data is present this indicates that the chip combined the issuer authentication function with the 2nd GEN AC command.

Requirements/Recommendations:

- If the chip does not support issuer authentication or if no Issuer Authentication Data is received, then the terminal must not execute the External Authenticate command.

12.12 Transaction Completion

- **2nd Generate Application Cryptogram:** The terminal sends a 2nd GEN AC command to the card requesting a final cryptogram. The EMV chip will respond to the 2nd GEN AC command based on the type of cryptogram requested:
  - 1. **AAC (Decline),** card must respond with:
    - AAC – Declined
  - **TC (Approval),** card may respond with either of the following:
    - TC – Approved
    - AAC – Declined, if the transaction was approved by the Issuer then a Reversal must be sent to the host

- **Issuer Script Processing** allows issuers to do management on the card (changing PIN, blocking a smartcard, unblocking an application, modifying offline limits).
  Tag 71 scripts will be executed before the 2nd GEN AC decision and Tag 72 scripts will be executed after the 2nd GEN AC completes. An issuer response will send either a Tag 71 or Tag 72 Issuer Scripts.
- **Card Removal Prompting:** When the transaction is completed, the cardholder should be prompted to remove their card before receipts are printed.

Requirements/Recommendations:

- Issuer Scripts sent in the issuer response must be executed.

12.13 EMV Credit and Debit Refund Transactions

EMV credit and debit transactions should be a FULL EMV online transactions; the refund transaction is submitted online for host approval to all payment schemes, including MDES (MasterCard Digital Enablement Service) for token transaction refunds

The mandate for a refund transaction be an online by Visa is effective starting October 2019 in the US. As for MasterCard, the same requirement is mandated effective starting April 2020

12.14 AFD and EMV Consideration (For Future Use)

In the petroleum industry pre-authorizations are performed prior to the pump being allowed to dispense. Pre-authorization transactions must contain the chip data that was sent to the issuer in the authorization request to generate the cryptogram.

Completions are sent as a follow up to the pre-auth where the final pump amount that will be billed to the cardholder is sent to the issuer. The completion message must also contain the same chip data, POS entry mode and settlement indicator as in the original pre-authorization.

Requirements/Recommendations:

- EMV transactions should always be sent as dual message/credit (Payment/Capture) requests.
- A recommended pre-authorization amount is $1.00.
- Merchants should always send in the pump shutoff / maximum pump amount for AFD transactions.
- If a merchant wishes to use AVS processing the transaction must be sent as a dual message/credit request with the final amount indicator set to force the transaction to a credit network.
- For all Brands, the CVM Limit is to be set to $0.
- PINless POS Debit is not supported for Automated Fuel Dispensers
- Signature CVM is supported on AFD solutions for Visa only.
- PIN Bypass is allowed on AFD in US region

12.15 Contactless Payments

Contactless payments are forms of payment that use radio-frequency identification (RFID) or near field communication (NFC) for making secure payments; compared with contact transactions, contactless payments are faster, more convenient, and most importantly more hygienic since it does not require the cardholder to directly touch the point of sale.

12.16 Contactless Magstripe vs Contactless EMV

Major card schemes including Amex, Discover, MasterCard and Visa have announced sunset dates for contactless magstripe support. Bank of America recommends not implementing payment solutions that support magstripe grade contactless transactions, but only EMV grade contactless transactions.

12.16.1 Terminal Compliance

Contactless kernel specifications are different for each card scheme. To get your level 3 contactless payment solution certified, the level 2 contactless kernel approval letter from each card scheme need to be obtained for your device.

12.16.2 Cardholder Verification

For card-based transactions, the contactless cardholder verification method (CVM) differs from contact in that the terminal checks the transaction amount against the CVM limit before deciding if CVM is required. When the transaction amount is below or equal to the CVM limit, No CVM is required for the transaction; if the transaction amount is above the CVM limit, a CVM is required for the transaction.

For mobile device (e.g., smartphones, smart watches, tablets, etc.) based transactions, consumer has the option to verify themselves by utilizing the native device authentications (e.g. fingerprint, pattern, facial recognition, etc.). This type of cardholder verification is referred to by the card schemes as the mobile CVM, consumer device cardholder verification method (CDCVM) or the on-device cardholder verification (ODCV). Since contactless kernel specification is different for each card scheme, the CDCVM process differs for each card scheme as well.

American Express

- Terminal Capabilities Tag 9F33 B2b8 need to be set to 1 to enable mobile CVM.
- Enhanced Contactless Reader Capabilities Tag 9F6E B1b4 (Expresspay Mobile) and B2b8 (Mobile CVM) must be set to 1 to enable mobile CVM.

Discover

- Terminal Transaction Qualifier Tag 9F66 B3b7 (Consumer Device CVM supported) should be set to 1 to enable CDCVM.

MasterCard

- MasterCard requires On-device Cardholder Verification (ODCV) to be supported for MasterCard and Maestro.
- ODCV support is not allowed for US Maestro.
- Kernel configuration Tag DF811B B1b6 should be set as 1 to indicate that ODCV is supported

Visa

- Terminal Transaction Qualifier Tag 9F66 B3b7 (Mobile functionality support) should be set to 1 to enable CDCVM.

12.17 Quick Chip

Quick Chip is a solution designed to reduce the perceived checkout time at POS where speed is critical to the merchant's business. Although different payment schemes have different names, Amex Quick Chip,

Discover Quick Chip, MasterCard M Chip Fast, and Visa Quick Chip, they all follow the same general principals.

12.17.1 Contact Quick Chip

Quick Chip retains the majority of standard EMV's security functionalities while remitting others that are less crucial for an online transaction. One thing to pay attention to is that offline transactions are not supported for Quick Chip. Compared with standard EMV, Quick Chip processing is different in the following aspects,

EMV Tag	Quick Chip	Standard EMV
9F02 Amount, Authorized	Constant Predefined placeholder amount	Variable Final transaction amount
8A (2nd GEN AC) Authorization Response Code	Constant Value = 'Z3'	Variable depending on the card/terminal decisions

For a contact Quick Chip transaction, the terminal uses the predefined placeholder amount for Tag 9F02 to generate ARQC for 1st GEN AC, then completes transaction by setting Tag 8A to 'Z3' to request AAC at 2nd GEN AC and prompts the customer to remove card. After final amount is known, the terminal sends authorization request with both the final amount and the ARQC generated with the placeholder amount 9F02. Note that the final transaction amount is different than the placeholder amount 9F02 used to generate ARQC.

Quick Chip creates a better user experience by removing the cardholder wait time for the final transaction amount. The payment terminal on the other hand still need to wait for the final transaction amount to be able to send the authorization request, and since the chip card is removed, functionalities such as issuer authentication and issuer scripting that happens at the EMV completion step are not compatible with Quick Chip.

12.17.2 Contactless Quick Chip/Contactless Pre-Tap

Contactless Quick Chip is also known as Contactless Pre-tap. It utilizes the same idea of the placeholder amount from contact Quick Chip. However, since the contactless CVM process involves checking the transaction amount against the CVM limit before deciding if a CVM is required, it creates a unique problem of which amount should be used to check against the CVM limit; different card schemes have different viewpoints.

American Express

- The final transaction amount should be used to check against the CVM limit. This means the terminal should not use the placeholder amount for CVM processing, and need to wait until the final amount is known to decide which CVM to use.
- The placeholder amount should exceed the CVM limit.

MasterCard

- The placeholder amount can be used to check against the CVM limit. The integrators should ensure that the placeholder amount is configured with a suitable value relative to the CVM limit.

- If the placeholder amount is greater than the CVM limit then a CVM will be requested for all contactless transactions. This is recommended if the typical transaction amount in the integrator's payment environment exceeds the CVM limit.
- If the placeholder amount is lower than the CVM limit, then No CVM will be requested for any contactless transaction. This is recommended if the transaction amount in the integrator's payment environment is highly unlikely to exceed the CVM limit.

Visa

- The placeholder amount can be used to check against the CVM limit if at the time of CVM processing the final amount is not known.
  - In this case the CVM limit should be set to $$0.00 which means that a CVM will be requested for all contactless transactions.
- The final transaction amount should be used to check against the CVM limit if at the time of CVM processing the final amount is known.

Requirements/Recommendations:

A payment solution cannot support both standard EMV and Quick Chip over the same interface at the same time.

Offline transactions are not allowed for Quick Chip or Contactless Pre-Tap.

There's no parity requirement for supporting Quick Chip over both contact and contactless interface; the integrator's payment solution may support Quick Chip over the contact interface and standard EMV over the contactless interface.

A payment solution that is certified for standard EMV can be deployed as Quick Chip after regression testing with the Bank's certification team, but a payment solution that is certified for Quick Chip can only be deployed as a Quick Chip solution.

12.17.3 Pre-Tap/Placeholder Requirements per brand

Brand	Requirements
VISA VISA quick Chip and Quick contactless implementation guide	• If the final amount is not yet known, then a proxy amount is sent to the EMV kernel for tag '9F02' (Amount, Authorized). The proxy amount can be any value consistent with the requirements of the merchant's processing environment. The proxy amount is not zero. The recommended proxy amount is 1 cent. This allows the card and EMV kernel interaction to begin without waiting for the final amount. • The amount used in the cryptogram generation should be the same as for contact Quick Chip, i.e. whichever amount contact Quick Chip uses, Quick Contactless should use as well. • For implementations that initiate chip processing when the final amount is not yet known, set the TTQ 'CVM required' bit (TTQ byte

Brand	Requirements
	2 bit 7) to 1b. If the final amount is lower than the VEPS limit, disregard the CVM requirements in the CTQ. If the final amount is higher than the VEPS limit, capture the CVM as required in the CTQ.
Discover Discover D-PAS: Discover Quick Chip Implementation Guide	**Transaction amount:** Before beginning a contactless Quick Chip transaction, the POS device determines the card transaction amount to be used: • If the actual transaction amount is known at the beginning of the transaction, the contactless transaction is completed using this amount • If the actual transaction amount is not yet entered in the POS device, a placeholder amount is used The card transaction amount that is sent to the card in the GET PROCESSING OPTIONS command can either be the actual card transaction amount or the placeholder amount **Risk Management:** Any risk management checks performed, including the POS device's decision whether to request a CVM, are based on the placeholder amount not the actual card transaction amount **Chargeback Right:** Merchants and Acquirers that choose a placeholder amount below the NO CVM limit should evaluate the potential impact on dispute rights Where a placeholder amount is used, it must be greater than zero.
Mastercard M/Chip Requirements For Contact and Contactless	M/Chip Fast M/Chip Fast is the Mastercard implementation of the EMV transaction flow specifically designed for environments where faster transaction times are particularly important. It allows an EMV transaction to be performed before the scanning of goods has been completed and the final transaction amount has been determined. An M/Chip Fast transaction is conducted based on a placeholder amount. The transaction is then authorized online once the final transaction amount is known. M/Chip Fast may be used for both contact and contactless transactions. M/Chip Fast has most benefit in environments where it may take some time before the final transaction amount is known (for example due to the scanning of goods in a multi-lane retail environment). It may also be used for merchants that wish to optimize the transaction in other environments, for example, Quick Service restaurants **Terminal Requirements:** • If the Terminal starts a transaction and activates the Reader when the final transaction amount is not yet known, it must use a non-zero Placeholder Amount. • The Placeholder Amount must not exceed the QPS/CVM limit if the Terminal wants to submit this transaction as a QPS transaction
Mastercard M/Chip Fast Technical Requirements	**Reader Requirements:** • If the final transaction amount is not known, the terminal shall implement a provisional transaction amount and populate Amount

Brand	Requirements
U.S. Market	authorized (Tag '9f02, Bit 55) [NW]/[ACQ] and use it for EMV processing purposes. The provisional transaction amount shall be greater the zero
AMEX American Express Quick Chip Technical Manual	• If the final transaction amount is not known, the terminal ***shall*** implement a provisional transaction amount and populate Amount, Authorized (Tag '9F02', Bit 55) [NW]/[ACQ] and use it for EMV processing purposes. The provisional transaction amount ***shall*** be greater than zero. • If PIN is the selected result of CVM processing, and if the terminal is using a provisional transaction amount, the terminal ***shall*** not display the provisional transaction amount to the Card Member on the PIN pad. Merchants that choose to implement Amex Quick Chip and the No Signature/No PIN program should take into account the following factors: A. **If the final transaction amount is not known when EMV processing begins**: • A provisional transaction amount shall be used for EMV processing purposes. • The provisional transaction amount shall not exceed the No Signature/No PIN threshold. • And the final transaction amount is over the No Signature/No PIN threshold, if a PIN capable card is presented and PIN was not performed, the Merchant may not qualify for Chip Card Lost/Stolen/Non-Received fraud liability shift. **B. If the final transaction amount is known when EMV processing begins:** • The final transaction amount shall be used for EMV processing purposes.

12.17.4 Device Type

This field is required to be sent in the transaction request for MasterCard when the value is present in tag 9F6E. it provides information about the device type used to identify mobile-initiated (m-commerce) or other EMV Contact, Magnetic stripe Contactless, or M/Chip Contactless transactions.

MasterCard defined code that indicates how the account information was obtained.

