Portico Developer Guide

Version 3.31

June 2023

Heartland

A Global Payments Company

Notice

THE INFORMATION CONTAINED HEREIN IS PROVIDED TO RECIPIENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTY OF TITLE OR NON-INFRINGEMENT. HEARTLAND PAYMENT SYSTEMS, LLC ("HEARTLAND") MAKES NO WARRANTIES OR REPRESENTATIONS THAT THE MATERIALS, INFORMATION, AND CONTENTS HEREIN ARE OR WILL BE ERROR FREE, SECURE, OR MEET RECIPIENT'S NEEDS. ALL SUCH WARRANTIES ARE EXPRESSLY DISCLAIMED.

RECIPIENT'S USE OF ANY INFORMATION CONTAINED HEREIN IS AT RECIPIENT'S SOLE AND EXCLUSIVE RISK. IN NO EVENT SHALL HEARTLAND BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, WHETHER RESULTING FROM BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, EVEN IF HEARTLAND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. HEARTLAND RESERVES THE RIGHT TO MAKE CHANGES TO THE INFORMATION CONTAINED HEREIN AT ANY TIME WITHOUT NOTICE.

THIS DOCUMENT AND ALL INFORMATION CONTAINED HEREIN IS PROPRIETARY TO HEARTLAND, RECIPIENT SHALL NOT DISCLOSE THIS DOCUMENT OR THE SYSTEM DESCRIBED HEREIN TO ANY THIRD PARTY UNDER ANY CIRCUMSTANCES WITHOUT PRIOR WRITTEN CONSENT OF A DULY AUTHORIZED REPRESENTATIVE OF HEARTLAND. IN ORDER TO PROTECT THE CONFIDENTIAL NATURE OF THIS PROPRIETARY INFORMATION, RECIPIENT AGREES:

- TO IMPOSE IN WRITING SIMILAR OBLIGATIONS OF CONFIDENTIALITY AND NONDISCLOSURE AS CONTAINED HEREIN ON RECIPIENT'S EMPLOYEES AND AUTHORIZED THIRD PARTIES TO WHOM RECIPIENT DISCLOSES THIS INFORMATION (SUCH DISCLOSURE TO BE MADE ON A STRICTLY NEED-TO-KNOW BASIS) PRIOR TO SHARING THIS DOCUMENT AND
- TO BE RESPONSIBLE FOR ANY BREACH OF CONFIDENTIALITY BY THOSE EMPLOYEES AND THIRD PARTIES TO WHOM RECIPIENT DISCLOSES THIS INFORMATION.

RECIPIENT ACKNOWLEDGES AND AGREES THAT USE OF THE INFORMATION CONTAINED HEREIN SIGNIFIES ACKNOWLEDGMENT AND ACCEPTANCE OF THESE TERMS. ANY SUCH USE IS CONDITIONED UPON THE TERMS, CONDITIONS AND OBLIGATIONS CONTAINED WITHIN THIS NOTICE.

THE TRADEMARKS AND SERVICE MARKS RELATING TO HEARTLAND'S PRODUCTS OR SERVICES OR THOSE OF THIRD PARTIES ARE OWNED BY HEARTLAND OR THE RESPECTIVE THIRD PARTY OWNERS OF THOSE MARKS, AS THE CASE MAY BE, AND NO LICENSE WITH RESPECT TO ANY SUCH MARK IS EITHER GRANTED OR IMPLIED.

To verify existing content or to obtain additional information, please call or email your assigned Heartland representative.

Release Notes

This table contains detailed changes to the current version of the document. For information on past changes, see the Release Notes in that version.

Documentation Section / Topic	Change Description
Portico Developer Guide	Updated release version number from 3.28 to 3.31. Updated release date from January 2023 to June 2023.
Various	Updated links to transaction types for consistency
Overview	Minor text clarifications
Encyption	Added note indicating some types are not supported for merchants processing on the GNAP-UK host.
Timeouts	Removed a reference to reversals when the Issuer RspCode is 91. A reversal is not necessary when that occurs.
Dynamic Currency Conversion	Clarified that DCC returns require the GatewayTxnId of the original request.
Dynamic Transaction Descriptor	Minor text correction
Fingerprint Service	Added new section
Heartland Platforms / Payment Facilitators	Renamed section for clarity.
Transaction Set for Payment Facilitator Sub-Merchants	Renamed section for clarity. Added debit transactions supported for Canadian merchants
Industries	Separated MOTO and eCommerce. Added In App transactions to
UnionPay	Added information on functionality that is **not** supported for UnionPay Minor text clarifications
Issuer Response Codes	Updated text for EL Added new code PR
Schema	Updated schema for v3.28.

Table of Contents

1 Overview

The Heartland Portico™ Gateway (referred to as Portico in this document) provides an application programming interface (API) to aid integrators and merchants with processing payment transactions. Portico's API includes services for a variety of payment methods (credit, debit, check, EBT, gift, etc.) and various industries (retail, restaurant, mail order/telephone order, lodging, eCommerce, and healthcare). Portico also provides integrators and merchants with several options for secure transaction processing.

This document details the services available via the API and provides guidelines on best practices for integrators. Following these guidelines can reduce integration and certification time, reduce fraud potential, and ensure proper interchange rates.

This document is based on Portico API **version 3.31**. The content is split into two distinct sites:

- **Portico Developer Guide site (this site)**: This site contains the front matter of the documentation and all static content. It is the default site when initially linking to the Portico Developer Guide. The title "Portico Developer Guide" appears above the topic title on each of its pages. Searches performed in this site will provide results for only this site. A PDF of this content is available here:

  
  Portico Developer Guide only pdf

- **Portico Schema site**: This site contains the content generated from the XML Schema. When you click a link to the Generated Content site, the page is opened in a new browser tab. For example, if you click a Request/Response link from the Transactions > Credit Card Transactions page, the page is opened in a new tab. The title "PosGateway Schema" appears above the topic title on each of its pages. Searches performed in this site will provide results for only this site. The nature of this content does not lend itself to be displayed in a PDF, so no PDF is provided. To get back to the Overview/Front Matter, click on the other browser tab.

See Release Notes for descriptions of the changes made to the documentation for this release.

1.1 Payment Application Data Security Standards

The Payment Card Industry (PCI) Security Standards Council (SSC) has released the Payment Application Data Security Standards (PA-DSS) for payment applications running at merchant locations. The PA-DSS assists software vendors to ensure their payment applications support compliance with the mandates set by the Bank Card Companies (Visa, Mastercard, Discover, American Express, and JCB).

In order to comply with the mandates set by the Bank Card Companies, Heartland Payment Systems:

- Requires that the account number cannot be stored in the clear in order to meet PCI and PA-DSS regulations. It must be encrypted while stored using strong cryptography with associated key management processes and procedures.

  > Refer to PCI DSS Requirements 3.4–3.6* for detailed requirements regarding account number storage. The retention period for the Account Number in the shadow file and open batch should be defined. At the end of that period or when the batch is closed and successfully transmitted, the account number and all other information must be securely deleted. This is a required process regardless of the method of transmission for the POS.

- Requires that, with the exception of the Account Number as described above and the Expiration Date, no other Track Data is to be stored on the POS if the Card Type is a:
  - Visa, including Visa Fleet;
  - Mastercard, including Mastercard Fleet, and Carte Blanche;
  - Discover, including JCB, UnionPay, Diner's Club, and PayPal;
  - American Express;
  - WEX;
  - Debit or EBT.

  > This requirement does not apply to FleetCor, Voyager, or Aviation cards; Stored Value cards; Proprietary or Private Label cards.

- Recommends that software vendors have their applications validated by an approved third party for PA-DSS compliance.
- Requires all software vendors to sign a Developer's Agreement (Non-Disclosure Agreement).
- Requires all software vendors to provide evidence of the application version listed on the PCI Council's website as a PA-DSS validated Payment Application or a written certification to Heartland Testing of the Developer's compliance with PA-DSS.
- Requires that all methods of cryptography provided or used by the payment application meet PCI SSC's current definition of "strong cryptography".

*Refer to www.pcisecuritystandards.org for the PCI DSS Requirements document and further details about PA-DSS.

1.2 Connectivity

Connectivity to Portico is through the Internet. A secure socket connection is required for all transactions to ensure the confidentiality of information passed between the merchant and Portico. While this provides protection for the message in transit, additional protection is still highly recommended for certain data elements (see Data Security for additional information).

> TLS 1.2 is the minimum requirement for certification including a select suite of ciphers. Refer to the Heartland Integrator's Guide for further information.

1.3 Protocol

This guide covers the Portico Simple Object Access Protocol (SOAP) API. The base elements and data types used in the Portico schema come from the "http://www.w3.org/2001/XMLSchema" namespace. Additional Portico schema elements are defined in the "http://Hps.Exchange.PosGateway" namespace.

The full Portico schema (PosGateway.xsd) is provided in the Portico SDK.

1.4 Authentication

The values in the header are used for authentication and validation. Portico responds with an "authentication error" response when these values are not set correctly. See Gateway Response Codes for additional information.

Portico Credentials

In order to process on Portico, a boarding event is required. This boarding event sets the appropriate configuration for the POS; the response contains values including LicenseId, SiteId, and DeviceId, and may include a means to obtain a Secret Key. These values are Portico-generated values that uniquely identify the POS.

During transaction processing, in order to identify the POS sending the request, Portico requires a valid secret key, or the following 5 credentials: LicenseId, SiteId, DeviceId, UserName, and Password.

- The LicenseId is used to chain multiple sites together for reporting and administration.
- The SiteId is the location and is tied to a specific Merchant Identification Number (MID).
- The DeviceId indicates a unique POS at a specific site.
- The username and password should be protected by the merchant. The password should never be made public. A temporary password is provided at the time of boarding. This temporary password should be changed by the merchant before processing any transactions. The password should then be changed periodically for security.

> LicenseId, SiteId, and DeviceId are integer values. The maximum length is 10 digits and the maximum value is 2147483647. Username is alphanumeric and the maximum length is 20 characters. Each Merchant is assigned a unique Merchant ID, also called Merchant Number or MID; this value is usually 15 digits and may start with zero.
>
> Each merchant must know their MID, but the value is not passed to Portico in transaction messages. Each MID corresponds to a unique SiteId.

Credential Token

The credential token is used to indicate a user session. Currently, this option is only available to internal Heartland applications and should not be used by integrators.

2 Data Security

Portico supports multiple methods of securing transmitted and stored data. The following sections cover the details around the supported encryption and tokenization options. The primary options are Heartland End-to-End Encryption (E3) and Heartland's Enterprise Tokenization Service (ETS). These options can be used together or independently.

- E3 encrypts card data at the point of entry in a hardware solution such that the POS never handles data in the clear.
- Tokenization allows merchants to store a value that represents a card number for future processing. These tokens are referred to as multi-use tokens, since they can be used over and over as a reference to the original card data.

> Portico also supports single-use tokens. These are obtained via Heartland's SecureSubmit product. They are helpful when the merchant has a client application (browser, mobile application, etc.) obtaining card data and sending it to a merchant server.
>
> If the client first exchanges the payment data for a single-use token and sends this to the server, the server never handles card data. This requires additional boarding, integration, and certification steps. This option can be used independently or along with the other data security methods.

2.1 Encryption

Portico supports two methods of encryption for securing PAN and track information: Heartland E3 and AES using DUKPT.

Heartland E3 is an implementation of the Voltage Identity-Based Encryption methodology offered by Heartland to allow card data to be encrypted from the moment it is obtained at the POS and throughout Heartland processing. Since software is vulnerable to intrusions, this technology is hardware based. Using E3 hardware, the merchant's POS software never sees card data. It also allows the card data to remain encrypted throughout all of Heartland's systems. This not only removes intrusion threats, it also greatly reduces the scope of PCI audits on the associated merchant POS software.

AES using DUKPT key management is provided for Heartland mobile by the IdTECH card reader. This technology offers near end-to-end encryption.

TDES using DUKPT key management offers end-to-end encryption using ANSI X9.24 part 1 standard.

For transactions using any of the encryption types, additional data must be provided. The EncryptionData element must be provided including the encryption version being used as well as any additional data items required.

Please note that Version 01, 02, and 04 are not supported for merchants processing on GNAP-UK.

The supported encryption versions and required data items are defined as follows:

Version	Encryption Type	When Encrypting PAN	When Encrypting Track Data
01	E3 (Voltage)	Not Supported	The EncryptionData element must be provided with the Version set to "01". No additional elements need to be provided inside the EncryptionData element. The TrackData provided must include the full E3/Voltage device output stream. Encryption Version 01 is supported only for the Heartland E3-M1 magnetic stripe reader wedge device, functioning in keyboard emulation mode.
02	E3 (Voltage)	Supported The EncryptionData element must be provided with the Version set to "02". In addition, the POS must parse the E3 MSR output and provide the Key Transmission Block in the KTB element. The CardNbr provided must only include the encrypted PAN parsed by the POS from the E3/Voltage device output stream.	The EncryptionData element must be provided with the Version set to "02". In addition, the EncryptedTrackNumber element must be set to "1" for Track 1 data or "2" for Track 2 data, and the POS must parse the E3/Voltage device output and provide the KTB in the KTB element. The TrackData provided must only include the encrypted Track 1 or Track 2 data parsed by the POS from the E3/Voltage device output stream.
03	AES	Not Supported	The EncryptionData element must be provided with the Version set to "03". In addition, the EncryptedTrackNumber element must be set to "1" for Track 1 data or "2" for Track 2 data, and the POS must parse the card reader output stream and provide the KSN in the KSN element. Both the KSN and the track data content must be Base-64 encoded strings.
04	E3 (Voltage)	Supported The EncryptionData element must be provided with the Version set to "04". In addition, the POS must parse the E3 MSR output and provide the Key Transmission Block in the KTB element. In addition to the CardNbr, version "04" expects the CVV2 to be encrypted.	The EncryptionData element must be provided with the Version set to "04". In addition, the EncryptedTrackNumber element must be set to "1" for Track 1 data or "2" for Track 2 data, and the POS must parse the E3/Voltage device output and provide the KTB in the KTB element. The TrackData provided must only include the encrypted Track 1 or Track 2 data parsed

Version	Encryption Type	When Encrypting PAN	When Encrypting Track Data
		The CardNbr and CVV2 provided must only include the encrypted PAN and encrypted CVV2 parsed by the POS from the E3/Voltage device output stream.	by the POS from the E3/Voltage device output stream.
05	TDES DUKPT	Supported The EncryptionData element must be provided with the Version set to "05". The CardNbr must only include the encrypted PAN. If a CVV2 is provided, it should not be encrypted.	The EncryptionData element must be provided with the Version set to "05". In addition, the EncryptedTrackNumber element must be set to "1" for Track 1 data or "2" for Track 2 data, and the POS must parse the card reader output stream and provide the KSN in the KSN element. Both the KSN and the track data content must be Base-64 encoded strings.

2.2 Multi-Use Tokenization

Portico supports tokenization of account numbers to provide clients with another layer of security. The tokenization process consists of the following two basic steps:

1. Request that an account number (from a PAN or track data) be tokenized and the token be returned to the client POS.
2. The client POS uses the token rather than the PAN or track data in subsequent transactions.

Tokenization provides a means to replace sensitive PAN values with surrogate, non-sensitive values that can be stored and referenced without the complexities of storing and securing PANs, as required by the PCI-DSS. Tokens thus stored can then be passed on supported Portico transactions in lieu of the card number. Heartland's tokenization service manages the association between the token and the PAN.

Multi-use tokenization can be used for Card Present or Card Not Present transactions. Supported services for tokenization are as follows:

Application Service	Request a Token	Use a Token
CreditAccountVerify	Yes	Yes
CreditAuth	Yes	Yes
CreditOfflineAuth	No	Yes
CreditOfflineSale	No	Yes
CreditReturn	No	Yes
CreditReversal	Yes	Yes
CreditSale	Yes	Yes
PrePaidBalanceInquiry	Yes	Yes
RecurringBilling	Yes	Yes
Tokenize	Yes	No

See the message definitions for more information on the token specific fields.

Additional fees apply for the multi-use tokenization service. Please contact your Heartland representative for further information.

> Service may not be available to all merchants; refer to Authorization Platform.

2.2.1 Requesting a Token

Using Tokenize

The Tokenize request provides an option to return a multi-use token without card issuer verification. If the Tokenize request contains bad data (for example, an invalid card number), when the Token is used in transaction processing, it will return an error. This risk is assumed by the merchant if they choose to use Tokenize instead of requesting a token for an approved credit transaction.

> Tokenize cannot be used to convert a Single Use token into a Multi Use token.

When data is tokenized, it includes both the PAN and the expiration date.

During Credit Transaction Processing

When a merchant requests that a token be returned, the associated transaction (auth, sale, reversal, etc.) is processed before requesting a token. The transaction response is always returned to the merchant POS.

If the associated transaction response is a non-approval, the token request is not processed. This is indicated in the TokenRspCode returned in the response to the client POS.

If the transaction is approved by the card issuer with a response of APPROVAL, PARTIAL APPROVAL, or CARD OK, a token is requested from the tokenization service and a TokenData response block is returned to the merchant POS. The TokenData response block may include the generated token in the TokenValue field depending on the success or failure of the tokenization request.

When data is tokenized, it includes both the PAN and expiration date.

2.2.2 Using a Token

After a token is successfully returned, the merchant presents this token rather than the account number or track data in one of the allowed transactions in the TokenData. Portico attempts to request the account number and expiration date associated with the provided token from the tokenization service. If the TokenData includes the expiration date, this overrides what is retrieved from the tokenization service. The included expiration date is only used for the current transaction and is not stored for future use. If TokenData includes a CardPresent indicator, then that will be used for this transaction. If one is not sent, then Card Not Present will be used. The Card Present indicator is not saved for future use.

If the PAN and expiration date are obtained successfully, the transaction proceeds.

If the PAN and expiration date cannot be obtained, the transaction is aborted and an error is returned to the merchant. The error code/text is returned in the GatewayRspCode and GatewayRspMsg fields.

2.2.3 Managing Tokens

Once a token has been created for a particular Merchant/PAN combination, it can be managed through the ManageTokens service. ManageTokens provides the following actions:

- **SetAttribute**—The ManageTokens.Set action adds or updates multiple token attribute name-value pairs. The currently allowed attribute names are as follows:

Attribute Name	Allowed Values
ExpMonth	Positive integer in the following range: 1-12
ExpYear	Positive integer greater than 1999

- **DeleteAttribute, DeleteToken**—The ManageTokens.Delete action removes multiple attributes or the token itself from the tokenization service database. If no attributes are provided for a token, the token is deleted.

3 Getting Started

This section is intended to provide an integrator with a starting point. This includes information that is needed to get started and process the most basic transactions with Portico.

3.1 Add a Reference

Portico provides several ways to begin integration:

- Portico Client DLL
- Web Services Description Language (WSDL)
- XSD

The Portico Client DLL provides an object-oriented interface for integration. This option hides the complexities of the lower-level protocols and handles serialization and deserialization of the various elements. For managed applications, integrators can utilize the library by adding a reference to the DLL. For unmanaged applications, the Portico Client DLL also provides a COM wrapper. To use the COM wrapper, the library must first be registered for use. For additional information on registering the library, refer to the appendix Register the Client Library.

The WSDL allows integrators to generate a service reference rather than using the supplied Portico Client DLL. The WSDL can be accessed by adding "?wsdl" to the end of the URL provided for certification. For example:

https://cert.api2.heartlandportico.com/Hps.Exchange.PosGateway/POSgatewayservice.asmx?wsdl

The W3C XML Schema Definition (XSD) is also available as another alternative for allowing an integrator to generate a service reference rather than using the supplied Portico Client DLL. The XSD types are defined at http://www.w3.org/TR/xmlschema-2/.

3.2 Use the Interface

There are three key classes exposed in the interface:

- PosGatewayInterface—Handles the interface and communication details with the Portico server.
- PosRequest—Object representation of the XML Heartland Portico Gateway request document.
- PosResponse—Object representation of the XML Heartland Portico Gateway response document.

The key steps involved when issuing a transaction to Portico are as follows:

- Build a PosRequest message object.
- Instantiate a PosGatewayInterface object.
- Invoke the DoTransaction() method of the PosGatewayInterface object.
- Interrogate the PosResponse message object.

The PosRequest and PosResponse classes are based on the PosGateway schema. Referring to this schema helps you to understand the layout of the PosRequest and PosResponse classes. All transactions described in this document conform to the schema.

3.3 SoapUI Examples

A sample SoapUI project is included in the SDK to provide working SOAP/XML examples of Portico transactions. The examples show the raw SOAP/XML and can be run against the certification environment, but SoapUI cannot be used for final certification.

To install and set up the SoapUI application with Portico samples, do the following:

1. Go to www.soapui.org.
2. Download and install the free, open-source functional testing application, SoapUI.
3. Save the Soap UI project file from Portico SDK to your hard drive.
4. Open the Soap UI project file with SoapUI application.

Portico Soap UI project is organized into TestSuites that match specific chapters in this document. Each TestSuite contains a collection of TestCases that represent Portico functionality or transactions. Each TestCase contains individual TestSteps that provide XML samples of detailed scenarios.

To view and use SOAP/XML samples for specific scenarios matching the functionality described in this document, you drill down in the SoapUI project following the same structure.

For example, execute TestSuite – Credit Card Transaction > TestCase – Credit Sale > Test Steps > CreditSale Request 2 – Swipe – Visa to process a sample request and response for a credit card sale described in CreditSale.

> The SoapUI examples contain properties (e.g., ${#Project#LicenseID-Retail}) that must be replaced with valid values in your SOAP messages.

3.4 Transaction Basics

The following sections provide useful information about Portico transaction functionality.

3.4.1 Transaction Request Header Fields

The transaction request header contains optional fields. This table provides a description of each optional field and how the data is used.

Field Name	Description	Usage
Site Trace	Allows a client to provide a value that can be searched for later. Clients are free to provide any value that is useful to them but it must not contain sensitive data. Echoed in the response if present	Stored in Portico; not passed to host
DeveloperId	Identifier assigned by Heartland during the certification process. Optional to support legacy integrations. Required for all new Heartland integrations.	Stored in Portico; not passed to host
VersionNbr	Software version number assigned by Heartland during the certification process. Optional to support legacy integrations. Required for all new Heartland integrations.	Stored in Portico; not passed to host
OptionalPOSData	**Required** for Canadian merchants; see your certification analyst for details.	Stored in Portico; not passed to host
ClientTxnId	A client-generated transaction id. This must be unique for this device. Echoed in the response. Can be used to initiate a reversal in the event of a timeout. See Also: Client Txn Id.	Stored in Portico; not passed to host

UniqueDeviceId	A client-supplied device identifier to be sent when transactions for multiple devices are aggregated in the same batch. Echoed in the response header.	Stored in Portico; if present, the field will be sent to the host, and passed to the issuer, on authorization and settlement requests. Supported for the Exchange and GSAP-NA authorization platforms.
SAFData>SAFIndicator	Indicates whether a transaction was initiated in "store and forward" (SAF) mode. See Also: Store and Forward	Stored in Portico; if present, sets appropriate indicators in the host request message which are also passed on to the issuer. Supported for the Exchange and GSAP-NA authorization platforms.
SAFData>SAFOrigDT	Date and time when the transaction was originally initiated.	Stored in Portico; if present, sets appropriate indicators in the host request message which are also passed on to the issuer. Supported for the Exchange and GSAP-NA authorization platforms.
PosReqDT	POS request date and time. Required for Interac processing. Required for Canadian merchants.	Stored in Portico; if present, passed to the host for Canadian merchants. Supported for the GSAP-NA authorization platform only.
DeviceConfiguration>Capabilities	Capabilities for a Device	Stored in Portico; if present, passed to the host for UK merchants. Supported for the GNAP-UK authorization platform only.
DeviceConfiguration>Attributes	Attributes for a Device	Stored in Portico; if present, passed to the host for UK merchants. Supported for the GNAP-UK authorization platform only.
DeviceConfiguration>SerialNbr	Serial number of PIN pad or PIN entry device (PED). Required for Interac debit services in Canada.	Stored in Portico; if present, passed to the host for Canadian merchants. Supported for the GSAP-NA authorization platform only.
DeviceConfiguration>TxnMCC	MCC value that is passed from POS. Overrides MCC value stored for the DeviceId. Usage is restricted.	Stored in Portico; if present, passed to the host. Supported for the GSAP-NA and GSAP-AP authorization platforms.
UPIAuthNetwork	Indicates the authorization network to be used for co-branded UnionPay	Stored in Portico; if true, authorizations will route to the UnionPay network. Supported

	cards, based on cardholder choice at the Point of Sale.	for GNAP-UK merchants only.
SDKNameVersion	Name and Version of the SDK used for integration, where applicable. Expected for users of the Heartland SDK.	Stored in Portico; not passed to host Included in ReportTxnDetail responses if populated.

3.4.2 Client Txn Id

It is strongly recommended that all transaction requests contain a unique identifier per request generated by the POS, included in the message request header in the ClientTxnId field and echoed in the response. This value can be used to initiate reversals or search for transactions. The value should be unique for a minimum of one year to search transactions.

ClientTxnId is required to initiate a reversal for any financial transaction in the event that response in not received (POS Timeout).

The ClientTxnId values must be unique for each transaction request for a DeviceId to ensure that any Reversal requests initiated by ClientTxnId are able to identify the correct transaction to be reversed.

3.4.3 Gateway Txn Id

All transaction responses contain an identifier generated by Portico, which is returned in the field GatewayTxnId in the response header. This value can be used to search for transactions or initiate voids, reversals, or returns. The value is guaranteed unique for 90 days and may be unique for up to one year.

3.4.4 Validating Response Codes

All request messages to Portico include a Header and a Transaction block. Responses always include a Header block, but only include the Transaction block when Portico was able to successfully process the request (i.e., GatewayRspCode is 0). See Gateway Response Codes for additional information.

When present, the Transaction block always includes the Transaction type (i.e., CreditSale).

The GatewayRspCode in the response header can be inspected to determine if the request was fully processed by Portico. A GatewayRspCode of 0 means that Portico was able to process the request and that the Transaction block is present. The GatewayRspCode does not indicate approval or decline of the transaction.

To get the final result of the transaction, the Transaction block must be further inspected to see if there is an Issuer RspCode. See Issuer Response Codes for additional information.

3.4.4.1 Gateway Response Codes and Reversals

Transaction response objects contain a Gateway Response Code in the header; when the Gateway Response Code indicates an approval, there will be a response body that contains a Response Code (RspCode) which is the host or issuer response code. Some response codes indicate that the result of the transaction is unknown.

When the result of the transaction is unknown, a reversal must be sent to clear any hold that the authorization placed on cardholder funds.

If any of the following Gateway Response Code values are received, the transaction result is unknown and it may have processed. In each case, a Reversal should be sent:

Gateway Response Code	Reason for Reversal
1	Gateway System Error
30	This can occur when Portico does not receive a response from the back end systems and Portico is not sure if the transaction was successful or not. In this case, the POS is responsible for deciding whether or not to issue a reversal for this transaction. This is used in cases where the transaction is an authorizing transaction, e.g., CreditAuth, CreditSale, DebitSale. If the transaction is non-authorizing, e.g., CreditAccountVerify, CreditReversal, and Portico receives no response, then Portico sends back a System Error (+1) to the POS.
31	This occurs when Portico attempts a reversal for the POS, but the reversal fails. In this case, the POS is responsible for issuing the reversal.
50	Processor System Error

3.4.5 Timeouts

Transactions are typically on Heartland systems for less than 600ms, but the POS system needs to allow sufficient time to receive a response, including considerations for network latency, processing delays, or other issues. Portico waits for other back-end systems to reply, which can vary by transaction type:

Transaction Type	Portico Timeout
Credit/Debit	30 seconds
Gift	20 seconds
ACH	30 seconds
Batch Close	95 seconds
Report Transactions	505 seconds

Portico recommends that the POS timeout value be set at least a few seconds above the Portico timeout value.

- If Portico returns a GatewayRspCode of 30 for a financial transaction, the POS should initiate a reversal using the GatewayTxnId. (For ACH transactions, use CheckVoid.)
- If the transaction does not receive a response from Portico for a financial transaction, a reversal should be initiated using the ClientTxnId. (For ACH transactions, use CheckVoid.)

> ClientTxnId is strongly recommended for all transactions; it is required for timeout reversals.

For the FindTransactions report, actual response time depends on the amount of data and the date range of the search.

To improve response time, adjust the criteria being used to obtain a smaller result set.

For Payment facilitator sub-merchants, Portico recommends a POS timeout of 150 seconds for all financial transactions.

3.4.6 Transaction Amounts

There are many amounts that are received, sent, stored, and maintained by Portico. The purpose of this section is to define some of the key amounts that appear in the messages, reports, and settlement:

Key Amount	Description
Amt	This may also be referred to as original amount or request amount. This is the amount that the POS originally sent to Portico for a particular transaction. This amount is kept by Portico for the life of the transaction and is not altered.
AuthAmt	This may also be referred to as an authorized amount. This is the amount that was originally authorized/approved by the issuer. In the case of a full approval, this matches the Amt. In the case of a partial approval, this is equal to or less than Amt. This amount is kept by Portico for the life of the transaction and is not altered.
SettlementAmt	This is the amount that is used if the transaction is settled. When a transaction is first approved, this matches the AuthAmt. This amount is maintained by Portico over the life of the transaction. This is altered by reversals, transaction edits, incremental transactions, etc.