Device Type Code	Description
00 (Default)	Card
01	Removable secure element that is personalized for use with a mobile phone and controlled by the wireless service provider. Example: subscriber identity module (SIM), universal integrated circuit card (UICC)

02	Key fob
03	Watch
04	Mobile tag
05	Wristband
06	Mobile Phone case or sleeve
07	Mobile phone with a non-removable, secure element that is controlled by the wireless service provider, for example, code division multiple access (CDMA)
08	Removable secure element that is personalized for use with a mobile phone and not controlled by the wireless service provider; example: memory card
09	Mobile phone with a non-removable , secure element that is not controlled by the wireless service provider
10	Removable secure element that is personalized for use with a tablet or e-book and is controlled by the wireless service provider; example: subscriber identity module (SIM), universal integrated circuit card (UICC)
11	Tablet or e-book with a non-removable, secure element that is controlled by the wireless service provider
12	Removable secure element that is personalized for use with a tablet or e-book and is not controlled by the wireless service provider
13	Tablet or e-book with a non-removable, secure element that is not controlled by the wireless service provider

12.18 EMV Tags

The EMV data is in the tag-length-value format and includes chip card tags, terminal tags, and transaction detail tags.

The following tags contain sensitive card data and MUST NOT be included in the transaction request API load.

12.18.1 Sensitive EMV Tag

Tag	Description
56	Track 1 equivalent data
57	Track 2 equivalent data
5A	Application PAN
5F20	Cardholder name
5F24	Application expiration date
99	Transaction PIN
9F0B	Cardholder name (extended)
9F1F	Track 1 discretionary data
9F20	Track 2 discretionary data

12.18.2 Transaction Request EMV Tags

The following tags if provided by the chip card or the terminal should be sent in the transaction request.

Tag	**Name**	**Description**
82	Application Interchange Profile (AIP)	Indicates the capabilities of the card to support specific functions in the application
84	Dedicated File (DF) Name	Identifies the name of the DF as described in ISO/IEC 7816-4
95	Terminal Verification Results (TVR)	Status of the different functions as seen from the terminal
9A	Transaction Date	Local date that the transaction was authorized
9C	Transaction Type	Indicates the type of financial transaction
5F2A	Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217
5F34	Application PAN Sequence Number	Identifies and differentiates cards with the same PAN
9F02	Amount Authorized	Authorized amount of the transaction (excluding adjustments)
9F03	Amount Other - (For cashback if provided by the terminal)	Secondary amount associated with the transaction representing a cashback amount . it is required to be present by AMEX and zero fill if cashback is not present or supported; it is conditional for other brands

Tag	Name	Description
9F06	Application Identifier (AID)	Identifies the application as described in ISO/IEC 7816-5
9F07	Application Usage Control (AUC)	Indicates issuer's specified restrictions on the geographic usage and services allowed for the application
9F09	Terminal Application Version Number	Version number assigned by the payment system for the application
9F10	Issuer Application Data – (if provided by the card)	Contains proprietary application data for transmission to the issuer in an online transaction.
9F1A	Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166
9F1E	Interface Device (IFD) Serial Number	Unique and permanent serial number assigned to the IFD by the manufacturer
9F26	Application Cryptogram	Cryptogram returned by the ICC in response of the GENERATE AC command
9F27	Cryptogram information Data	Indicates the type of cryptogram and the actions to be performed by the terminal
9F33	Terminal Capabilities	Indicates the card data input, CVM, and security capabilities of the terminal
9F34	Card Verification Method (CVM) Results	Indicates the results of the last CVM performed
9F35	Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control
9F36	Application Transaction Counter (ATC) – If Received from the card	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)
9F37	Unpredictable Number (UN)	Value to provide variability and uniqueness to the generation of a cryptogram
9F41	Transaction Sequence Counter	Counter maintained by the terminal that is incremented by one for each transaction
9F53	Transaction Category Code	Indicates the type of transaction being processed
9F6E	Form Factor Indicator	May indicate the form factor of the consumer payment device or contain proprietary information from a third-party device
9F7C	Customer Exclusive Data	In U.S. contactless transactions, issuer proprietary info

Tag	Name	Description
C0 0C0B	Secondary PIN Block	Visa (C0) and Discover (0C0B) may allow cardholders to change PINs at the terminal. This is the encrypted PIN Block for the new PIN
DF3F	Storage Data	Storage data
9F0A	Application Selection Registered Proprietary Data	Application Selection Registered Proprietary Data
9F66	Terminal Transaction Qualifiers (TTQ)	Indicates reader capabilities, requirements, and preferences to the card. TTQ byte 2 bits 8-7 are transient values, and reset to zero at the beginning of the transaction. All other TTQ bits are static values, and not modified based on transaction conditions. TTQ byte 3 bit 7 shall be set by the acquirer-merchant to 1b
9F7C	Customer Exclusive Data (CED)	In U.S. contactless transactions, issuer proprietary info
DF38	Kernel Id	Kernel ID
DF86	Form factor	Form factor

12.18.3 Transaction Response EMV Tags

The following tags may be returned from the host.

Tag	Name	Description
8A	Authorization Response Code	Value generated by the authorization authority for an approved transaction
71	Issuer Script Template 1	Contains proprietary issuer data for transmission to the ICC before the second GENERATE AC command
72	Issuer Script Template 2	Contains proprietary issuer data for transmission to the ICC after the second GENERATE AC command
91	Issuer Authentication Data (IAD)	Data sent to the ICC for online issuer authentication
9F5B	Issuer Script Result	Present if scripts were sent by issuer in original response

13 EMV Parameter Files and Keys

Please contact your analyst for Certificate Authority Public Key (CAPK).

13.1 Test/Certification Configuration Parameters

EMV parameters are a set of values loaded into the terminal that define processing rules for EMV contact and contactless transactions. Each AID has its own set parameters and is tested during the certification. It is the integrator responsibility to manage the EMV parameters. Bank of America will work with the integrator to ensure the parameter values used during the certification and when the certified solution is deployed are accurate and up to date.

13.1.1 American Express Credit

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A00000002501
RID		A000000025
PIX		01
Application Version Number Primary	9F09	0001
Application version Number Secondary	9F09	-
Default AID Label		American Express
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	N/A
TAC – Default		AMEX test plan configuration
TAC – Denial		AMEX test plan configuration
TAC – Online		AMEX test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		AMEX test plan configuration
TAC – Denial		AMEX test plan configuration
TAC – Online		AMEX test plan configuration
TTQ	9F66	-
Floor Limit		$0.00
CVM Required Limit		$20.00 (recommended – ISV configuration)
Transaction Limit		99999.99.
Certificate Authority Public Key file (CAPK)		
CAPK format and a file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document		

American Express Contactless Dynamic Reader Limits Configuration

Contactless Limits	Amount Limit	Default DRL	DRL Set 6*	DRL Set 11*
Contactless Expresspay Floor Limit	0	12.00	4.00	1.00
Contactless Expresspay CVM Limit	20$0.00	1$0.00	2.00	2.00
Contactless Expresspay Transaction Limit	Null	15.00	7.00	3.00

There are three major limits involved in Amex contactless transactions:

- Reader Contactless floor limit - the amount limit at which online authorization is requested
- Reader CVM required limit - the amount limit at which cardholder verification is requested
- Reader Contactless transaction limit - the amount limit allowed for contactless transactions.

These limits are usually configured by Application Identifier (AID) inside the terminal. In addition, American Express allows an **optional** feature that supports **card-specific limits** which can be used instead of the terminal AID limits. This feature is called the *Expresspay Dynamic Reader Limits*.

Amex allows for flexibility of up to 16 sets of contactless reader limits by enabling the *Default Dynamic Reader Limits*. And the transaction process can be described as follows:

- If the terminal does not support *Default Dynamic Reader Limits*, it proceeds to normal processing of applying AID reader limits.
- If the terminal supports *Default Dynamic Reader Limits*, it proceeds to checking if the card supports *Dynamic Reader Limits*.
    - If the card does not support *Dynamic Reader Limits*, then the terminal proceeds to normal processing of applying AID reader limits.
    - If the card supports *Dynamic Reader Limits*, then the terminal proceeds to checking if a mutually supported *Dynamic Reader Limits Set* can be found within the maximum of 16 sets.
        - If there's no match, then normal AID reader limits are applied.
        - If there's a match, then the matching *Dynamic Reader Limits* are applied.

For more details on the dynamic reader limits, please refer to *Expresspay Terminal Specification (Expresspay 4.0.1)*.

Requirements/Recommendations:

Payment devices that are on earlier kernels may not support the Expresspay Dynamic Reader Limits feature. Before you implement your contactless Amex solution, consult with your terminal vendor to see if this feature is supported on your payment device.

13.1.2 American Express U.S. Common Debit

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A00000002504
RID		A000000025
PIX		04
Application Version Number Primary	9F09	0001
Application version Number Secondary	9F09	-
Default AID Label		American Express Debit
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	N/A
TAC – Default		AMEX test plan configuration
TAC – Denial		AMEX test plan configuration
TAC – Online		AMEX test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		AMEX test plan configuration
TAC – Denial		AMEX test plan configuration
TAC – Online		AMEX test plan configuration
TTQ	9F66	-
Floor Limit		$0.00
CVM Required Limit		50.00 (recommended – ISV configuration)
Transaction Limit		15.00
Certificate Authority Public Key file (CAPK)		
CAPK format and a file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document		

13.1.3 UnionPay

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A000000333010102
RID		A000000333
PIX		010102
Application Version Number Primary	9F09	0001
Application version Number Secondary	9F09	0001
Default AID Label		UnionPay Credit
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	-
TAC – Default		CRF test plan configuration
TAC – Denial		CRF test plan configuration
TAC – Online		CRF test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		-
TAC – Denial		-
TAC – Online		-
TTQ	9F66	-
Floor Limit		$0.00
CVM Required Limit		(recommended – ISV configuration)
Transaction Limit		99999.99 (recommended – ISV configuration)
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document		

13.1.4 Discover Credit

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000001523010
RID		A000000152
PIX		3010
Application Version Number Primary	9F09	0001
Application version Number Secondary	9F09	0001
Default AID Label		Discover Credit
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	-
TAC – Default		CRF test plan configuration
TAC – Denial		CRF test plan configuration
TAC – Online		CRF test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		-
TAC – Denial		-
TAC – Online		-
TTQ	9F66	-
Floor Limit		$0.00
CVM Required Limit		(recommended – ISV configuration)
Transaction Limit		99999.99 (no limit – ISV configuration)
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document.		

13.1.5 JCB

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000651010
RID		A000000065
PIX		1010
Application Version Number Primary	9F09	0200
Application version Number Secondary	9F09	0120
Default AID Label		JCB
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	-
TAC – Default		CRF test plan configuration
TAC – Denial		CRF test plan configuration
TAC – Online		CRF test plan configuration
Random Selection Threshold		$0.00
Random Selection Maximum Percentage		99
Random Selection Target Percentage		99
Allow Fallback		Y
Allow PIN Bypass		N
EMV Contactless		
TAC – Default		-
TAC – Denial		-
TAC – Online		-
TTQ		-
Floor Limit		$0.00
CVM Required Limit		10.00 (recommended – ISV configuration)
Transaction Limit		99999.99 (recommended – ISV configuration)
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document.		

13.1.6 MasterCard Credit

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000041010
RID		A000000004
PIX		1010
Application Version Number Primary	9F09	0002
Application version Number Secondary	9F09	-
Default AID Label		MasterCard Credit
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	9F02065F2A029A039C0195059F3704
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Floor Limit		1
CVM Required Limit		10.00 (MC recommendation)
Transaction Limit		No limit – TSE configuration - ODCVM
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document.		

13.1.7 MasterCard U.S. Maestro

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000042203
RID		A000000004
PIX		2203
Application Version Number Primary	9F09	0002
Application version Number Secondary	9F09	0002
Default AID Label		Debit MasterCard
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	9F02065F2A029A039C0195059F3704
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Floor Limit		$0.00
CVM Required Limit		50.00 (MC recommendation)
Transaction Limit		No limit – TSE configuration - ODCVM
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document.		

13.1.8 MasterCard Maestro

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000043060
RID		A000000004
PIX		3060
Application Version Number Primary	9F09	0002
Application version Number Secondary	9F09	0002
Default AID Label		Maestro
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	9F02065F2A029A039C0195059F3704
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Floor Limit		$0.00
CVM Required Limit		10$0.00 (MC recommendation)
Transaction Limit		No limit – TSE configuration - ODCVM
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document.		

13.1.9 Visa Credit

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000031010
RID		A000000003
PIX		1010
Application Version Number Primary	9F09	008C
Application version Number Secondary	9F09	0096
Default AID Label		Visa Credit
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	9F0206
TAC – Default		DC4000A800
TAC – Denial		0010000000
TAC – Online		DC4004F800
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
TTQ		B6804000
Floor Limit		$0.00
CVM Required Limit		25.00
Transaction Limit		No limit (ISV Configuration)
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document.		

13.1.10 Visa Interlink

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000033010
RID		A000000003
PIX		3010
Application Version Number Primary	9F09	008C
Application version Number Secondary	9F09	0096
Default AID Label		Interlink
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	9F0206
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		TSE test plan configuration
TAC – Denial		TSE test plan configuration
TAC – Online		TSE test plan configuration
TTQ		B6804000
Floor Limit		$0.00
CVM Required Limit		$0.00
Transaction Limit		No limit (ISV Configuration)
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document		

13.1.11 Visa U.S. Common Debit

Name	Tag	Value
EMV Contact		
Application Identifier (AID)	9F06	A0000000980840
RID		A000000003
PIX		0840
Application Version Number Primary	9F09	008C
Application version Number Secondary	9F09	0096
Default AID Label		Visa US Debit
Partial Name Selection		Y
Terminal Type	9F35	Terminal configuration
Terminal Capabilities	9F33	Terminal configuration
Additional Terminal Capabilities	9F40	Terminal Configuration
Terminal Country Code	9F1A	0840
Transaction Currency Code	5F2A	0840
Terminal Floor Limit	9F1B	$0.00
Transaction Currency Exponent	5F36	2
Default DDOL	9F49	9F3704
Default TDOL	97	9F0206
TAC – Default		DC4000A800
TAC – Denial		0010000000
TAC – Online		DC4004F800
Random Selection Threshold		1
Random Selection Maximum Percentage		1%
Random Selection Target Percentage		1%
Allow Fallback		Y
Allow PIN Bypass		Y
EMV Contactless		
TAC – Default		DC4000A800
TAC – Denial		0010000000
TAC – Online		DC4004F800
TTQ		B6804000
Floor Limit		$0.00
CVM Required Limit		25.00 (recommended – ISV configuration)
Transaction Limit		No limit (ISV Configuration)
Certificate Authority Public Key file (CAPK)		
CAPK format and file example are included in Appendix C. Your certification analyst will provide the test and live CAPK files in a separate document		

14 Reporting Guidelines

Reporting guidelines are useful to help clients identify any trends related to device, entry mode or terminal behavior. The following list are sample reports that are recommended for Bank of America clients.

14.1 EMV Parameter and Key Load Reports

Bank of America recommends certified EMV solutions be able to generate an EMV parameter files and key load reports. This will allow to verify the EMV parameters and key loaded into the terminal are the same as the ones that were certified.

At the end of the certification, the partner will be asked to produce an EMV parameter configuration and key load reports that will be kept on file.

14.1.1 EMV Parameter Report

EMV Parameter Report	
Merchant name	
MID (last 4)	XXXX1234
Report Date	XX/XX/XXXX
EMV Contact	
EMV Kernel Version	01.01.01
AID	A00000002501
RID	A000000025
PIX	01
App. Ver Pri.	0001
App Ver Sec.	-
Aid Label	American Express
Partial Name Selection	Y
Term Type	22
Term Capabilities	EOFBCB
Add Term Capabilities	F000F0A001
Term Country Code	0840
Currency Code	0840
Term Floor Limit	$0.00
Trans Currency Exp	2
Default DDOL	9F3704
Default TDOL	9F0206
TAC - Default	DC50FC9800
TAC - Denial	0010000000
TAC Online	DE00FC9800
Rand Selection Treshold	
Rand Selection Max %	
Rand Selection Target %	
Allow Fallback	
Allow Pin Bypass	
EMV Contactless	
TAC Default	
TAC Denial	
TAC Online	
Term Floor Limit	
CVM Required Limit	
Trans Limit	

14.1.2 EMV Key Load Report

CAPK Report	
Merchant name	
MID (last 4)	XXXX1234
Report Date	XX/XX/XXXX
RID	A000000025
Key Index	04
Exp Date	12312025
Modulus	AA94A8C6DAD24F9BA56A27C09 B01020819568B81A026BE9FD0A 3416CA9A71166ED5084ED91CED 47DD457DB7E6CBCD53E560BC5 DF48ABC380993B6D549F5196CF A77DFB20A0296188E969A2772E 8C4141665F8BB2516BA2C7B5FC 91F8DA04E8D512EB0F6411516F B86FC021CE7E969DA94D339379 09A53A57F907C40C22009DA753 2CB3BE509AE173B39AD6A01BA5 BB85
Exponent	03
Hash	A7266ABAE64B42A3668851191D 49856E17F8FBCD

14.2 EMV Transaction Reports

EMV Transaction Report prints out the final EMV data Tags per transaction. This is beneficial because it can help detect any EMV failures. Reports should be available for both approved and declined transactions.

EMV Transaction Report	
Merchant name	
MID	XXXX1234
Report Date	XX/XX/XXXX
EMV Contact	
5A PAN	XXXXXXXXXXXX1234
50 Application Label	Visa Credit
82 AIP	5C00
58 Dedicated File Name	A0000000031010
9A Transaction Date	YYMMDD
9F21 Transaction Time	HHMMSS
9C Transaction Type	00
5F34 PAN Seq Number	01
5F2A Tran Currency Code	840
9F02 Amount, authorized	000000001000 ($1$0.00)

9F03 Amount, Other	000000000000
9F08 ICC App Version Num	008C
9F09 Term App Version Num	008C
9F1A Term Country Code	840
9F33 Terminal Capabilities	EOFBCB
9F34 CVM Results	040302
9F35 Terminal Type	22
9F36 ATC	0197
9F37 Unpredictable Number	1234567890
9F0D IAC Denial	0010000000
9F0E IAC Online	F040009800
9F0F IAC Default	F040008800
TAC Denial	0010000000
TAC Online	DE00FC9800
TAC Default	DC50FC9800
1st Generation Application Cryptogram	
95 TVR	0000008000
9F10 Issuer Application Data	06010A03A40002
9F26 Application Cryptogram	1234567890ABCDEF
9F27 CID	80
2nd Generation Application Cryptogram	
91 Issuer Authentication Data	7A1416ECA2F20F7E3030
95 TVR	0000008000
9F26 Application Cryptogram	1234567890ABCDEF
9F27 CID	40
Final	
8A Auth Response Code	3030
9B TSI	F800

14.3 Fallback Reports

Fallback reports can help merchants discover if there is a high occurrence of fallback transactions and if it relates to a pin pad issue or possible fraud. Two types of fallback reports that are useful are Clerk technical fall back and PIN Pad technical fallback reports. According to the payment networks, a fallback rate of over 2% at one particular merchant location is indicative of a problem. The integrator and merchants should proactively implement a monitoring mechanism to detect fallback to avoid charge back or other compliance action by the networks.

14.3.1 Clerk Technical Fallback Reports

Clerk Fallback Report Sample			
Merchant Name			
MID (last 4): XXXXXXXX1234 Report Date XX/XX/XXXX			
Period: From XX/XX/XXXX XX:XX AM/PM To XX/XX/XXXX XX:XX AM/PM			
Threshold%: 5.0%			
Clerk	**Total Trans #**	**Fallback Trans #**	Fallback %
12345	124	16	13
56789	67	6	9
09876	**78**	4	5
Total	**269**	**24**	**9**

14.3.2 PIN Pad Technical Fallback

PIN Pad Technical Fallback reports are useful because they identify percentage of fallback per PIN Pad. This reporting alerts to particular devices and can help identify a faulty device. Below is an example of a PIN Pad Fallback report.

PIN Pad Fallback Report Sample			
Merchant Name			
MID: XXXXXXXX1234 Report Date XX/XX/XXXX			
Period: From XX/XX/XXXX XX:XX AM/PM To XX/XX/XXXX XX:XX AM/PM			
Threshold%: 5.0%			
PIN Pad	**Total Trans #**	**Fallback Trans #**	**Fallback %**
12345	256	54	21
56789	349	45	13
09876	459	67	14
Total	**1069**	**166**	**15**

14.4 POS Entry Mode Report

The POS Entry Mode report identifies how card information is being captured. This provides a view of the type of cards being used by cardholders and the cardholders preferred method of payment. This report can be configured for a particular TID (shown below) or can be developed at the location level. Below is an example of a POS Entry Mode report

POS Entry Mode Report Sample		
Merchant Name		
TID: 12345678 Report Date XX/XX/XXXX		
Period: XX/XX/XXXX XX:XX AM/PM XX/XX/XXXX XX:XXAM/PM		
Transactions: 1069		
Mode	**Transactions**	**% of Transactions**
Chip Read	693	65
Contactless	251	23
Swiped	96	9
Keyed	29	3
Total	**1069**	**166**

15 Card-On-File transaction Processing

A) Overview

The Payment Networks have a set of requirements for merchants/acquirers who store the cardholder payment information for future use, initiated either by the customer - Customer Initiated Transaction (CIT) or by the merchant - Merchant Initiated Transactions (MIT).
Transactions that use stored customer credentials are called Card-On-File (COF) transactions.
The Stored Credentials framework sets standards for the storage and subsequent use of stored customer credentials. By following the Stored Credentials framework, merchants are expected to:

- Gain greater visibility of transaction risk levels.
- Achieve higher authorization approval rates and completed sales.
- Improve the customer experience.
- Reduce customer complaints.
- Enables participation in the Real Time Visa Account Updater service.

All COF transactions start with customer-initiated transactions where customers elect to store their credentials for future use. COF can be either merchant or customer initiated for both the initial, as well as subsequent transactions.

B) Requirements

Merchants that offer stored credentials must:

- Disclose to cardholders how those credentials will be used.
- Obtain the cardholder's consent to store credentials – The merchant must obtain an explicit agreement from the cardholder to store their card information. This is considered the "Establishment of the Relationship" between the merchant and the cardholder.
- Notify cardholders when changes are made to stored credential terms of use.
- Inform the card issuer during an authorization that the payment credentials are now stored on file.
- Identify transactions that use stored credentials.

15.1 Initial Transactions (SALE/AUTH)

The following table shows the required Processing Information fields and values for initial transactions.

Initial Transactions	Visa, MC, Disc, Amex COF	Visa, Discover, Amex Recurring & Installment	MasterCard Recurring/Subscription, Standing Order & Installment
Type	Customer or Merchant	Customer or Merchant	Customer or Merchant
StoredCredentialUsed	false	false	false
CredentialStoreOnFile	true	true	true
CommerceIndicator	Internet	Recurring or Install	Recurring or Install
Reason[1]	n/a	n/a	7,8, or 9
Capture	true or false	true or false	true or false

[1] Reason Values:
Subscription (fixed amount at fixed interval) = 7
Standing Order (variable amount at fixed interval) = 8
Installment = 9

15.1.1 Sample initial transaction log for Card-On-File (SALE/AUTH) for Visa, MasterCard, Discover & Amex

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "securityCode": "XXX",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": CUSTOMER or MERCHANT,
        "storedCredentialUsed": false,
        "credentialStoredOnFile": true,
        }
      }
    },
    "commerceIndicator": "internet",
    "capture": TRUE or FALSE
}
```

15.1.2 Sample initial transaction log for Recurring & Instalment – Visa, Discover, Amex

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "securityCode": "XXX",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": CUSTOMER or MERCHANT,
        "storedCredentialUsed": false,
        "credentialStoredOnFile": true,
        }
      }
    },
    "commerceIndicator": RECURRING or INSTALL,
    "capture": TRUE or FALSE
}
```

15.1.3 Sample initial transaction log for Recurring, Subscription/Standing Order & Instalment for Mastercard

Note: Subscription (fixed amount at fixed interval) = 7
Standing Order (variable amount at fixed interval) = 8
Instalment = 9

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "securityCode": "XXX"
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE or FALSE,
      "initiator": {
        "type": CUSTOMER or MERCHANT,
        "credentialStoredOnFile": true,
        "storedCredentialUsed": false
        "merchantInitiatedTransaction": {
        "reason": 7, 8, or 9
      }
    },
    "commerceIndicator": RECURRING or INSTALL,
    "capture": TRUE or FALSE
  }
}
```

15.2 Subsequent Transactions (SALE/AUTH)

The following table shows the required Processing Information fields and values for subsequent transactions.

Subsequent Transactions	Visa, MC, Disc, Amex COF	Visa Recurring & Installment	MC - Recurring, Subscription/Standing Order & Installment	AMEX Recurring	AMEX Installment	Discover Recurring & Installment
Type	Customer or Merchant	Merchant	Merchant	Recurring	Merchant	Merchant
StoredCredentialUsed	true	true	true	true	true	true
CredentialStoreOnFile	false	false	false	false	false	false
MIT - PreviousTransactionid	ID Number	ID Number	ID Number	ID Number	ID Number	ID Number
CommerceIndicator	Internet	Recurring or Install	Recurring or Install	Recurring	Install	Recurring or Install
OriginalAuthorizedAmount (Discover Only)	Amount	n/a	n/a	n/a	n/a	Amount
Reason [1]	n/a	n/a	7,8, or 9	n/a	n/a	n/a
Capture	True or False	True or False	True or False	True or False	True or False	True or False

[1] Reason Values:
Subscription = 7
Standing Order = 8
Installment = 9

15.2.1 Sample subsequent transaction log for Card-On-File (SALE/AUTH) for Visa, MasterCard, Discover & Amex

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": CUSTOMER or MERCHANT,
        "storedCredentialUsed": true,
        "credentialStoredOnFile": false,
        "merchantInitiatedTransaction": {
          "previousTransactionId": "XXXXXXXXXXXXXX"
        }
      }
    },
    "commerceIndicator": "internet",
    "capture": TRUE or FALSE
  }
}
```

15.2.2 Sample subsequent transaction log for Recurring & Installment for Visa


```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": merchant,
        "storedCredentialUsed": true,
        "credentialStoredOnFile": false,
        "merchantInitiatedTransaction": {
          "previousTransactionId": "XXXXXXXXXXXXXX"
        }
      }
    },
    "commerceIndicator": RECURRING or INSTALL,
    "capture": TRUE or FALSE
  }
}
```