Maximum Size of Amount Fields

Portico supports a maximum of 12 digits in amount fields, inclusive of decimal places. Please note that the GNAP-UK Authorization Platform supports a maximum of 11 digits for amount values, inclusive of decimal places.

Currency and Amounts

Portico supports many different currency codes. The currency codes for a TID must be one that is supported by the settlement systems of the Authorization Platform. The format of any amount fields in a transaction request must be consistent with the currency code of the TID.

Currency Minor Units	Amount in Transaction Request	Format to Issuer
0	1	1
	1.0	1
	1.1	Returns Error
2	1	1.00
	1.1	1.10
	1.11	1.11
	1.111	Returns Error
3	1	1.000

Currency Minor Units	Amount in Transaction Request	Format to Issuer
	1.1	1.100
	1.11	1.110
	1.111	1.111
	1.1111	Returns Error

Estimated and Final Amounts

Portico supports the option to indicate whether the amount requested in a credit transaction is Estimated or Final. This indicator is passed through to the host and the appropriate card brands for merchants processing on all authorization platforms. It is expected that CreditAuth or RecurringBillingAuth is used when the amount is estimated (for example, where a tip may be added afterwards or an hourly rental is not returned on time), and that CreditSale or RecurringBilling is used when the final amount is known at the time of the request.

To indicate whether the transaction amount is estimated or final, send the AmountIndicator field.

3.4.7 Transaction Currency

For merchants processing on the Exchange authorization platform, the only allowed currency is United States Dollar (USD / ISO Code 840).

For merchants processing on the GSAP-NA or GSAP-AP authorization platforms, transactions process in the currency specified for the DeviceId at boarding (DeviceSetting "Currency"); if a Currency is not specified for the DeviceId, then the value set for the SiteId at boarding (Site "CurrCode") is used.

The currency value set in Portico must match the currency value for the TID on the authorization platform and must, therefore, be a currency value that the authorization platform also supports.

The currency specified will apply to all "Amt" fields in the Portico schema except for Dynamic Currency Conversion>CardholderAmt.

> **Note**: Portico supports all ISO currencies that are supported by Global Payments settlement systems, including currencies with 0, 2, or 3 minor units.

This is different from Dynamic Currency Conversion.

3.4.8 Specified Flags for Optional Elements

Optional elements are notated in the XML schema by a minOccurs="0" attribute. In order to provide a value in an element that is optional, it may be required to also set a "specified" flag. This is required for optional elements that are of a type that is not nullable. The specified flag is generated in code from the service reference as <fieldname>Specified.

The problem is that fields in .NET that cannot be null will always have a valid value (i.e., "0"). On the other hand, the

XML schema defines it as optional:

```
<xs:element minOccurs="0" name="ID" type="xs:int"/>
```

Given this, there is no way for the .NET client to know whether the value of "0" means there is no value defined or if the true intent is to send the value "0" to the server.

The Specified flag takes care of this situation:

- If the field value is "0" and <field>Specified="false", no value was defined and the element will not be included in the message that results from serialization.
- If the field value is "0" and <field>Specified="true", the element will be included in the message that results from serialization with the value "0".

Unfortunately, this is not only in the "0" value case. For data types such as xs:int, xs:long, xs:decimal, xs:dateTime, and xs:string elements with specific enumeration values (i.e., booleanType, currencyType), the specified flag must be set to true in addition to setting the desired value.

For example, the optional field GatewayTxnId (type xs:int) needs to have an associated flag of GatewayTxnIdSpecified. To send a transaction id of 1234, the client must set GatewayTxnId="1234" and set GatewayTxnIdSpecified="true".

3.5 TestCredentials

A TestCredentials transaction validates the credentials passed in the transaction, but does not perform an action. TestCredentials should only be used at the beginning of the certification period to validate credentials and connectivity to the certification environment.

> This should not be used as a "heartbeat" check and it is not required for running transactions.

The TestCredentials transaction includes the transaction request and response headers with only the transaction type in the Transaction block of the request and response. This represents the least of the possible Portico request and response messages.

3.6 API Key Activation

To support secure credential handling for terminal hardware, the Activation transaction may be used to exchange an activation code for the authentication token. See Activation in Transactions.

> The request and response header for Activation is unique.

4 Transactions

The following table provides links to all the available Portico transactions, including detailed documentation and code examples:

Transaction	Schema Documentation	Description
Activation	Request / Response	Activation is used to obtain the authentication token for the terminal hardware.
AddAttachment	Request / Response	AddAttachment can be used to store and associate data (e.g., images, documents, signature capture, etc.) to a prior transaction.
Authenticate	Request / Response	Authenticate is used to authenticate a specific user. For this call, the header must include username and password.
BatchClose	Request / Response	BatchClose is used to settle and close the current open batch.
CancelImpersonation	Request / Response	CancelImpersonation is used to terminate a previously started impersonation session.
CashReturn	Request / Response	CashReturn creates a log of a transaction that is returning cash to a customer. NOTE: This is processed offline.
CashSale	Request / Response	CashSale creates a log of a transaction, in which cash is collected from a customer. This is processed offline.
CheckSale	Request / Response	CheckSale transactions use bank account information as the payment method. There are sub-actions that can be taken as part of the CheckSale as indicated by the CheckAction field.
CheckQuery	Request / Response	CheckQuery is used to query info about a check transaction.
CheckVoid	Request / Response	CheckVoid is used to cancel a previously successful CheckSale transaction. It can also be used to cancel a prior CheckSale transaction. This should be used in timeout situations or when a complete response is not received.
ChipCardDecline	Request / Response	ChipCardDecline is used to record an offline decline by an EMV chip card.
CreditAccountVerify	Request / Response	CreditAccountVerify is used to verify that the associated account is in good standing with the Issuer.
CreditAdditionalAuth	Request / Response	CreditAdditionalAuth is typically used in a bar or restaurant situation where the merchant obtains the payment information for an original CreditAuth but does not want to

		hold the card or ask for it on each additional authorization. This service has been deprecated. See CreditIncrementalAuth
CreditAddToBatch	Request / Response	CreditAddToBatch is primarily used to add a previously approved open authorization (CreditAuth, CreditOfflineAuth, or RecurringBillingAuth) to the current open batch. If a batch is not open, this transaction will create one. It also provides the opportunity to alter data associated with the transaction (i.e., add a tip amount).
CreditAuth	Request / Response	CreditAuth authorizes a credit card transaction. These authorization only transactions are not added to the batch to be settled. They can be added to a batch at a later time using CreditAddToBatch. Approved authorizations that have not yet been added to a batch are called open auths.
CreditCPCEdit	Request / Response	CreditCPCEdit attaches Corporate Purchase Card (CPC) data to a prior transaction. This information will be passed to the issuer at settlement when the associated card was a corporate card or an AMEX card.
CreditIncrementalAuth	Request / Response	CreditIncrementalAuth adds to the authorized amount for a prior transaction.
CreditIPQuery	Request / Response	CreditIPQuery returns the Installment Payment terms available to the cardholder. This is currently only supported for the AP Region. Refer to the Authorization Platform section for further details.
CreditOfflineAuth	Request / Response	CreditOfflineAuth records an authorization obtained outside of the gateway (e.g., voice authorization, chip card offline approval). These authorization only transactions are not added to the batch to be settled. They can be added to a batch at a later time using CreditAddToBatch. Approved authorizations that have not yet been added to a batch are called open auths.
CreditOfflineSale	Request / Response	CreditOfflineSale records an authorization obtained outside of the gateway (e.g., voice authorization, chip card offline approval).
CreditReturn	Request / Response	CreditReturn allows the merchant to return funds back to the cardholder.

		Returns can be for the entire amount associated with the original sale or a partial amount. Returns made using the GatewayTxnId can be performed for up to one year from the original authorization date. For the Exchange host only, refunds may be processed offline or online, depending on merchant settings. To enable online refunds, contact your representatve. For all other Authorization Platforms, refunds are sent online to the host and the host determines whether the issuer participates in online returns.
CreditReversal	Request / Response	CreditReversal cancels a prior authorization in the current open batch. This can be used in timeout situations or when a complete response is not received. In either case, the client is unsure of the outcome of the prior transaction.
CreditSale	Request / Response	CreditSale authorizes a credit card transaction. These authorizations are automatically added to the batch to be settled. If a batch is not already open, this transaction will create one.
CreditTxnEdit	Request / Response	CreditTxnEdit allows the merchant to alter the data on a previously approved CreditSale, CreditAuth, CreditOfflineSale, or CreditOfflineAuth (i.e., add a tip amount).
CreditVoid	Request / Response	CreditVoid is used to cancel an open auth or remove a transaction from the current open batch. The original transaction must be a CreditAuth, CreditSale, CreditReturn, CreditOfflineAuth, CreditOfflineSale, RecurringBilling, or Recurring Billing Auth.
DebitAddToBatch	Request / Response	DebitAddToBatch is used to add a pre-authorized debit transaction to the open batch. If a batch is not open this transaction will create one. **NOTE**: For Canadian Interac debit only.
DebitAuth	Request / Response	DebitAuth obtains a pre-authorization of funds on a debit card. These authorization-only transactions are not added to the batch to be settled. They can be added to a batch at a later time using DebitAddToBatch. **NOTE**: For Canadian Interac debit only.
DebitReturn	Request / Response	DebitReturn allows the merchant to return funds from a prior debit sale back to the cardholder. Returns can be for the entire amount associated with the original sale or a partial amount. Returns made using the GatewayTxnId can be performed for up to one year from the original authorization date.

		Support for EMV PIN Debit has been added.
DebitReversal	Request / Response	DebitReversal cancels a previous DebitSale transaction. This should be used in timeout situations or when a complete response is not received. In either case, the client is unsure of the outcome of the prior transaction. Support for EMV PIN Debit has been added.
DebitSale	Request / Response	DebitSale authorizes a debit card transaction. Support for EMV PIN Debit has been added.
EBTBalanceInquiry	Request / Response	EBTBalanceInquiry returns the available balance for an EBT account.
EBTCashBackPurchase	Request / Response	EBTCashBackPurchase is used to purchase goods with EBT Cash Benefits.
EBTCashBenefitWithdrawal	Request / Response	EBTCashBenefitWithdrawal is used to disburse cash from an EBT Cash Benefits account.
EBTFSPurchase	Request / Response	EBTFSPurchase is used to purchase goods with SNAP.
EBTFSReturn	Request / Response	EBTFSReturn is used to credit previously debited funds to a SNAP account for merchandise returned.
EBTFSReversal	Request / Response	EBTFSReversal cancels a previous EBTFSPurchase, EBTCashBackPurchase, EBTFSReturn, and EBTCashBenefitWithdrawal transactions. This should be used in timeout situations or when a complete response is not received. In either case, the client is unsure of the outcome of the prior transaction.
EBTVoucherPurchase	Request / Response	EBTVoucherPurchase is obsolete and should no longer be used.
EndToEndTest	Request / Response	EndToEndTest for internal use only.
FindTransactions	Request / Response	FindTransactions is used to search all current gateway transactions based on provided filter criteria.
GetAttachments	Request / Response	GetAttachments is used to retrieve attachments (i.e., documents, images, etc.) associated with a particular transaction.
GetUserDeviceSettings	Request / Response	GetUserDeviceSettings is for internal use only.
GetUserSettings	Request / Response	GetUserSettings is for internal use only.
GiftCardActivate	Request / Response	GiftCardActivate is used to activate a new stored value account and load it with an initial balance.
GiftCardAddValue	Request / Response	GiftCardAddValue loads an amount onto a stored value account.
GiftCardAlias	Request / Response	GiftCardAlias allows the client to manage stored account

		aliases. An alias is an alternate identifier used to reference a stored value account.
GiftCardBalance	Request / Response	GiftCardBalance is used to retrieve the balance(s) for each currency supported by a stored value account.
GiftCardCurrentDayTotals	Request / Response	GiftCardCurrentDayTotals is used to retrieve stored value transaction totals for the current day. This transaction is obsolete and should no longer be used. FindTransactions can be used as an alternative.
GiftCardDeactivate	Request / Response	GiftCardDeactivate is used to deactivate an active stored value account that otherwise has not been used.
GiftCardPreviousDayTotals	Request / Response	GiftCardPreviousDayTotals is used to retrieve stored value transaction totals for the previous day.
GiftCardReplace	Request / Response	GiftCardReplace transfers balances from one stored value account to another. This is typically to replace a lost or stolen account with a new one or to consolidate two or more accounts into a single account.
GiftCardReversal	Request / Response	GiftCardReversal is used to cancel a prior stored value transaction. This should be used in timeout situations or when a complete response is not received. In either case, the client is unsure of the outcome of the prior transaction.
GiftCardReward	Request / Response	GiftCardReward is used when an account holder makes a payment using a payment form other than a stored value account (e.g., cash or credit card). The account holder may present their stored value account to earn points or other loyalty rewards, which would be added to their account.
GiftCardSale	Request / Response	GiftCardSale is used to redeem value from a stored value account.
GiftCardVoid	Request / Response	GiftCardVoid is used to cancel a prior successful transaction. When voiding a transaction, all changes to the account are reversed, including any additional value added by rewards programs or automated promotions.
Impersonate	Request / Response	Impersonate is for internal use only.
InteracDeviceKeys	Request / Response	InteracDeviceKeys allows a merchants to re-synchronize the keys for Canadian Debit transactions.
InvalidateAuthentication	Request / Response	InvalidateAuthentication is for internal use only.
ManageSettings	Request / Response	ManageSettings is for internal use only.

ManageTokens	Request / Header (response only)	ManageTokens allows merchants to update information referenced by a specific multi-use token.
ManageUsers	Request / Response	ManageUsers is for internal use only.
ParameterDownload	Request / Response	ParameterDownload is used to initiate an EMV parameter download by clients interfacing to an EMV device.
RecurringBilling	Request / Response	RecurringBilling authorizes a one-time or scheduled recurring transaction.
RecurringBillingAuth	Request / Response	Like the RecurringBilling service, this also authorizes a one-time or scheduled recurring transaction. However, these authorization only transactions are not added to the batch to be settled. They can be added to a batch at a later time using CreditAddToBatch. Approved authorizations that have not yet been added to a batch are called open auths.
ReportActivity	Request / Response	ReportActivity returns all activity between the client devices and gateway for a period of time. This can be filtered to a single DeviceId if needed. This report is obsolete and should not be used. FindTransactions can be used as an alternative.
ReportBatchDetail	Request / Response	ReportBatchDetail returns information on each transaction currently associated to the specified batch. This report is for the SiteId and DeviceId referenced in the header.
ReportBatchHistory	Request / Response	ReportBatchHistory returns information about previous batches over a period of time. This report is for the SiteId referenced in the header.
ReportBatchSummary	Request / Response	ReportBatchSummary returns a batch's status information and totals broken down by payment type. This report is for the SiteId and DeviceId referenced in the header.
ReportOpenAuths	Request / Response	ReportOpenAuths returns all authorizations that have not been added to a batch for settlement. This report is for the SiteId referenced in the header.
ReportSearch	Request / Response	ReportSearch returns transaction information for a specified time period. This report is obsolete and should not be used. FindTransactions can be used as an alternative.
ReportTxnDetail	Request / Response	ReportTxnDetail returns detailed information about a single transaction.

		This report is for the SiteId and DeviceId referenced in the header.
RewardCashQuery	Request / Response	RewardCashQuery returns the available points from a stored account, if any, and authorizes a loyalty transaction. It is applicable only for Reward Cash terminals in the AP Region and is for future use.
RewardCashRedeem	Request / Response	RewardCashRedeem is a loyalty transaction that redeems value from a stored account. This transaction is automatically added to the Reward Cash batch. It is applicable only for Reward Cash terminals in the AP Region and is for future use.
SendReceipt	Request / Response	SendReceipt is for internal use only. It allows a client to send a receipt from a prior transaction out to specific destinations. The prior transaction must belong to the SiteId and DeviceId referenced in the header.
TestCredentials	Request / Response	TestCredentials validates the credentials passed in the header, but does not perform an action.
Tokenize	Request / Header (response only)	Tokenize allows the client to request a multi-use token using the provided card data without having the card data verified by the issuer. Card input data may not be a Single Use token.

4.1 Credit Card Transactions

The following table provides links to the credit card transactions:

Transaction Name	Request	Response
ChipCardDecline	Request	Response
CreditAccountVerify	Request	Response
CreditAdditionalAuth	Request	Response
CreditAddToBatch	Request	Response
CreditAuth	Request	Response
CreditCPCEdit	Request	Response
CreditIncrementalAuth	Request	Response
CreditIPQuery	Request	Response
CreditOfflineAuth	Request	Response
CreditOfflineSale	Request	Response
CreditReturn	Request	Response
CreditReversal	Request	Response
CreditSale	Request	Response
CreditTxnEdit	Request	Response
CreditVoid	Request	Response
RecurringBilling (one-time payment)	Request	Response
RecurringBillingAuth	Request	Response

4.2 Debit Card Transactions

The following table provides links to the debit card transactions:

Transaction Name	Request	Response
DebitAddToBatch	Request	Response
DebitAuth	Request	Response
DebitReturn	Request	Response
DebitReversal	Request	Response
DebitSale	Request	Response

4.3 Cash Transactions

The following table provides links to the cash transactions:

Transaction Name	Request	Response
CashReturn	Request	Response
CashSale	Request	Response

4.4 Check/ACH Transactions

The following table provides links to the check/ACH transaction type pages:

Transaction Name	Request	Response
CheckSale	Request	Response
CheckQuery	Request	Response
CheckVoid	Request	Response
RecurringBilling (one-time payment)	Request	Response

4.5 EBT Transactions

The following table provides links to the EBT transactions. Portico does not impose any industry-specific limitations on EBT transactions, but downstream systems may. Typical industries for EBT would be Restaurant and Retail:

Transaction Name	Request	Response
EBTBalanceInquiry	Request	Response
EBTCashBackPurchase	Request	Response
EBTCashBenefitWithdrawal	Request	Response
EBTFSPurchase	Request	Response
EBTFSReturn	Request	Response
EBTFSReversal	Request	Response
EBTVoucherPurchase	Request	Response

4.6 Gift Card and Loyalty Transactions

The following table provides links to the gift card and reward cash transactions:

Transaction Name	Request	Response
GiftCardActivate	Request	Response
GiftCardAddValue	Request	Response
GiftCardAlias	Request	Response
GiftCardBalance	Request	Response
GiftCardDeactivate	Request	Response
GiftCardReplace	Request	Response
GiftCardReversal	Request	Response
GiftCardReward	Request	Response
GiftCardSale	Request	Response
GiftCardVoid	Request	Response
RewardCashQuery*	Request	Response
RewardCashRedeem*	Request	Response

*These transactions are for future use and will only be applicable to the Asia Pacific Region.

4.7 Utility Transactions

The following table provides links to some utility function transactions:

Transaction Name	Request	Response
Activation*	Request	Response
GetAttachments	Request	Response
InteracDeviceKeys	Request	Response
ManageTokens	Request	Header (response only)
ParameterDownload	Request	Response
TestCredentials	Request	Response
Tokenize	Request	Header (response only)

*Activation transactions have a unique header format that is different from all other transactions.

4.8 Batch Transactions

The following table provides links to the batch transactions:

Transaction Name	Request	Response
BatchClose	Request	Response

4.9 Report Transactions

The following table provides links to the report transactions:

Transaction Name	Request	Response
FindTransactions	Request	Response
ReportBatchDetail	Request	Response
ReportBatchHistory	Request	Response
ReportBatchSummary	Request	Response
ReportOpenAuths	Request	Response
ReportTxnDetail	Request	Response

4.10 Internal Use Only Transactions

The following table provides links to transactions that are only available internal to Heartland:

Transaction Name	Request	Response
Authenticate	Request	Response
CancelImpersonation	Request	Response
EndToEndTest	Request	Response
GetUserDeviceSettings	Request	Response
GetUserSettings	Request	Response
Impersonate	Request	Response
InvalidateAuthentication	Request	Response
ManageSettings	Request	Response
ManageUsers	Request	Response
SendReceipt	Request	Response

5 Authorization Platform

Portico routes transactions to different authorization platforms. Some services are handled differently for each platform (also referred to as a Host). Supported authorization platforms for transaction processing are:

- Exchange (US)
- GNAP-UK (United Kingdom)
- GSAP-AP (Asia Pacific), and
- GSAP-NA (US, Canada, Mexico, & Bermuda)

If you are unsure which Authorization Platform you process on, contact your representative.

For merchants using Dynamic Currency Conversion, transactions may be routed to:

- FexCo (UK merchants only), routed via the GNAP-UK host, or
- Planet Payments (supported for GSAP-AP and GSAP-NA)

5.1 GNAP-UK

The GNAP-UK platform supports merchants processing in the UK. For merchants processing on GNAP-UK, please note the following:

- Portico supports Credit processing with the UK authorization platform for card present and MOTO card not present transactions
- Merchants processing on this host must perform Batch Close daily, either POS-initiated, or using Portico's auto-close functionality
- ECommerce industry support is not available at this time
    - In the UK, Recurring processing is considered an eCommerce function and therefore Recurring Billing is not supported
- Credential/Card on File support is not applicable to this integration
- Tip/gratuity is added by the cardholder at the time of purchase and is included in the total authorization amount
- Credit Offline Auth is not supported
- Gift card and ACH processing is not available at this time
- Multi-use tokenization via the ETS service is not available at this time
- EMV Parameter Download is not available through Portico; please contact your representative for information
- Interchange benefits for Corporate Cards do not apply in the UK
- Dynamic Descriptor is not supported in the UK market
- Device Configuration data is required on every transaction; this must reflect the capabilities for which the DeviceId is certified
- Amount values for the UK host are limited to 11 total digits
- Union Pay transactions may now be processed direct to UnionPay

5.2 GSAP-NA

The GSAP-NA platform supports merchants processing in the US, Canada, Mexico, & Bermuda. For merchants processing on GSAP-NA, please note the following:

- Check/ACH and HMS Gift transactions are not available for US merchants at this time
- HMS Gift transactions are supported for Canadian merchants
- EMV Parameter Download may not be handled by Portico; please contact your representative for information
- Multi-use tokenization is supported; please contact your representative for information
- For merchants using CreditTxnEdit, the request may either contain final (completion) EMV tags **or** other updates
- For merchants using Incremental Authorizations, the initial transaction **must** be a CreditAuth
- Batch management may be handled by either the host or Portico; see Batch Processing

For merchants processing in **Canada**, please note:

- Canadian debit transactions are processed via Interac; see Interac Processing for further details
- There are different options for routing for UnionPay transactions; see UnionPay for further details

For merchants processing in **Mexico**, please note:

- Cashback may be requested on credit transactions, for local Mexican-issued cards only
- Installment Payments may be supported via CreditAuth and CreditSale transactions; see Installment Payments for further details
- CreditAuth and CreditSale requests may include cashback amount in the request; approval is determined by the issuer
- Card on File is not supported in Mexico

5.3 GSAP-AP

The GSAP-AP platform supports merchants processing in Macao, Hong Kong, Singapore, Philippines, Malaysia, Maldives, and Sri Lanka . For merchants processing on GSAP-AP, please note the following:

- Check and Gift transactions are not available at this time
- EMV Parameter Download may not be handled by Portico; please contact your representative for information
- Multi-use tokenization is supported; please contact your representative for information
- Installment payments are support. See: Installment Payments
- For merchants using Incremental Authorizations, the original transaction **must** be a CreditAuth
- Each new TID must be initialized on the AP host. Initialization can be performed via Portico by sending an empty BatchClose request prior to processing transactions
- Batch management may be handled by either the host or Portico; see Batch Processing

5.4 Planet Payment

Planet Payment is a provider of international payment processing and multi-currency processing services. It is an authorization host for Dynamic Currency Conversion (DCC). Please note that merchants using Planet Payment must have Portico-based batch management; see Batch Processing.

6 Special Processing Rules

While the schema includes some requirements and restrictions, it also provides many options for the integrator to choose from.

This section is intended to provide additional details around specific processing scenarios that should be considered during integration. These details include special payment methods and industries, assistance in getting improved interchange rates, settlement processing, Portico storage rules, card brand and issuer requirements that are not enforced by the schema, and more.

6.1 Address Verification Service (AVS)

The Address Verification Service is a system that verifies the personal address and billing information provided by a customer at the time of the transaction against the information the credit card Issuer has on file. AVS enhances fraud protection and must be present on keyed transactions to receive the best Interchange rates.

Some Issuers decline the sale if the AVS data does not match; however, most Issuers approve the sale and it is up to the merchant to make a decision to go forward with the sale based upon the AVS response code. It is strongly recommended that the merchant ask the cardholder for another form of payment if the AVS data does not match ("N" AVS response).

A POS system may develop logic to reject a transaction when the AVS data does not match. For example, if a mismatch response is received, the application may generate a CreditReversal for the original CreditSale or CreditAuth and prompt for another form of payment. Generating a CreditReversal is recommended since the original authorization was approved even though the AVS data did not match.

AVS data submitted as part of a transaction requesting a token, e.g., CreditAccountVerify, is completely independent from any other transaction using that token. Subsequent transactions using the token may or may not need AVS data depending on the transaction characteristics.

Portico only supports AVS for US and Canadian addresses.

The following table outlines the AVS Response Codes that may be returned by Portico:

Application Service	Visa	Discover/JCB	Mastercard	AMEX
Address matches, zip code does not	A	A	A	A
Neither address or zip code match	N	N	N	N
Retry — system unable to respond	R	R	R	R
AVS not supported	U	U	S	S
No data from Issuer/auth system	U	U	U	U
9-digit zip code match, address does not match	Z	Z	W	W
9-digit zip code and address match	Y	Y	X	X
5-digit zip code and address match	Y	Y	Y	Y
5-digit zip code match, address does not match	Z	Z	Z	Z
Address and zip code match (UK only)	F	(N/A)	Y	Y
Address information not verified for International transaction	G	G	(N/A)	(N/A)
Address matches, postal code does or request does not include postal code (international address)	A	A	(N/A)	(N/A)
Address match, postal code not verified due to incompatible formats (international address)	B	B	(N/A)	(N/A)
Address and postal code not verified due to incompatible formats (international address)	C	C	(N/A)	(N/A)
Street address and postal code match (international address)	D	D	(N/A)	(N/A)
Address information not verified for International transaction	I	I	(N/A)	(N/A)
Street address and postal code matches	M	M	(N/A)	(N/A)
Postal code match and street address not verified due to incompatible formats (international address)	P	P	(N/A)	(N/A)
AVS not requested	0	0	0	0
Unrecognized AVS code	?	?	?	?

6.1.1 Card Not Present Transactions

Full AVS (street address and zip code) is required on all Mail Order/Telephone Order (MOTO) and eCommerce transactions.

6.1.2 Card Present Transactions

AVS is optional on retail and restaurant card present keyed transactions.

6.2 Adjustments

An original financial transaction can be adjusted using CreditAddToBatch or CreditTxnEdit. If the edit service is used, the client will still need to add the transaction to the batch in order for it to settle. Adjustments can be made for additional charges, gratuity, additional detail, fees, EMV data, etc.

For adjustments regarding corporate card transactions, see Corporate Cards.

To increase the authorized amount of a CreditAuth, use CreditIncrementalAuth.

> **Note**: CreditIncrementalAuth is restricted to certain MCCs.

6.3 Auto-Substantiation

An Auto-Substantiation transaction is applied to either a CreditAuth or to a CreditSale transaction. The first additional amount must be the "Total_Healthcare_Amt" followed by up to three additional optional data amount elements, which include the amount type and the amount. Valid amount types are as follows:

- Total_Healthcare_Amt—Indicates the total of all healthcare amounts.
- Subtotal_Prescription_Amt—Indicates the subtotal amount of prescriptions.
- Subtotal_Vision_Optical_Amt—Indicates the subtotal amount of vision/optical.
- Subtotal_Clinic_Or_Other_Amt—Indicates the subtotal amount of clinic and other qualified medical.
- Subtotal_Dental_Amt—Indicates the subtotal amount of dental.

> The value supplied in the Total_Healthcare_Amt is the combined total of the four subtotal amounts. The Total_Healthcare_Amt can include over-the-counter (OTC) amounts only or, if there are other healthcare expenses, the total of all categories: OTC, prescriptions, vision, clinic, and dental.

> The total amount of the associated transaction must be at least equal to (not less than) the Total_Healthcare_Amt. It can be greater than the Total_Healthcare_Amt if non-healthcare items are also being purchased as part of the transaction.

The Auto-Substantiation data also includes a field containing the Merchant Verification Value. It is not necessary to submit this field. It is populated from the merchant profile by Heartland.

See the AutoSubstantiation Complex Type in the Portico Schema. Applicable to US merchants only.

6.4 Batch Processing

Merchant batches may be handled by Portico for all merchants on all Authorization Platforms. Merchants processing on the GSAP-NA and GSAP-AP Authorization Platforms have the option to be set up for the host to manage their batch.

Portico-Based Batch Management

Portico supports Portico-based batch management for merchants processing on all Authorization Platforms. Portico-based batch management is the default configuration for a DeviceId. For merchants processing on the GSAP-NA and GSAP-AP Authorization Platforms, this is known to the host as HBMI. When Portico manages the batch, the POS can use the Portico API to manipulate transactions and batches. It can also request Portico to close a batch. However, the POS does not provide any additional details or updates in the close request itself and does not stream a batch to Portico.

Batches are maintained at the DeviceId level. If a site (merchant) has multiple DeviceIds, each is closed individually. If a DeviceId does not have an open batch, the next financial transaction will create a new open batch. This means that a CreditAccountVerify or CreditAuth request does not open a batch, but a CreditSale or CreditAddtoBatch would open a new batch.