15.2.3 Sample subsequent transaction log for Subscription/Standing Order & Installment for Mastercard

Note: Subscription = 7
Standing Order = 8
Installment = 9

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "securityCode": "XXX"
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": merchant,
        "credentialStoredOnFile": false,
        "storedCredentialUsed": true
        "merchantInitiatedTransaction": {
        "previousTransactionId": "XXXXXXXXXXXXXX",
          "reason": 7, 8, or 9
      }
    },
    "commerceIndicator": RECURRING or INSTALL,
    "capture": TRUE or FALSE
  }
```

```
}
```

15.2.4 Sample subsequent transaction log for Recurring - American Express

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": merchant,
        "storedCredentialUsed": true,
        "credentialStoredOnFile": false,
        "merchantInitiatedTransaction": {
          "previousTransactionId": "XXXXXXXXXXXXXX"
        }
      }
    },
    "commerceIndicator": "recurring",
    "capture": TRUE or FALSE
  }
}
```

15.2.5 Sample subsequent transaction log for Installment - American Express

```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": merchant,
        "storedCredentialUsed": true,
        "credentialStoredOnFile": false,
        "merchantInitiatedTransaction": {
          "previousTransactionId": "XXXXXXXXXXXXXX"
        }
      }
    },
    "commerceIndicator": " install",
    "capture": TRUE or FALSE
  },
 "installmentInformation": {
  "sequence": "2",
THIS VALUE INDICATES THE CURRENT TRANSACTION BEING SENT IN THE SEQUENCE.
  "totalCount": "03"
```

THIS VALUE REPRESENTS HOW MANY TOTAL INSTALLMENT TRANSACTIONS ARE SCHEDULED.
NOTE: THIS VALUE SHOULD ALWAYS BE TWO DIGITS AS INDICATED.
  }
}

15.2.6 Sample subsequent transaction log for Recurring & Installment – Discover


```
{
  "clientReferenceInformation": {
    "code": "XXXXXXXXXXXX",
    "partner": {
      "solutionId": "XXXXXXXX"
    }
  },
  "orderInformation": {
    "billTo": {
      "firstName": "Bofa",
      "lastName": "Tester",
      "address1": "400",
      "locality": "Atlanta",
      "administrativeArea": "GA",
      "postalCode": "40000",
      "country": "US",
      "email": "example@bofa.com",
      "phoneNumber": "888-555-1234"
    },
    "amountDetails": {
      "totalAmount": "$$.$$",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "card": {
      "number": "xxxx",
      "expirationMonth": "12",
      "expirationYear": "2030",
      "type": "XXX",
    }
  },
  "processingInformation": {
    "authorizationOptions": {
      "partialAuthIndicator": TRUE OR FALSE,
      "initiator": {
        "type": merchant,
        "storedCredentialUsed": true,
        "credentialStoredOnFile": false,
        "merchantInitiatedTransaction": {
          "previousTransactionId": "XXXXXXXXXXXXXX"
          "originalAuthorizedAmount": "$$.$$",
        }
      }
    },
    "commerceIndicator": RECURRING or INSTALL,
    "capture": TRUE or FALSE
  }
}
```

16 Fraud Management with Device Fingerprinting

Fraud Management is a Card Not Present (CNP) fraud solution provided to all e-Commerce merchants as part of the Bank of America Gateway features and functionality. Fraud Management evaluates CNP transactions during pre-authorization using merchant reference lists, rules, and a machine learning model risk score. Fraud Management also evaluates a transaction a second time during post authorization for AVS and CVV rules. Optional rules configurations within Fraud Management supports the following outcomes, presented in order of precedence:

1. Reject
    a. Pre-authorization – stops the transaction prior to the authorization attempt.
    b. Post-authorization – based on applicable rule logic tied to the authorization responses (example – partial AVS match).
    Fraud Management contains an optional preference setting to send automatic authorization reversals when a Reject trigger occurs post-authorization.
2. Review – A transaction is pended for manual review. While a pre-authorization Review outcome does not circumvent the authorization call, in a sale scenario (authorization + capture), the capture action flag is not maintained, merchants may trigger a capture manually or automatically as part of the review process if when a transaction is approved. It should not be assumed that an accepted transaction is also captured, since auth-only transactions follow the same review flow. See more on the review process and outcomes below.
3. Accept – An 'Accept' outcome refers to a scenario where no Reject or Review outcomes were triggered by the evaluation of the transaction. In this scenario, Fraud Management will not interfere with the payment processing.
4. Monitor – This is an internal outcome for reporting purposes only. If a transaction triggers a rule configured with a Monitor outcome, the payment is processed the same as an 'Accept' outcome flow.

A given transaction may trigger multiple rules with different outcomes (for example, a risk score in the Review outcome range set by the merchant and Reject list match). In this case, Fraud Management will affect a single (pre-authorization) Reject outcome as per the order of precedence above. This outcome is reflected in the 'status' field of the payment call response.

Contact your Solutions Engineer to obtain the full Fraud Management with Device Fingerprinting configuration and implementation guide.

16.1 Fraud Management with Device Fingerprinting Workflow

16.1.1 Website Implementation

You can deploy device fingerprinting by configuring your website as described below. To ensure your customers' privacy, fingerprints are encoded as soon as they are received. Fingerprints persist for approximately 24 hours. This interval begins when the customer opens the HTML page with the tags, and it ends when the transaction request is sent. Add the fingerprinting code to your request as early in the transaction process as soon as possible.

- Fingerprinting does **not** work when the adblockers are running in the browser
- Device fingerprinting stops working when the IP address of the domain name changes. To avoid interruptions in device fingerprinting, use domain names instead of using IP addresses and relying on domain name resolution.

16.1.2 Adding the Fingerprinting Code to your website

The profiling tag specifies these parameters:

- <***org ID***> (mandatory): to obtain this value, contact your sales or support representative and specify whether it is for testing or production.
- <***merchant ID***> (mandatory): your unique merchant ID.
- <***session ID***> (mandatory): A session ID must be a unique identifier for the transaction, such as an order number. It can contain lowercase and uppercase English letters, digits, hyphens (-), and underscores (_). The maximum length is 88 characters. The session ID must be unique for each transaction and for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID. Do not use the same uppercase and lowercase letters to indicate different session IDs.

The session ID must be unique for each page load regardless of an individual's web session ID. If a user navigates to a profiled page and is assigned a web session, navigates away from the profiled page, then navigates back to the profiled page, the generated session ID should be different and unique. You may use a web session ID, but it is preferable to use an application GUID (Globally Unique Identifier). This measure ensures that a unique ID is generated every time the page is loaded, even if it is the same user reloading the page.

- ***Custom Profiling Domain*** (optional): domain that serves the JavaScript tag. The default is `h.online-metrix.net`. As an alternative, you can implement Enhanced Profiling so that all profiling requests are made to a domain that is secured by your SSL/TLS digital certificates.

Be sure to copy all characters correctly and to omit the angle brackets (< >) when substituting your values for the variables.

16.1.3 Supported Tag Deployments

Two methods are available to deploy the profiling tag as described in the "Tag Placement" section. To allow device profiling time to complete, ensure that 3 to 5 seconds elapse between the execution of the profiling code and when your customers submit their orders.

16.1.3.1 Tag Placement

Place the basic <script> **tag in the** <head> **tag for optimal performance for either method**. **For the basic** <script> **tag with** <noscript> **tag method, place the** <noscript> **tag in the** <body> **tag, as shown in Example 1**. **Do not place the** <noscript> **tag in the** <head> **tag because it contains an** <iframe> **tag**. **Placing iframes in the head tag violates W3C validation and might cause problems**

- **JavaScript Code**

```
<head>
       <script type="text/javascript" src="https://h.online-metrix.net/fp/
tags.js?org_id=<org ID>&session_id=<merchant ID><session ID>"></
script>
</head>
<body>
       <noscript>
<iframe style="width: 100px; height: 100px; border: 0; position:
absolute; top: -5000px;" src="https://h.online-metrix.net/fp/tags?org_
id=<org ID>&session_id=<merchant ID><session ID>"></iframe>
</noscript>
```

```
</body>
```

- **Basic <script> Tag with <noscript> Tag (Recommended)**

This deployment method includes a basic <script> tag, which loads Javascript resource tags.js, as well as an additional <noscript> tag. Using the <noscript> tag ensures that profiling occurs, even if JavaScript is disabled.

Example 1 Basic <script> Tag with <noscript> Tag

```
<head>
        <script type="text/javascript" src="https://h.online-metrix.net/fp/
tags.js?org_id=sample_orgID&session_id=sample_merchantIDsample_ sessionID"></script>
</head>
<body>
        <noscript>
<iframe style="width: 100px; height: 100px; border: 0; position: absolute; top: -5000px;"
src="https://h.online-metrix.net/fp/tags?org_
id=sample_orgID&session_id=sample_merchantIDsample_sessionID"></iframe>
</noscript>
</body>
```

- **Basic <script> Tag without <noscript> Tag**

This deployment method includes a single <script>tag that loads JavaScript resource tags.js. If JavaScript is disabled, this tag does not load, and profiling does not occur.

Example 2 Basic <script> Tag without <noscript> Tag

```
<head>
        <script type="text/javascript" src="https://h.online-
metrix.net/fp/
tags.js?org_id=sample_orgID&session_id=sample_merchantIDsample_
sessionID"></script>
</head>
```

16.1.4 The Review Process

When a Review outcome is triggered during pre-authorization, the authorization call continues, and the merchant is required to complete a manual review of the pended order. When merchants access a transaction from the Review queue in Fraud Management, they can either approve or reject the transaction.

While Fraud Management is available for merchants using the Bank of America merchant portal, the merchant plug-in must support the following workflows:

1. When Fraud Management rejects a transaction pre-authorization, the transaction may appear as a rejected transaction (if the plug-in shows all transactions) or be absent from the orders screen (if the plug-in only presents valid orders).
2. When Fraud Management rejects a transaction post-authorization, the transaction may appear as a rejected transaction (if the plug-in shows all transactions) or be absent from the orders screen (if the plug-in only presents valid orders).

3. When Fraud Management pends a transaction for Review, indicated in the merchant plug-in UI that the order in question requires manual risk review in the Bank of America merchant portal.
4. Transactions that are in a Review status may not be settled or auth-reversed using the merchant plug-in.
5. The merchant plug-in is required to periodically retrieve the Conversion Detail Report to update Review decisions on previously pended transactions and reflect their status in the UI. For the best merchant experience, it is recommended to automatically run the service every 2 minutes. Developers may choose to run the Order Conversion Report in intervals of up to 15 minutes, but such long intervals may result with more noticeable latency and thus degrade the merchant experience.
    a. A transaction in Review status that is subsequently approved should not assumed to be captured.
    b. A transaction that was pended for Review and subsequently rejected should not be assumed to have been auth-reversed.

Notes  A Sale or Auth+capture scenario that is pended by FME will drop the capture, and must be manually captured for settlement when accepted, or manually reversed when rejected

16.1.5 Required fields for CNP transactions:

1. billTo.email
2. billTo.firstname
3. billTo.lastname
4. billTo.street1
5. billTo.city
6. billTo.country
7. billTo.postalCode
8. billTo.administrativeArea (US and Canada only, refers to states, territories, or provinces)
9. billTo.phoneNumber

Different use cases require different subsets of the full set of possible fields. Generally, it is best to send all available data elements according the API Specification . Please refer below to a basic event example and a basic event with a shipping address device information object.

16.1.6 Basic Ecommerce event:


```
{
 "clientReferenceInformation": {
  "code": "_Eh_FE_01"
 },
 "paymentInformation": {
  "card": {
   "number": "4111111111111111",
   "expirationMonth": "11",
   "expirationYear": "2025"
  }
 },
 "orderInformation": {
  "amountDetails": {
   "totalAmount": "10",
   "currency": "USD"
  },
  "billTo": {
   "firstName": "JSON",
   "lastName": "RTS",
   "address1": "201 S. Division St._1",
   "locality": "Foster City",
   "administrativeArea": "CA",
   "postalCode": "94404",
   "country": "US",
   "email": "beforeauth@testurl.com",
   "phoneNumber": "6504327113"
  }
 }
}
```

16.1.7 Basic eCommerce sample including shipping and device information


```
{
 "clientReferenceInformation": {
  "code": "54323007"
 },
 "paymentInformation": {
  "card": {
   "number": "4444444444444448",
   "expirationMonth": "12",
   "expirationYear": "2020"
  }
 },
 "orderInformation": {
  "amountDetails": {
   "totalAmount": "144.14",
   "currency": "USD"
  },
  "billTo": {
   "firstName": "James",
   "lastName": "Smith",
   "address1": "96, powers street",
   "locality": "Clearwater milford",
   "administrativeArea": "NH",
   "postalCode": "03055",
   "country": "US",
   "email": "test@visa.com",
   "phoneNumber": "7606160717"
  },
  "shipTo": {
   "firstName": "James",
   "lastName": "Smith",
   "address1": "96, powers street",
   "locality": "Clearwater milford",
   "administrativeArea": "KA",
   "postalCode": "560056",
   "country": "IN",
   "phoneNumber": "7606160717"
  },
    "deviceInformation": {
   "hostName": "host.com",
   "ipAddress": "64.124.61.215",
   "userAgent": "Chrome",
   "httpBrowserEmail": "xyz@gmail.com"
  }
}
```

16.1.8 Basic Response (no Reject / Review rules triggering)


```
{
 "_links": {
  "authReversal": {
   "method": "POST",
   "href": "/pts/v2/payments/647382718107669090400 4/reversals"
  },
  "self": {
   "method": "GET",
   "href": "/pts/v2/payments/64738271810766909040 04"
  },
  "capture": {
   "method": "POST",
   "href": "/pts/v2/payments/647382718107669090400 4/captures"
  }
 },
 "clientReferenceInformation": {
  "code": "TSYS_Eh_FE_01"
 },
 "id": "6473827181076690904004",
 "orderInformation": {
  "amountDetails": {
   "authorizedAmount": "1$0.00",
   "currency": "USD"
  }
 },
 "paymentAccountInformation": {
  "card": {
   "type": "001"
  }
 },
 "paymentInformation": {
  "tokenizedCard": {
   "type": "001"
  },
  "card": {
   "type": "001"
  }
 },
 "pointOfSaleInformation": {
  "terminalId": "111111"
 },
 "processorInformation": {
  "approvalCode": "888888",
  "networkTransactionId": "123456789619999",
  "transactionId": "123456789619999",
  "responseCode": "100",
  "avs": {
   "code": "X",
   "codeRaw": "I1"
  }
 },
 "reconciliationId": "72236390W0RR5HWB",
 "status": "AUTHORIZED",
```

```
 "submitTimeUtc": "2022-03-15T22:18:38Z"
}
```

16.1.9 Basic Response (Review outcome triggered)


```
{
  "_links": {
    "authReversal": {
      "method": "POST",
      "href": "/pts/v2/payments/661880296119618980374 9/reversals"
    },
    "self": {
      "method": "GET",
      "href": "/pts/v2/payments/661880296119618980374 9"
    },
    "capture": {
      "method": "POST",
      "href": "/pts/v2/payments/661880296119618980374 9/captures"
    }
  },
  "clientReferenceInformation": {
    "code": "83689156",
    "partner": {
      "solutionId": "MYE93851"
    }
  },
  "consumerAuthenticationInformation": {
    "token":
"Axj/7wSTZs5X0UlyeOTlABUYyZNGTFuwYt3DhqmlQg6S5QFNKhB0ly6QNk9EYS8G3/2LirQYzsC8mzZyvopLk8cnKAAAyR7R"
  },
  "errorInformation": {
    "reason": "DECISION_PROFILE_REVIEW",
    "message": "The order is marked for review by Decision Manager"
  },
  "id": "XXXX",
  "orderInformation": {
    "amountDetails": {
      "authorizedAmount": "47.30",
      "currency": "USD"
    }
  },
  "paymentInformation": {
    "accountFeatures": {
      "category": "A"
    }
  },
  "processorInformation": {
    "approvalCode": "000066",
    "cardVerification": {
      "resultCodeRaw": "N",
      "resultCode": "N"
    },
    "networkTransactionId": "752242626961310",
    "retrievalReferenceNumber": "224217017885",
    "transactionId": "752242626961310",
    "responseCode": "00",
    "avs": {
      "code": "N",
```

```
        "codeRaw": "N"
      }
    },
    "reconciliationId": "224217017885",
    "riskInformation": {
      "localTime": "13:24:56",
      "score": {
        "result": "0",
        "factorCodes": ["H", "P"],
        "modelUsed": "default"
      },
      "infoCodes": {
        "address": ["UNV-ADDR"],
        "phone": ["RISK-PH", "UNV-OC"],
        "globalVelocity": ["VEL-ADDR", "VEL-NAME"],
        "suspicious": ["MUL-EM", "UNV-BIN"],
        "identityChange": ["ID-X-HPOS", "MORPH-C"]
      },
      "profile": {
        "earlyDecision": "ACCEPT",
        "destinationQueue": "Review Queue",
        "name": "Standard mid-market profile",
        "selectorRule": "Default Active Profile"
      },
      "rules": [{
          "decision": "REVIEW",
          "name": "CVV Mismatch",
          "executionTiming": "POST_AUTH"
        }
      ],
      "casePriority": "3"
    },
    "status": "AUTHORIZED_PENDING_REVIEW",
    "submitTimeUtc": "2022-08-30T17:24:56Z"
}
```

16.2 Interpreting the Response

The status field may contain any of the below flags:

- AUTHORIZED
- PARTIAL_AUTHORIZED
- AUTHORIZED_PENDING_REVIEW
- AUTHORIZED_RISK_DECLINED
- PENDING_AUTHENTICATION
- PENDING_REVIEW
- DECLINED
- INVALID_REQUEST

Click here for additional information on the Fraud Management response

Please note that AUTHORIZED_PENDING_REVIEW is a status flag used in two mutually exclusive scenarios:

1. When a Review outcome is triggered by Fraud Management.
2. When a merchant that does not have a Fraud Management subscription (for example, a Card Present only MID) receives a soft decline response from the issuer.

When Fraud Management is enabled on a given MID, soft decline are handled by the post-authorization rules that are controlled by the merchant. In other words, even if a merchant decides to turn all the rules off, a soft decline an AUTHORIZED_PENDING_REVIEW flag is not possible since disabling the post-authorization rules implicitly sets all soft decline scenarios to ACCEPT. As a result, an AUTHORIZED_PENDING_REVIEW flag returned for a MID with Fraud Management always means that a rule set to Review has triggered, and in the opposite scenario the same flag would indicate a soft decline for a MID without Fraud Management.

The functional requirements and user stories regarding the Review flow in this section (see The Review Process above) only pertain to merchants with Fraud Management. These requirements do not apply to MIDs without Fraud Management (Card Present only, for example). Merchants 'review' soft declines by making a capture of authorization decision, meaning that such scenarios the ability to capture and auth-reverse should be exposed. The two use cases are distinguishable from the API response in a manner that does not require positive knowledge of whether Fraud Management is active by evaluating the errorInformation object:

16.3 Fraud Management Review outcome

16.3.1 General Decline

```
...
  },
  "errorInformation": {
    "reason": "DECISION_PROFILE_REVIEW",
    "message": "The order is marked for review by Decision Manager"
  },
```

...

16.3.2 Soft Decline

any other permutation of the object, for example:

```
...
   },
   "errorInformation": {
      "reason": "CV_FAILED",
      "message": "Soft Decline - The authorization request was approved by the issuing bank but declined by CyberSource because it did not pass the card verification number (CVN) check."
   },
...
```

16.4 Additional Functionality

16.4.1 Device fingerprinting

Fraud Management supports end point device data collection for the purpose of device ID generation by Threatmetrix. All ISV partners are **required** to implement the Threatmetrix SDK to enable this functionality as part of their Fraud Management integration.

The TM SDK is only for mobile devices, iOS & Android. The only required implementation is running the java collectors on the ISV's HPP

Please reach out to your Bank of America Integrated Payments point of contact for more information and developer resources.

16.4.2 EMV 3DSecure

Bank of America is partnering with Cardinal Commerce (a Visa company) to offer 3DSecure 2.x to all ecommerce merchants in the US. It is **recommended** that ISV partners include this functionality in their integration or as part of their integration roadmap. Please reach out to your Bank of America Integrated Payments point of contact for more information on availability and developer resources.

16.5 Order conversion Report

This report shows the results of the rule evaluation. It is available in HTML and XLS formats. You can choose a search date and time interval ranging from the past hour to the past month, or you can choose a custom range.

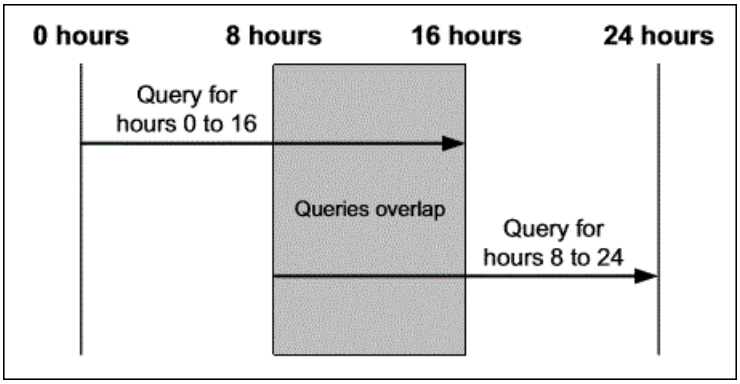
16.5.1 Order Conversion Detail Report (On-Demand)

The On-Demand Conversion Detail Report can help you verify that orders are reviewed and processed on time. For instance, you may have multiple fulfillment cycles during the day and offer same-day shipping for orders received before a certain time.

You can program the on-demand query to run automatically or request it as needed. You can request orders for the past 24 hours.

Because the query is passive, you can use it more than once with the same set of data. However, ensure that you only count converted orders once. The example below shows two queries for the same 24-hour period and how they overlap. The first query scans the immediate past 16 hours, but another query scans the past 8 to 24 hours.

A query Example:



16.5.2 View the Conversion Detail Report (On-Demand)

The Conversion Detail Report contains details of transactions for a merchant. You can download the report using REST.

1. Your client application must send an HTTP GET message to the report server. The default format for responses is JSON, but some reports can also return CSV or XML. You can set the response to return CSV or XML in the request header by setting the Accept value to either application/xml or text/csv
2. Format the URL as follows:
   https://<url_prefix>/reporting/v3/conversion-details&startTime={startTime}&endTime={endTime}&organizationId={organizationId}
3. Send the required On-Demand Conversion Detail Report URL Values:
   < url_prefix> **(Required)**
   Name of the server from which to download the report. Use one of these values:
   Production: api.merchant-services.bankofamerica.com
   Test: apitest.merchant-services.bankofamerica.com
   < startTime> **(Required)**
   Report start date to search on in ISO 8601 format.
   Example: 2016-11-22T12:00:0$0.000Z
   < endTime> **(Required)**
   Report end date to search on in ISO 8601 format.
   Example: 2016-11-22T12:00:0$0.000Z
   < organizationId> **(Optional)**
   The organization ID under which the report is subscribed. This can be the merchant ID, account ID, or reseller ID.
4. This call can return one of these HTTP status codes:
   200: Ok.
   400: Invalid request.
   404: Report not found, or no transactions are available

16.5.3 JSON Example of Conversion Detail Report (On-Demand)

This example shows the conversion of six orders originally marked for review. After being reviewed, the first orders were accepted but the last one was rejected.


```
{
        "organizationId": "testMerchantId",
        "startTime": "2022-07-13T00:00:0$0.000Z",
        "endTime": "2022-07-13T23:59:59.000Z",
        -"conversionDetails": [
        -{
                "merchantReferenceNumber": "1234567890",
                "conversionTime": "2022-07-13T06:43:05.000Z",
                "requestId": "123456789012345678 9012"
                "originalDecision": "REVIEW",
                "newDecision": "ACCEPT",
                "reviewer": "Reviewer1",
                "reviewerComments": null,
                "queue": "Review Queue",
                "profile": "Test Profile",
                        + "notes":
                                [ {"time":"2022-07-13T06:43:05.000Z","comments":"Sample
                                comments.","requestId":"123456789012345678 9012","addedB
                                y":"Reviewer1"}]

                "merchantReferenceNumber": "1234567890",

                "conversionTime": "2022-07-13T06:47:54.000Z",

                "requestId": "123456789012345678 9012"

                "originalDecision": "REVIEW",

                "newDecision": "ACCEPT",

                "reviewer": "Reviewer1",

                "reviewerComments": null,

                "queue": "Review Queue",

                 "profile": "High Risk Profile",

                        + "notes":

                                [ {"time":"2022-07-13T06:47:54.000Z","comments":"Verified order.",
                                "requestId":"123456789012345678 9012","addedBy":"Reviewer1"}]

        "merchantReferenceNumber": "1234567890",

         "conversionTime": "2022-07-13T07:46:42.000Z",
```

"requestId": "123456789012345678901 2",

"originalDecision": "REVIEW",

"newDecision": "ACCEPT",

"reviewer": "Reviewer2",

"reviewerComments": null,

"queue": "Review Queue",

"profile": "Low Risk Profile",

+ "notes":

[{"time":"2022-07-13T07:35:22.000Z","comments":"Verified order.","requestId":"123456789012345678901 2","addedBy":"Reviewer 2"}]

"merchantReferenceNumber": "1234567890",

"conversionTime": "2022-07-13T07:48:59.000Z",

"requestId": "123456789012345678901 2",

"originalDecision": "REVIEW",

"newDecision": "ACCEPT",

"reviewer": "Reviewer3",

"reviewerComments": null,

"queue": "Review Queue",

"profile": "Low Risk Profile",

+ "notes":

"merchantReferenceNumber": "1234567890",

"conversionTime": "2022-07-13T07:49:25.000Z",

"requestId": "123456789012345678901 2"

"originalDecision": "REVIEW",

"newDecision": "ACCEPT",

"reviewer": "Reviewer4",

"reviewerComments": "White pages: shipping address and name match.",

"queue": "Review Queue",

```
"profile": "High Risk Profile",
                + "notes":
                    [ {"time":"2022-07-13T07:30:47.000Z","comments":"Verified order.",
                    "requestId":"123456789012345678901 2","addedBy":"Reviewer4"}]
"merchantReferenceNumber": "1234567890",
"conversionTime": "2022-07-13T07:49:2$0.000Z",
"requestId": "123456789012345678901 2"
"originalDecision": "REVIEW",
"newDecision": "REJECT",
"reviewer": "Reviewer3",
"reviewerComments": null,
"queue": "Review Queue",
"profile": "Low Risk Profile",
                + "notes":
                    [ {"time":"2022-07-13T07:30:47.000Z","comments":"Order mistyped.",
                    "requestId":"123456789012345678901 2","addedBy":"Reviewer3"}]
        }
      ]
 }
```

16.6 Receipt Requirements and Receipt Generation

A Merchant must provide a transaction receipt to the cardholder upon completion of the transaction as follows:

- For a card present transaction, the merchant must offer a paper transaction receipt unless the cardholder agrees to an electronic transaction receipt or choose not to have a receipt.
- For an Electronic Commerce transaction or mail/phone order transaction, or a transaction that occurs at a contactless only acceptance device, the merchant may choose to offer either a paper or an electronic receipt.