Please note that due to the requirements for Portico to stream batch details to payment facilitators, payment facilitators and their submerchants must be set up for Portico-based batch management. Due to split batch management, the following merchant configurations require Portico-based batch management:

- Merchants using Dynamic Currency Conversion with Planet Payment
- UK merchants processing Union Pay transactions via the GSAP-AP host

Batch information will be removed from Portico after 90 days.

Host-Based Batch Management

Portico supports Host-based batch management for merchants processing on the GSAP-NA and GSAP-AP Authorization Platforms. This is known to the host as HBTI. With HBTI, the host manages and closes the batch at a specified time or as needed, for example, when a transaction count threshold has been met. There is no concept of a batch in Portico. Batch reports and the BatchClose request are not supported.

Please note that the DeviceId must be configured in Portico to properly enable HBTI.

Maximum Batch Amount

The total amount of all transactions in a batch cannot exceed 9,999,999,999.99

Batch Size

Exchange: The Exchange host has not published a maximum batch size. For ideal batch management, maximum size should be less than 10,000 transactions.

GSAP-AP: The maximum Batch Size is limited to 900 transactions. Portico will return an error when this threshold is reached. No additional transactions can process until the current batch is closed.

GSAP-NA: The Maximum Batch Size is limited to 9,999 transactions. The GSAP host will return an error when this threshold is reached. No additional transactions can process until the current batch is closed.

GNAP-UK: Maximum batch size is 9,999 transactions

Batch Handling

For Portico-based batch management, batch handling is custom to each Host Processor.

Exchange: Portico is the system of record for transactions, batches, and settlement details. During BatchClose, Portico streams the batch to the Exchange Host.

GSAP-AP: Portico is the system of record for transactions, batches, and settlement details. During BatchClose, Portico checks the batch count and batch total with the host. If the totals match, the batch is closed. If the totals do not match, Portico streams the batch to the host.

GSAP-NA: The GSAP-NA host is the system of record for transactions, batches, and settlement details. During BatchClose, Portico checks the batch count and batch total with the host. If the totals match, the batch is closed. If the totals do not match, Portico requests that the host force close the batch.

GNAP-UK: The GNAP host is the system of record for transactions, batches, and settlement details. During BatchClose, Portico sends the batch count and batch total with the host and closes the batch.

Planet Payment: Portico is the system of record for transactions, batches, and settlement details. During BatchClose, Portico checks the batch count and batch total with the host. If the totals match, the batch is closed. If the totals do not match, Portico uploads the batch to Planet Payment. Portico verifies the batch count and total with Planet Payment and closes the batch.

Batch Management for Merchants using DCC

Most DeviceIds have one authorization host only. Merchants accepting DCC with Planet Payments have an authorization host for their domestic transactions and have Planet Payment host their DCC transactions. In this situation, the Portico DeviceId maintains separate counts and totals for domestic and DCC transactions. During batch close, Portico sends the appropriate settlement message to each host and manages the responses to close the batch successfully. If one host batch does not close, the batch will be in error status.

Merchants enabled for Planet Payment must have Portico-based batch management.

6.4.1 Settlement

For Portico-based batch management, Portico supports auto and manual batch close options. The POS can use either or both of these options.

- Auto-Close
- Manual Batch Close

6.4.1.1 Auto-Close

Any DeviceId, with the exception of those set up for Host-based batch management, can be configured to request that the current open batch be closed automatically by Portico. When auto-close is enabled in the device configuration, a specific time of day is specified in local time. This is recommended, but optional, and can be disabled if only the manual close option is desired.

When the auto-close time is reached each day, Portico queues up the associated batch to be closed.

> There can be a delay between the chosen auto-close time and the actual processing of the batch. This can vary based on the number of devices closing at the same time, system issues, or other factors.

The default on Portico is to continue to add the transactions to the same batch until it is processed. This ensures that the maximum number of transactions are processed at the time of settlement.

Portico does provide an option to ensure that no new transactions are added to a batch after the auto-close time. This can be important to some merchants in the case that there is a delay in the batch processing after the auto-close time.

6.4.1.2 Manual Batch Close

Any DeviceId, with the exception of those set up for Host-based batch management, can be configured to request that the current open batch be closed. See Batch Transactions > BatchClose.

6.5 Card Data Manual Entry

Card data information must be manually keyed into the application when any of the following is true:

- a card is not present
- a card or chip reader is unavailable
- the magnetic stripe or chip is unreadable

For card present transactions, manual entry is discouraged because it usually results in higher transaction fees for the merchant and increases the likelihood of keying errors, which result in delays and/or chargebacks.

For card not present transactions, manual entry is the only method for entering the card number. The use of a Mod 10 check routine (also known as the Luhn algorithm) reduces the number of keying errors. The routine is a checksum formula used to validate the card number that is keyed into your application.

6.6 CAVV Results Codes

For secure eCommerce, the Cardholder Authentication Verification Value (CAVV) validates information provided by a customer at the time of the transaction. The CAVV Results Code contains the Visa or Discover Cardholder Authentication Verification Value Results Code or the American Express Verification Value (AEVV) Validation Results. The following table outlines the CAVV Result Codes that may be returned by Portico:

Code	Visa	AMEX	Discover
Blank or not present	CAVV not present		
0	CAVV could not be verified or CAVV data was not provided when expected	Reserved for future use	Unable to perform CAVV authentication
1	CAVV failed validation—authentication	AEVV failed—Authentication, Issuer	CAVV authentication failed
2	CAVV passed validation—authentication	KeyAEVV passed—Authentication, Issuer Key	CAVV authentication successful
3	CAVV passed validation—attempt	AEVV passed—Attempt, Issuer Key	
4	CAVV failed validation—attempt	AEVV failed—Attempt, Issuer Key	
5	Not used (reserved for future use)	Reserved for future use	
6	CAVV not validated, issuer not participating in CAVV validation	Reserved for future use	
7	CAVV failed validation—attempt	AEVV failed—Attempt, Issuer not participating, Network Key	
8	CAVV passed validation—attempt	AEVV passed—Attempt, Issuer not participating, Network Key	
9	CAVV failed validation—attempt	AEVV failed—Attempt, Participating, Access Control Server (ACS) not available, Network Key	
A	CAVV passed validation—attempt	AEVV passed—Attempt, Participating, Access Control Server (ACS) not available, Network Key	
B	CAVV passed validation—information only, no liability shift	Reserved for future use	
C	CAVV was not validated—attempt	Reserved for future use	
D	CAVV was not validated—authentication	Reserved for future use	
U		AEVV Unchecked	

6.7 Cash Advance

Portico supports Cash Advance transactions for merchants processing on the GSAP-NA, GNAP-UK, and Exchange Authorization Platforms. Cash Advance requests must be sent as a CreditSale. This functionality is restricted by MCC. When the DeviceId is boarded with the applicable MCC value, all CreditSale transaction requests will be formatted as a Cash Advance to the host. CreditSale is the only allowed primary transaction for this MCC.

6.8 Check/ACH Transactions

Timeouts

For a CheckSale, if Portico does not return a response the POS should initiate a Check Void request using the ClientTxnId passed in the original request message. If the Portico response has a GatewayRspCode of 30, the POS should initiate a Check Void request using either the GatewayTxnId in the response or the ClientTxnId passed in the original request message.

Transaction Status

Check/ACH transactions are not batched in Portico. A CheckSale transaction will not display a transaction status of C-Closed on Portico. For Check/ACH transactions, CheckQuery may used to query the status of a Check/ACH transaction on the Colonnade host. The POS can query either by GatewayTxnId or by ClientTxnId.

> Not yet supported for Paya/GETI/Sage.

6.9 Corporate Cards

A merchant has the option to participate in Corporate Purchase Card (CPC) transactions. These are also known as "Level II" and "Level III" transactions and are for B2B purchases. In order to achieve the proper interchange rates for these transaction types, additional data elements are required to be passed to the card issuer. This is done by populating the CPCReq field in a CreditSale, CreditAuth, CreditOfflineSale, CreditOfflineAuth, RecurringBillingAuth, or RecurringBilling transaction. Level II data can be included directly in the transaction request or via CreditCPCEdit; Level III can only be sent via CreditCPCEdit.

6.9.1 Credit CPCEdit

The CPC Edit transaction allows a merchant to add corporate data to an approved financial transaction.

For online transactions, if the transaction request contains CPCReq set to Y, and the Issuer identifies the associated card as a Corporate Purchase Card, than the response message will contain a value in the CPCInd field indicating the specific card type of business, corporate, or purchasing card.

If CPCData is included directly in the original transaction, the subsequent call to CreditCPCEdit is not required.

If the CPC data was not included in the original transaction, the client inspects the CPCInd for one of the valid values. If it contains any of the valid values, the client should then prompt for the purchase order number and tax. This new information must then be passed to Portico using CreditCPCEdit.

CreditAccountVerify will also return the CPCInd value, but this transaction is non-financial and therefore a CreditCPCEdit cannot be used as it does not apply.

CPC Indicator

If commercial card was specified in the request, the commercial card response indicator from the issuer will be returned in the CPCInd field.

Valid values for CPCInd are:

- B (Business Card)
- R (Corporate Card)
- S (Purchasing Card)
- L (B2B - Settlement amount may not exceed Authorized amount)

6.9.2 Level II

Level II data requires Tax Type and, if applicable, TaxAmt. Cardholder PO Number can be provided; if one is not sent, Portico will auto-populate a value so the transaction has the opportunity to qualify for the best B2B interchange rate.

6.9.3 Level III

In order to qualify for Level III data rates, the merchant must provide specific line item details for a transaction processed for a corporate, purchasing, or government card. Visa and MasterCard offer these enhanced data programs, which can reduce the cost of accepting commercial cards for B2B businesses.

> Level II data is also required for a transaction to be eligible for Level III rates.

Multiple line items may be sent for each transaction record.

The line item detail information may pass to the cardholder statement. MasterCard line items should include all fields. Visa transactions should include the summary information as well as the Line Items; a certification analyst can help determine the applicable fields for your business to qualify for Visa Level III rates.

> Special characters are not allowed in Level III data fields.

6.10 Credential/Card on File

Card brand rules require merchants to identify initial storage and usage of stored payment credentials. A stored credential is payment information that will be used to process future transactions for a cardholder. This can be a credit or debit account number or a payment token. Merchants must be able to demonstrate that they have cardholder consent to store the payment information.

Credential/Card on File (CoF) transactions are categorized in two ways: initial and subsequent. Initial CoF transactions are requests that put the credential to be stored into the system. Whereas, subsequent CoF transactions are requests that use the previously stored credential.

CoF transactions are initiated either by the cardholder or by the merchant.

- Cardholder initiated transactions are authorizations initiated by a cardholder in person, on a phone, or on a web site. These transactions typically include CVV2/CVC2 data or wallet generated cryptogram to prove the cardholder's participation.
- Merchant initiated transactions are authorizations initiated by the merchant when the cardholder is not present, for example, recurring payments.

CoF processing is supported with the Exchange, GSAP-NA, and GSAP-AP authorization platforms.

- For merchants using an external card on file system, an update should be made to pass in the Credential on File data block with the appropriate data for all transaction requests.
- For merchants using Portico's PayPlan card on file system, no changes are needed for schedule processing; PayPlan automatically populates the appropriate fields. For one-time charges via PayPlan, the appropriate CardOnFile indicator should be included in the transaction request.

6.10.1 Services Supporting CoF Processing

Portico supports CoF processing for the following financial transactions:

- CreditAccountVerify
- CreditAuth
- CreditIncrementalAuth
- CreditReturn
- CreditSale
- RecurringBilling
- RecurringBillingAuth

The CardOnFileData block in the transaction request is used to communicate the required CoF data and is composed of two fields:

- CardOnFile
  - This indicates who initiated the CoF request.
  - This must be included in all CoF transactions.
  - Valid values are:
    - C = customer initiated
    - M = merchant initiated
- CardBrandTxnId
  - This must be included in all subsequent CoF transaction requests.
  - This is the CardBrandTxnId value from the authorization response message of either the initial CoF transaction or the most recent transaction using the stored credential.

The CardBrandTxnId in the transaction response is a Brand transaction identifier that is passed back to the POS if received. When placing a credential on file the POS should save this value for use with subsequent CoF transactions. If a transaction indicating that the credential is being placed on file fails then the credential cannot be considered a stored credential and the merchant must not use the credential for any subsequent transactions.

Each transaction request that either will store or is using previously stored credentials should now include the CardOnFileData block, as shown below:

- Initial CoF—Transaction request that puts the credential on file in the system.
  - Include the CardOnFile indicator in the request.
  - Store the CardBrandTxnId from the authorization response with the stored credentials.
- Subsequent CoF—Transaction request that uses previously stored credentials.
  - Include the CardOnFile indicator in the request.
  - Include the CardBrandTxnId of the initial or most recently approved transaction using the stored credentials.
- Existing CoF—For merchants that already have credentials on file.
  - Include the CardOnFile indicator in the request.
  - Include the CardBrandTxnId of the most recently approved transaction using the stored credentials.

Merchant Initiated Transactions

Additional information is provided below regarding specific merchant initiated transactions.

The following types of transactions should not be used to place a credential on file but are considered subsequent CoF transactions if a stored credential is being used. The CardOnFileData block should be included in these requests.

- Incremental Authorizations
- Lodging Delayed charges
  - The Card Brands require the CardBrandTxnId of the original authorization regardless of whether the credential was placed on file or not.
- Lodging No Show charges
  - The Card Brands require the CardBrandTxnId of the original authorization regardless of whether the credential was placed on file or not.
- Repeat Sales

Recurring billing requests are usually subsequent CoF transactions. Portico does allow these transactions to be formatted as initial CoF in order to support that scenario. The CardOnFileData block should be included in the request message to Portico for:

- Recurring Payments (recurring payments where the One Time Indicator = N)
- Unscheduled CoF (e.g., tolltag top-up)

CreditReversal/CreditVoid

Portico is handling the necessary CoF requirements on behalf of the merchant or integrator for the CreditReversal and CreditVoid services.

6.10.2 Merchants Using Enterprise Tokenization Service (ETS)

The Brands consider tokenization a form of stored credential and therefore merchants using tokenization should obtain cardholder consent to put the credentials on file. Each transaction processed with an ETS token should include the CardOnFileData block.

It is the merchant's responsibility to provide the CardOnFileData block in the transaction request to Portico:

- When requesting a new token, request as Initial CoF.
- When processing a transaction with a token, request as Subsequent CoF.
- When storing the token, merchant systems should be updated to also store the CardBrandTxnId of the first or most recent approved transaction.

6.10.3 In App or By Browser and CoF

The Brands expect a wallet token being put on file with a merchant to be done via a CreditAuth or CreditSale transaction including the cryptogram. Any subsequent CoF purchases would not include the cryptogram. The cryptogram should not be saved by the merchant. Standard subsequent CoF data is still required for subsequent CoF transactions using a wallet token.

6.11 Credit Return

CreditReturn allows the merchant to return funds back to the cardholder. Some issuers now support online Credit Return, but some issuers support offline refunds only. When a return is processed offline, the transaction is not sent to the Issuer, but included in the batch during batch close. When a return is processed online, the transaction is authorized by the Issuer and also included in the batch during batch close.

Exchange Authorization Platform

For the Exchange host only, legacy merchant refunds default to offline; in this case, the CreditReturn transaction request is not sent to the Exchange host until batch close.

A merchant setting is avilable to allow online refunds. When this is set to True, the CreditReturn transaction request is sent to the Exchange host and the host determines whether the issuer participates in online returns.

Response Object

When a refund is processed offline to Exchange, only a transaction header is returned in the response. When a refund is processed online to any host, the transaction response contains both the header and a response body.

To enable online refunds, contact your representatve. Please note that since the response object changes, a POS update may be needed.

All Other Authorization Platforms

For all other Authorization Platforms, refunds are sent online to the host and the host determines whether the issuer participates in online returns. The response will contain both a header and a response body.

6.12 Cross-Site and Cross-Device Processing

Previously, Portico did not allow secondary transactions (e.g., CreditTxnEdit, CreditIncrementalAuth) to be made from a different SiteId or DeviceId from where the original purchase was run. Cross-Site or Cross-Device processing allows merchants to send secondary transactions from a different SiteId and/or DeviceId from where the original purchase was made. For example, If a merchant is set up for Cross-Device processing, a tip adjust can be submitted from a different device than from where the sale was made as long as both devices are associated with the same SiteId. If a merchant is set up for Cross-Site processing, then a secondary transaction can be submitted from a different SiteId or DeviceId from where the original purchase was made. An example of Cross-Site processing is when a customer makes a purchase from a merchant's eCommerce Site and then the customer returns the purchase at the brick-and-mortar store, where each entity has a unique MID.

Generally, secondary transactions affect the original authorization or purchase and thus their processing is conducted on the same DeviceId associated with that original transaction. Transaction processing, reporting, and settlement on the device of the original authorization will reflect any Cross-Site or Cross-Device secondary transaction processing associated with that original authorization. This means that batches associated with the original transaction's device will reflect the Cross-Site or Cross-Device secondary transaction processing and not the batches of the DeviceId from where the secondary transaction was run. This is true except for Return processing where the Return is processed on the same SiteId and DeviceId where the cardholder returned their purchase. The batch where the Return was made is adjusted versus the one where the original purchase was made.

Cross-Site and Cross-Device processing is supported with the following services:

- AddAttachment
- BatchClose (Cross-Device only)
- CheckVoid
- CreditAdditionalAuth
- CreditAddToBatch
- CreditCPCEdit
- CreditIncrementalAuth
- CreditReturn
- CreditReversal
- CreditTxnEdit
- CreditVoid
- DebitReturn
- DebitReversal (Cross-Site or Device processing is not supported for Canadian Interac Debit transactions)
- EBTFSReturn
- EBTFSReversal
- FindTransactions
- GetAttachments
- GetTransactionStatus
- GiftCardReversal
- GiftCardVoid
- ReportBatchSummary
- ReportTxnDetail

Cross-Site and Cross-Device processing is supported with the Exchange, GSAP-NA, and GSAP-AP Authorization Platforms.

Merchants wanting to take advantage of this functionality must be enabled for it.

6.13 Duplicate Checking

Duplicate Checking logic checks for duplicate transactions submitted by a specific DeviceId. This provides a safeguard from submitting the same transaction multiple times within a given time frame. The default time frame used for duplicate checks is thirty seconds and is configurable per DeviceId. The base matching criteria used in the duplicate check consists of the following criteria:

- Portico service used
- Cardholder Primary Account Number
- Transaction amount

If a transaction is submitted that matches a previously "Approved" transaction based on the above criteria and is within the configured time frame (e.g., 30 seconds), then a response code/message of "02 - Transaction was rejected because it is a duplicate." is returned in the response. Portico merchants may elect to receive details about the original duplicate transaction. See Duplicate Error Response.

Device configuration is required to enable Duplicate Checking logic. Enabling Duplicate Checking includes Credit, Debit, and EBT transactions. Duplicate Checking for Gift Card transactions is not automatically included and requires additional settings.

6.13.1 Additional Criteria

The Portico Service, Cardholder Primary Account Number, and Transaction Amount make up the base matching criteria used when Duplicate Checking is enabled on the customer account. Optionally, Client Transaction ID and Invoice Number can be added to this matching criterion. This would allow transactions being submitted to the same service with the same primary account number and transaction amount to succeed given the Client Transaction ID and Invoice Number are also different.

Client Transaction ID duplicate checking adds the following attributes to the matching criteria when present in the request transaction:

- Header.ClientTxnId

Invoice Number duplicate checking adds the following attributes to the criteria when present in the request transaction:

- DirectMktData.DirectMktInvoiceNbr
- AdditionalTxnFields.InvoiceNbr

> In the case where Client Transaction ID or Invoice Number matching is enabled and no ClientTxnId, DirectMktInvoiceNbr, or InvoiceNbr is specified on the request, then only past transactions without a ClientTxnId, DirectMktInvoiceNbr, or InvoiceNbr are considered a duplicate transaction given the base criteria matches.

> AdditionalTxnFields.InvoiceNbr is supported for EBT transactions.

For Gift Card transactions, duplicate checking is for card data only. If the transaction request uses Alias, duplicate checking will not occur.

6.13.2 Override Duplicate Checking

Duplicate checking can be bypassed on a per transaction basis by sending "Y" in the "AllowDup" attribute of the request.

6.13.3 Portico Services Supporting Duplicate Checking

The following Services provide Duplicate Checking support:

- ChipCardDecline
- CreditAdditionalAuth
- CreditAuth
- CreditOfflineAuth
- CreditOfflineSale
- CreditReturn
- CreditSale
- DebitAuth
- DebitReturn
- DebitSale
- EBTCashBackPurchase
- EBTCashBenefitWithdrawal
- EBTFSPurchase
- EBTFSReturn
- EBTVoucherPurchase
- GiftCardActivate
- GiftCardAddValue
- GiftCardSale
- RecurringBillingService

6.13.4 Duplicate Error Response

If a transaction is submitted that matches a previously "Approved" transaction based on the Duplicate Checking criteria enabled for the device, then Portico rejects the message and returns a Gateway Response of "02 - Transaction was rejected because it is a duplicate."

The device may be configured to receive details about the original duplicate transaction, such as the Original Gateway Txn Id, Authorization Code, and Reference Number. Refer to AdditionalDuplicateData, in the header of the transaction response.

> **Note:** Device configuration is required.

6.14 Dynamic Currency Conversion

Dynamic Currency Conversion (DCC) is a service for credit cards that allows the cardholder to make a POS credit card purchase in a foreign country using the currency of their home country. DCC is an optional one-time service that the merchant may present to the cardholder to allow them to see the purchase price in their home currency. If the customer agrees to use the service, they also agree to additional service fees for the service. DCC is only offered for in-person credit transactions.

This is supported on CreditAuth, CreditSale, CreditReturn, CreditTxnEdit, CreditAddToBatch, CreditReversal and CreditVoid request transactions.

A cardholder cannot change their DCC preferences between the original authorization and any subsequent secondary transaction. The card used for the original DCC authorization must be the same card used for any subsequent transaction, such as CreditReturn.

If the original transaction contains the CurrencyConversion data block, then any CreditReturn must also contain that data block.

- Please note that GatewayTxnId is required for returns containing the CurrencyConversion data block

Use of this service requires a merchant to enter into an agreement with a Dynamic Currency Conversion processor, integrate to support the POS functionality, and support the Dynamic Currency data elements in transaction request messages. There are no DCC-specific fields in the Portico response object. See CurrencyConversion.

Dynamic Currency Conversion is available for merchants in the Restaurant, Retail and Lodging industries.

Integration to this service is not available for Direct-to-Portico integrations. Merchants using this service must use Global Payments' Unified Commerce Platform.

> **Note:** Device batch must be managed by Portico. DCC is not supported with host-based batch management.

6.15 Dynamic Merchant Category Code

For **eligible** merchants processing on the GSAP-NA or GSAP-AP Authorization Platforms, Portico supports the option to allow a Merchant Category Code (MCC) to be specified in a credit transaction request that is different from the value stored for the DeviceId.

A MCC value can be sent in the request header to override the MCC value defined for the DeviceId; this value will be passed in the host request message, and used to format any MCC-specified fields. This should be sent on primary transactions only. Any secondary transaction or transaction performed using a previous transaction id will use the MCC from the original transaction.

> **Note:** For eligible aggregator merchants only. Must be set up as an aggregator on the host.

6.16 Dynamic Transaction Descriptor

Dynamic Transaction Descriptors allow merchants to define the information that appears on a customer's credit card statement on a per-transaction basis. Without dynamic descriptors, the merchant DBA name on file with Heartland will be populated on the cardholder statement. With dynamic descriptors, merchants can add transaction-specific details to a shortened version of the merchant DBA name. This is intended to help customers recognize transactions on their statement and reduce the number of cardholder disputes and chargebacks, and is most frequently used by "Payment Facilitators" (otherwise known as aggregators) who have multiple sub-merchants that need to be distinguished.

The dynamic Merchant Name value is sent to the card issuers to display on cardholder statements. Portico includes the dynamic MerchantName in the authorization response. Merchants can display the dynamic Merchant Name on printed or online receipts, so customers are notified how the transaction appears on their statement.

The Maximum characters of the dynamic Merchant Name, inclusive of the TxnDescriptorFormat length plus the separator, is 22 characters for MasterCard and 25 characters for Visa and Discover. Merchants processing via the Exchange host are limited to a maximum of 22 characters for all card brands.

The value passed in the TxnDescriptor field provided on CreditSale or CreditAuth request transactions is only used when the merchant is configured correctly.

Restricted Characters

The following special characters must not be used in the dynamic Merchant Name passed in the TxnDescriptor field :

- < (less than)
- > (greater than)
- % (percent)
- & (ampersand)
- + (plus)
- ' (single apostrophe)
- " (quotation mark)
- \' (backslash-escaped apostrophe)
- \" (backslash-escaped quotation mark)
- ((opening parenthesis)
-) (closing parenthesis)
- ; (semicolon)

Merchant Configuration

To enable Dynamic Transaction Descriptor functionality, there are settings that must be configured on Portico for the DeviceId:

Settings	Value/Description
AllowTxnDescriptor	Must be True.
ShortDBAName	If used, contains the prefix value to appear on the statement for all transactions for the DeviceId; may be 3, 7 or 12 characters in length.
TxnDescriptorFormat	Valid Values are: 0 - Turns off descriptor functionality; any value passed in the request message is ignored

Settings	Value/Description
	1 - Indicates the merchant will not use ShortDBAName and the full value for the cardholder statement will be sent in the transaction request; any value stored in ShortDBAName is ignored 3, 7, 12 - Sets the length of the ShortDBAName

Using Short DBA Name

When ShortDBAName is used, Portico generates a merchant name by concatenating the value stored in ShortDBAName with the TxnDescriptor field provided on CreditSale or CreditAuth request transactions.

The ShortDBAName is separated from the TxnDescriptor by a "*" in a fixed position based on the TxnDescriptorFormat length; the characters populated are set by the value in TxnDescriptorFormat. If the ShortDBAName value is fewer characters than the value in TxnDescriptorFormat, it will be space-filled to the separator.

Examples	
If the TxnDescriptorFormat = 3	The first 3 characters of the value in ShortDBAName are placed in the first three positions, the separator "*" is fixed in position 4 and the TxnDescriptor Maximum characters is 18 characters.
If the TxnDescriptorFormat = 7	The first 7 characters of the value in ShortDBAName are placed in the first three positions, the separator "*" is fixed in position 8 and the TxnDescriptor Maximum characters is 14 characters.
If the TxnDescriptorFormat = 12	The first 12 characters of the value in ShortDBAName are placed in the first three positions, the separator "*" is fixed in position 13 and the TxnDescriptor Maximum characters is 9 characters.

Using Passthrough

Merchants passing through a dynamic merchant name should follow the same pattern of [short DBA name] {space} [asterisk] [descriptor name].

If a value is stored in ShortDBAName, it will not be used when the TxnDescriptorFormat indicates passthrough.

> The Dynamic Transaction Descriptor feature is not currently available for American Express.
>
> Updates to Portico device settings are required to use this feature. Contact your Heartland representative for more information.

> The Dynamic Transaction Descriptor feature is not supported in the UK market at this time.

6.17 EMV

The Portico API supports clients that interact with EMV capable terminals through the EMV data elements defined on Credit based services of the Portico API. If an EMV capable client/terminal is interfacing with a chip card, then the EMV tag data must be present in the transaction (e.g., CreditSale, CreditAuth, CreditReturn, DebitSale, DebitReturn, and DebitReversal. For a normal EMV transaction, the transaction should contain the EMV tag data obtained from the terminal/chip card. However, if the terminal has an issue reading the chip card, then the chip card can be processed as a normal swipe transaction with the EMV chip condition indicating whether the previous read of a chip card failed or succeeded.

For additional information, see the Heartland Integrator's Guide.

6.17.1 Service Tag Validation

EMV tags sent on transactions are passed on to Heartland authorization and issuer systems as received. They are validated at the syntax-level, but in order to allow for future flexibility, the EMV tags are not checked to determine if all required or optional tags are present. Required or optional tags will be verified during the certification process of the client.

There is an exception to the validation rule. In the case of offline services (e.g.,CreditOfflineAuth, CreditOfflineSale, ChipCardDecline) where the chip card approves or declines a transaction offline, the corresponding service does validate tag 8A to ensure the appropriate service is being called.

Service	Tag	Condition
CreditOfflineAuth	8A	equals Y1 (8A025931) or Y3 (08A025933)
CreditOfflineSale	8A	equals Y1 (8A025931) or Y3 (08A025933)
ChipCardDecline	8A	equals Z1 (8A025A31) or Z3 (08A025A33)

6.17.2 EMV Conversation Flow

EMV tags are persisted by Portico and can be edited prior to the transaction being settled. This allows for the conversational nature of interfacing with a chip card using an EMV capable terminal. For example, the following is a general flow of an EMV conversation to complete a CreditSale transaction. For other flows, see the EMV section of the sample SoapUI project that is included in the SDK.