During the certification the integrator provides sample receipts that meet the Payment Networks, Reg-E and the Bank of America receipt requirements. We understand sometimes, the Payment Application or the Gateway being certified is not the endpoint that generates the receipt and some of the required fields that are supposed to be printed on the receipt (product or service description) are not available to the Payment Application or the Gateway. In this situation, the receipt generation will be handled as follow based on the Bank of America Gateway classification:

- Off-site Gateway: Off-site Gateway is a gateway that handles a "Redirect" payment processing from a Payment Application or another gateway. The Off-site gateway typically has a User Interface with a Virtual Terminal capabilities that will automatically produce its own receipts and store them within its system for ready merchant access; however typically it doesn't have access to product information or service description that needs to be printed on the receipt as required by the networks; they are not the immediate interaction point for either the merchant or their consumer/cardholder.
    - Receipt Requirement:
        - Off-site Gateway receipt requirements will be limited to the transaction payment information during certification, no product or service description related information will be required to be printed on the receipt.
- Hybrid Gateway: Hybrid Gateway is a gateway that processes API payload request from their ISV partners, or directly integrated merchants web server. The ISV or merchant is responsible for generating and displaying receipts for their customers.
    - Receipt Requirement:
        - Provide a sample of the payload returned to a payment application needed to generate a receipt, and any additional receipt configuration information provided to the merchant or the ISV partner.
        - Produce a mock-up receipt that displays all receipt requirements as outlined in the Developer guide
- On-site Application: An On-site Application is a non-gateway application that integrates directly to gateways and processors. These types of application consume the payment data received from the off-site gateway, hybrid gateway or the processor to send payment confirmations directly to the consumers, with description of goods sold, shipping/billing addresses, Tax/Duty, and other details about the purchase; the merchant configures the payment application to generate the receipt page.
    - Receipt Requirement:
        - Provide full receipt samples as outlined in the Developer Guide

- For the bank's Hosted Payment page, Secure Acceptance Checkout and Microform, the integrator generates the receipts.
- **Note**: It is prohibited to print Merchant ID (MID) and Terminal ID (TID) on the transaction receipts; however, an exception is made for the solutions using payment card industry validated point-to-point encryption (P2PE) or cryptographic keys for all host connectivity, in this case it is allowed to print:
    - The full Merchant ID (MID) and Terminal ID (TID) on the merchant receipt.
    - A truncated (last 4 digits) values of the MID/TID for the cardholder receipt.

16.7 Retail/Restaurant Card Present Receipt Requirements – Cardholder/Merchant template

The following table defines the receipt requirements for the Retail/Restaurant industry. The integrator may customize the layout to fit their receipt format.

Card Present Receipt Requirements	Cardholder	Merchant
Merchant DBA Name The merchant's name as disclosed to the cardholder at the Point of interaction (POI) and on the transaction receipt must be the same as what is provided in authorization and clearing transaction messages	X	X
Merchant DBA Location Street address, City, State, Country if applicable (must match what is sent in clearing file)	X	X
Merchant DBA Telephone Number	X	X
Reconciliation ID / Retrieval Reference Number (RRN)	X	X
General description of goods or services	X	X
Truncated Card Number Last 4 digits of the PAN or Token used for the transaction	X	X
Transaction Amount Price of goods and services including taxes, fees and any card discounts that may have been applied	X	X
Transaction Currency Currency symbol	X	X
Authorization Code	X	X
Transaction Date and Time	X	X
Transaction Type Sale, Refund, Balance Inquiry, Void, Activation, etc.	X	X
Card Network Name Visa, MasterCard, American Express, Debit, EBT Food Stamp, EBT Cash, Gift, eWIC, Loyalty etc.	X	X
Card Entry Mode Contact/Chip, Contactless, Fallback, Swipe, Manual/Keyed	X	X
Cardholder signature line or space for cardholder signature **Customer receipt may be printed or sent electronically** This applies only to a transaction that requires signature • Optional to print signature on Customer's Receipt • A signature may be captured electronically • The transaction occurs in face-to-face environment • The transaction is not a Visa Easy Payment Services (VEPS) • A PIN is not used for verify the cardholder		X
Cardholder Name If present on the card - Printed below the signature line	X	X

<table>
<tr><th>Card Present Receipt Requirements</th><th>Cardholder</th><th>Merchant</th></tr>
<tr><td>EMV Tag Data
<table>
<tr><th>Tag</th><th>Name</th><th>Description</th></tr>
<tr><td>9F12</td><td>Application Name</td><td>Application Preferred Name if present on the card in character set supported by the printer, otherwise Application Label (Tag 50) should be printed</td></tr>
<tr><td>4F</td><td>AID</td><td>Application Identifier</td></tr>
<tr><td>95</td><td>TVR</td><td>Terminal Verification Results</td></tr>
<tr><td>9B</td><td>TSI</td><td>Transaction Status Indicator</td></tr>
<tr><td>9F26</td><td>AC</td><td>Application Cryptogram</td></tr>
<tr><td>8A</td><td>ARC</td><td>Application Response Code</td></tr>
</table></td><td>X</td><td>X</td></tr>
<tr><td>PIN Statement (only required for EMV PIN) e.g., PIN Verified, PIN Locked</td><td>X</td><td>X</td></tr>
<tr><td>Response Literal Message
(Approve, Decline)</td><td>X</td><td>X</td></tr>
<tr><td>EBT Voucher Number
(For EBT voucher Transactions only)</td><td>X</td><td>X</td></tr>
<tr><td>Credit Disclaimer (optional for cardholder copy)
I agree to pay the total above amount according to card issuer agreement</td><td></td><td>X</td></tr>
<tr><td>Return Policy
(Applicable if merchant restricts the return of goods or cancelation of services)
Must be displayed in close proximity to the cardholder signature line)</td><td>X</td><td>X</td></tr>
<tr><td>Receipt Identifier
(Cardholder copy, Merchant Copy)</td><td>X</td><td>X</td></tr>
<tr><td>Reprinted Receipt (optional)
Indicates “Reprint” or “Duplicate”</td><td>X</td><td>X</td></tr>
<tr><td>Demo Mode (optional)
Indicates “DEMO” if transaction is ran in demo mode</td><td>X</td><td>X</td></tr>
<tr><td>Balance – EBT Cash/EBT Food, Gift and Loyalty
Account balance returned by the host must be printed on the receipt</td><td>X</td><td>X</td></tr>
<tr><td>Cash Back amount
(Conditional - Printed on a separate line and added to the total amount)</td><td>X</td><td>X</td></tr>
<tr><td>Tip Amount
(Conditional - Printed on a separate line and added to the total amount)</td><td>X</td><td>X</td></tr>
<tr><td>Transaction Fee</td><td>X</td><td>X</td></tr>
</table>

Card Present Receipt Requirements	Cardholder	Merchant
(Conditional – Printed on a separate line and added to the total amount, example: Convenience Fee, Service Fee, Surcharge)		

16.7.1 Receipt Examples

16.7.1.1 Approved Signature EMV Contact online transaction

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Amount:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

X_____
Signature
<Cardholder's name>

Merchant Copy

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Amount:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

Customer Copy

16.7.1.2 Approved Online PIN EMV Contact transaction

Merchant Name Merchant Street City, State, Zip Phone	
MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Subtotal:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

Cardholder Verified by PIN

Merchant Copy

Merchant Name Merchant Street City, State, Zip Phone	
MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Subtotal:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

Cardholder Verified by PIN

Customer Copy

16.7.1.3 EMV Contact Debit Transaction – Denied online

For EMV declined transactions, all the EMV tags that were submitted in the transaction **can** be printed on the receipt for troubleshooting purposes.

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Subtotal:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>

DENIED BY ISSUER

Cardholder Verified by PIN

Merchant Copy

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Subtotal:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>

DENIED BY ISSUER

Cardholder Verified by PIN

Customer Copy

16.7.1.4 EBT Receipt

- Account balances from the host response should be printed on the receipt
- Declined transaction should print a receipt with the balance returned from the host

Approved EBT Food Stamps

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY HH:MM:SS
Transaction Type EBT Food Stamp Sale
Card Network Name EBT
Card Number XXXXXXXXXXXX1234
Entry Mode Swipe

Your item description $20.31
Your item description $10.31
Subtotal: **$30.62**
Tax **$1.00**

Total: **$31.62**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
EBT Balance $102.45

Approved

Approved EBT Cash Sale

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY HH:MM:SS
Transaction Type EBT Cash Sale
Card Network Name EBT
Card Number XXXXXXXXXXXX1234
Entry Mode Swipe

Your item description/EBT Cash $15.00

Total: **$15.00**

Approval Code: <XXXXXXX>
RRN: <XXXXXXXXXXXX>
EBT Balance $9.00

Approved

Approved EBT Food Stamps Voucher Sale

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	EBT Sale Voucher
Card Network Name	EBT
Card Number	XXXXXXXXXXXX1234
Entry Mode	Keyed
Your item description	$20.31
Your item description	$10.31
Subtotal:	**$30.62**
Tax	**$1.00**

Total:	**$31.62**
Voucher # <XXXXXXXX>	
Approval Code: <XXXXXXX>	
RRN: <XXXXXXXXXXXX>	
EBT Balance	$102.45

Approved

Declined EBT Food Stamp Sale

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	EBT Food Stamps
Card Network Name	EBT
Card Number	XXXXXXXXXXXX1234
Entry Mode	Swipe
Your item description	$15.31
Your item description	$1$0.00
Subtotal:	**$25.31**
Tax	**$1.00**

Total:	**$26.31**
RRN: <XXXXXXXXXXXX>	
EBT Balance	$$0.00

Denied
Insufficient Funds

16.8 Retail/Restaurant Card Present Receipt Requirements – Single template

The following table defines the receipt requirements for Retail/Restaurant industry. The integrator may customize the layout to fit their receipt template.

Card Present Receipt Requirements	Cardholder/Merchant
Merchant DBA Name The merchant's name as disclosed to the cardholder at the Point of interaction (POI) and on the transaction receipt must be the same as what is provided in authorization and clearing transaction messages	X
Merchant DBA Location Street address, City, State, Country if applicable (must match what is sent in clearing file)	X
Merchant DBA Telephone Number	X
Reconciliation ID / Retrieval Reference Number (RRN)	X
General description of goods or services	X
Truncated Card Number Last 4 digits of the PAN or Token used for the transaction	X
Transaction Amount Price of goods and services including taxes, fees and any card discounts that may have been applied	X
Transaction Currency Currency symbol	X
Authorization Code	X
Transaction Date and Time	X
Transaction Type Sale, Refund, Balance Inquiry, Void, Activation, etc.	X
Card Network Name Visa, MasterCard, American Express, Debit, EBT Food Stamp, EBT Cash, Gift, eWIC, Loyalty etc.	X
Card Entry Mode Contact/Chip, Contactless, Fallback, Swipe, Manual	X
Cardholder signature line or space for cardholder signature **Customer receipt may be printed or sent electronically** This applies only to a transaction that requires signature • Optional to print signature on Customer's Receipt • A signature may be captured electronically • The transaction occurs in face-to-face environment • The transaction is not a Visa Easy Payment Services (VEPS) • A PIN is not used for verify the cardholder	X
Cardholder Name If present on the card - Printed below the signature line	X

<table>
<tr><th>Card Present Receipt Requirements</th><th>Cardholder/Merchant</th></tr>
<tr><td>EMV Tag Data
<table>
<tr><th>Tag</th><th>Name</th><th>Description</th></tr>
<tr><td>9F12</td><td>Application Name</td><td>Application Preferred Name if present on the card in character set supported by the printer, otherwise Application Label (Tag 50) should be printed</td></tr>
<tr><td>4F</td><td>AID</td><td>Application Identifier</td></tr>
<tr><td>95</td><td>TVR</td><td>Terminal Verification Results</td></tr>
<tr><td>9B</td><td>TSI</td><td>Transaction Status Indicator</td></tr>
<tr><td>9F26</td><td>AC</td><td>Application Cryptogram</td></tr>
<tr><td>8A</td><td>ARC</td><td>Application Response Code</td></tr>
</table></td><td>X</td></tr>
<tr><td>PIN Statement (only required for EMV PIN) e.g., PIN Verified, PIN Locked</td><td>X</td></tr>
<tr><td>Response Literal Message
(Approve, Decline)</td><td>X</td></tr>
<tr><td>EBT Voucher Number
(For EBT voucher transactions only)</td><td>X</td></tr>
<tr><td>Credit Disclaimer
I agree to pay the total above amount according to card issuer agreement</td><td>X</td></tr>
<tr><td>Return Policy
(Applicable if merchant restricts the return of goods or cancelation of services)
Must be displayed in close proximity to the cardholder signature line)</td><td>X</td></tr>
<tr><td>Receipt Identifier
(Cardholder copy, Merchant Copy)</td><td>X</td></tr>
<tr><td>Reprinted Receipt (optional)
Indicates “Reprint” or “Duplicate”</td><td>X</td></tr>
<tr><td>Demo Mode (optional)
Indicates “DEMO” if transaction is ran in demo mode</td><td>X</td></tr>
<tr><td>Balance – EBT Cash/EBT Food, Gift and Loyalty
Account balance returned by the host must be printed on the receipt</td><td>X</td></tr>
<tr><td>Cash Back amount
(Conditional - Printed on a separate line and added to the total amount)</td><td>X</td></tr>
<tr><td>Tip Amount
(Conditional - Printed on a separate line and added to the total amount)</td><td>X</td></tr>
<tr><td>Transaction Fee
(Conditional – Printed on a separate line and added to the total amount, example: Convenience Fee, Service Fee, Surcharge)</td><td>X</td></tr>
</table>

16.8.1 Receipt Examples single template

16.8.1.1 Credit Sale EMV Contact – Approved

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Amount:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

X_____
Signature
<Cardholder's name>

16.8.1.2 Credit Sale EMV Contact – Declined

For EMV denied transactions, EMV tags that were submitted in the transaction request **can** be printed on the receipt for troubleshooting purposes.