EMV Conversation Flow	
1.	Client interfaces with the EMV terminal and initiates a conversation with the chip card. The result of this conversation includes obtaining credit authorization EMV tags for the request. Portico is not involved in this conversation between the client and the terminal.
2.	Client initiates a Portico CreditSale request with Track 2 and EMV tag data. ⚠ An error will be generated if EMV tag data is not accompanied by Track data.
3.	Portico initiates a request with the Heartland authorization system which includes the Tag Length Value (TLV) fields passed in by the client: a. Portico receives the response from the Heartland authorization system. b. Portico persists the terminal EMV tag data and issuer response tags to the database. c. Portico returns the response to the client which includes the tags returned by the issuer.
4.	Client passes the issuer response tags to the EMV chip card/ terminal and receives the result from the chip card/terminal.
5.	If the EMV chip card/terminal accepts the transaction: a. Optionally, the client initiates a CreditTxnEdit using the Gateway Transaction ID returned in the Portico response, sending the EMV terminal result tags in the CreditTxnEdit request. i. Portico looks up the original transaction and applies the EMV chip card/terminal result tags to the original EMV tag data.
6.	If the EMV chip card/terminal declines: a. After receiving online issuer approval, the client initiates a CreditReversal using the Gateway Transaction ID returned in the Portico response, sending the EMV terminal result tags in the CreditReversal request. i. Portico initiates a reversal with the Heartland authorization system. The tags in the reversal that Portico sends are the tags sent by the client in the CreditReversal as well as any tags from the original transaction that weren't included in the CreditReversal. b. Before requesting online authorization, the client initiates a ChipCardDecline, sending the EMV terminal result tags in the ChipCardDecline request.

6.17.3 Services That Support EMV Tags

Services that support passing of EMV tags are below:

> EMV tags should be passed in the TagData field.

CreditAuth/CreditSale

For EMV, CreditAuth/CreditSale transactions, either the EMV chip condition or tag data is required. This data is required when the Portico client is interfacing with an EMV chip card/terminal. The tag data will be included in the request to the issuer and any issuer response tags will be returned to the client.

CreditTxnEdit

CreditTxnEdit allows for updating EMV tag data already persisted on the database from the original CreditAuth or CreditSale. The EMV tag data on the request consists of the TLV field list associated with security data and/or script results obtained from the chip card/terminal upon applying the issuer response from the CreditAuth or CreditSale.

CreditAddToBatch

Like the CreditTxnEdit, CreditAddToBatch allows for updating EMV tag data already persisted on the database from the original CreditAuth. CreditAddToBatch allows for an alternate flow for editing EMV tag data on a CreditAuth which is not automatically added to the open batch like CreditSale. Thus for CreditAuth, two flows are allowed when editing EMV tag data:

- CreditAuth -> CreditTxnEdit with tags -> CreditAddToBatch
- CreditAuth -> CreditAddToBatch with tags

CreditReversal

There may be many reasons for reversing an EMV transaction (communication errors, etc.). For normal reversals no additional requirements or passing of EMV tag data are required when reversing EMV transactions. However, if the reversal is due to a chip card declining a transaction upon applying issuer response tags obtained online, then the resulting EMV tag data obtained from the terminal/chip card when applying the issuer response tags should be sent on the CreditReversal request.

CreditOfflineAuth/CreditOfflineSale

The CreditOfflineAuth and CreditOfflineSale services allow for "offline" chip card approvals. If the chip card approves the transaction offline (e.g., does not require the authorization to go online for approval), then the offline authorization services must be called with the resulting EMV tag data obtained from the terminal. The tags recorded by these services are utilized in the settlement process.

> In North America, EMV is mandated to $0.00 floor limit, to force all authorization requests online, with exceptions for certain transportation industry MCCs.

ChipCardDecline

The ChipCardDecline service allows for the recording of an "offline" chip card decline. This occurs when the chip card declines the transaction without requesting that the transaction go online.

The ChipCardDecline is an inactive transaction and is for recording purposes which may be required by some issuers.

CreditReturn

The CreditReturn service allows for EMV Credit Return transactions to be initiated using an EMV chip card. EMV CreditReturn transactions are stand-alone transactions, meaning they do not depend on the card data or tags obtained from a previous transaction via a Gateway Transaction Id. For an EMV CreditReturn to take place, both card data and EMV tag data must be present in the request.

If the CreditReturn is based solely on a reference transaction via a Gateway Transaction Id and the referenced transaction is an EMV transaction, then the CreditReturn will be based solely on the card information of the referenced transaction.

DebitSale

For EMV, DebitSale transactions, either the EMV chip condition or tag data is required. This data is required when the Portico client is interfacing with an EMV chip card/terminal. The tag data will be included in the request to the issuer and any issuer response tags will be returned to the client.

DebitReturn

The DebitReturn service allows for EMV Debit Return transactions to be initiated using an EMV chip card. EMV DebitReturn transactions are stand-alone transactions, meaning they do not depend on the card data or tags obtained from a previous transaction via a Gateway Transaction Id. For an EMV DebitReturn to take place, both card data and EMV tag data must be present in the request.

If the DebitReturn is based solely on a reference transaction via a Gateway Transaction Id and the referenced transaction is an EMV transaction, then the DebitReturn will be based solely on the card information of the referenced transaction.

DebitReversal

There may be many reasons for reversing an EMV transaction (communication errors, etc.). For normal reversals no additional requirements or passing of EMV tag data are required when reversing EMV transactions. However, if the reversal is due to a chip card declining a transaction upon applying issuer response tags obtained online, then the resulting EMV tag data obtained from the terminal/chip card when applying the issuer response tags should be sent on the DebitReversal request. In addition, for Canadian Debit transactions, when the reversal is due to Customer Cancellation, the card must be present and card data and tags must be included in the reversal request.

Report Services

The Portico reporting services indicate whether the transaction has EMV tag data associated with the transaction. In addition, EMV tag data will be returned when requesting detailed information about a transaction through the ReportTxnDetail service. The following is a list of those reporting services that include EMV Tag information:

- FindTransactions
- ReportActivity
- ReportBatchDetail
- ReportOpenAuths
- ReportSearch
- ReportTxnDetail

6.17.4 EMV Tags

The EMV tag data consists of a list of Tag Length Value (TLV) Tags in BER-TLV format. It is highly recommended to limit the tags sent in the EMV tag data field to those defined in the EMV Request Tags section.

There are three parts to a TLV tag.

> [Tag][Value Length][Value] (ex. "9F4005F000F0A001")
> where
> Tag Name = 9F40
> Value Length (in bytes) = 05 Value (Hex representation of bytes. Example, "F0" – 1-byte) = F000F0A001

Heartland only supports up to two-byte tags, thus TLV-BER rules for subsequent byte tag number continuation (bit-8 indicates continuation of tag name) do not apply. For example, FFC6 is a valid Heartland tag even though C6 results in bit-8 being set.

The length subfield may be one or more bytes.

- If bit 8 of the most significant byte is set to 0, the length subfield consists of 1 byte. Bits 7 to 1 code the number of bytes of the value subfield.
- If bit 8 of the most significant byte is set to 1, bits 7 to 1 code the number of subsequent bytes in the length subfield.

The subsequent bytes in the length subfield code an integer representing the number of bytes in the value subfield.

6.17.4.1 EMV Request Tags

The following table contains a sample list of EMV tags associated with authorization or return requests. A full list of these tags can be found in the Heartland Integrator's Guide along with field descriptions, usage conditions, and examples.

Field Name	Tag	Usage	Description
ADDITIONAL TERMINAL CAPABILITIES	9F40	C	The 10-character Additional Terminal Capabilities field contains the POS terminal input and output capabilities. Example (5 bytes binary) = FF-80-F0-F0-01 TLV = 9F4005FF80F0F001
AMOUNT, AUTHORISED (NUMERIC)	9F02	M	The 12-character numeric Amount, Authorised (Numeric) contains the authorized amount of the transaction. In the authorization request message this is the amount used by the chip card when calculating the Application Cryptogram. It must contain numeric right-justified data with leading zeros. If the transaction includes a cashback amount, the Amount, Authorised (Numeric) includes the purchase amount plus the cashback amount. Example (decimal value) = 12345 TLV = 9F0206000000012345

Field Name	Tag	Usage	Description
AMOUNT, OTHER (NUMERIC)	9F03	M	The 12-character numeric Amount, Other (Numeric) contains the cashback amount used by the chip card when calculating the Application Cryptogram. It must contain numeric right-justified data with leading zeros. If the transaction does not include a cashback amount, the Amount, Other (Numeric) field must be all zeros. Example (decimal value) = 4000 TLV = 9F0306000000004000
APPLICATION CRYPTOGRAM	9F26	M	The 16-character Application Cryptogram contains the cryptogram returned by the chip card in response to the Generate AC command. Example (8 bytes binary) = 8E-19-ED-4B-CA-5C-67-0A TLV = 9F26088E19ED4BCA5C670A
APPLICATION INTERCHANGE PROFILE	82	M	The 4-character Application Interchange Profile indicates the capabilities of the chip card to support specific functions in the application. Example (2 bytes binary) = 5C-00 TLV = 82025C00
APPLICATION LABEL	50	C	The mnemonic associated with the AID according to the ISO/IEC 7816-5. Example (1 to 16 bytes alphanumeric special characters) = Credit
APPLICATION PREFERRED NAME	9F12	C	The mnemonic associated with the AID. Example (1 to 16 bytes alphanumeric special characters) = Credit
APPLICATION PRIMARY ACCOUNT NUMBER (PAN) SEQUENCE NUMBER	5F34	C	The 2-character numeric Application PAN Sequence Number contains a counter maintained and supplied by the chip card. This field identifies the card when multiple chip cards are associated with a single account number. If the chip card does not contain an Application PAN Sequence Number, then the Application PAN Sequence Number value subfield must be set to 00. Example (decimal value) = 2 TLV = 5F340102
APPLICATION TRANSACTION COUNTER (ATC)	9F36	M	The 4-character numeric (binary) Application Transaction Counter contains the counter value maintained by the chip card. The chip card increments this value for each transaction (including failed transactions). Example (decimal value) = 10 TLV = 9F3602000A

Field Name	Tag	Usage	Description
APPLICATION USAGE CONTROL	9F07	C	The 4-character Application Usage Control indicates the Issuer's specified restrictions on the geographic usage and services allowed for the chip card application. Example (2 bytes binary) = FF-00 TLV = 9F0702FF00
APPLICATION VERSION NUMBER (ICC)	9F08	C	The 4-character Application Version Number (ICC) is the version number of the chip card application. Example (2 bytes binary) = 08-C1 TLV = 9F080208C1
APPLICATION VERSION NUMBER (TERMINAL)	9F09	C	The 4-character Application Version Number (Terminal) is the version number of the POS terminal payment application. Example (2 bytes binary) = 10-01 TLV = 9F09021001
AUTHORISATION RESPONSE CODE	8A	C	The 4-character Authorisation Response Code is generated by the issuer and returned in the authorization response message. The most commonly used authorisation response codes are online approval (00), online decline (05), and referral (01). The POS terminal must not alter the Authorisation Response Code value. The POS terminal generates an authorisation response code in the following conditions: • Y1 - Offline approved • Z1 - Offline declined • Y3 - Unable to go online (offline approved) • Z3 - Unable to go online (offline declined) Example (2 bytes alphanumeric) = Y1 TLV = 8A025931
CARDHOLDER VERIFICATION METHOD (CVM) RESULTS	9F34	C	The 6-character Cardholder Verification Method (CVM) Results indicate the results of the last CVM performed. Example (3 bytes binary) = A4-00-02 TLV = 9F3403A40002
CRYPTOGRAM INFORMATION DATA	9F27	C	The 2-character Cryptogram Information Data indicates the type of cryptogram generated (TC, ARQC, or AAC), why the cryptogram was generated, and actions that the chip card instructed the POS terminal to perform. Example (1 byte binary) = 80

Field Name	Tag	Usage	Description
			TLV = 9F270180
INTERFACE DEVICE (IFD) SERIAL NUMBER	9F1E	C	The 16-character Interface Device (IFD) Serial Number contains a unique and permanent identification number assigned to the IFD by the manufacturer. Example (8 bytes alphanumeric) = SERIAL12 TLV = 9F1E0853455249414C3132
ISSUER ACTION CODE – DEFAULT	9F0D	C	A 10-character Issuer Action Code – Default specifies the issuer's conditions that cause a transaction to be rejected when the POS terminal is unable to process the transaction online (even when the transaction has already been approved online). Example (5 bytes binary) = F0-40-00-88-00 TLV = 9F0D05F040008800
ISSUER ACTION CODE – DENIAL	9F0E	C	A 10-character Issuer Action Code – Denial specifies the issuer's conditions that cause the denial of a transaction without an attempt to go online. Example (5 bytes binary) = FC-F8-FC-F8-F0 TLV = 9F0E05FCF8FCF8F0
ISSUER ACTION CODE – ONLINE	9F0F	C	A 10-character Issuer Action Code – Online specifies the issuer's conditions that cause a transaction to be transmitted online. Example (5 bytes binary) = FC-F8-FC-F8-F0 TLV = 9F0F05FCF8FCF8F0
ISSUER COUNTRY CODE	5F28	C	The 4-character numeric Issuer Country Code indicates the country of the issuer according to ISO 3166. Example (decimal value) = 840 TLV = 5F28020840
POS ENTRY MODE	9F39	C	A 2-character POS Entry Mode field indicates the method by which the PAN was entered, according to the first two digits of the ISO 8583:1987 POS Entry Mode. Example (decimal value) = 0 TLV = 9F390100
TERMINAL ACTION CODE – DEFAULT	FFC6	C	A 10-character Terminal Action Code – Default specifies the acquirer's conditions that cause a transaction to be rejected when the POS terminal is unable to process the transaction online (even when the transaction has already been approved online).

Field Name	Tag	Usage	Description
			Example (5 bytes binary) = FC-F8-FC-F8-F0 TLV = FFC605FCF8FCF8F0
TERMINAL ACTION CODE – DENIAL	FFC7	C	A 10-character Terminal Action Code – Denial specifies the acquirer's conditions that cause the denial of a transaction without an attempt to go online. Example (5 bytes binary) = FC-F8-FC-F8-F0 TLV = FFC705FCF8FCF8F0
TERMINAL ACTION CODE – ONLINE	FFC8	C	A 10-character Terminal Action Code – Online specifies the acquirer's conditions that cause a transaction to be transmitted online. Example (5 bytes binary) = FC-F8-FC-F8-F0 TLV = FFC805FCF8FCF8F0
TERMINAL CAPABILITIES	9F33	C	The 6-character Terminal Capabilities indicates the card data input, the cardholder verification method (CVM), and the security capabilities supported by the POS terminal. Example (3 bytes binary) = 01-01-01 TLV = 9F3303010101
TERMINAL COUNTRY CODE	9F1A	M	The 4-character numeric Terminal Country Code indicates the country of the terminal, represented according to ISO 3166. Example (decimal value) = 840 TLV = 9F1A020840
TERMINAL TYPE	9F35	C	The 2-character numeric Terminal Type indicates the environment of the POS terminal, its communications capability, and its operational control. Example (decimal value) = 22 TLV = 9F350122
TERMINAL VERIFICATION RESULTS	95	M	The 10-character Terminal Verification Results (TVR) contains a series of indicators set by the POS terminal recording both offline and online processing results. Example (5 binary bytes) = 00-00-04-80-00 TLV = 95050000048000
TRANSACTION CURRENCY CODE	5F2A	M	The 4-character numeric Transaction Currency Code contains the currency code of the transaction according to ISO 4217.

Field Name	Tag	Usage	Description
			Example (decimal value) = 840 TLV = 5F2A020840
TRANSACTION DATE	9A	M	The 6-character numeric Transaction Date contains the local date used to generate the cryptogram. The Transaction Date is in the format YYMMDD. Example (decimal value - YYMMDD) = 140131 TLV = 9A03140131
TRANSACTION STATUS INFORMATION	9B	C	The 4-character Transaction Status Information contains the functions performed in the transaction. Example (2 binary bytes) = 48-00 TLV = 9B024800
TRANSACTION TIME	9F21	C	The 6-character numeric Transaction Time subfield contains the local time that the transaction was authorized. Example (decimal value - HHMMSS) = 123456 TLV = 9F2103123456
TRANSACTION TYPE	9C	M	The 2-character numeric Transaction Type indicates the type of financial transaction as represented by the first two digits of the ISO 8583:1987 Processing Code. Example (decimal value) = 00 TLV = 9C0100
UNPREDICTABLE NUMBER	9F37	M	The 8-character numeric (binary) Unpredictable Number is randomly generated by the POS Terminal and is used to provide variability and uniqueness to the cryptogram. Example (decimal value) = 12345678 TLV = 9F370400BC614E
APPLICATION DEDICATED FILE (ADF) NAME	4F	M	A 10- to 32-character Application Dedicated File (ADF) Name is used to address an application in the chip card. An ADF Name consists of a registered application provider identifier (RID) of 5 bytes, which is issued by the ISO/IEC 7816-5 registration authority. This is followed by a proprietary application identifier extension (PIX), which enables the application provider to differentiate between the different applications offered. The ADF Name is obtained during the application selection process. Previous versions of the EMVCo specifications refer to this tag as Application Identifier (AID) – ICC.

Field Name	Tag	Usage	Description
			Example (7 bytes binary) = A0-00-00-00-03-10-10 TLV = 4F07A0000000031010
APPLICATION IDENTIFIER (AID) – TERMINAL	9F06	C	The 10- to 32-character Application Identifier (AID) – Terminal is used to address an application in the chip card. An AID consists of a registered application provider identifier (RID) of 5 bytes, which is issued by the ISO/IEC 7816-5 registration authority. This is followed by a proprietary application identifier extension (PIX) which enables the application provider to differentiate between the different applications offered. The AID is obtained during the application selection process. Example (7 bytes binary) = A0-00-00-00-03-10-10 TLV = 9F0607A0000000031010
CUSTOMER EXCLUSIVE DATA (CED)	9F7C	C	The up to 64-character variable length Customer Exclusive Data contains issuer proprietary data for transmission to the issuer. Example (4 bytes binary) = 12-34-56-78 TLV = 9F7C0412345678
DEDICATED FILE (DF) NAME	84	C	The 10- to 32-character Dedicated File Name identifies the name of the Dedicated File as described in ISO/IEC 7816-4. Example (7 bytes binary) = A0-00-00-00-03-10-10 TLV = 8407A0000000031010
FORM FACTOR INDICATOR (FFI) / PAYPASS THIRD-PARTY DATA	9F6E	C	FORM FACTOR INDICATOR (FFI) The 8-character Form Factor Indicator indicates the form factor of the consumer payment device and the type of contactless interface over which the transaction was conducted. The Form Factor Indicator is both an implementation and issuer option. Example (5 bytes binary) = 12-34-56-78-9A PAYPASS THIRD-PARTY DATA A 10- to 64-character PayPass Third-Party Data subfield contains proprietary data from a third party. The PayPass Third-Party Data value subfield is formatted in -coded binary format. Example (4 bytes binary) = 01-02-03-04 TLV = 9F6E0401020304
ICC DYNAMIC NUMBER	9F4C	C	The 4- to 16-character ICC Dynamic Number is a time-variant numerical value generated by the chip card. Example (4 bytes binary) = 01-02-03-04

Field Name	Tag	Usage	Description
			TLV = 9F4C080000000000000000
ISSUER APPLICATION DATA	9F10	M	The up to 64-character Issuer Application Data contains proprietary application data for transmission to the issuer. Example (6 bytes binary) = 01-0A-03-60-00-00 TLV = 9F1006010A03600000
ISSUER SCRIPT RESULTS	9F5B	C	The up to 40-character Issuer Script Results contains the results of the card issuer script update to the chip card. The Issuer Script Results value subfield is formatted in coded binary format. Conversion from to coded binary is dependent on the kernel API. Example (5 bytes binary) = 20-00-00-00-00 TLV = 9F5B052000000000
TRANSACTION SEQUENCE COUNTER	9F41	C	The 4- to 8-character numeric (binary) Transaction Sequence Counter uniquely identifies each transaction on a POS terminal. Example (decimal value) = 435 TLV = 9F4104000001B3

Usage = (C) Conditional, (M) Mandatory, (O) Optional

Sensitive cardholder data must not be sent to the Host in authorization or settlement messages even if received from the card and terminal. If Portico receives the following data, it will not be sent to the Host:

- 56 – Track 1 Equivalent Data
- 57 – Track 2 Equivalent Data
- 5A – Application PAN
- 5F20 – Cardholder Name
- 5F24 – Application Expiration Date
- 99 – Transaction PIN Data
- 9F0B – Cardholder Name Extended
- 9F1F – Track 1 Discretionary Data
- 9F20 – Track 2 Discretionary Data

6.17.4.2 EMV Response Tags

Field Name	Tag	Usage	Description
ISSUER AUTHENTICATION DATA	91	O	The 16- to 32-character Issuer Authentication Data field contains data delivered to the chip card including the ARPC cryptogram for online issuer authentication. The data is in the format required by the card. The Issuer Application Data value subfield is formatted in coded binary format. Conversion from to coded binary is dependent on the kernel API. Example (10 bytes binary) = 22-63-BC-C1-C2-D9-C4-42-00-13 TLV = 91102263BCC1C2D9C4420013
ISSUER SCRIPT TEMPLATE 1	71	O	The 2- to 254-character Issuer Script Template 1 contains proprietary issuer data for transmission to the chip card before the second GENERATE AC command. Conversion from to coded binary is dependent on the kernel API. example (10 bytes binary) = 01-02-03-04-05-06-07-08-09-0A TLV = 710A01020304050607080 90A
ISSUER SCRIPT TEMPLATE 2	72	O	The 2- to 254-character Issuer Script Template 2 contains proprietary issuer data for transmission to the chip card after the second GENERATE AC command. Conversion from to coded binary is dependent on the kernel API. Example (10 bytes binary) = 01-02-03-04-05-06-07-08-09-0A TLV = 7210A01020304050607080 90A

Usage = (C) Conditional, (M) Mandatory, (O) Optional

6.17.5 EMV Parameter Data Download

Some clients that interface with EMV capable terminals are required to accept Parameter Data Downloads when notified (refer to the Authorization Platform for more information).

Notification of a Parameter Data Download (PDL) being available for the terminal is returned in the Response Header for the following transactions.

- CreditAccountVerify
- CreditAdditionalAuth
- CreditAuth
- CreditIncrementalAuth
- CreditSale
- DebitSale

The Notification is specifically applicable to the terminal issuing one of the above transactions and will be returned once per day until the download is confirmed using the ParameterDownload service or the flag is reset in the Parameter Data Download system.

Portico allows access to the Parameter Data Download system via the ParameterDownload service. Two options exist in terms of accessing the Parameter Data Download system via the ParameterDownload service:

ParameterDownload Service	Description
Parameter Data Download system interface pass-thru	Portico is totally out of the formatting/processing of the PDL request. Portico receives the ParameterDownload service request and passes the PDL request data (PDLBlockReq) through to the Parameter Data Download system unmodified. The ParameterDownload response message sent to the client contains the requested PDL data (PDLBlockResp).
Parameter Data Download system interface partially abstracted	This option allows for a portion of the PDL request to be abstracted (e.g., defined by XML).

Portico receives the Parameter Data Download service request and derives the block to be sent to the Parameter Data Download system based on the request data (PDLRequest) received. This allows the use of XML data elements for defining the query and determining the contents of the response.

The ParameterDownload response message sent to the client contains the requested PDL data (PDLResponse).

Regardless of the method utilized to obtain PDL responses, the data returned will be in the form of table blocks (see Table Definitions below).

6.17.6 ParameterDownload Service

To request an initial or subsequent PDL, the terminal sends a PARAMETER TYPE of 06 to request an EMV PDL from the host and the TABLE-ID should be 10 to reflect the first Table.

The host will send back a response message containing the Table Versions and Flags:

- A Flag value of "Y" will direct the POS to request the data for that table in a subsequent PDL request.
- A Flag value of "N" indicates that the table is utilized by the location, but there is no new data to download at this time.

  > If the POS needs to download all applicable tables upon new installation or software upgrade, it should process the table as if the Flag value was "Y".

- A Table Version value of "###" and Flag value of "@" will inform the POS that the table is not utilized by the location. If using the "Parameter Data Download system interface partially abstracted" interface, the Flag/Version for the given table will not exist on the response.
- A field that is filled with spaces indicates that it is not applicable to the corresponding Application Identifier (AID).

The POS sends a request for each Table-ID with a Flag value of "Y" using the indicated Table Version and Card Type values. Some of the tables must be downloaded in multiple blocks, and the POS must keep track of the Block Sequence Number it needs and increment it appropriately until all blocks are successfully received. When the POS receives an END-OF-TABLE FLAG of "Y", it sends a PARAMETER TYPE of 07 to confirm receipt of that table.

> Numeric (N) fields will be right-justified, zero-filled. Alphanumeric (A/N) and hexadecimal (HEX) fields will be left-justified, space-filled.

6.17.6.1 PDL Request Definition

The following table defines the PDLBlockReq which is applicable when using the "Parameter Data Download system interface pass-thru" method for interfacing with the Parameter Data Download system. If using the "Parameter Data Download system interface partially abstracted" method, then see the PDLRequest schema definition.

Field Name	Length	Format	Source	Value/Description
PARAMETER TYPE	2	N	TERM	Indicates the action the terminal is requesting or terminal confirmation that the PDL data has been received. • 06 = Request EMV PDL • 07 = Confirm EMV PDL Table Data. This value should be sent for each Table when POS receives "Y" in END-OF-TABLE FLAG field in EMV PDL Response.
TABLE-ID	2	N	TERM	Indicates the type of EMV PDL data the POS is requesting. • 10 = Table Versions & Flags • 30 = Terminal Data • 40 = Contact Card Data • 50 = Contactless Card Data • 60 = Public Key Data
CARD TYPE	2	N	TERM	Indicates the card type as returned in Table-ID 10 Table Versions & Flags. This field is required for Table-IDs 40-60. For Table-IDs 10-30, this field is space-filled. • 01 = Visa • 02 = Mastercard • 03 = American Express • 04 = Discover • 07 = JCB • 08 = Union Pay International
PARAMETER VERSION or TABLE VERSION	3	A/N	TERM	The Parameter Version is used in a request for Table-ID 10 only—space filled for most current version, otherwise valid version number (e.g., 001, 002). Table Version is used in requests for Table-IDs 30-60. The POS should echo back the version needed for the appropriate Table that was sent back from the Host in the initial PDL response.
BLOCK SEQUENCE NUMBER	2	N	TERM	• 00 = Value to be used when requesting Table-ID 10 or sending a confirmation. • 01-99 = Values to be used when requesting Table-IDs 30-60.

6.17.6.2 PDL Response Definition

The following tables define the PDLBlockRsp, which is applicable when using the "Parameter Data Download system interface pass-thru" method for interfacing with the Parameter Data Download system. If using the "Parameter Data Download system interface partially abstracted" method, then see the PDLResponse schema definition.

6.17.6.2.1 Table 10—Table Versions and Flags

EMV PDL Response – Table-ID 10 Table Versions Flags

Field Name	Length	Format	Source	Value/Description
PARAMETER VERSION	3	A/N	HOST	Echoed from PDL request if sent or most current version sent from host.
BLOCK SEQUENCE NUMBER	2	N	HOST	Echoed from PDL request.
TABLE-ID	2	N	HOST	Echoed from PDL request.
CARD TYPE	2	N	HOST	Echoed from PDL request.
END-OF-TABLE FLAG	1	A/N	HOST	Y = No more blocks available for this Table-ID.
Start of Table Versions Flags				
EMV ENABLED	1	A/N	HOST	• Y = EMV should be enabled on this terminal. Table versions and flags will follow. • N = EMV should be disabled on this terminal. Table versions and flags will not follow. This may be used to at least temporarily disable EMV on a terminal exhibiting compliance issues, e.g., excessive fallback transactions.
TABLE-ID 30 VERSION	3	A/N	HOST	
TABLE-ID 30 FLAG	1	A/N	HOST	• Y = Data available • N = No new data available
The following fields will be repeated, dependent upon the number of card types.				
CARD TYPE	2	N	HOST	Indicates the card type. • 01 = Visa • 02 = Mastercard • 03 = American Express • 04 = Discover
TABLE-ID 40 VERSION	3	A/N	HOST	

Field Name	Length	Format	Source	Value/Description
TABLE-ID 40 FLAG	1	A/N	HOST	• Y = Data available • N = No new data available
TABLE-ID 50 VERSION	3	A/N	HOST	
TABLE-ID 50 FLAG	1	A/N	HOST	• Y = Data available • N = No new data available
TABLE-ID 60 VERSION	3	A/N	HOST	
TABLE-ID 60 FLAG	1	A/N	HOST	• Y = Data available • N = No new data available

6.17.6.2.2 PDL Response Tables 30-60

This is a generic response for tables 30-60. The first section of data is returned for all tables. The contents of the table data block returned are specific to the individual table and are specified in subsequent sections.

EMV PDL Response – Table-ID 30-60 Data

Field Name	Length	Format	Source	Value/Description
TABLE VERSION	3	A/N	HOST	Echoed from PDL request.
BLOCK SEQUENCE NUMBER	2	N	HOST	Echoed from PDL request.
TABLE-ID	2	N	HOST	Echoed from PDL request.
CARD TYPE	2	N	HOST	Echoed from PDL request.
END-OF-TABLE FLAG	1	A/N	HOST	Y = No more blocks available for this Table-ID.
Start of Table Data				
TABLE DATA BLOCK LENGTH	3	N	HOST	Length of Table Data to follow. Valid values are 000-875.
TABLE DATA BLOCK DATA	up to 875	A/N	HOST	The block of data contained in the requested Table-ID and Block Sequence Number.