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Account	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Amount:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXX>
ARC: <XX>

DENIED BY ISSUER

16.8.1.3 Debit Sale EMV Contact transaction – Approved

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Subtotal:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

Cardholder Verified by PIN

16.8.1.4 Debit Sale EMV Contact – Denied Online

For EMV denied transactions, EMV tags that were submitted in the transaction request can be printed on the receipt for troubleshooting purposes.

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Your item description	$90.51
Subtotal:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>

DENIED BY ISSUER

Cardholder Verified by PIN

16.8.1.5 Refund EMV Contact - Approved

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Refund
Card Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contactless
Your item description	$90.51
Amount:	**$90.51**
Tip:	**$1$0.00**

Total:	**$100.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

X_____
Signature
<Cardholder's name>

16.8.1.6 EMV Fallback – Approved

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network Name	Visa
Card Number	XXXXXXXXXXXX1234
Entry Mode	Fallback

Your item description

Amount:	**$90.51**

Total:	**$90.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>

Approved

I agree to pay above total amount according to card issuer agreement

X_____
Signature
<Cardholder's name>

16.9 Retail/Restaurant Card Not Present/Electronic Commerce Receipt Requirements

The following table defines the receipt requirements for Retail/Restaurant Card Not Present industry. The integrator may customize the layout to fit their receipt template.

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
Card Network Name (Visa, MC, Amex, Discover etc.)	X	X
Truncated Card Number Last 4 digits of the PAN or Token used for the transaction	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
Transaction Type Sale, Refund etc..	X	X
Ship to address (if shipped)	X	X
Fee Assessed (if any) Convenience or Service Fees must be shown separate and clearly on the receipt	X	X
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	

16.9.1 Retail/Restaurant - 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:
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:
Transaction Type: <XXXXXX>
Card Network Name : <XXXXXX>
Last 4 PAN/token digit: <XXXX>
Authorization Code: <XXXXXX>
Reconciliation ID/RRN: <XXXXXXXXXX>

RETURN POLICY

<Insert the merchant refund/return policy here>

16.10 Card Not Present / Bill Pay Receipt Requirements

The following table defines the receipt requirements for Bill Pay. The integrator may customize the layout to fit their receipt template.

Bill Pay Receipt Requirements	Cardholder	Merchant
Pay To Account Description (Optional - Account nickname the payment is being made to)		
Pay To Account Number (Truncated Account Number - Last 4 digits)	X	X
Pay From Account Description (Optional - Account the payment is debited from)		
Transaction Amount and Currency Symbol	X	X
Payment Method used/Network Name (Visa, MC, Amex, Discover, Debit, Check etc.)	X	X
Transaction Date and Time	X	X
Transaction Description (Bill Pay)	X	X
Invoice Number (optional)		
Authorization Code/Confirmation Code	X	X
Reconciliation ID/Retrieval Reference Number	X	X
Transaction Type (Sale)	X	X
Fee Assessed (if any) Convenience or Service Fees must be shown separate and clearly on the receipt	X	X
Merchant Customer Service Phone Number	X	
Merchant DBA and Address (The name used by the merchant to identify itself to its customers)	X	

C) Healthcare Receipt Requirements

This table outlines the data elements that should be printed on receipts for the healthcare industry, the information should be limited to the payment information. No Protected Health information (PHI) or Personal Identifying Information (PII) such as the actual treatment received by the patient, the date of service, a numerical or a verbal description of the service rendered should be included on the payment receipt. The layout of the receipt can be customized to the merchant current receipt template.

16.10.1 Healthcare Card Present - Cardholder/Merchant template

The following table defines the receipt requirements for Healthcare Card Present industry. The integrator may customize the layout to fit their current receipt template.

Card Present Receipt Requirements	Cardholder	Merchant
Merchant DBA Name The merchant's name as disclosed to the cardholder at the Point of interaction (POI) and on the transaction receipt must be the same as what is provided in authorization and clearing transaction messages	X	X
Merchant DBA Location Street address, City, State, Country if applicable (must match what is sent in clearing file)	X	X
Transaction Date and Time	X	X
Merchant DBA Telephone Number	X	X
Host Reconciliation ID / Retrieval Reference Number (RRN) Processor or gateway transaction reference number	X	X
Truncated Card Number Last 4 digits of the PAN or Token used for the transaction	X	X
Transaction Amount Price of goods and services including taxes, fees, gratuity and any card discounts that may have been applied	X	X
Transaction Currency Currency symbol	X	X
Transaction Fee (Conditional – Printed on a separate line and added to the total amount, example: Convenience Fee, Service Fee, Surcharge)	X	X
Tax Amount (Conditional - Printed on a separate line and added to the total amount)	X	X
Authorization Code	X	X
Transaction Type Example - Sale, Refund, Reversal etc.	X	X

<table>
<tr><th>Card Present Receipt Requirements</th><th>Cardholder</th><th>Merchant</th></tr>
<tr><td>Card Network Name
Visa, MasterCard, American Express, Discover, JCB etc.</td><td>X</td><td>X</td></tr>
<tr><td>Card Entry Mode
Contact/Chip, Contactless, Fallback, Swipe, Keyed</td><td>X</td><td>X</td></tr>
<tr><td>Pre-authorized Healthcare
(For a Healthcare Auto-Substantiation Transaction, the word “Preauthorized Healthcare”)</td><td>X</td><td>X</td></tr>
<tr><td>Cardholder signature line or space for cardholder signature
Customer receipt may be printed or sent electronically
This applies only to a transaction that requires signature
• A signature may be captured electronically
• The transaction occurs in face-to-face environment
• The transaction is not a Visa Easy Payment Services (VEPS)
• A PIN is not used to verify the cardholder</td><td></td><td>X</td></tr>
<tr><td>EMV Tag Data
<table>
<tr><th>Tag</th><th>Name</th><th>Description</th></tr>
<tr><td>9F12</td><td>Application Name (labelled on the receipt as Card Network Name)</td><td>Application Preferred Name if present on the card in character set supported by the printer, otherwise Application Label (Tag 50) should be printed</td></tr>
<tr><td>4F</td><td>AID</td><td>Application Identifier</td></tr>
<tr><td>95</td><td>TVR</td><td>Terminal Verification Results</td></tr>
<tr><td>9B</td><td>TSI</td><td>Transaction Status Indicator</td></tr>
<tr><td>9F26</td><td>AC</td><td>Application Cryptogram</td></tr>
<tr><td>8A</td><td>ARC</td><td>Application Response Code</td></tr>
</table></td><td>X</td><td>X</td></tr>
<tr><td>PIN Statement (only required for EMV PIN) e.g., PIN Verified, PIN Locked</td><td>X</td><td>X</td></tr>
<tr><td>Response Literal Message
(Approve, Decline)</td><td>X</td><td>X</td></tr>
<tr><td>Credit Disclaimer (optional for cardholder copy)
I agree to pay the total above amount according to card issuer agreement</td><td></td><td>X</td></tr>
<tr><td>Receipt Identifier
(Cardholder copy, Merchant Copy)</td><td>X</td><td>X</td></tr>
<tr><td>Reprinted Receipt (optional)
Indicates “Reprint” or “Duplicate”</td><td>X</td><td>X</td></tr>
<tr><td>Demo Mode (optional)
Indicates “DEMO” if transaction is ran in demo mode</td><td>X</td><td>X</td></tr>
</table>

16.10.2 Healthcare Receipt Samples

16.10.2.1 Approved Signature EMV Contact online transaction - Auto-Substantiated Transaction

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network	Visa Credit
Card Number	XXXXXXXXXX1234
Entry Mode	Contact

Pre-authorized Healthcare

Transaction Amount	$90.51

Total:	**$96.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

X_____
Cardholder Signature

Merchant Copy

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network	Visa Credit
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact

Pre-authorized Healthcare

Transaction Amount	$90.51

Total:	**$96.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

Customer Copy

16.10.2.2 Approved Signature EMV Contact online transaction - Non Auto-Substantiated Transaction

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network	Visa Credit
Card Number	XXXXXXXXXX1234
Entry Mode	Contact
Transaction Amount	$90.51

Total:	**$96.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

X_____
Cardholder Signature

Merchant Copy

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY	HH:MM:SS
Transaction Type	Sale
Card Network	Visa Credit
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Transaction Amount	$90.51

Total:	**$96.51**

Approval Code: <XXXXXX>
RRN: <XXXXXXXXXXXX>
APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>
ARC: <XX>

APPROVED BY ISSUER

I agree to pay above total amount according to card issuer agreement

Customer Copy

16.10.2.3 Healthcare EMV Contact Credit Online PIN Transaction – Denied online

For EMV declined transactions, all the EMV tags that were submitted in the transaction **can** be printed on the receipt for troubleshooting purposes.

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY HH:MM:SS

Transaction Type	Sale
Card Network	Visa Credit
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Transaction Amount	$90.51
Tax:	$1$0.00
Total:	$100.51

APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>

DENIED BY ISSUER

Cardholder Verified by PIN

Merchant Copy

Merchant Name
Merchant Street
City, State, Zip
Phone

MM/DD/YYYY HH:MM:SS

Transaction Type	Sale
Card Network	Visa Credit
Card Number	XXXXXXXXXXXX1234
Entry Mode	Contact
Transaction Amount	$90.51
Tax	
$1$0.00	
Total:	$100.51

APP Name: <XXXXXXXXXX>
AID: <XXXXXXXXXXXXXXXX>
TVR: <XXXXXXXXXX>
TSI: <XXXX>
AC: <XXXXXXXXXXXXXXXX>

DENIED BY ISSUER

Cardholder Verified by PIN

Customer Copy

16.10.3 Healthcare Hosted Payment Page / Electronic Commerce Receipt Requirements

The following table defines the receipt requirements for Healthcare Card not Present industry. The integrator may customize the layout and the data fields placement to fit their receipt template.

Card Not Present Receipt Requirements	Cardholder	Merchant
Merchant DBA Name The merchant's name as disclosed to the cardholder at the Point of interaction (POI) and on the transaction receipt must be the same as what is provided in authorization and clearing transaction messages	X	X
Merchant DBA Location Street address, City, State, Country if applicable (must match what is sent in clearing file)	X	X
Merchant DBA Telephone Number		
Merchant URL (Internet Address)	X	X
Transaction Date and Time	X	X
Transaction Amount Price of goods or services including taxes and any card discount	X	X
Transaction Currency Currency symbol	X	X
Authorization Code	X	X
Host Reconciliation ID / Retrieval Reference Number (RRN) Processor or gateway transaction reference number	X	X
Card Network Name (Example: Visa, MC, Amex, Discover etc.)	X	X
Truncated Account Number Last 4 digit of the PAN/token	X	X
Transaction Type (Example: Sale, Refund)	X	X
Transaction Fee (Conditional – Printed on a separate line and added to the total amount, example: Convenience Fee, Service Fee, Surcharge)	X	X
Merchant Customer Service contact information	X	

16.10.3.1 Healthcare Hosted Payment Page – Card Not present Receipt Sample

MERCHANT INFORMATION
Merchant DBA Merchant Street Address Merchant City State zip Merchant Phone Number
PAYMENT INFORMATION
Date/Time: MM-DD-YYYY 12 :00 :00 Transaction Amount: $1.00 Transaction Type: <Sale/Refund> Card Network Name: <XXXXXXXXXX> Last 4 PAN/token digit: 1234 Authorization Code: <XXXXXX> Retrieval Reference Number: <XXXXXXXXXXXX>

17 Appendix A - Token

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

18 Appendix B

18.1 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 U.S
C	No match: street address and postal code do not match. Returned only for Visa cards not issued in the U.S
D	Match: street address and postal code match. Returned only for Visa cards not issued in the U.S
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: o Street address and postal code do not match. o 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: o The U.S. bank does not support AVS outside the U.S. o 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: o AVS is not supported for this processor or card type. o 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

18.2 CVN Codes

Code	Description
Processors CVN	
D	The transaction was determined to be suspicious by the issuing bank.
I	he 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

19 Appendix C

19.1 CA public key load file format

Field Name	Length	Description
RID	5b	Register Application Identifier (Visa, MasterCard, Amex, Discover etc…)
Key Index	1b	CA key index Number (01, C1, FA etc…)
Expiration Date	4b	Expiration date
Modulus	248b	Value of the modulus part of the CAPK
Exponent	1b	CAPK exponent
Hash	20b	A check value calculated on the concatenation of all parts of the CAPK

19.2 CAPK load Example

A000000025
C9
12312016
B362DB5733C15B8797B8ECEE55CB1A371F760E0BEDD3715BB270424FD4EA26062C38C3F4AAA3732A8
3D36EA8E9602F6683EECC6BAFF63DD2D49014BDE4D6D603CD744206B05B4BAD0C64C63AB3976B5C8C
AAF8539549F5921C0B700D5B0F83C4E7E946068BAAAB5463544DB18C63801118F2182EFCC8A1E85E53
C2A7AE839A5C6A3CABE73762B70D170AB64AFC6CA482944902611FB0061E09A67ACB77E493D998A0C
CF93D81A4F6C0DC6B7DF22E62DB
03
Hash=8E8DFF443D78CD91DE88821D70C98F0638E51E49

20 Appendix D - Device Type

This field is required to be sent in the transaction request for MasterCard when the value is present in tag 9F6E. it provides information about the device type used to identify mobile-initiated (m-commerce) or other EMV Contact, Magnetic stripe Contactless, or M/Chip Contactless transactions.