Table Definitions 30-60

The table definitions in the subsequent sections define the table data blocks received when requesting Table 30-60. These definitions are applicable to both methods of interfacing with the Parameter Data Download system. When using the "Parameter Data Download system interface partially abstracted" method, these table data blocks will be returned in the "TableBlock" data element of the response.

6.17.6.2.2.1 PDL Response Table 30—Terminal Data

Table-ID 30—Terminal Data

Field Name	Length	Format	Source	Value/Description

TERMINAL TYPE	2	N	HOST	EMV Tag 9F35 – Indicates the environment of the terminal, its communications capability, and its operational control.
				• Financial Institution Controlled
				  ○ 11 – Attended, Online only
				  ○ 12 – Attended, Online with offline capability
				  ○ 13 – Attended, Offline only
				  ○ 14 – Unattended, Online only
				  ○ 15 – Unattended, Online with offline capability
				  ○ 16 – Unattended, Offline only
				• Merchant Controlled
				  ○ 21 – Attended, Online only
				  ○ 22 – Attended, Online with offline capability
				  ○ 23 – Attended, Offline only
				  ○ 24 – Unattended, Online only
				  ○ 25 – Unattended, Online with offline capability
				  ○ 26 – Unattended, Offline only
				• Cardholder Controlled
				  ○ 34 – Unattended, Online only
				  ○ 35 – Unattended, Online with offline capability
				  ○ 36 – Unattended, Offline only

ADDITIONAL TERMINAL CAPABILITIES	10	HEX	HOST	EMV Tag 9F40 – Indicates the data input and output capabilities of the terminal.
				• Byte 1 – Transaction Type Capability
				Indicates all the types of transactions supported by the terminal.
				  ○ Bit 8 – Cash
				  ○ Bit 7 – Goods
				  ○ Bit 6 – Services
				  ○ Bit 5 – Cashback
				  ○ Bit 4 – Inquiry
				  ○ Bit 3 – Transfer
				  ○ Bit 2 – Payment
				  ○ Bit 1 – Administrative
				• Byte 2 – Transaction Type Capability
				  ○ Bit 8 – Cash Deposit
				  ○ Bits 7-1 – RFU
				• Byte 3 – Terminal Data Input Capability
				Indicates all the methods supported by the terminal for entering transaction-related data into the terminal.

Field Name	Length	Format	Source	Value/Description
				◦ Bit 8 – Numeric keys ◦ Bit 7 – Alphabetic and special character keys ◦ Bit 6 – Command keys ◦ Bit 5 – Function keys ◦ Bits 4-1 – RFU • Byte 4 – Terminal Data Output Capability Indicates the ability of the terminal to print or display messages and the character set code table(s) referencing the part(s) of ISO/IEC 8859 supported by the terminal. ◦ Bit 8 – Print, attendant ◦ Bit 7 – Print, cardholder ◦ Bit 6 – Display, attendant ◦ Bit 5 – Display, cardholder ◦ Bits 4-3 – RFU ◦ Bit 2 – Code table 10 ◦ Bit 1 – Code table 9 • Byte 5 – Terminal Data Output Capability Indicates the ability of the terminal to print or display messages and the character set code table(s) referencing the part(s) of ISO/IEC 8859 supported by the terminal. ◦ Bit 8 – Code table 8 ◦ Bit 7 – Code table 7 ◦ Bit 6 – Code table 6 ◦ Bit 5 – Code table 5 ◦ Bit 4 – Code table 4 ◦ Bit 3 – Code table 3 ◦ Bit 2 – Code table 2 ◦ Bit 1 – Code table 1
TERMINAL COUNTRY CODE	3	N	HOST	EMV Tag 9F1A – Indicates the country of the terminal, represented according to ISO 3166.
TRANSACTION CURRENCY CODE	3	N	HOST	EMV Tag 5F2A – Indicates the currency code of the transaction according to ISO 4217.
TRANSACTION CURRENCY EXPONENT	1	N	HOST	EMV Tag 5F36 – Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217.
TRANSACTION REFERENCE CURRENCY CODE	3	N	HOST	EMV Tag 9F3C – Code defining the common currency used by the terminal in case the Transaction Currency Code is different from the Application Currency Code.
TRANSACTION REFERENCE CURRENCY EXPONENT	1	N	HOST	EMV Tag 9F3D – Indicates the implied position of the decimal point from the right of the transaction amount, with the Transaction Reference Currency Code represented according

Field Name	Length	Format	Source	Value/Description
				to ISO 4217.

6.17.6.2.2.2 Table 40—Contact Card Data

Table-ID 40—Contact Card Data

Field Name	Length	Format	Source	Value/Description
AID COUNT	2	N	HOST	Number of contact chip card Application Identifiers (AIDs) supported for the specified CARD TYPE.
The following fields will be repeated, dependent upon the AID COUNT.				
APPLICATION IDENTIFIER (AID)	32	HEX	HOST	EMV Tag 9F06 – Identifies the application as described in ISO/IEC 7816-5. Consists of the Registered Application Provider Identifier (RID) + a Proprietary Application Identifier Extension (PIX), e.g., A0000000031010 for Visa Debit/Credit.
APPLICATION SELECTION INDICATOR	1	N	HOST	For an application in the ICC to be supported by an application in the terminal, the Application Selection Indicator indicates whether the associated AID in the terminal must match the AID in the card exactly, including the length of the AID, or only up to the length of the AID in the terminal. There is only one Application Selection Indicator per AID supported by the terminal. • 0 = Exact match required • 1 = Partial match allowed
APPLICATION VERSION NUMBER	4	HEX	HOST	EMV Tag 9F09 – Version number assigned by the payment system for the application. Current version supported by the terminal, e.g., 1.5.0 for Visa VIS would be HEX "0096".
APPLICATION COUNTRY CODE	3	N	HOST	This is a Heartland proprietary field, not an EMVCo specified field. Indicates the country code associated with the AID. • If this field is zero-filled, the AID is internationally accepted and its use is unrestricted. • If this field is non-zero, the AID can only be used domestically within the country indicated, and may be automatically selected for applicable transaction types when present on the card.
TRANSACTION TYPES	4	HEX	HOST	Indicates the transaction types associated with the AID. May need this information in order to customize the AID list on the

Field Name	Length	Format	Source	Value/Description

				terminal to restrict application selection to only the appropriate AIDs based on whether the merchant/cardholder selects credit, debit, or other transaction type.
				
				• Byte 1
				  ◦ Bit 8 – Credit
				  ◦ Bit 7 – Debit
				  ◦ Bit 6 – EBT
				  ◦ Bit 5 – Gift
				  ◦ Bit 4 – Loyalty
				  ◦ Bit 3 – Stored Value
				  ◦ Bits 2-1 – RFU
				• Byte 2
				  ◦ Bits 8-1 – RFU

TERMINAL CAPABILITIES	6	HEX	HOST	EMV Tag 9F33 – Indicates the card data input, CVM, and security capabilities of the terminal for the AID.
				
				• Byte 1 – Card Data Input Capability
				Indicates all the methods supported by the terminal for entering the information from the card into the terminal.
				  ◦ Bit 8 – Manual key entry
				  ◦ Bit 7 – Magnetic stripe
				  ◦ Bit 6 – IC with contacts
				  ◦ Bits 5-1 – RFU
				• Byte 2 – CVM Capability
				Indicates all the methods supported by the terminal for verifying the identity of the cardholder at the terminal.
				  ◦ Bit 8 – Plaintext PIN for ICC verification
				  ◦ Bit 7 – Enciphered PIN for online verification
				  ◦ Bit 6 – Signature (paper)
				  ◦ Bit 5 – Enciphered PIN for offline verification
				  ◦ Bit 4 – No CVM Required
				  ◦ Bits 3-1 – RFU
				• Byte 3 – Security Capability
				Indicates all the methods supported by the terminal for authenticating the card at the terminal and whether or not the terminal has the ability to capture a card.
				  ◦ Bit 8 – SDA
				  ◦ Bit 7 – DDA
				  ◦ Bit 6 – Card capture
				  ◦ Bit 5 – RFU
				  ◦ Bit 4 – CDA
				  ◦ Bits 3-1 – RFU

Field Name	Length	Format	Source	Value/Description
TERMINAL FLOOR LIMIT	12	N	HOST	EMV Tag 9F1B – Indicates the floor limit in the terminal in conjunction with the AID. Indicates the amount above which an online authorization is required for contact transactions.
THRESHOLD VALUE FOR BIASED RANDOM SELECTION	12	N	HOST	Transactions with amounts less than this value will be subject to selection at random without further regard for the value of the transaction. Transactions with amounts equal to or greater than this value, but less than the floor limit will be subject to selection with bias toward sending higher value transactions online more frequently (biased random selection).
TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION	2	N	HOST	For transactions with amounts less than the Threshold Value for Biased Random Selection, the terminal shall generate a random number from 1 to 99, and if this number is less than or equal to this value, the transaction shall be selected to go online.
MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION	2	N	HOST	This is the desired percentage of transactions "just below" the floor limit that will be selected to go online.
TERMINAL ACTION CODE (TAC) – DENIAL	10	HEX	HOST	Specifies the acquirer's conditions that cause the denial of a transaction without attempt to go online. For each bit set to 1, if the corresponding bit in the Terminal Verification Results (TVR) is set to 1, the transaction will be offline declined, e.g., 0010000000 causes a decline for the "Service Not Allowed" condition.
TERMINAL ACTION CODE (TAC) – ONLINE	10	HEX	HOST	Specifies the acquirer's conditions that cause a transaction to be transmitted online. For each bit set to 1, if the corresponding bit in the TVR is set to 1, the transaction will be sent online.
TERMINAL ACTION CODE (TAC) – DEFAULT	10	HEX	HOST	Specifies the acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online. For each bit set to 1, if the corresponding bit in the TVR is set to 1, the transaction will be offline declined if the terminal is unable to go online.
TERMINAL RISK MANAGEMENT DATA	16	HEX	HOST	EMV Tag 9F1D – Application-specific value used by the card for risk management purposes.
DEFAULT TRANSACTION CERTIFICATE DATA OBJECT	32	HEX	HOST	TDOL to be used for generating the TC Hash Value if the TDOL in the card is not present.

Field Name	Length	Format	Source	Value/Description
LIST (TDOL)				
DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)	32	HEX	HOST	DDOL to be used for constructing the INTERNAL AUTHENTICATE command if the DDOL in the card is not present.

6.17.6.2.2.3 Table 50—Contactless Card Data

Table-ID 50—Contactless Card Data

Field Name	Length	Format	Source	Value/Description
AID COUNT	2	N	HOST	Number of contact chip card Application Identifiers (AIDs) supported for the specified CARD TYPE.
The following fields will be repeated, dependent upon the AID COUNT.				
APPLICATION IDENTIFIER (AID)	32	HEX	HOST	EMV Tag 9F06 – Identifies the application as described in ISO/IEC 7816-5. Consists of the Registered Application Provider Identifier (RID) + a Proprietary Application Identifier Extension (PIX), e.g., A0000000031010 for Visa Debit/Credit.
APPLICATION SELECTION INDICATOR	1	N	HOST	For an application in the ICC to be supported by an application in the terminal, the Application Selection Indicator indicates whether the associated AID in the terminal must match the AID in the card exactly, including the length of the AID, or only up to the length of the AID in the terminal. There is only one Application Selection Indicator per AID supported by the terminal. • 0 = Exact match required • 1 = Partial match allowed
APPLICATION VERSION NUMBER	4	HEX	HOST	EMV Tag 9F09 – Version number assigned by the payment system for the application. Current version supported by the terminal, e.g., 1.5.0 for Visa VIS would be HEX "0096".
MAGSTRIPE APPLICATION VERSION NUMBER	4	HEX	HOST	Version number assigned by the payment system for the contactless magstripe application. Current version supported by the reader, e.g., 0001 for Mastercard PayPass Mag Stripe.
APPLICATION COUNTRY CODE	3	N	HOST	Indicates the country code associated with the AID. If this field is space-filled, the AID is internationally accepted and its use is unrestricted. If this field is populated, the AID can only be used domestically within the country indicated, and should be automatically selected for applicable transaction types when present on the card.

TRANSACTION TYPES	4	HEX	HOST	Indicates the transaction types associated with the AID. May need this information in order to customize the AID list on the terminal to restrict application selection to only the appropriate AIDs based on whether the merchant/cardholder selects credit, debit, or other transaction type.
				• Byte 1
				  ◦ Bit 8 – Credit
				  ◦ Bit 7 – Debit

Field Name	Length	Format	Source	Value/Description
				○ Bit 6 – EBT ○ Bit 5 – Gift ○ Bit 4 – Loyalty ○ Bit 3 – Stored Value ○ Bits 2-1 – RFU • Byte 2 ○ Bits 8-1 – RFU
TERMINAL CAPABILITIES	6	HEX	HOST	EMV Tag 9F33 – Indicates the card data input, CVM, and security capabilities of the terminal for the AID. • Byte 1 – Card Data Input Capability Indicates all the methods supported by the terminal for entering the information from the card into the terminal. ○ Bit 8 – Manual key entry ○ Bit 7 – Magnetic stripe ○ Bit 6 – IC with contacts ○ Bits 5-1 – RFU • Byte 2 – CVM Capability Indicates all the methods supported by the terminal for verifying the identity of the cardholder at the terminal. ○ Bit 8 – Plaintext PIN for ICC verification ○ Bit 7 – Enciphered PIN for online verification ○ Bit 6 – Signature (paper) ○ Bit 5 – Enciphered PIN for offline verification ○ Bit 4 – No CVM Required ○ Bits 3-1 – RFU • Byte 3 – Security Capability Indicates all the methods supported by the terminal for authenticating the card at the terminal and whether or not the terminal has the ability to capture a card. ○ Bit 8 – SDA ○ Bit 7 – DDA ○ Bit 6 – Card capture ○ Bit 5 – RFU ○ Bit 4 – CDA ○ Bits 3-1 – RFU
TERMINAL CONTACTLESS FLOOR LIMIT	12	N	HOST	EMV Tag 9F1B – Indicates the floor limit in the terminal in conjunction with the AID. Indicates the amount above which an online authorization is required for contactless transactions.
TERMINAL CVM REQUIRED LIMIT	12	N	HOST	Indicates the amount above which a CVM is required for contactless transactions.

Field Name	Length	Format	Source	Value/Description
TERMINAL CONTACTLESS TRANSACTION LIMIT	12	N	HOST	Indicates the amount above which a contactless transaction is not allowed and the cardholder should be directed to use the contact chip instead.
TERMINAL ACTION CODE (TAC) – DENIAL	10	HEX	HOST	Specifies the acquirer's conditions that cause the denial of a transaction without attempt to go online. For each bit set to 1, if the corresponding bit in the Terminal Verification Results (TVR) is set to 1, the transaction will be offline declined, e.g., 0010000000 causes a decline for the "Service Not Allowed" condition.
TERMINAL ACTION CODE (TAC) – ONLINE	10	HEX	HOST	Specifies the acquirer's conditions that cause a transaction to be transmitted online. For each bit set to 1, if the corresponding bit in the TVR is set to 1, the transaction will be sent online.
TERMINAL ACTION CODE (TAC) – DEFAULT	10	HEX	HOST	Specifies the acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online. For each bit set to 1, if the corresponding bit in the TVR is set to 1, the transaction will be offline declined if the terminal is unable to go online.
TERMINAL TRANSACTION QUALIFIERS (TTQ)	8	HEX	HOST	Indicates the requirements for online and CVM processing as a result of Entry Point processing. The scope of this tag is limited to Entry Point. Kernels may use this tag for different purposes. This field is referred to as Terminal Transaction Capabilities in the American Express Expresspay specification.
TERMINAL RISK MANAGEMENT DATA	16	HEX	HOST	EMV Tag 9F1D – Application-specific value used by the card for risk management purposes.
DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)	32	HEX	HOST	TDOL to be used for generating the TC Hash Value if the TDOL in the card is not present.

6.17.6.2.2.4 Table 60—Public Key Data

Table-ID 60—Public Key Data

Field Name	Length	Format	Source	Value/Description
KEY COUNT	2	N	HOST	Number of Certificate Authority Public Keys defined for the specified EMV PDL CARD TYPE. Each card brand may have up to 6 keys.
The following fields will be repeated, dependent upon the KEY COUNT.				
REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	10	HEX	HOST	Unique identifier assigned to an application provider (card brand) according to ISO/IEC 7816-4, e.g., A000000003 for Visa.
CERTIFICATION AUTHORITY PUBLIC KEY INDEX	2	HEX	HOST	Identifies the certification authority's public key in conjunction with the RID.
KEY STATUS	1	A/N	HOST	Indicates the status of the Certification Authority Public Key. • A = Active • E = Expired • R = Revoked If the status is (E)xpired or (R)evoked, the key must be removed from the POS.
The following fields will only be present if the KEY STATUS is (A)ctive.				
CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	4	N	HOST	Number of hexadecimal characters in the field that follows that contains the modulus part of the Certification Authority Public Key.
CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	per length field above	HEX	HOST	Value of the modulus part of the Certification Authority Public Key.
CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	2	HEX	HOST	Value of the exponent part of the Certification Authority Public Key.
CERTIFICATION AUTHORITY PUBLIC KEY CHECK SUM	40	HEX	HOST	A check value calculated on the concatenation of all parts of the Certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1.

6.17.6.2.3 PDL Response—Confirmation

This response is sent to the client upon confirming receipt of the table data.

EMV PDL Response – Confirmation

Field Name	Length	Format	Source	Value/Description
TABLE VERSION	3	A/N	HOST	Echoed from PDL request.
BLOCK SEQUENCE NUMBER	2	N	HOST	Echoed from PDL request.
TABLE-ID	2	N	HOST	Echoed from PDL request.
CARD TYPE	2	N	HOST	Echoed from PDL request.
CONFIRMATION FLAG	1	A/N	HOST	C = Host received EMV PDL table download confirmation from POS.

6.18 Fingerprint Service

Portico now offers the option for merchants to enroll in a Card-Based Loyalty Program by using Global Payments' Fingerprint Service. This service offers merchants the ability to provide their own card-based loyalty program. Merchant benefits include the ability to:

- Offer Loyalty Card Programs
- Build customer profiles
- Track customer behavior across channels
- Offer marketing campaigns based on customer behavior

NOTE: Fees may apply for this service; where applicable, the merchant must agree to the monthly pricing before the settings are enabled on Portico.

6.19 Gratuity

Tips can be processed on the initial purchase ("tip on purchase") or can be added later as an adjustment. For tip on purchase, there is a gratuity field that can be included to indicate the portion of the sale that is specific to tip.

After the purchase, CreditAddToBatch or CreditTxnEdit can be used to add a tip and adjust the original transaction amount to include the tip amount. CreditAddToBatch or CreditTxnEdit can also be used to alter tip information in the case that the transaction amount had been adjusted with the tip amount, but the gratuity field had not been included with the correct amount. If the edit service is used, the client will still need to add the transaction to the batch in order for it to settle.

6.19.1 Mastercard Gratuity Rules

For merchants in the US, Mastercard credit transactions are subject to additional rules for gratuity:

- If the card data source is Chip/PIN, Contactless, or Card-not-present, any gratuity must be **included** in the authorization request. A gratuity must not be added to the authorized amount.
  Exception: Restaurants (MCC 5812, 5814) have a 20% gratuity tolerance for Mastercard transactions; if the gratuity exceeds 20 percent of the authorized amount, these merchants may request an additional or incremental authorization for the amount in excess of the authorized amount.
- If the card data source is a signature-based magnetic stripe or Chip (without PIN), a gratuity may be added **after** authorization is obtained; a 20% tolerance applies to the gratuity. If the gratuity exceeds 20 percent of the authorized amount, then the Merchant may request an additional or incremental authorization for the amount in excess of the authorized amount.

For any request, if the authorization response indicates a Partial Approval (RspCode = 10), gratuity may not be added.

6.20 Heartland Platforms / Payment Facilitators

In support of **Heartland Platforms** and **ProPay**, Portico provides an integration point for platform-based partners, such as payment facilitators and marketplaces, where the processing merchant location is a sub-merchant of a payment facilitator. The Payment Facilitator is responsible for underwriting and funding of the sub-merchant.

> Enrollment with a partner Payment Facilitator is required for sub-merchants, contact your representative for assistance.

Portico supports integrations directly by a Payment Facilitator or by the sub-merchant.

6.20.1 Sub-Merchant Integrations

For sub-merchant integrations, the sub-merchant is boarded as a unique DeviceId on Portico, under a MID set up for a Payment Facilitator or Partner.

Sub-merchant integrations are supported on the following Authorization Platforms:

- Exchange
- GSAP-NA

During transaction processing, the sub-merchant POS sends the request. Portico requests authorization from the Payment Facilitator.

- If declined, Portico returns RspCode with the value “PF”, and RspText is preceded with “Transaction rejected by Payment Facilitator” followed by any text provided by the Payment Facilitator.
- If approved, Portico processes the transaction to the front end host. When the response is received, Portico shares the result with the Payment Facilitator and the sub-merchant POS.

The sub-merchant is expected to obtain reporting from the Payment Facilitator.

6.20.1.1 Sub-merchant Transaction Elements

For Sub-merchant integrations, the transaction **response** includes two unique fields returned in the response Header:

- PaymentFacilitatorTxnId—Unique transaction identifier assigned by the Payment Facilitator.
- PaymentFacilitatorTxnNbr—Unique sub-merchant account identifier assigned by the Payment Facilitator.

These fields allow the sub-merchant to identify the transaction in the Payment Facilitator's reporting system.

6.20.2 Payment Facilitator Integrations

For Payment Facilitator integrations, the Payment Facilitator is boarded as a unique MID on Portico. The sub-merchant POS sends the request to the Payment Facilitator, which passes it to Portico for authorization.

Payment Facilitator integrations are supported on the GSAP-NA Authorization Host.

During transaction processing, the sub-merchant POS sends the request to the Payment Facilitator, which passes it to Portico for processing. Portico sends the request to the front end host and passes the response back to the Payment Facilitator, which passes it back to the sub-merchant's POS.

6.20.2.1 Payment Facilitator Transaction Elements

For Payment Facilitators, the SubMerchantData block is required in each transaction **request**. This data block provides the details about the Sub-Merchant processing location. This data passes through to the card issuer to ensure that the cardholder can identify the merchant on their statement. This information includes:

- Sub-merchant DBA name
- Payment Facilitator account and terminal ID reference IDs for the Sub-Merchant
- MCC for the Sub-Merchant processing location

See the SubMerchantData Complex Type in the Portico Schema.

6.20.3 Transaction Set for Payment Facilitator Sub-Merchants

For Payment Facilitator submerchants, Portico supports credit processing on following transactions:

- CreditAccountVerify
- CreditAddToBatch
- CreditAuth
- CreditCPCEdit
- CreditReturn
- CreditReversal
- CreditSale
- CreditTxnEdit
- CreditVoid
- RecurringBilling
- RecurringBillingAuth

For Canadian sub-merchants, the following are also supported:

- DebitAddToBatch
- DebitAuth
- DebitReturn
- DebitReversal
- DebitSale

Portico-based batch management is required, since Portico streams the batch details to ProPay. Please note that AutoClose is required for all ProPay submerchants. The recommended auto-close times are 11PM for Retail and 3AM for Restaurant. Each DeviceId may be configured on the Device to any time that is appropriate for the business, but auto-close may not be disabled. Additional manual BatchClose is allowed.

6.21 Industries

Portico supports all the major payment processing industries. The following sections provide information on how to use the different Portico services based on the target industry.

6.21.1 Retail

The majority of retail transactions are processed using the CreditSale transaction type.

6.21.2 Restaurant

A typical restaurant transaction is processed using the CreditAuth transaction type to hold the initial amount. This transaction can be followed by a CreditAddToBatch transaction, which finalizes the total amount, may also adjust the transaction for the tip (if necessary), and adds the transaction to the current batch.

An alternative to using CreditAuth and CreditAddToBatch for tip handling is to use CreditTxnEdit to adjust the transaction, prior to using CreditAddToBatch to finalize the amount and add the transaction to the batch.

CreditAuth+CreditAddToBatch has the advantage of ensuring that no unadjusted transactions are inadvertently settled if the merchant is wanting to use auto-settlement.

> NOTE: Merchants hosted on the Exchange Authorization host may use a CreditSale transaction followed by CreditTxnEdit, but this is not recommended. All new Restaurant integrations should use the CreditAuth transaction type.

Portico supports CreditIncrementalAuth for bars and restaurants. The original transaction must be an open CreditAuth that has not yet been added to the batch.

> NOTE: For new integrations, Portico no longer supports the CreditAdditionalAuth service for the handling of bar tabs. This service has been deprecated. Please use CreditIncrementalAuth.

6.21.3 Lodging

The Lodging data is supplied as an extension on existing transactions listed in this document and the schema documentation. Support for Lodging is provided by the LodgingDataType elements and its sub-elements.

The following are some typical use cases for Lodging:

Check In

Upon Check-In, the merchant may use a CreditAuth transaction to authorize the card and reserve the funds. If all that is needed at check-in is to validate the card, a CreditAccountVerify can be used. If the final amount of the stay is known, a CreditSale can be used.

Check Out

Upon Check-Out, the merchant closes out a CreditAuth by using the CreditAddToBatch transaction (if the Check-In used a CreditAuth that has not yet been added to a batch). Otherwise, a CreditSale can be run. or the original authorized amount can be reduced using a CreditTxnEdit transaction. The transaction request must include the GatewayTxnID from the Check-In authorization transaction, and optionally the amount of the transaction.

Incremental Authorization for the Lodging Industry

Use the CreditIncrementalAuth transaction to increase the authorized amount on a credit card. Incremental authorization in the lodging industry is typically used for extended duration and extra charges added to a customer's stay.

Single Stay

- To charge for a Single Stay use the CreditSale transaction. This will authorize the associated amount and add it to the current batch. If a batch does not exist, this transaction creates one.

  > The duration for a Single Stay defaults to one day.

Advance Deposit

- To run an Advance Deposit, use the CreditSale transaction. The merchant must ensure that the transaction amount does not exceed the total price of the reserved services or activity. The cardholder must be informed of the total price of the services or activity, the advance deposit amount, the advance deposit confirmation code, and the cancellation terms.

> **Note**: For American Express, see also Amex Special Programs.

Additional Charge

- To include an additional charge prior to check-out, use the CreditTxnEdit transaction to alter the original transaction.
- For additional charges after check-out, see Delayed Charges.

No Show

- A merchant may charge for a No Show if the cardholder does not stay and does not cancel by the agreed timeframe
- For all card brands, to charge penalties for a No Show, use a CreditSale transaction:
  - The Card Brands require the CardBrandTxnId from the original authorization response to be sent in the No Show request; this is achieved by sending the CardBrandTxnId in the CardOnFileData block in the No Show authorization request
  - Set the NoShow Indicator to True for all card brands

> The CardOnFile indicator is not required in this case unless a stored credential is being used. Refer to Credential/Card on File for further details.

> **Note**: For American Express, see also Amex Special Programs.

Delayed Charges

- To charge for extra charges after check-out, use a CreditSale transaction.
  - The Card Brands require the CardBrandTxnId from the original authorization response to be sent in the Delayed Charges request. This is achieved by sending the CardBrandTxnId in the CardOnFileData block in the Delayed Charges authorization request.

    > The CardOnFile indicator is not required in this case unless a stored credential is being used. Refer to Credential/Card on File for further details.

> The check-in date is the initial authorization date and the stay duration is one day.
>
> The valid stay duration is from 1 to 99 days.

Extra Charges

Lodging merchants may specify which types of Extra Charges were incurred during a stay. These charges must be sent in the appropriate fields for the authorization platform.

- For merchants processing on the GSAP-NA, GNAP-UK, and Exchange authorization platforms, Extra Charges are sent as Boolean (true/false) indicators
- For merchants processing on the GSAP-AP authorization platform, Extra Charges are sent as amounts

Amex Special Programs

The AdvancedDepositType data block is used for American Express cards only.

- ASSURED_RESERVATION - This is an American Express Special Program Code. The merchant may do an Assured Reservation. A room is guaranteed for the cardholder. The cancellation policy must be shared with the cardholder. If the cardholder does not stay or cancel by the agreed timeframe, the merchant may charge a NoShow fee, in accordance with the cancellation policy.
- CARD_DEPOSIT- This is an American Express Special Program Code. The merchant may do Card Deposit (Advanced Deposit) , usually for 1 night stay including the cost of the room, taxes and for incidentals.
- PURCHASE - This is an American Express Special Program Code. For a regular check-in, use CreditSale with AdvancedDepositType set to PURCHASE.

6.21.4 Healthcare

Auto-substantiation is used in the healthcare industry as a result of IRS Notice 2006-69 for consumers to use flexible spending account (FSA/HRA) debit cards where the transaction is automatically substantiated at the POS. For merchants who support auto-substantiation at the POS, consumers no longer need to file a separate claim for benefits

To take advantage of auto-substantiation, the merchant must use an Inventory Information Approval System (IIAS). The IIAS identifies the qualified healthcare products being purchased by the cardholder at the POS. The IIAS must identify the FSA and HRA cards, automatically differentiate between qualified and non-qualified products at the POS, flag the items on the customer receipt, subtotal the qualified healthcare products amount including tax and discounts, and accommodate split-tender capability for non-qualified products.

> Requests should never contain Protected Healthcare Information (PHI), nor should PHI be passed on to Heartland in any form of communication.

See the AutoSubstantiation Complex Type in the Portico Schema.

6.21.5 Mail Order Telephone Order(MOTO)

Mail Order/Telephone Order (MOTO transactions are handled as "card not present" transactions. These process as credit transactions.

6.21.6 eCommerce

eCommerce transactions are handled as "card not present" transactions. This includes In-Application and online payments. These process as credit transactions.

6.21.6.1 3D Secure and Wallet Payments

Portico now supports 3D Secure 2.x, also known as EMV 3D Secure, which is an improved version of 3D Secure (“3DS”) and delivers an improved checkout experience for online e-commerce card-not-present transactions. This is also known as Verified by VISA, MasterCard Identity or SecureCode, Discover ProtectBuy and American Express SafeKey.

To support 3D Secure 2.x, two data blocks have been added to the credit transactions, one for 3DS Version1 and Version2 transactions (MC, Visa, Discover, UnionPay), and one for Wallet transactions.

> These data blocks contain the result of consumer authentication of the account through the Issuer and Brands.

6.21.6.1.1 Secure3D

The data block Secure3D should be used to carry 3DS Version1 and Version2 transactions and include the cardholder authentication details from card brand-specific 3D Secure based protocols.

Subfield	Description
Version	Identifies the version of 3DS protocol used for authentication. Possible values 1 or 2.
Authentication Value	This value is the reference generated by the issuer to recognize that the authentication has taken place. Supported formats are CAVV, AEVV, UCAF. CAVV—Cardholder authentication verification value used by Visa, Disc, UP AEVV—American Express Verification value UCAF—Universal cardholder authentication field used by MasterCard Must be encoded using base16 (Hex encoding) or base64 encoding
ECI	Electronic Commerce Indicator shows the value of the result of the authentication. Valid values: • MasterCard 2, 1 ,0 • Visa, Amex, Disc 5, 6, 7 2 or 5 = **Fully Authenticated Transaction** 1 or 6 = **Attempted Authenticated Transaction** 0 or 7 = **Non 3D Secure Transaction**
DirectoryServerTxnId	The unique transaction identifier assigned by the Directory Server to identify a single transaction. Required for MasterCard Identity Check (3DS Version 2) transactions in Authorization.

6.21.6.1.2 WalletData

The data block WalletData should be used for Wallet Transactions (ApplePayApp, ApplePayWeb, GooglePayApp, GooglePayWeb). Wallets can also be secured with 3DS processing meaning that it supports sending an authorization request containing both the wallet and 3D Secure information in it.

Subfield	Description
PaymentSource	Supported sources: • Apple Pay • ApplePayApp • ApplePayWeb • GooglePayApp • GooglePayWeb
Cryptogram	Cryptogram received from wallet payment. Supported formats: • DSRP • TokenBlocks • TAVV cryptograms Must be encoded using base16 (Hex encoding) or base64 encoding
ECI	Electronic Commerce Indicator associated with the Cryptogram (optional).
DigitalPaymentToken	Payment payload used to send encrypted ApplePay or GooglePay data

Portico supports passing both encrypted and decrypted data for InApp Wallet payments. Payments with encrypted data are only available to merchants processing on the **Exchange** host.

A DigitalPaymentToken should be unique per transaction.

> Wallet payments such as Applepay and Google Pay are not intended for recurring use and may decline on subsequent transactions.

Decrypted Data

CardData block should be populated with DPAN.

WalletData block should include:

- PaymentSource
- Cryptogram
- ECI

Encrypted Data

For Exchange-hosted merchants, Portico has expanded support for Google Pay and Apple Pay to allow merchants to send encrypted card data. It is a requirement that merchants enroll with Google or Apple and have Heartland Developer Portal access to request and manage certificates.

The encrypted data is passed in a new field in Wallet Data: Digital Payment Token. When present, no data is passed in the CardData block.

WalletData block should include:

- PaymentSource
- Cryptogram
- ECI
- Digital Payment Token

Note: Merchant enrollment is required. Please contact your Heartland representative.

6.21.6.2 Secure eCommerce Data Block (Deprecated)

This page is for reference only, please refer to 3D Secure and Wallet Payments for new integrations.

In Application and Secure eCommerce use the SecureECommerce block in the transaction schema. This block consists of:

- PaymentDataSource
- TypeOfPaymentData
- PaymentData
- ECommerceIndicator
- XID

NOTE: This section will be removed in future versions.

6.21.6.2.1 In Application Payments

This page is for reference only, please refer to 3D Secure and Wallet Payments for new integrations.

At a high level, cardholders have registered their payment information with a 3rd party such as a mobile phone vendor, e.g., Apple, with a token being returned that is stored on their device. The cardholder then uses this stored token to purchase goods/services within a merchant's application that is on their device. The merchant's application sends the authorization message to Portico using the standard CreditAuth or CreditSale transactions. However, the SecureECommerce field is sent within those messages containing the necessary eCommerce InApp data that is required by the brands and issuers to settle correctly.

ECI Indicator

If an EcommerceIndicator is sent in for ApplePay or GooglePay, it will be passed along to the host.

If an ECI value is **not** passed in, the following default values will be assigned:

- Exchange the value is 4
- GSAP-NA the value is 5

This functionality is currently only supported for ApplePay and GooglePay for Visa, MasterCard, American Express, and Discover.

ApplePay or GooglePay In App

For ApplePay or GooglePay In-App, the following SecureECommerce data elements apply:

- PaymentDataSource set to the appropriate value, eg, "ApplePay", "ApplePayInApp", "GooglePayInApp"
- TypeOfPaymentData
  - 3DSecure
- PaymentData
  - Visa CAVV, Discover CAVV, AMEX Token Data Token Data Block A followed by Token Data Block B, and Mastercard UCAF
- ECommerceIndicator

- Numeric value from 0–7

> If sent, this value is ignored.

American Express Payment Data

For AMEX only, the following is also supported, but both token data blocks may be sent in PaymentData:

- PaymentData
  - AMEX Token Data Token Data Block B
- XID
  - AMEX Token Data Token Data Block A

6.21.6.2.2 3D Secure Authentication

> This page is for reference only, please refer to 3D Secure and Wallet Payments for new integrations.

An eCommerce consumer authentication strategy that verifies the owner of the card account. After consumer authentication of the account through the Issuer and Brands, the merchant sends the CreditAuth or CreditSale authorization message to Portico.

The SecureECommerce field is sent within those messages containing the necessary eCommerce 3D Secure data that is required by the brands and issuers to settle correctly.

The ECommerceIndicator field within the SecureECommerce block should contain the ECI received from the 3DS Payment Authenticator. Both manual entry and token data are acceptable payment method forms for this functionality.

For Secure eCommerce, the following SecureECommerce data elements apply:

- PaymentDataSource
  - AMEX 3D Secure
  - Discover 3D Secure
  - Mastercard 3D Secure
  - Visa 3D Secure
- PaymentData
  - For Verified by Visa—Visa CAVV
  - For Discover ProtectBuy—Discover CAVV
  - For AMEX Safekey—Amex Safekey
  - For Mastercard 3D Secure—Mastercard UCAF
- ECommerceIndicator
  - Numeric value from 0–7

6.22 Incremental Authorization

An incremental authorization is used to increase the amount of a previous authorization. Card brand rules have expanded support for incremental authorizations beyond the travel and entertainment industries to additional retail and restaurant merchant category codes (MCCs).

> Note: Supported MCCs vary by card brand. For assistance determining whether incremental authorization is appropriate for your business, contact your Heartland representative.

For industry-specific guidelines, see also:

- Restaurant
- Lodging

6.22.1 Rules

The following rules apply to all Incremental Authorizations:

- Incremental authorizations are not standalone transactions. They must reference an **original** CreditAuth
- Approved Incremental authorizations increase the total settlement amount of the **original** CreditAuth
- The transaction ID of the **original** CreditAuth is used for all subsequent actions (i.e., voids, reversals, edits, etc); the transaction ID of the incremental authorization should never be referred to by subsequent transactions.
- If the final settlement amount of the **original** transaction is less than the cumulative authorized amount (original authorization + incremental authorizations), a partial reversal will automatically be generated for the difference
- The **original** transaction must be a fully approved CreditAuth

NOTE: Merchants processing via Portico to the Exchange authorization platform may perform incremental authorizations where the original transaction is either a CreditSale or a CreditAuth; however, CreditAuth should be used for all new integrations.

6.22.2 Managing Timeout Scenarios

CreditReversal is not supported for incremental authorizations. If a response is not received for an Incremental authorization request, ReportTxnDetail or FindTransactions can be used to verify whether it was received by the host. A card present POS may repeat the incremental authorization. The original can be voided or reversed, and a new Credit Auth processed for the updated amount.

6.22.3 Voids

All voids are performed against the **original** CreditAuth. Any corresponding incremental authorizations will be automatically voided along with the original transaction.

If an incremental authorization is submitted in error, the original transaction should be voided and resubmitted.

> On the GNAP-UK authorization platform, a transaction that has been added to the batch cannot be voided. If CreditAddToBatch was already performed, a CreditReturn is required.

6.23 Installment Payments

Portico supports installment payment programs in both Asia Pacific and Mexico. These programs allow the cardholder to select the terms and the number of payments. The merchant's transaction settles for the full amount, but the cardholder gets billed a flat amount for a set number of months.

The IPSelectedTerms data block is included in a CreditSale to indicate the Installment Plan terms selected by the cardholder. Only specific fields should be provided, based on the location of the merchant.

- Asia Pacific
- Mexico

6.23.1 Asia Pacific

Portico supports the following Installment Payment programs in the Asia Pacific region:

- HSBC Installment Payment Plan (HSBCIPP)
- Multi-Issuer Installment Payment Plan (mIPP)
- BPI Special Installment Plan (SIP)

Programs are not available in all countries.

The IPSelectedTerms data block is included in a CreditAuth or CreditSale to indicate the Installment Plan terms selected by the cardholder. Only specific fields should be provided, based on the location of the merchant.

Asia Pacific merchants provide the following fields:

- NbrInstallments
  - The number of months the cardholder will be billed
- Program
  - The value sent should match what is configured for the merchant on the Global Payments host
- SIPOptions (Optional)

CreditIPQuery may used to query the Installment Payment terms available to the cardholder.

6.23.2 Mexico

Portico supports Installment Payments for merchants located in Mexico. Valid card types for Installment Payments include Visa, Mastercard, American Express, Carnet, and Mexico Privada/Propia cards.

Merchants must provide the following fields:

- NbrInstallments
  - The number of months the cardholder will be billed
- InstallmentPlan
  - Indicates the terms, such as whether interest will be applied
- GracePeriod
  - The period before the first payment

When sending installment payment data, the currency of the transaction must be Mexican Pesos. See Transaction Currency.

6.24 Interac Processing

The Portico API supports Canadian clients processing Interac debit on Debit based services of the Portico API. These transactions require debit EMV certification. A normal Interac EMV transaction should contain the EMV tag data obtained from the terminal/chip card. All card present debit requests in Canada must process as Interac with the appropriate application id in the request.

All Interac transactions must send the POSReqDT in the request header and must also include both CardholderLanguage and POSSequenceNbr in Block 1.

Interac debit processing is supported on the following transactions:

- DebitAddToBatch
- DebitAuth
- DebitReturn
- DebitReversal
- DebitSale

For additional information, contact your representative.

6.24.1 Transaction Security

Interac transaction requests require the use of a PIN Pad device. Messages must use one of the following:

- Voltage encryption of the Card Data
- Message Authentication Code (MAC)
- PIN Pad (PED) Serial Number

Both Voltage and MAC cannot be used on a single PIN Pad device. If Voltage encryption is used, then any references to MessageAuthenticationCode do not apply.

> Device TID must be set up on the Host for the type of transaction security in use.

6.24.2 Debit Transaction Responses

The RspCode indicates whether a transaction is approved or not. Interac-specific data is returned to the POS in the DebitMac data block. In this block, the BankResponseCode indicates the status of the transaction on the host. The value returned in HostRspDT is adjusted to the local date and time of the POS. The time and date returned in the Response message header must be used on all printed receipts and reports.

6.24.2.1 Approvals

If the transaction is approved, the transaction is complete. A copy of the debit receipt **must** be printed for the cardholder in the language specified on Track 2 of the debit card. The merchant copy of the receipt is optional.

6.24.2.2 Declines

If the transaction is not approved:

- The result must be displayed on the PIN pad.
- A debit receipt **must** be printed. Optionally the transaction result may be stored and itemized on the final debit receipt.
- If the BankResponseCode allows the transaction to be resubmitted (e.g., 810 or 899):
    - The cardholder must complete the Interac prompting sequence on the PIN pad.
    - It is not necessary to re-present the card.
    - A new transaction Request message should be sent.
        - This will require updated POS Sequence Number and MAC value (if applicable).
- If the BankResponseCode does not allow the transaction to be resubmitted, the transaction should be cancelled or restarted.

6.24.3 Reversals

All Interac customer cancellations require the customer to be present (card must be inserted; track data must be sent.) These are sent as DebitReversal requests, with ReversalReasonCode set to CUSTOMERCANCELLATION.

6.24.4 POSSequenceNbr

The POSSequenceNbr field is required in Debit request messages.

6.24.4.1 POSSequenceNbr Structure

Position	Length	Description	Value
01-03	3	Shift Number	Always 001
04-06	3	Batch Number	Always 001
07-09	3	Sequence Number	###
10	1	Control Flag	Always 0

6.24.4.2 Incrementing POSSequenceNbr

The SequenceNumber of the POSSequenceNbr **must** be incremented on each transaction. After the value reaches "999", it should be reset to "001" on the next transaction. The rules for incrementing the values are:

Incrementing POSSequence Nbr	Rules
Approval	Increment the value.
Timeout/No Response	Send a timeout reversal, then increment the value.
Host Out of Sync	If the value in the POS and on the Host gets out of sync, then the host will return a decline message with Bank Response Code = 899, along with a value in TraceNumber; that value must be sent in PosSequenceNbr of the next request from the POS.
Response Received without BankResponseCode	This scenario is treated as "Transaction Not Completed." Do not increment the value.
Response Received with BankResponseCode = 898	Do not increment the value.
After Successful MACKey Exchange	Increment the value.

6.24.5 MessageAuthenticationCode

If MessageAuthenticationCode (MAC) is used, details are available from your certification analyst on how to implement this. Message Authentication Code (MAC) data is not required for contactless-only Interac transactions; it is required for all contact transactions unless Voltage encryption is used. The calculation for building the MAC String uses the POSSequenceNbr value.

Some responses indicate that the MAC value must be reset.

6.24.5.1 MAC Verification on Transaction Response

The 16-character alphanumeric MessageAuthenticationCode should be Encrypted using the MAC Encryption Key. The value is calculated and sent in the Debit request message. The Debit response contains a MessageAuthenticationCode value; the value in the response **must** be verified as follows:

Transaction Response	Rules
Approval	Verify the value.
Timeout/No Response	No value to verify. Send a reversal with ReversalReasonCode set to TIMEOUT.
Response Indicates MAC Verification Failed	No value to verify. Send DebitReversal with ReversalReasonCode set to MACFAILURE.
Host Out of Sync	If the POSSequenceNbr value in the POS and on the Host get out of sync, then the host will return a decline message with Bank Response Code = 899; when this occurs, the MAC value will need to be recalculated before the next Debit request message is sent. After POSSequenceNbr is reset, recalculate the MessageAuthenticationCode. If a MACKey was returned in the response, use that key in the MAC calculation. If the POS automatically resends the transaction without re-initializing from the beginning where cardholder enters PIN, the request will be declined with BankResponseCode 877 (Invalid PIN BLOCK). A response with 877 would necessitate a Key Exchange, which must be performed before the Debit transaction request is sent (see InteracDeviceKeys).
Response Received without BankResponseCode	This scenario is treated as "Transaction Not Completed." Do not verify the value.
Response Received with BankResponseCode = 877	Key Exchange required. Perform InteracDeviceKeys request to reset the value.
Response Received with BankResponseCode = 898	Key Exchange required. Perform InteracDeviceKeys request to reset the value.

6.24.5.2 Resetting the MAC Value

Some responses indicate that the MAC value must be reset. A new key may be returned in the response MacKey field, or the POS can perform a Key Exchange using the InteracDeviceKeys request.

6.24.5.2.1 Mac Key

A MacKey is used in the calculation of the MessageAuthenticationCode value. If the transaction response contains a value in MacKey, that key must be used in the MAC verification process prior to sending the next transaction.

6.24.5.2.2 Key Exchange

If the transaction response indicates that a KeyExchange is required, perform InteracDeviceKeys request to reset the value and synchronize the keys with the host.

6.24.6 Interac Device Keys

For Canadian merchants, this message can be used to synchronize the keys used for encrypting data in debit card messages for the Canadian debit card network, also referred to as Interac.

6.24.7 Interac PED Serial Number

Interac rules require tracking the location of any PIN Entry Device (PED) used to process debit transactions. To facilitate this, the PED serial number should be sent in the SerialNbr field in the Header for any Canadian debit transaction request.

The PED serial number may also be used as an alternate method for Interac transaction security, instead of Voltage encryption or the Message Authentication Code (MAC). Special host setting configuration is required, contact your Heartland representative for assistance.

See the Device Configuration Complex Type in the Portico Schema. Applicable to Canadian merchants only.

6.24.8 Interac Pre-Authorization & Completion

Interac allows for a pre-authorization on debit cards to place a temporary hold on funds before the final purchase amount is determined, for example, to allow a vending machine or kiosk to dispense multiple items within a single sale.

A DebitAuth places a hold on the cardholder's account for the funds specified. A DebitAddToBatch is then used to complete the sale; this is also called "capturing" the authorization. The DebitAddToBatch places the completed authorization in the batch.

The POS Sequence Number must be incremented for the DebitAuth and for the DebitAddtoBatch.

The following rules apply:

- AccountType must be CHECKING or SAVINGS
- The amount on the DebitAddToBatch cannot exceed the DebitAuth amount
- Cashback is not allowed on debit pre-authorizations or completions
- DebitAuth cannot be voided once approved
- If the cardholder cancels the DebitAuth, a DebitAddToBatch must be sent to Portico with an Amount of $0.00
    - **NOTE**: Portico also allows the POS to send a DebitReversal, as this message is formatted to the GSAP Host as a Capture for $0.00; the POS Sequence Number must be incremented and sent in the DebitReversal request
- In the event a DebitAuth request times out, a DebitReversal or Debit AddtoBatch for $0.00 should be sent
    - **NOTE**: When acting on a DebitAuth, both a DebitAddToBatch and a DebitReversal are formatted to the GSAP Host as a Debit Capture for $0.00
    - This notifies Interac to release the funds held by the authorization
- Once a Debit preauthorization has been completed with a DebitAddToBatch, the transaction cannot be reversed

- If the cardholder cancels the DebitAuth after it has been completed by a DebitAddToBatch, a DebitReturn is required to return the funds to the cardholder
- TagData is required in DebitAuth and DebitAddtoBatch transaction requests
- DebitAddToBatch must be submitted **within 2 hours** after approval of the DebitAuth

> NOTE: Interac regulations state that the Pre-Authorizations **must** be completed within two (2) hours of approval. If this is not done, the issuer has the right to reject the transaction and not credit the merchant.

6.25 Invoice Number

There are two invoice number fields in the Portico Transaction request messages, one in the AdditionalTxnData block and the other in the DirectMktData block. These fields are handled differently depending on the host and the transaction type.

Exchange

- Invoice number is sent to the host for credit messages only
- When either Invoice Number field is populated, the value passed in the Portico request is sent to the Exchange host
- When both Invoice Number fields are populated, the value in Direct Market Data takes precedence and is passed to the Exchange host
- If neither invoice number field is populated, then Portico has logic to send the GatewayTxnId of the transaction as Invoice Number to the Exchange host for Credit transactions only

GSAP-NA & GSAP-AP

- Invoice number is sent to the host for credit and debit messages
  - For credit transactions, an invoice number value is passed for all Industry Codes for all card types to help a merchant to qualify for the best interchange rates
  - For debit transactions, an invoice number value is passed when the industry code is H (lodging), E (ecommerce), or D (Direct Marketing/MOTO)
- When either Invoice Number field is populated, the value passed in the Portico request is sent to the GSAP host
- When both Invoice Number fields are populated, the value in Direct Market Data takes precedence and is passed to the GSAP host
- If neither invoice number field is populated, then Portico has logic to send the GatewayTxnId of the transaction as Invoice Number to the GSAP host during authorization

GNAP-UK

- Invoice Number is not sent to the GNAP host

6.26 Partial Authorization

A partial authorization is supported for a credit or PIN debit authorization request. The merchant must submit a CreditAuth, CreditSale, DebitSale, EBTFSPurchase, EBTCashBenefitWithdrawal, or EBTCashBackPurchase transaction that includes the AllowPartialAuth value set to "Y".

If approved, the merchant receives a "10" response code indicating the merchant must collect other funds to complete the sale. The Issuer also responds with the amount that is authorized.

For example, if an authorization request of $12.00 is sent along with the AllowPartialAuth value set to "Y" and the Issuer approves $7.00, the response is returned with an approval for $7.00. The merchant's software applies the approved $7.00 to the sale and the cardholder pays the remaining $5.00 using another form of payment (different credit card, check, cash, etc.).

Partial authorization can be used in any industry, provided the POS system has the ability to partially authorize a sale. It is recommended that the merchant be presented with a prompt to Void or Accept the transaction if a partial authorization is received. The following Merchant Category Codes (MCCs) **must** support partial authorization for American Express, Mastercard, Visa, and Discover:

MCC	Description
4812	Telecommunication Equipment including Telephone Sales
4814	Telecommunication Services
5111	Stationery, Office Supplies
5200	Home Supply Warehouse Stores
5300	Wholesale Clubs
5310	Discount Stores
5311	Department Stores
5331	Variety Stores

MCC	Description
5399	Miscellaneous General Merchandise Stores
5411	Grocery Stores, Supermarkets
5499	Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores and Vending Machines
5541	Stations (with or without Ancillary Services) Services
5542	Fuel Dispenser, Automated
5732	Electronic Sales
5734	Computer Software Stores
5735	Record Shops
5812	Eating Places, Restaurants
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5921	Package Stores, Beer, Wine, and Liquor
5941	Sporting Goods Stores
5942	Book Stores
5943	Office, School Supply and Stationery Stores
5999	Miscellaneous and Specialty Retail Stores
7829	Motion Picture—Video Tape Production–Distribution
7832	Motion Picture Theaters
7841	Video Entertainment Rental Stores
8011	Doctors—not elsewhere classified
8021	Dentists, Orthodontists
8041	Chiropractors
8042	Optometrists, Ophthalmologists
8043	Opticians, Optical Goods, and Eyeglasses
8062	Hospitals
8099	Health Practitioners, Medical Services—not elsewhere classified
8999	Professional Services—not elsewhere classified
4111	Transportation—Suburban and Local Commuter Passenger, including Ferries
4816	Computer Network/Information Services
4899	Cable, Satellite, and Other Pay Television and Radio Services
7996	Amusement Parks, Carnivals, Circuses, Fortune Tellers

MCC	Description
7997	Clubs—Country Membership
7999	Recreation Services—not elsewhere classified
9399	Government Services—not elsewhere classified

Partial authorization support is required by the card brands for many face-to-face industries in order to maximize support for debit and prepaid open-loop gift cards (those branded by one of the major card brands).

For Gift Card transactions, partial approvals are supported by default. If the Gift Card account balance is non-zero, but insufficient to cover the full redemption amount, the remaining balance is drained and the amount still owed is returned in the response for additional payment.

If approved, the merchant receives a "13" response code with a message stating that partial approval has been given. The merchant may accept any additional tender to cover the amount still owed.

If the account holder is unable to provide additional payment and the purchase is cancelled, this transaction should be voided to return the balance back to the account. See the "split tender card amount" and "split tender balance due amount" fields in the response.

> Tip adjustments are not allowed on partial authorizations. If adjustments are made through the CreditTxnEdit or CreditAddToBatch on a CreditSale or CreditAuth that received a partial authorization, an error is returned.

6.27 Personal Identification Number (PIN) Block

Debit and Electronic Benefit Transfer (EBT) transactions that require a cardholder-entered PIN must be submitted to Portico with a PIN block. The programmer guide for your PIN pad device contains details on how to obtain the PIN block including information on the request and response messages.

The response message to a PIN block request includes data containing a serial number and PIN. This data is used to generate the PIN block in the format required by Portico.

> Portico requires the order of the data to be PIN then serial number.

The format of the PIN Block response is as follows: <STX>71[fkey flag][Key Serial#][PIN]<ETX>[LRC]

The following table provides the encrypted PIN Block response field values:

Field	Length	Value and Description
STX	hexadecimal	0x02
Message ID	2	This value is always "71".
[fkey flag]	1	This value is always "0". > This field is kept to retain old model compatibility.
[Key Serial#]	10..20	The key serial number used in encrypting a PIN. It is included only when the PIN is entered. Format: hexadecimal string
[PIN]	16	Encrypted PIN block format: hexadecimal string
<ETX>	hexadecimal	<0x03>
[LRC]	1	Checksum

Example

The following is an example of an encrypted PIN block response from an E3 PIN entry request. It is in a Derived Unique Key Per Transaction (DUKPT) format.

The example uses the following values:

[fkey flag] = 0
[Key Serial#] = 1111111111111111
[PIN] = 2222222222222222

The response should be as follows:

<STX>7101111111111111111122222222222222222<ETX>[LRC]

The format for mapping the encrypted PIN block response data to Portico debit sale PIN block is as follows:

<PinBlock>[PIN][Key Serial#]</PinBlock>

Map the encrypted PIN block response data to Portico debit sale PIN block as follows:

```
<DebitSale>
<Block1>
...
<PinBlock>2222222222222222111111111111111111</PinBlock>
...
</Block1>
</DebitSale>
```

6.28 Store and Forward

Portico supports the ability to indicate a transaction was processed in Store and Forward (SAF) mode. In the transaction request header, the SAF data block allows a merchant to set a Store and Forward Indicator as well as the date and time when the transaction was originally initiated.

The FindTransactions report allows a merchant to search for transactions processed with the SAFIndicator populated.

6.29 Swiped or Proximity Entry

A swiped entry transaction occurs when a card is swiped (or passed) through a magnetic card reader or chip reader to capture the card information stored on the magnetic stripe or chip. A proximity entry transaction occurs when a card/mobile wallet is read by a proximity reader to capture the card/token information stored on the magnetic stripe, chip, or mobile device.

A swipe read or proximity payment read are the preferred methods of gathering the cardholder information because it typically results in lower interchange fees and provides for better security for the merchant. Swiped or proximity entry transactions require that you have a card reader attached to your application. The card reader reads the card information into your application for transmission to Portico.

For more information, see the TrackData method attribute.

6.30 Union Pay

UnionPay International offers card acceptance in multiple regions throughout the world through a combination of direct authorization processing and partnerships with other brands. Portico supports multiple UnionPay authorization routing options for merchants located in Canada and in the United Kingdom.

For all merchants using the UnionPay authorization network, the following conditions apply to all transactions authorizing directly with the UnionPay network:

- The following credit card transaction types are supported:
  - CreditAuth
  - CreditAddToBatch
  - CreditReturn
  - CreditSale
  - CreditReversal
  - CreditVoid
- Partial reversals are not allowed
- Void transactions routed to the UnionPay network are sent online.
  - If a response is not received for a CreditVoid request, resend the request
- Card on File is not available for transactions being routed to the UnionPay network
- Online PIN is required for EMV and non-EMV transactions:
  - For EMV cards, the PINBlock is sent within the EMVData element
  - For magstripe cards sending TrackData, the PINBlock is sent within the Block1 element

Please note that UnionPay **does not support:**

- Recurring Billing
- Card on File
- Offline Purchase / Voice authorization
- Card Verification
- Incremental Auth

Canada

Merchants located in Canada can choose between the Discover and UnionPay networks. This routing options is a merchant-level configuration, and all UnionPay cards will route the designated network for authorization. The configuration in Portico must match the configuration for the Host.

Within Portico, the default is to process via the Discover network, unless Union Pay direct is specified within the Portico DeviceId configuration.

Card on File is not available for transactions being routed to the UnionPay network

> **Note:** To enable Union Pay Direct routing, special configuration is required. Please contact your representative for further information.

United Kingdom

Merchants located in the UK may choose routing through the UnionPay network or a partner authorization network on a per-transaction basis indicated within the request Header. Available routing options vary for different BIN ranges, and not all BINs support alternate routing. Portico does not determine routing or validate BINs, it is the responsibility of the POS to maintain accurate BIN records to determine whether the card's BIN allows authorization through a partner network. If an invalid path is chosen Portico will pass the request to the authorization network and allow the issuer to decline the authorization.

> **Note:** To enable Union Pay Direct routing, special configuration is required. Please contact your representative for further information.

6.31 Voice Authorization

A voice authorization takes place when the response message requests the merchant to call the processing center or if the Internet or merchant application is unable to process credit card transactions. The processing center provides a voice authorization code if the transaction is approved. Once the voice authorization code is obtained, the merchant must submit either a CreditOfflineAuth or CreditOfflineSale transaction that includes the authorization code.

7 Appendices

The following sections contain general information about codes, indicators, and other helpful information.

7.1 Register the Client Library

The following steps register the client library:

Download and Install the .NET Runtime

1. Go to http://www.microsoft.com/downloads/.
2. Search for "Microsoft .NET Framework 4.5.2 Developer Pack" and click the link for the download.
3. Click **Download**.

Unregister the Old Version

If this is the first time you have installed the client library, skip the following steps.