MasterCard defined code that indicates how the account information was obtained

Device Type Code	Description
00 (Default)	Card
01	Removable secure element that is personalized for use with a mobile phone and controlled by the wireless service provider. Example: subscriber identity module (SIM), universal integrated circuit card (UICC)
02	Key fob
03	Watch
04	Mobile tag
05	Wristband
06	Mobile Phone case or sleeve
07	Mobile phone with a non-removable, secure element that is controlled by the wireless service provider, for example, code division multiple access (CDMA)
08	Removable secure element that is personalized for use with a mobile phone and not controlled by the wireless service provider; example: memory card
09	Mobile phone with a non-removable , secure element that is not controlled by the wireless service provider
10	Removable secure element that is personalized for use with a tablet or e-book and is controlled by the wireless service provider; example: subscriber identity module (SIM), universal integrated circuit card (UICC)
11	Tablet or e-book with a non-removable, secure element that is controlled by the wireless service provider
12	Removable secure element that is personalized for use with a tablet or e-book and is not controlled by the wireless service provider
13	Tablet or e-book with a non-removable, secure element that is not controlled by the wireless service provider

21 Appendix E – Transaction Endpoints

A. Sandbox Transaction Endpoints

Integration Type	Endpoint
Hosted Checkout	https://sasit.pnrstage.ic3.com:7449/token/create https://sasit.pnrstage.ic3.com:7449/embedded/token/create https://sasit.pnrstage.ic3.com:7449/embedded/pay https://sasit.pnrstage.ic3.com:7449/embedded/token/update https://sasit.pnrstage.ic3.com:7449/oneclick/pay https://sasit.pnrstage.ic3.com:7449/pay https://sasit.pnrstage.ic3.com:7449/token/update
Checkout API	https://sasit.pnrstage.ic3.com:7449/silent/token/create https://sasit.pnrstage.ic3.com:7449/silent/embedded/token/create https://sasit.pnrstage.ic3.com:7449/silent/embedded/pay https://sasit.pnrstage.ic3.com:7449/silent/embedded/token/update https://sasit.pnrstage.ic3.com:7449/silent/pay https://sasit.pnrstage.ic3.com:7449/silent/token/update
Flex Microform	'https://pnrstage.ic3.com:7448/flex/v1/keys?format=JWT
REST API	https://pnrstage.ic3.com:7448/pts/v2/payments https://pnrstage.ic3.com:7448/pts/v2/payments/{id}/captures https://pnrstage.ic3.com:7448/pts/v2/payments/{id}/reversals https://pnrstage.ic3.com:7448/pts/v2/credits https://pnrstage.ic3.com:7448/pts/v2/payments/{id}/refunds https://pnrstage.ic3.com:7448/pts/v2/captures/{id}/refunds https://pnrstage.ic3.com:7448/pts/v2/payments/{id}/voids https://pnrstage.ic3.com:7448/pts/v2/captures/{id}/voids https://pnrstage.ic3.com:7448/pts/v2/credits/{id}/voids https://pnrstage.ic3.com:7448/pts/v2/refunds/{id}/voids https://pnrstage.ic3.com:7448/pts/v2/reversals https://pnrstage.ic3.com:7448/pts/v2/voids

B. DCE Transaction Endpoints

Integration Type	Endpoint
Hosted Checkout	https://testsecureacceptance.merchant-services.bankofamerica.com/token/create https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/token/create https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/pay https://testsecureacceptance.merchant-services.bankofamerica.com/embedded/token/update https://testsecureacceptance.merchant-services.bankofamerica.com/oneclick/pay https://testsecureacceptance.merchant-services.bankofamerica.com/pay https://testsecureacceptance.merchant-services.bankofamerica.com/token/update https://testsecureacceptance.merchant-services.bankofamerica.com/pay
Checkout API	https://testsecureacceptance.merchant-services.bankofamerica.com/silent/token/create https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/create https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/pay https://testsecureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/update https://testtestsecureacceptance.merchant-services.bankofamerica.com/silent/pay https://testsecureacceptance.merchant-services.bankofamerica.com/silent/token/update
Flex Microform key request	https://apitest.merchant-services.bankofamerica.com/flex/v1/keys
Flex Microform token request	https://apitest.merchant-services.bankofamerica.com/flex/v1/tokens
REST API	https://apitest.merchant-services.bankofamerica.com/pts/v2/payments https://apitest.merchant-services.bankofamerica.com/pts/v2/payments/{id}/captures https://apitest.merchant-services.bankofamerica.com/pts/v2/payments/{id}/reversals https://apitest.merchant-services.bankofamerica.com/pts/v2/credits https://apitest.merchant-services.bankofamerica.com/pts/v2/payments/{id}/refunds https://apitest.merchant-services.bankofamerica.com/pts/v2/captures/{id}/refunds https://apitest.merchant-services.bankofamerica.com/pts/v2/payments/{id}/voids https://apitest.merchant-services.bankofamerica.com/pts/v2/captures/{id}/voids https://apitest.merchant-services.bankofamerica.com/pts/v2/credits/{id}/voids https://apitest.merchant-services.bankofamerica.com/pts/v2/refunds/{id}/voids https://apitest.merchant-services.bankofamerica.com/pts/v2/reversals https://apitest.merchant-services.bankofamerica.com/pts/v2/voids

C. Production Transaction Endpoints

Integration Type	Endpoint
Hosted Checkout	https://secureacceptance.merchant-services.bankofamerica.com/token/create https://secureacceptance.merchant-services.bankofamerica.com/embedded/token/create https://secureacceptance.merchant-services.bankofamerica.com/embedded/pay https://secureacceptance.merchant-services.bankofamerica.com/embedded/token/update https://secureacceptance.merchant-services.bankofamerica.com/oneclick/pay https://secureacceptance.merchant-services.bankofamerica.com/pay https://secureacceptance.merchant-services.bankofamerica.com/token/update https://secureacceptance.merchant-services.bankofamerica.com/pay
Checkout API	https://secureacceptance.merchant-services.bankofamerica.com/silent/token/create https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/create https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/pay https://secureacceptance.merchant-services.bankofamerica.com/silent/embedded/token/update https://secureacceptance.merchant-services.bankofamerica.com/silent/pay https://secureacceptance.merchant-services.bankofamerica.com/silent/token/update
Flex Microform	https://api.merchant-services.bankofamerica.com/flex/v1/keys
REST API	https://api.merchant-services.bankofamerica.com/pts/v2/payments https://api.merchant-services.bankofamerica.com/pts/v2/payments/{id}/captures https://api.merchant-services.bankofamerica.com/pts/v2/payments/{id}/reversals https://api.merchant-services.bankofamerica.com/pts/v2/credits https://api.merchant-services.bankofamerica.com/pts/v2/payments/{id}/refunds https://api.merchant-services.bankofamerica.com/pts/v2/captures/{id}/refunds https://api.merchant-services.bankofamerica.com/pts/v2/payments/{id}/voids https://api.merchant-services.bankofamerica.com/pts/v2/captures/{id}/voids https://api.merchant-services.bankofamerica.com/pts/v2/credits/{id}/voids https://api.merchant-services.bankofamerica.com/pts/v2/refunds/{id}/voids https://api.merchant-services.bankofamerica.com/pts/v2/reversals https://api.merchant-services.bankofamerica.com/pts/v2/voids

22 Appendix F – Sample Transaction Requests and Responses Using REST API

22.1 EMV Contact Payment with an Online PIN

Request

```
{
    "processingInformation": {
        "commerceIndicator": "retail"
    },
    "orderInformation": {
        "amountDetails": {
            "totalAmount": "99.98",
            "currency": "usd"
        }
    },
    "pointOfSaleInformation": {
        "cardPresent": "Y",
        "catLevel": "6",
        "entryMode": "contact",
        "terminalCapability": "4",
        "encryptedPin": "1234567812345678",
        "emv": {
            "tags":
 "9F3303204000950500000000009F3704518823719F100706011103A000009F26081E1756ED0E2134
E29F3602001582020009C01009F1A0208409A030006219F02060000000020005F2A0208409F030600
0000000000"
        },
        "trackData":
 "%B4111111111111111^LEE/TANYA^25121200123456789025**XXX******?;4111111111111111=2
5121200XXXX00000000?*"
    }
}
```

Response


```
{
  "_links": {
    "authReversal": {
      "method": "POST",
      "href": "/pts/v2/payments/6479727275146063203006/reversals"
    },
    "self": {
      "method": "GET",
      "href": "/pts/v2/payments/6479727275146063203006"
    },
    "capture": {
      "method": "POST",
      "href": "/pts/v2/payments/6479727275146063203006/captures"
    }
  },
  "clientReferenceInformation": {
    "code": "1647972727494"
  },
  "id": "6479727275146063203006",
  "orderInformation": {
    "amountDetails": {
      "authorizedAmount": "99.98",
      "currency": "usd"
    }
  },
  "paymentAccountInformation": {
    "card": {
      "type": "001"
    }
  },
  "paymentInformation": {
    "tokenizedCard": {
      "type": "001"
    },
    "card": {
      "type": "001"
    }
  },
  "pointOfSaleInformation": {
    "terminalId": "111111",
    "emv": {
      "tags":
 "9F02060000000009009C01009A030608025F2A0209789F1A0208409F260856BF299472BDB0C78202
5C009F360245679F37041213541495054080008000 9F1E04001122339F102006011A03900000112233
445566778899AABBCCDD03900000112233445566778899F5301039F41030122339F0306000102030405
8407A000000004101 09F2701809F34035E03009F090243219F3501059F3303E0B8C891100011223344
5566778801020304050607 9F5B10001122334455667788010203040506 07"
    }
  },
  "processorInformation": {
    "approvalCode": "888888",
    "networkTransactionId": "123456789619999",
    "transactionId": "123456789619999",
    "responseCode": "100",
    "avs": {
      "code": "1"
    }
  },
  "reconciliationId": "66700013011ZJ52O",
  "status": "AUTHORIZED",
  "submitTimeUtc": "2022-03-22T18:12:07Z"
}
```

22.2 EMV Fallback Payment Using the REST API

Request

```
{
    "clientReferenceInformation": {
        "code": "OrderABC12"
    },
    "processingInformation": {
        "commerceIndicator": "retail"
    },
    "orderInformation": {
        "amountDetails": {
            "totalAmount": "99.98",
            "currency": "usd"
        }
    },
    "pointOfSaleInformation": {
        "cardPresent": "Y",
        "entryMode": "swiped",
        "emv": {
            "fallback": "Y"
        },
        "trackData":
 "%B4111111111111111^LEE/TANYA^25121200123456789025**XXX******?;4111111111111111=2
5121200XXXX00000000?*"
    }
}
```

Response


```
{
    "_links": {
        "authReversal": {
            "method": "POST",
            "href": "/pts/v2/payments/6473256016126696903006/reversals"
        },
        "self": {
            "method": "GET",
            "href": "/pts/v2/payments/647325601612669690 3006"
        },
        "capture": {
            "method": "POST",
            "href": "/pts/v2/payments/6473256016126696903006/captures"
        }
    },
    "clientReferenceInformation": {
        "code": "OrderABC12"
    },
    "id": "6473256016126696903006",
    "orderInformation": {
        "amountDetails": {
            "authorizedAmount": "99.98",
            "currency": "usd"
        }
    },
    "paymentAccountInformation": {
        "card": {
            "type": "001"
        }
    },
    "paymentInformation": {
        "tokenizedCard": {
            "type": "001"
        },
        "card": {
            "type": "001"
        }
    },
    "pointOfSaleInformation": {
    },
    "processorInformation": {
        "approvalCode": "888888",
        "networkTransactionId": "123456789619999",
        "transactionId": "123456789619999",
        "systemTraceAuditNumber": "246802",
        "responseCode": "100"
    },
    "reconciliationId": "6580310700JCYR8J",
    "status": "AUTHORIZED",
    "submitTimeUtc": "2022-03-15T06:26:41Z"
}
```