1. Open a command prompt and navigate to the old client library directory.
2. Unregister the old assembly using the following command:

```
> regasm /unregister Hps.Exchange.PosGateway.Client.dll /tlb
```

The assembly registration tool is invoked by the regasm command. The tool is provided with the Microsoft .NET runtime. If this directory is not in your path, you need to fully qualify the command.

Register the Client Library

1. Open a command prompt and navigate to the client library directory.
2. Register the assembly using the following command:

```
> regasm /codebase Hps.Exchange.PosGateway.Client.dll /tlb
```

7.2 Gateway Response Codes

When checking response codes, be sure to check both the Gateway Response Codes and Issuer Response Codes. See Validating Response Codes for more information.

System Response Codes

Response Code	Description
-21	Unauthorized
-2	Authentication error—Verify and correct credentials.
-1	Portico error—Developers are notified.
0	Success
+1	Gateway system error
+2	Duplicate transactions
+3	Invalid original transaction
+4	Transaction already associated with batch
+5	No current batch
+6	Invalid return amount—This can occur if a credit return request is against a specific original transaction, and the return amount is greater than the original transaction settle amount, or the return amount is zero.
+7	Invalid report parameters
+8	Bad track data
+9	No transaction associated with batch
+10	Empty report
+11	Original transaction not CPC
+12	Invalid CPC data
+13	Invalid edit data
+14	Invalid card number
+15	Batch close in progress
+16	Invalid Ship Date—Transaction rejected because the ship date and month are invalid. Try again in a few seconds and resubmit.
+17	Invalid encryption version
+18	E3 MSR failure—The message returned with this code is the parsed error message from the MSR data stream.

Response Code	Description
+19	Invalid Reversal Amount—This can occur if a reversal request includes a new settlement amount that is not less than the current total authorization amount. The total authorization amount is the original authorization plus any incremental authorization minus any previous reversal amounts.
+20	Database operation time out—This may occur when Portico is trying to communicate to the database for large amounts of data. If this is due to a search, it can be corrected by adding more specific criteria.
+21	Archive database is currently unavailable—Try the transaction again later.
+22	Archive database is currently unavailable, but an attempt was made to retrieve the data from the real-time database. If there was data available from the real-time database that met the request criteria, then it was returned, however, it is not guaranteed to be complete. The request may need to be tried again later.
+23	An error was returned from the tokenization service when looking up a supplied token. This typically means that the provided token is bad, but it can also be returned when the data on the tokenization service has expired, been removed, or is no longer valid.
+24	This typically means that a token was supplied in the request but tokenization is not yet supported for the requested service type (see the section on tokenization for a list of supported services). This can also occur when tokenization is disabled for the entire system.
+25	This error is returned if the merchant provides a token (TokenData.TokenValue) and requests a token (TokenRequest) in CardData. In this case, the transaction is rejected because a token cannot be presented and requested in the same request.
+26	This error is returned if there is an error setting the token attribute. When possible the tokenization service error/return code is returned in the message text.
+27	This error is returned if the requested token was not found. This error can occur during TokenToPan (Lookup) or ManageTokens->Set (Update) requests.
+30	This can occur when Portico does not receive a response from the back end systems and Portico is not sure if the transaction was successful or not. In this case, the POS is responsible for deciding whether or not to issue a reversal for this transaction. This is used in cases where the transaction is an authorizing transaction, e.g., CreditAuth, CreditSale, DebitSale. If the transaction is non-authorizing, e.g., CreditAccountVerify, CreditReversal, and Portico receives no response, then Portico sends back a System Error (+1) to the POS.
+31	This occurs when Portico attempts a reversal for the POS, but the reversal fails. In this case, the POS is responsible for issuing the reversal.
+32	Missing KTB error—This can occur when a POS is attempting to send encrypted data, but the expected KTB value was corrupted or not received.
+33	Missing KSN error—This can occur when a POS is attempting to send encrypted data, but the expected KSN value was corrupted or not received.
+34	Invalid data received—This error is returned from a CreditAuth or CreditSale if both GatewayTxnId and a CardData subfield are received.

Response Code	Description
+35	Device setting error—This error is returned from SendReceipt if the "AllowEmail" setting is not set to true for the DeviceId being used.
+36	Invalid Original Txn for Repeat—This error is returned from a CreditAuth or CreditSale if the original transaction referenced by GatewayTxnId cannot be found. This is typically because the original does not meet the criteria for the sale or authorization by GatewayTxnID. This error can also be returned if the original transaction is found, but the card number has been written over with nulls after 30 days.
+37	Missing element—This error is returned if a required (or conditional) element is missing from the transaction.
+38	Invalid auth amount—This error is returned from a CreditAuth or CreditSale by GatewayTxnId when the requested amount is over the threshold set for the transaction type, which is some percentage of the original amount (default = 100%).
+39	Transaction rejected because EMV TLV data was invalid.
+40	Transaction rejected because the referenced transaction has invalid EMV TLV data.
+41	Transaction declined because possible fraud was detected.
+42	Communication Error—System Level Communication Error was detected.
+43	Currency error—This error is returned when there is a discrepancy between the currency format of the Amount and the selected currency at the Site or Device
+44	Transaction must be in a closed batch
+45	Debit Return is not allowed
+47	Invalid amount—Transaction rejected. Amount exceeds the maximum length for the Authorization Platform.
+50	Processor System error
+51	Processor Configuration error
+52	Service Not Allowed
+53	Communication Error - Host Unavailable - This error is returned when Portico experiences excessive timeouts for a specific Authorization Platform.
+54	DWS Amount Error - Transaction rejected because the DWS token amount and Transaction amount do not match.
+55	Transaction Failed - Transaction failed after host response.
+95	MUST CLOSE BATCH - Maximum batch size has been reached. Please close batch and retry transaction.

7.3 Tokenization-Specific Response Codes

Error Code	Description
0	Tokenization was successful. The GatewayRspCode can still be used to determine if the transaction was processed successfully or not regardless of the outcome of the tokenization process. If the transaction is successfully processed but tokenization fails, the transaction response is still provided but no token is returned.
1	An error was returned from the tokenization service when generating a new token. This typically means that the service is down or there are internal connectivity issues.
2	This typically means that a token was requested but tokenization is not yet supported for the requested service type. See Tokenization for a list of supported services. This can also occur when tokenization is disabled for the entire system.
3	An error occurred while trying to encrypt the data prior to tokenization.
4	Tokenization requires that the associated data be encrypted internally. This response indicates that the internal encryption processing is disabled, so tokenization is not available.

7.4 Issuer Response Codes

97

When checking response codes, be sure to check both the Gateway Response Codes and Issuer Response Codes. See Validating Response Codes for more information.

Response Code	Description
00	APPROVAL
02	CALL—No original no match. Often returned when the cardholder has exceeded daily credit limits/# of uses. Usually the Issuer wants to make sure the cardholder is still in possession of the card.
03	TERM ID ERROR—Terminal ID error.
04	HOLD-CALL—Retain card. Usually returned when the Issuer would like the merchant to take possession of the card due to potential fraud. Can also be returned if the transaction declines due to an AVS/CVV setting. The response text in this case is "DO NOT HONOR DUE TO AVS/CVV SETTINGS".
05	DECLINE—Do not honor. Normally occurs when a cardholder has exceeded their allowable credit line. Can also be returned as: STOP PAY ORDERED - Stop all future recurring payments. (Mastercard only) Can also be returned as: RETRY WITH EMV 3DS - Authentication may improve the likelihood of the transaction being approved. (Mastercard only)
06	ERROR—Merchant closed, no match.
07	HOLD—CALL
09	NO ORIGINAL—Incremental or Void doesn't reference an original transaction.
10	PARTIAL APPROVAL
12	INVALID TRANS
13	AMOUNT ERROR. Occurs when the POS submits an amount field equal to $0.00. Re-enter transaction.
14	CARD NO. ERROR—Card number error. Issuer cannot find the account. Re-enter transaction.
15	NO SUCH ISSUER. Returned when the first 6 digits of the card number are not recognized by the Issuer. Re-enter transaction.
19	RE-ENTER—Re-enter transaction.
22	Invalid SIP Option
23	Invalid minimum amount
25	INVALID ICC DATA—Required data for processing chip transactions was missing from the authorization request or data could not be parsed.
41	HOLD-CALL—Lost card.
43	HOLD-CALL—Stolen card.

44	HOLD-CALL—Pick up card.
51	DECLINE—Insufficient funds.
52	NO CHECK ACCOUNT. Occurs when the debit/check card being attempted is not linked to a Checking Account.
53	NO SAVE ACCOUNT. Occurs when the debit/check card being used is not tied to a Savings Account.
54	EXPIRED CARD—Card is expired. This response can also be returned in a Card Not Present environment if the cardholder tries to provide a valid expiration date, but the Issuer knows it has expired (indicates potential fraud).
55	WRONG PIN. Occurs in PIN-based Debit when the consumer enters the wrong 4-digit PIN.
56	INVALID CARD
57	SERV NOT ALLOWED—Service not allowed. Can be an incorrect MID or terminal number, or attempt to process an unsupported card.
58	SERV NOT ALLOWED—Service not allowed. Occurs when the POS attempts a transaction type that they are not set up for based on their MCC. (i.e., a merchant set up with a Direct Marketing MCC trying to perform a Debit transaction).
61	DECLINE. Occurs in PIN-based debit when the cardholder has exceeded their withdrawal limit when performing cash back.
62	DECLINE. Occurs on swiped transactions when the Service Code encoded on the mag stripe does not equal the one stored at the Issuer (potential fraudulent card).
63	SEC VIOLATION
65	DECLINE—CHIP READ REQ., INSERT CARD. Occurs on contactless transactions that need to be processed as contact. Can also be returned due to Activity Limit. The response text in this case is DECLINE—activity Limit. Occurs when the cardholder has exceeded the number of times the card can be used in a specific time period. (i.e., 10x in a 48 hr span).
75	PIN EXCEEDED. Occurs when the number of attempts to enter the PIN has been exceeded.
76	NO ACTION TAKEN. Occurs when the reversal data in the POS transaction does not match the Issuer data.
77	NO ACTION TAKEN—Duplicate reversal or duplicate transaction.
78	NO ACCOUNT—Account suspended, cancelled, or inactive.
80	DATE ERROR
82	CASHBACK NO APP
85	CARD OK
86	CANT VERIFY PIN
88	ARPC Cryptogram Failure
91	NO REPLY—Time out.
94	DUPLICATE TRANSACTION—Transaction entered is a duplicate on the Host.

96	SYSTEM ERROR
97	TRANSLATE ERROR—Decryption error: Contact Customer Service.
1A	ADDTNL AUTHN REQD- Additional Customer authentication is required
6P	VERIFICATION DATA FAIL—Verification Data Failed.
CA	AVS Referral
D1	DO NOT RETRY- Do not attempt to submit this transaction again. The issuer will not approve the transaction.
D2	RETRY LATER- The transaction cannot be completed at this time. Retry later.
D3	DECLINE NEW INFO
EB	CHECK DIGIT ERR
EC	CID FORMAT ERROR—Format error.
EL	EXCEEDS LIMIT - Exceeds maximum number of PIN attempts
N1	Currency not allowed
N5	MUST CLOSE BATCH—(GSAP). Terminal has not been balanced within time specified by Global Payments for this merchant. Send a batch close request to resume processing.
N7	CVV2 MISMATCH—Incorrect number of CVV2/CID digits sent.
N8	INVALID DATA- Format of the transaction is incorrect.
PD	PARAMETER DOWNLOAD—EMV PDL system response. Response text indicates EMV PDL status code.
PF	PAYMENT FACILITATOR. Response text as provided by a payment facilitator.
PR	PROMPT PIN - Prompt the customer to enter the PIN number (Union Pay only)
R0	STOP SPECIFIC—Stop a specific payment.
R1	REVOKE AUTH—Revoke authorization for further payments.
R3	CANCEL PAYMENT—Cancel all recurring payments for the card number in the request.

7.5 EMV PDL Status Codes

Status Code	Status Code Name	Message	Note
00	SUCCESS	A response has been sent out successfully.	
Request—Header error			

Status Code	Status Code Name	Message	Note
01	INVALID MESSAGE LENGTH	Message Length is invalid.	If Message Length is not binary code.
02	INVALID HEADER ID	Header ID [ID] is invalid. Example: Header ID NF is invalid.	If the Header ID is not HH or NT.
03	INVALID HEADER VERSION	Header Version [VERSION] is invalid.	If the Header Version is not 01.
04	INVALID CORRELATION ID	Invalid Correlation ID.	If the Correlation ID is not binary codes.
05	INVALID RESPONSE CODE	Response Code [CODE] is invalid.	If the Response Code is not numeric.
06	INVALID HOST	Host [HOST] is invalid.	If the Host is not E, N, or V.
07	INVALID MERCHANT OR COMPANY ID	Merchant/Company ID [ID] is invalid.	Based on the host selected, display this error if the ID is not the correct length and data type.
08	INVALID LOCATION OR UNIT ID	Location/Unit ID [ID] is invalid.	Based on the host selected, display this error if the ID is not the correct length and data type.
09	INVALID TERMINAL OR DEVICE ID	Terminal/Device ID [ID] is invalid.	Based on the host selected, display this error if the ID is not the correct length and data type.
10	INVALID TERMINAL IDENTIFIER LENGTH	The length of the terminal identifier field is invalid.	If the length of the Terminal Identifier field is not 30 bytes.
Request—Body error			
11	EMPTY MESSAGE BODY	The request has no message body.	If receives a request that contains only the header (unless this is a keep-alive request).
12	TERMINAL NOT FOUND	Terminal identifiers are not provided. -OR- The terminal record cannot be found.	For Exchange terminals, Location/Unit ID is not needed. But if it is provided, the system will log it, but won't use it when searching for the terminal record.
13	INVALID PARAMETER TYPE	Parameter Type is not provided.	If the Parameter Type is space-filled.
13	INVALID PARAMETER TYPE	Parameter Type [PARM TYPE] is invalid. **Example:** Parameter Type 10 is invalid.	If the provided Parameter Type is not 06 or 07.
14	INVALID TABLE-ID	Table-ID is not provided.	If the Table-ID is space-filled.
14	INVALID TABLE-ID	Table-ID [TABLE ID] is invalid. Example: Table-ID 90 is invalid.	If the provided Table-ID is not in 10, 30, 40, 50, 60.
15	INVALID CARD TYPE	Card Type is not provided.	If the Card Type is space-filled.

Status Code	Status Code Name	Message	Note
15	INVALID CARD TYPE	Card Type [CARD TYPE] cannot be found. **Example:** Card Type 99 cannot be found.	If the Card Type is not numeric or cannot be found. Card Type is host specific.
16	INVALID VERSION	The Table/Parameter received is invalid. Check the data type and length.	This error shows up when the Parameter/Table version is less than the required length.
17	VERSION NOT FOUND	Table Version is not provided.	If the Table Version is space-filled. **Important:** Space-filled value is a valid value for Parameter Version, which means the POS is requesting the latest version of parameter version. Because of the same reason, attention needs to be paid on report logging when receiving an empty Parameter Version; the system should log the latest parameter version number in the database.
17	VERSION NOT FOUND	Version [TABLE VERSION] cannot be found.	If the received Table Version cannot be found in the system. In phase I, the system is not matching Parameter Version. In other words, even if the received Parameter Version can't be found in the database, it will still be processed successfully.
18	INVALID BLOCK SEQUENCE	Block Sequence is not provided.	If the Block Sequence is space-filled.
18	INVALID BLOCK SEQUENCE	Block Sequence [SEQUENCE] does not exist.	If the requested Sequence ID does not exist or if it is not numeric.
18	INVALID BLOCK SEQUENCE	The Block Sequence must be 00 for Table-ID 10 and confirmation.	Because 00 is supposed to be used by Table-ID 10 or confirmation only, use this error code if: • received 00 when is requested for Table-ID 30-60, or • received other than '00' when requested for Table-ID 10 or confirmation.

Status Code	Status Code Name	Message	Note
Before sending response—Table error			
50	NO TAC CODE	AID [AID] of card type [CARD TYPE] does not have matching TAC codes for the requested terminal. **Example:** AID A0000000031010 of card type 02 does not have matching TAC codes for the requested terminal.	Occurs when a table has no matching TAC codes for a terminal. This happens when requesting Table-ID 40 and 50.
Other error			
97	CLIENT CONNECTION LOST	Lost the connection with the client. Detail: [ERROR]	Example: If disconnected with payment gateway socket close.
98	DATABASE CONNECTION LOST	Cannot connect to database. Detail: [ERROR]	If cannot connect to the database. (This error won't be logged in the database, though.)
99	SYSTEM ERROR	A system error has occurred. Detail: [ERROR]	Any errors that don't fall into the above categories.

7.6 Gift Card Response Codes

Response Code	Description
0	OK—Transaction successful.
1	System error—Transaction unsuccessful because of an internal system error. Retry transaction. If the error persists, contact Heartland support.
2	System unavailable—Gift card system is temporarily unavailable. Retry transaction.
3	Invalid card—Transaction unsuccessful because the card is not a valid gift card.
4	Deactivated card—Transaction unsuccessful because the gift card is deactivated.
5	Insufficient funds—GiftCardSale transaction unsuccessful because the gift card did not have a sufficient balance to complete the sale. This error code is not returned if split-tender processing is enabled.
6	Card already active—GiftCardActivate transaction unsuccessful because the gift card is already active.
7	Duplicate transaction—Transaction unsuccessful because a transaction with identical parameters was completed less than 3 minutes ago.
8	Inactive card—Transaction unsuccessful because the gift card is not active.
9	Invalid amount—Transaction unsuccessful because an invalid amount was specified.
10	Cannot void.
11	Unknown error.
12	Do not honor.
13	Partial approval.

7.7 Status Indicators

The tables below provide the descriptions for the Portico status of a transaction or a batch.

For Check/ACH transactions, CheckQuery may used to query the status of a Check/ACH transaction on the Colonnade host.

> Not yet supported for Paya/GETI/Sage.

Transaction Status Indicators

Indicator	Status	Description
A	Active	The transactions can be modified by additional processing (i.e., edit amount, edit tip, add to batch, void, reverse, settlement, etc.).
I	Inactive	The transaction cannot be acted on by any processing actions and will not be settled.
C	Cleared	The transaction was part of a batch that is now closed.
V	Voided	The transaction was voided.
X	Autovoided	The transaction was voided by Portico's automated process. > Credit transactions are auto-voided after 30 days when not associated with a batch.
R	Reversed	The associated transaction has been reversed and will not be settled.
T	Timed-Out	The transaction failed due to a time-out with a back-end processor.

Batch Status Indicators

Indicator	Status	Description
O	Open	The current batch for a DeviceId. There is only one open batch per DeviceId.
P	Pending	The batch is currently in the process of being closed.
V	Voided	The batch has been voided.
E	Error	The batch received an error during the close attempt.

7.8 HMS Gift Card Certification

The following sections include details about HMS certification.

7.8.1 Certification Host Response Matrix

The Heartland Portico Gateway provides a way to force responses based on user input, typically an amount or SVA. This allows a client developer to test various transaction scenarios by simply using well-chosen input values.

7.8.1.1 Amount Response Matrix

Responses to activate, load, redeem, and reward requests can be controlled by the amount parameter.

All whole dollar amounts (e.g., 100, 200, 1000, etc) return a status code of 200 and status name of Okay. All non-whole dollar amounts (any amount that does not end in "00") return the 400 error Response:

[[status.code=400], [status.description=Certification test error], [status.name=ApiError]]

The request amounts enumerated in the table below cause the corresponding error response to be returned:

These request amounts will return the corresponding response for all currencies, including Points.

Amount	Status Code	Status Name
101	503	ServiceUnavailable
201	403	ProfileError
301	400	InsufficientFunds
304	400	SystemError
305	400	InvalidPin
306	400	EditError
307	400	DuplicateTxn
308	400	InvalidCard
500	200	CannotVoid

7.8.2 Certification Host Stored Value Accounts

All account numbers in the following ranges:

Start of Range	End of Range
5022440000000000001	5022440000000000099

All aliases (phone numbers) in the following ranges:

Start of Range	End of Range
XXX5550100	XXX5550199

You may use whatever area code (NPA) you would like, but the exchange (NXX) must be 555 and the line must be in the range 0100-0199 or the host will reject the alias with an error.

8 Glossary

3

3-D Secure™
Three-Domain Secure™ (merchant, acquirer, issuer). A Visa-approved Authentication Method that is the global authentication standard for Electronic Commerce Transactions.

A

ABA Transit Number
American Bankers Association Transit Number. The ABA Transit Number, known as the routing transit number (RTN), is a 9-digit bank code used in the United States. It appears on the bottom of negotiable instruments, such as checks identifying the financial institution on which it was drawn.

ACH
Automated Clearing House. An electronic payment network most commonly associated with payroll direct deposit and recurring payments. The ACH can also be used to clear electronic checks and other demand deposit account (DDA) transactions.

ACI
Authorization Characteristics Indicator. A value determined by Visa based on the data included with the authorization request. It is returned with the electronic authorization response.

Acquirer
A company that enters into contractual relationships with merchants, therefore allowing the merchant to accept credit/debit cards. Heartland Payment Systems is an acquirer.

Acquiring Financial Institution
An acquiring financial institution contracts with a bank and merchants to enable credit card transaction processing. Also known as an Acquirer.

Acquiring Host
The processing system that communicates with the card acceptor or a communications network processor and is responsible for receiving the data relating to a transaction and obtaining an approval or denial for the transaction. The system maintains reconciliation totals for all financial transactions.

Activation
Terminal Hardware Device Transaction used to exchange an activation code for the authentication token; used for secure credential handling for terminal hardware.

Activation – Gift Card
Changing the state of a fixed denomination account from "inactive" to "active", enabling a stored value/prepaid card for use.

Activation and Initial Load – Gift Card
Changing the state of a stored value/prepaid account from "inactive" to "active", enabling the card for use, and requesting the loading of a variable amount to the account.

AES
Advanced Encryption Standard. It is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology.

AFD
Automated Fuel Dispenser. A pump at a service station or truck stop that is operated by the cardholder to

obtain credit for pumping fuel. The pump contains a card reader. Also called an ICR, CRIND, or CAT.

Age Verification
A security process used to verify a consumer's age. Age verification is typically used by liquor and tobacco outlets, bars and casinos.

Agents
Those who sell bankcard services to merchants on behalf of ISOs, acquirers and processors. Also known as merchant level salespeople (MLSs) and independent sales agents (ISAs), most agents are independent contractors. Others are paid employees of ISOs, acquirers and processors.

ANSI
American National Standards Institute. Governing institute that establishes guidelines for business practices.

APR
Annual Percentage Rate. The percentage rate charged for a credit card (or other loan) for a whole year. It is the finance charge, expressed as an annual rate.

ASP
Active Server Page. Part of Microsoft's .NET platform. ASPX is a text file format used to create Webform pages.

ASV

Approved Scanning Vendor. The PCI Security Standards Council maintains a structured process for security solution providers to become Approved Scanning Vendors (ASVs), as well as to be re-approved each year.

The five founding members of the Council recognize the ASVs certified by the PCI Security Standards Council as being qualified to validate adherence to the PCI DSS by performing vulnerability scans of Internet facing environments of merchants and service providers.

The major requirement of the process is a rigorous remote test conducted by each vendor on the PCI Security Standards Council's test infrastructure, which simulates the network of a typical security scan customer. The Council has set up the test infrastructure in such a way as to deliberately introduce vulnerabilities and misconfigurations for the vendor to identify and report as part of the compliance testing process.

Authorization
A process where a merchant issues a request to an authorization center to obtain an approval for a cardholder transaction for a specific amount. This process verifies that a credit or debit card has sufficient funds available to cover the amount of the transaction. This process also reserves the specified amount and ensures the card is authentic and not reported lost or stolen. This authorization request is usually submitted through a point-of-sale device. The merchant may also obtain authorizations by telephoning the authorization center.

Authorization Code
A code that a credit card issuing bank returns to the POS indicating an approval of the request transaction.

Authorization Request
A request sent to a financial institution to determine if a credit or debit card has sufficient funds to cover the amount of the transaction.

Authorization Response
A response to an authorization request indicating a financial institution's approval or disapproval of a transaction.

Auto-Substantiation
This transaction is applied to either a Credit Authorization or Credit Sale Transaction. Amount types included in this transaction are healthcare, prescription, vision/optical, clinic or other qualified medical, and dental amounts.

Auto-Voiding Transactions
Portico Gateway automatically voids all active credit transactions that have not been added to a batch after the Issuer time limits.

AVS
Address Verification Service. A system that verifies the personal address and billing information provided by a customer at the time of the transaction against the information the credit card Issuer has on file. This system enhances fraud protection.

B

B2B
Business-to-Business. A marketing term that refers to the commerce between business as opposed to business-to-consumer or business-to-government.

Back-End Vendor/Processor
A company that receives data, captures it from the front-end processor, and submits the data for clearing and settlement. The back-end vendor generates the merchant's monthly statement, causes the merchant to be paid for their transactions, causes the merchant to be charged their processing fees and causes the cardholder to be charged. Examples of back-end vendors are: Passport and Vital.

Balance Inquiry
Requesting the balance of an existing stored value/prepaid account to provide to the customer at the POS.

Bank Card
In general, a bank card refers to a plastic card issued by a bank and used to access funds from an account.

Bank Routing Number
Every bank is assigned a unique 9-digit number for identification purposes. This routing number appears as the first 9 digits across the bottom of a check. (See also Transit Routing Number)

Batch
A set of credit and/or debit transactions submitted together for settlement, clearing, and funding.

Batch Close
The process of sending transactions to the processor for clearing and settlement (the cardholders are charged and the merchant is paid).

BIN
Bank Identification Number. The primary account number found on credit cards and bank cards. It is a 6-digit number, maintained by the American Bankers Association that identifies the bank and type of card. The first number identifies the card type (i.e., American Express = 3, Visa = 4, Mastercard = 5, Discover = 6). Also referred to as IIN (Issuer Identification Number).

Buy Rate
The acquiring bank's fee. It is equal to interchange (which is paid to the issuing bank) plus the acquiring bank's markup. The wholesale price of a transaction to which processing and other fees are added to come up with the cost to a merchant. Buy rates have not been widely used since the multitude of interchange rates came into being. Many ISOs and acquirers now use pricing models that involve splits of

net revenue.

C

CAB Program Code
Card Acceptor Business Program Code (formerly MCC – Merchant Category Code) is a numerical representation of the type of business in which the card acceptor (merchant) engages. Mastercard assigns these codes.

CAPN
Card Acceptance Processing Network. A set of requirements mandated by American Express to ensure processing of AMEX transactions according to their security standards. CAPN enhances POS security, supports expanded amounts, and adds a transaction lifecycle identifier for all AMEX transactions.

Card Acceptor
The facility at which a purchase is made and a payment transaction is initiated. Also known as a merchant.

Card Issuing Bank
A financial institution that issues payment cards such as credit/debit cards.

Card Laundering
When a merchant processes sales through its merchant account on behalf of another merchant. Laundering violates the terms of merchant agreements. Also called draft laundering and factoring.

Card Not Present
Card transactions (Internet or MO/TO purchases, for example) for which the customer's card is not physically handled by the merchant. Interchange is set higher on these transactions because there is a greater likelihood of fraud.

Cardholder

A consumer doing business with a merchant using one or more of the following payments cards:

- Credit or bank card
- Debit card
- Private label card
- Existing prepaid or stored value card with a corresponding stored value/prepaid account.

CAT
Card Acceptor Terminal. Unattended terminals that accept bank cards for payment. These terminals are frequently installed at rail ticketing stations, gas stations, toll roads, parking garages, and other merchant locations.

CAVV
Cardholder Authentication Verification Value. A unique value transmitted by an issuer (or Visa on behalf of an issuer) in response to an authorization request message.

Cellular CDMA
Code Division Multiple Access. Digital cellular technology that converts audio signals into a stream of digital information (made up of 1s and 0s).

Cellular GPRS
General Packet Radio Service Packet-based wireless communication service.

Chargeback
A procedure where a cardholder or card issuer is disputing all or part of the amount of a credit or debit card transaction. A chargeback is therefore the act of taking back funds from a merchant for a disputed

or improper transaction.

Check Reader or Check Scanner
A counter-top device used to scan images of checks, according to legal specifications, for electronic clearing and settlement. Also known as check scanner.

CID
Card Identifier. A 3 or 4-digit code appearing on the front or back of Discover or American Express credit cards (Discover is 3 digits, American Express is 4 digits). CID is used for fraud prevention. For all other bankcards, see CVN.

CISP
Cardholder Information Security Program. A program established by Visa to ensure the security of cardholder information. CISP has been superseded by the PCI Data Security Standard.

Client
A company that has contracted to use the services provided by Heartland Payment Services.

Client Libraries
See Heartland POS Gateway Client Libraries.

Close Batch
The end-of-day or end-of-shift process where the merchant balances and submits their credit and debit card transactions for clearing and settlement. (See also Settlement)

CMDA - Verizon
Code Division Multiple Access. A communication channel access principle that employs spread-spectrum technology and a special coding scheme (where each transmitter is assigned a code).

CNP
Card Not Present. See Card Not Present.

CoF
Credential/Card on File. Represents cardholder payment information that the merchant stores with permission that will be used for future purchases.

Commercial Cards
Credit cards issued to businesses for travel, entertainment and other business expenses.

Conditional
Conditional fields are required in the message under certain conditions. These conditions are indicated in the description or in an associated note.

Consumer
See Cardholder.

Corporate Cards
See Commercial Cards.

Counter-Top POS
A category of POS devices that typically only fit on a counter for use.

CPS
Custom Payment Services. Visa's regulations for the information that must be submitted with each transaction. Transactions must meet CPS criteria in order to qualify for lowest transaction processing fees available. This is similar to Mastercard's Merit system.

Credit Cards
Standard-size plastic token, with a magnetic stripe that holds a machine readable code. Credit cards are a convenient substitute for cash or check, and an essential component of electronic commerce and internet

commerce. Credit cardholders (who may pay annual service charges) draw on a credit limit approved by the card-issuer such as a bank, store, or service provider (an airline, for example). Cardholders normally must pay for credit card purchases within 30 days of purchase to avoid interest and/or penalties. Cards can be issued by banks and non-banks and are associated with such brand names as AMEX, Discover Financial Services, Mastercard, JCB International Co. Ltd. and Visa.

CSC
Card Security Code. The security code on a credit card is the brief number that is printed on the card that helps verify its legitimacy. Depending on the card, the security code can be a 3-digit or 4-digit number, printed on either on the back of the card or the front, and goes by several names. The most common is CVV, which stands for "card verification value" code. Other card issuers call their security codes CVV2 (Visa), CVC2 (Mastercard) or CID (American Express).

CUP
China UnionPay. The only domestic bank card organization in the People's Republic of China.

Customer
See Cardholder.

CUT
Coordinated Universal Time. The time scale used as the basis of a coordinated dissemination of standard frequencies and time signals. Formerly known as Greenwich Mean Time (GMT).

CVC2
See CVV2.

CVN

Card Verification Number. This is a 3- or 4-digit number that appears on either the front or back of a credit card. It is not included in the magnetic stripe data. It is provided as a fraud deterrent to ensure the card is physically present when a POS transaction is initiated. These codes are only required at authorization time. The following terms are used by various card issuers:

- CVV2 and CVC2 (3 digits) used by Visa and Mastercard account numbers.
- CID (3 digits) used by Discover account numbers.
- CID (4 digits) used by American Express account numbers.

CVV
Card Verification Value. An authentication procedure established by credit card companies to reduce fraud for internet transactions. It consists of requiring a cardholder to enter the CVV number in at transaction time to verify that the card is on hand. The CVV code is a security feature for "card not present" transactions (e.g., Internet transactions), and now appears on most (but not all) major credit and debit cards. This new feature is a 3- or 4-digit code which provides a cryptographic check of the information embossed on the card. The CVV code is not part of the card number itself.

CVV2
Card Verification Value. A 3-digit code appearing on the front or back of Visa or Mastercard. CVV2 is used for fraud prevention. For all other bankcards see CVN.

D

DBA
Doing Business As

DCC
Dynamic Currency Conversion - Allows a cardholder to make a purchase in a foreign country in the

currency of their home country.

DDA
Demand Deposit Account. A merchant's checking account that is credited or debited with their deposits, fees and adjustments (also referred to as Direct Deposit Account).

Debit Card
Issued by financial institutions and tied to cardholders' DDAs. Debit card funds are withdrawn directly from a cardholder's checking account. Debit cards come in online/offline and offline-only versions. Online in this context means able to interface with the card brand networks for authorization at the POS. Debit cards can be co-branded with Discover, Mastercard or Visa. Online debit requires customers to enter PINs; offline debit card payments are authorized with cardholder signatures.

DES
Data Encrypted Standard. A standard method for encrypting and decrypting data which was developed by the U.S. National Institute of Standards & Technology.

Dial-up
A temporary communication connection through a telephone line.

Discount
A fee charged to a merchant for card processing services. This fee is usually represented as a percentage of the merchant's daily or monthly credit/debit sales. (Also known as "discount fee" or "discount rate.")

Discount Fee
A fee charged to a merchant for card processing services. This fee is usually represented as a percentage of the merchant's daily or monthly credit/debit sales. (Also known as "discount" or "discount rate.")

Discount Rate
The percentage of card sales acquirers collect from merchants for transaction authorization and settlement.

Downgrade
A transaction is downgraded because it does not qualify for the best interchange rate possible, therefore the transaction costs more to process. Examples of why a transaction downgrades are: a) credit card is not swiped; b) merchant does not close their batch within 24 hours; c) the credit card used is a business, corporate or foreign credit card; d) the credit card was voice authorized.

Download
The passing of programming information and parameters from a processor to a point-of-sale device such as a terminal. This passing or transfer of information is typically accomplished by the point-of-sale device "dialing out" and connecting to the processor's remote computer.

DPAN
Device Primary Account Number or Digital Primary Account Number that represents a cardholder PAN. This is a network token which can be used to process transactions via from a specific device, such as the cardholder's mobile phone.

Draft Laundering
See Card Laundering.

DSL
Digital Subscriber Line. DSL is a family of technologies that provides digital data transmission over the wires of a local telephone network.

DSOP
Data Security Operations Policy. A standard developed by American Express to protect cardholder information. PCI is now used as a standard.

DSS
Data Security Standard. See PCI-DSS.

DTMF
Dial tone multi-frequency. Used for telephone signaling over the line in the voice-frequency band to the call switching center.

DUKPT
Derived Unique Key Per Transaction. Reference standard X9.24, Retail Key Management for this definition. It is a key management technique in which for every transaction a unique key is used, which is derived from a fixed key. If a derived key is compromised, future and past transaction data are still protected since the next or prior keys cannot be easily determined.

E

E3
Heartland End-to-End Encryption. New technology offered by Heartland to allow encryption of card data from initial swipe or input at the POS through arrival at the Issuer. This system not only removes intrusion threats but it also greatly reduces the scope for PCI audits on the associated merchant POS software.

EBT
Electronic Benefits Transfer. EBT is an electronic system in the United States that allows state governments to provide financial and material benefits to authorized recipients through a plastic debit card. Common benefits provided are typically in two different categories: Food Stamp and Cash Benefits.

ECA
Electronic Check Acceptance. Electronic process of depositing a check into a merchant account. A check is processed through an electronic system that captures bank account information and the amount of the check. The 'paper' check is handed back to the customer, voided or marked so that it cannot be used again. The merchant electronically sends information from the check (but not the check itself) to a bank or other financial institution, and the funds are transferred into the merchant's account.

EDC
Electronic Data Capture. The process of electronically authorizing, capturing and settling a credit card transaction.

EDI
Electronic Data Interchange. The structured transmission of data between organizations electronically. It is used to transfer electronic documents or business data from one computer system to another computer system.

EEPROM
Electronically-Erasable Programmable Read-Only Memory. EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge. Like other types of PROM, EEPROM retains its contents even when the power is turned off. EEPROM is similar to flash memory. The principal difference is that EEPROM requires data to be written or erased 1 byte at a time whereas flash memory allows data to be written or erased in blocks.

EFT
Electronic Funds Transfer. A way of performing financial transactions electronically. The Pulse and Star networks are examples of EFT systems.

EIFR
Electronic Interchange Reimbursement Fee. The fee that a merchant's bank or acquiring bank pays the customer's bank or the issuing bank after a merchant accepts the use of a card for a particular

transaction. The issuing bank, in a payment transaction, deducts the interchange fee in which it pays the acquiring bank that handles the transaction on behalf of the merchant or business owner. In turn, the merchant is paid by the acquiring bank the amount for the purchase minus the interchange fee. Some smaller fees may also apply, which are commonly referred to as the discount rate, the passthru or the add-on rate.

EIPP
Electronic Bill and Invoice Presentment and Payment. This is a business-to-business system for billing, invoice presentment, and payment.

EMV
Europay, Mastercard and Visa. EMV is a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

EMVCo
Europay International, Mastercard International and Visa International. EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including POS terminals and ATMs. EMVCo establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, Mastercard and Visa.

Encryption
A method of protecting data by "scrambling" data. Encryption transforms readable information using an algorithm (called a cipher) and makes it unintelligible to anyone except those who possess a key that converts the information back into readable form.

End-to-End Encryption
See E3 definition.

EPPS
Encrypting PIN Pads. EPPs form a component of unattended PIN Entry Devices (PEDs). Typically, EPPs are used to enter a cardholder's PIN in a secure manner. EPPs are used in conjunction with ATMs, automated fuel dispensers, kiosks, and vending machines.

EPROM
Erasable Programmable Read-Only Memory. A type of memory chip that retains its data when its power supply is switched off.

ERC
Electronic Receipt Capture. A paperless system that securely stores and retrieves electronic card receipts on demand. This reduces bank chargeback losses and the costs associated with merchants' storage and manual retrieval of paper receipts.

F

Factoring
See Electronic Funds Transfer.

File Extension
Part of a filename that indicates the file type.

Financial Transaction
A message that either notifies the host of the completion of a previously authorized payment transaction or that requests the approval and completion of the payment transaction by the host causing the reconciliation totals to be increased.

Floor Limit
The payment amount above which credit and debit card transactions must be authorized. This amount is specified in each merchant's processing agreement.

Force/Offline Transaction (Prior Authorization)
The after-the-fact entry of a sale transaction. The merchant obtains an approval code for the transaction by telephoning the authorization center. The transaction must now be entered into the terminal by "forcing it" or "offline entry." When pressing the "force" or "offline" key on the terminal, the terminal does NOT dial out to the authorization center, as the merchant has already obtained an authorization by telephone. The merchant simply swipes the credit card or manually enters the credit card number and expiration date, amount of the sale and the authorization code. The terminal simply "captures and stores" the transaction in the merchant's batch, due to already having obtained a valid authorization code.

Fraud Monitoring
An operational process, usually done in the risk management area that involves setting alert parameters for review at the time each transaction is presented to the system. Examples of these parameters are: excessive chargebacks, excessive credits/refunds, duplicate transaction amounts, excessive sales, higher than expected average sale amounts.

Front-End Vendor/Processor
A company that provides communication and data processing to authorize card transactions and transfer the data between the merchant's point-of-sale equipment to the back-end clearing/back-end settlement processor. Examples of front-end vendors are: Heartland Exchange, VISANet, MAPP, BuyPass, NDC, MDI, Paymentech, Envoy, and FDR.

FSA
Flexible Spending Accounts. A tax-advantaged financial account that can be set up through an employer in the United States. An FSA allows an employee to set aside a portion of his or her earnings to pay for qualified expenses as established in the cafeteria plan, most commonly for medical expenses or purchases.

FTIN
Federal Taxpayer Identification Number An identification number assigned to taxpayers by the IRS.

FTP
File Transfer Protocol. Standard network protocol used to transfer files from one host to another over a TCP-based network such as the Internet.

G

Gift Card
A card that can be used for purchases as well as for storing value on the card.

GPRS - Cingular
General Packet Radio Service. Charges by the data and not connection time.

Gratuity
This is an adjustment to a transaction for a tip.

GSA
General Services Administration. Visa Purchasing Card that is issued to federal government agencies by an Issuer contracted with the General Services Administration.

GSM
Global System for Mobile communications. Standard for mobile phones.

H

HBMI
Defined by the GSAP-NA and GSAP-AP authorization platforms as Host Based Merchant Initiated batch close. Portico acts as the merchant in managing the batch details. The merchant may send a BatchClose request to Portico, or be set up for Auto-Close.

HBTI
Defined by the GSAP-NA and GSAP-AP authorization platforms as Host Based Time Initiated batch close. The host manages the batch details. Requires configuration in Portico.

Help Desk Center
Organization or department that is tasked with supporting the clerks in the various client locations when a problem is encountered with the POS system or its operation. The type of support available depends on the operating environment and service agreements.

HIM
Heartland Information Marquee. Found on the merchant serving page (merchant viewer).

HMS
Heartland Marketing Solutions. An HPS Specialty Team that services HMS merchants. Paperwork or questions regarding HMS should be directed to 1-866-402-8056 or to HeartlandmarketingSolutions@e-hps.com.

Hold Back
The money set aside from a merchant's credit card receipts to cover potential chargebacks or other disputes. Typically, the amount is returned after a specified period.

HOST
Any networked computer that provides services to other computers, systems or users.

Host Batch Close
A system where the merchant's transactions are stored at the "host" and not in the actual terminal or point-of sale device. The host computer captures and retains all the transactions. The host automatically closes all batches at a predetermined time if the merchant does not initiate a "close batch" function.

HRA
Health Reimbursement Arrangement. HRAs are Internal Revenue Service sanctioned programs that allow an employer to set aside funds to reimburse medical expenses paid by participating employees. Using an HRA yields tax advantages to offset health care costs for both employees as well as an employer.

I

ICR
Island Card Reader. An ICR is an unattended device that accepts payment cards, typically used with fuel pumps at gasoline stations. Also known as AFD, CRINDS, DCR, and pay-at-the-pump.

IEEE
Institute of Electrical and Electronics Engineers. The IEEE is a non-profit professional association dedicated to advancing technological innovation related to electricity.

IIAS
Inventory Information Approval System (healthcare). This system identifies the qualified healthcare products being purchased by the cardholder at the point of sale. This system must be used for merchants utilizing auto-substantiation.

IIN
Issuer Identification Number. See BIN.

Incremental Authorization
Unique authorization for the Lodging Industry. Occurs when an authorization is adjusted above a threshold amount.

Integrated POS
A category of POS devices that typically combine several Point of Service locations in such industries as Retail, Parking, and Petroleum.

Interchange
The process by which all parties involved in a credit card transaction (processors, acquirers, and issuers) manages the processing, clearing and settlement of credit card transactions.

Interchange Fees
Fees paid by the acquirer (Heartland) to the card issuing bank to compensate for transaction-related costs.

IP Address
Internet Protocol Address. A unique number assigned to any computer or printer that uses internet protocol.

ISA
Independent Sales Agent. See Agent.

ISC
Information Security and Compliance. Program used by Discover to implement and maintain efficient data security requirements and procedures. PCI is now used as a standard.

ISDN
Integrated Services Digital Network. A set of standards for digital transmission over ordinary telephone copper wire as well as over other media. ISDN requires adapters at both ends of the transmission so an access provider also needs an ISDN adapter.

ISO

International Organization for Standardization. Founded in 1946, ISO is an international organization composed of national standards bodies from over 75 countries. ANSI is a member of ISO. ISO has defined a number of important computer standards.

Also an organization registered with Visa and sponsored by an acquiring bank to sell Visa card acceptance services. Can refer to an organization that works with and does business under the name of such a registered ISO. ISOs may also service merchant accounts once they are registered, dependent upon the contract with the acquirer. Mastercard uses the term "member service provider" to describe ISOs. However, it is common within the payments industry to use the term "ISO" when referring to independent sales organizations registered with either or both card brands.

Issuer
A company that enters into contractual relationships with consumers and/or businesses through the issuance of plastic credit/debit cards. An issuer is also known as a "card issuing center." Examples of issuers are Bank of America and Citi-Bank.

Issuing Bank
A federally insured financial institution that issues credit and debit cards. This is the cardholder's financial institution.

Issuing Host

The processing system that acts under the authority of the card issuer to receive a transaction and to approve funds to be given to the card acceptor or to guarantee checks.

ITU
International Telecommunication Union. An international organization within which governments and the private sector coordinate global telecom networks and services.

J

JCB
Japan Credit Bureau. An independent card company originally established in Japan. JCB International Credit Card Company, Ltd. was established in Los Angeles in 1988 to issue credit cards as well.

K

Key Data
Data related to a security key. Reference standard X9.24, Retail Key Management.

KSN
Key Serial Number. Used in PIN encryption/decryption.

KTB
Key Transmission Block. Also known as the Encryption Transmission Block.

L

LLVAR
L is for length (LLL = 3 bytes). The field is parsed as 3 bytes of length and remaining of bytes as text content.

Load Amount
The amount of value that is added to the account. See Activation and Reload.

Load Value
To deposit funds into a cash account.

LRC
Longitudinal Redundancy Character. The LRC is used as an error checking method by both host and terminal to validate that the data was received without error.

LUHN Formula
The LUHN formula, also known as the MOD-10 Checksum, is used to generate and/or validate and verify the accuracy of account numbers.

M

Maestro
Maestro is a multi-national debit card service owned by Mastercard.

Magnetic Stripe
A strip of magnetic material on the back of credit cards which contains data identifying the cardholder, such as account number and cardholder name.

Manual Entry (Key Entered)
Card information is entered manually, or key-entered into a terminal, usually because the magnetic stripe

could not be read or the card is not present at the time of sale (i.e., a mail/phone order merchant).

MCC
Merchant Category Code. Usually a 4-digit number that identifies the type of business in which a merchant is engaged by the type of goods or services it provides. Visa and Mastercard have specific numbers for each type of merchant business.

Member Service Provider
See ISO.

Merchant
Business that is a Heartland customer that processes transactions.

Merchant Bank
A banking or financial institution that provides merchant services.

Merchant Discount Fee
A fee charged to a merchant for card processing services. This fee is usually represented in a percent format (example 2.25%). This merchant discount fee is used to determine part of a merchant's monthly processing charge.

Merchant Service Fee
A fee assessed to a merchant for Heartland's value-add services such as the Merchant Center, 24/7 customer support and local servicing by Heartland Payment Systems Relationship Managers.

Message
A set of data elements used to exchange information between a POS system and the Heartland Payment Systems.

Message Authentication Code
A block of encrypted data to be sent from the POS on every contact Interac sale and return request. Required for Canadian merchants processing debit reversals.

MICR
Magnetic Ink Character Recognition. Character-recognition technology that uses a countertop reader device used to scan magnetic ink character recognition lines. A MICR line is a sequence of digits at the bottom of a check that provides details about the bank and account on which the check is drawn, and supports authorization and clearing routines.

MID
Merchant Identification Number. A number assigned by an acquirer to identify each merchant for the purpose of reporting, processing and billing. All Heartland Payment Systems merchant numbers begin with a 65. All Heartland Payment Systems merchant numbers are 15 digits in length.

MIME
Multipurpose Internet Mail Extensions. An Internet standard that extends the format of email to support: Text in character sets other than , non-text attachments, Message bodies with multiple parts, and Header information in non- character sets.

MOD-10 Checksum
Modulus 10 Checksum. The "modulus 10" or "mod 10" algorithm, also known as the Luhn formula, is a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers.

MOTO/eCommerce
Mail Order/Telephone Order (MOTO). Typically, credit transactions handled as "card not present." These transactions generally involve purchases made through mail order or telesales companies. In this type of transaction, the merchant typically has a card terminal and manually keys in required card information for

transmission to the appropriate authorization network. Interchange rates for these transactions are among the highest.

MPLS
Multiprotocol Label Switching. A mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. It can encapsulate packets of various network protocols. MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. Packet-forwarding decisions are made solely on the contents of the MPLS label, without the need to examine the packet itself. This allows creation of end-to-end circuits across any type of transport medium, using any protocol.

MSP
Merchant Services Provider (Heartland). Handles the setup with the Front-End and Back-End Processors.

MSR
Magnetic Strip Reader. The device that a payment card is swiped through as the Track Data is read.

N

NACHA
National Automated Clearing House Association. It manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data in the United States.

NACS
National Association of Convenience Stores. The association for convenience and fuel retailing.

NDA
Non-Disclosure Agreement. A confidentiality agreement signed by a customer and delivered to Heartland Payment Systems. Completion of NDA is required before receiving Heartland SDK, documentation and specifications.

O

Optional
Optional fields are never required. Optional fields in the response are only present when they were present in or generated due to the associated request.

OTB
Open to Buy. The amount of credit left on an account. For example, before a purchase, a customer has $600.00 OTB. The customer purchases $100.00 worth of products. After the purchase, the amount of OTB for that account is $500.00.

OTC
Over-the-Counter. Used in healthcare industry transaction descriptions.

P

PAD
PIN Acceptance Devices. Numeric key pad a consumer uses to enter a Personal Identification Number (PIN) when paying with a debit card.

PA-DSS
Payment Application Data Security Standard. Standards established by Payment Card Industry Security Standards Council to ensure compliance with mandates set by Bank Card Companies.

PAN
Primary Account Number. Also known as the card number. Number code embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

PAPB
Payment Application Best Practices. PCI SSC took over management of PABP and renamed to PA-DSS. See PA-DSS.

Partial Authorization
A process to complete a transaction if the full amount requested is not approved but a partial portion of the requested amount is approved. A merchant must be set up for this capability. If a merchant is set up for this capability, the Portico Gateway Issuer response will contain the full amount requested or a lesser or partial amount authorized.

Payment Facilitator
A third-party merchant services provider with their own sub-merchant portfolio, which commonly includes underwriting, transaction monitoring, funding, and chargeback control.

A Payment Facilitator may aggregate multiple sub-merchants under a single MID.

PayPlan
The Portico PayPlan application allows a merchant to set up and manage recurring payments. It also provides other important and useful functionality, including: customer information management, secure payment information storage, one-time payment from cards or ACH on file, automated email notifications to merchants and customers, predefined and customizable reports, and the ability to load existing customer and payment information into the Portico PayPlan database.

PCI
Payment Card Industry. The payment card industry (PCI) denotes the debit, credit, prepaid, and the POS cards and associated businesses. The term is sometimes more specifically used to refer to the Payment Card Industry Security Standards Council (PCI SSC), an independent council originally formed with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standards (PCI-DSS).

PCI CAP

Visa PCI Compliance Acceleration Program. Under the CAP plan, acquirers are required to validate Level 1 and 2 merchant compliance with PIN security. This means that Level 1 and Level 2 merchants must not use payment devices such as PIN pads, and encourages the use of unique encryption keys for every device.

For Level 3 and 4 merchants, acquirers must establish a thorough compliance program for those merchants. According to Visa, as of November 1, 2007, acquirers whose transactions qualify for lower interchange rates available in the Visa and Interlink tiers must ensure that the merchants generating the transactions are PCI compliant in order to receive this benefit.

PCI-DSS
Payment Card Industry Data Security Standard. The framework for developing a robust payment card data security process including prevention, detection, and appropriate reaction to security incidents.

PED
PIN Entry Devices. PCI PED requirements were established to protect against fraud by ensuring the security of devices that process financial data. Approval is granted for devices that have been evaluated by an approved laboratory and determined to be compliant with PCI Security Requirements.

Peripheral
Any device that attaches to a computer and is controlled by its processor.

PIN
Personal Identification Number. A PIN is used to help ensure that the cardholder is really the cardholder. It is typically a 4-digit number that is not found anywhere on the card or in the track data.

PIN Debit
A debit card transaction authorized by the cardholder using a personal identification number.

PIP
Plural Interface Processing. The process that routes (through an American Express terminal or software) Visa, Mastercard and Discover card transactions to a financial services provider and American Express transactions directly to American Express for both authorization and settlement.

PL
Private Label. Private Label products or services are typically those manufactured or provided by one company for offer under another company's brand. Private Label Payment Cards tend to be exclusive to one merchant or company and can include special features, such as a rewards program.

POS
Point of Sale or Point of Service. The hardware and software used to collect and transmit non-cash payments for goods and/or services. The device where retail sales occur and payment transactions are initiated.

POS Sequence Number
POS sequence number for Canadian Debit transactions.

POS System
Point of Sale System or Point of Service System. The system that processes the transaction messages at a point of service. The system may handle other non-transaction functions also.

Post-Authorization (Post-Auth)
An offline transaction, also called a force, in which a transaction is created and placed in the merchant's batch using an existing authorization (normally received from a voice authorization center). (See also Offline/Force Transaction).

POTS
Plain Old Telephone Service. A basic wireline telecommunication connection.

Prepaid Card
A card representing a proxy for a stored value/prepaid account where value resides that the consumer can use for the purchase of specific goods or services provided by a prepaid product's service provider.

Private Label Cards
Credit, debit or stored value cards that are used only at a specific merchant's store. Proprietary cards.

Processor
An acquirer (such as Heartland Payment Systems) or an acquirer's agent that provides authorization, clearing or settlement services for merchants.

PROM
Programmable Read-Only Memory. A form of digital memory where the setting of each bit is locked. Such PROMs are used to store programs permanently. The key difference from a strict ROM is that the programming is applied after the device is constructed.

Proprietary Cards
See Private Label Cards.

Proximity Entry
This transaction occurs when a card is read by a proximity reader to capture the card information stored

on the magnetic strip or chip.

PTS Program
POS Terminal Security Program. This is a security evaluation program for Internet Protocol-enabled POS devices to ensure the necessary level of protection for transaction and cardholder data at Merchants that use equipment that support the TCP/IP protocol suite. The security evaluation verifies that POS devices meet the relevant Mastercard requirements in terms of confidentiality, integrity and communicating parties' authentication. By addressing the interface of POS terminals to open networks using open protocols, this new security program complements existing security programs at Mastercard that already address merchants or POS, such as PCI POS PED (security of PIN provided by PIN Entry Devices) and SDP (based on the PCI Data Security Standard).

Purchase
This term represents a sale transaction of services or goods.

Q

QRG
Quick-Reference Guide. A document or chart, used as a guide, to give a merchant quick reference to terminal operation procedures, such as batch settlement, offline/force entries, refunds, etc.

QSA
Qualified Security Assessor. An individual who meets specific information security education requirements, has taken the appropriate training from the PCI Security Standards Council, and who performs PCI compliance assessments as they relate to the protection of credit card data.

QSR
Quick Service Restaurant. A specific type of restaurant characterized by fast-food cuisine and by mini-meal table service.

R

RDC
Remote Deposit Capture. A check deposit process whereby paper checks are converted into digital images for electronic clearing and settlement, through either electronic check or ACH systems.

Recharge
See Replenish.

Reconciliation
The process of confirming the accuracy of partial or final totals by comparing totals from different systems.

Reload
To load an amount of funds into a stored value/prepaid account.

Replenish
To deposit funds into either the cash or credit account.

Reports
Various transaction reporting functionality available from Heartland Portico Gateway. Transactions supported are: ReportActivity, ReportBatchDetail, ReportBatchHistory, ReportOpenAuths, ReportTxnDetail, and ReportBatchSummary

Request
A message directing or instructing the receiver to perform a specified action and respond with the results

of the action.

Required
Required fields are always required to be sent in the message.

Reserve
See Hold Back.

Response
A message that provides the results of an action requested by the sender.

Response Codes
Codes returned from Portico Gateway or the Issuer down to the POS. Codes verify that a particular transaction was accepted or reflect why it was declined.

Retrieval
A request for a legible copy of a sales slip and/or other documentation relating to a credit or debit card transaction. This is the process or stage before a disputed transaction becomes a chargeback.

Reversal
A message that cancels the specified financial transaction that was previously reported as complete, causing the reconciliation totals to be decreased.

Reversal Reason Code
Defines the reason for reversing a previously approved transaction. Required for Canadian merchants processing debit reversals. See enumerations for specific values supported.

RFID
Radio Frequency Identification or Radio Frequency Input Device. Radio-frequency identification (RFID) is the use of an RFID tag applied to or incorporated into a product for the purpose of identification using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader.

RTN
Routing Transit Number. A routing transit number is a 9-digit bank code, used in the United States, which appears on the bottom of negotiable instruments, such as checks, identifying the financial institution on which it was drawn.

S

SAF
Store and Forward.

SDK
Software Development Kit. Compilation of software and documents for communicating to Heartland Portico Gateway. NDA must be completed by processing customer and on file with HPS before receipt of the SDK. Kit includes:
Heartland Developers Guide, XML Schema, HTTP XLM Schema Documentation, Source Code Examples, and the Heartland POS Gateway Client Library.

SDP
Site Data Protection. Mastercard's program to maintain data security requirements and compliance validation requirements to protect stored and transmitted payment account data. PCI is now used.

Service Fee
A fee assessed to a merchant for Heartland’s value-add services such as the Merchant Center, 24/7 customer support and local servicing by Heartland Payment Systems Relationship Managers.

Settlement

The process of transferring funds for sales and credits between acquirers and issuers, including the final debiting of a cardholder's account and the crediting of a merchant's account. (See also Close Batch).

SIC
Standard Industry Code (MIC). Usually a 4-digit number that identifies the type of business in which a merchant is engaged (also called Merchant Category Code (MCC)). Visa and Mastercard share specific numbers for each type of merchant business.

Signature Debit
A Visa Debit or Debit Mastercard transaction authorized by a cardholder's signature.

SNAP
Supplemental Nutrition Assistance Program. Offers nutrition assistance to millions of eligible, low-income individuals and families and provides economic benefits to communities. SNAP is the largest program in the U.S. domestic hunger safety net.

SOAP
Simple Object Access Protocol. A communication protocol for use between applications using XML messages through the Internet. It is platform and language independent, simple, extensible, and allows for communication around firewalls.

Sponsor Bank
See Acquirer.

SSL
Secure Sockets Layer. A protocol for transmitting data over the internet. SSL uses a cryptographic system to provide safety and privacy of data.

Super ISO
A large, independent sales organization that supports multiple downstream ISOs and MLSs. Some super ISOs are also processors.

SVA
Stored Value Account. Stored Value Accounts are card-based payment systems that assign a specific value to the card. Such cards are often referred to as gift cards or pre-paid cards. The card's value is stored on the card itself (on the magnetic stripe or in a computer chip) or in a network database. As the card is used for purchases, the total of each transaction amount is subtracted from the card's balance. As the balance approaches zero, some cards can be "reloaded" through various methods and others are designed to be discarded.

Swiped Entry
A transaction where a card is swiped (or passed) through a magnetic card reader or chip reader to capture card information stored on the magnetic strip or chip.

System
A processing system that provides transaction services to the card acceptor. The term includes acquiring host, authorizing host, and issuing host.

System/Device
A single hardware unit (device) or a group of units (system) that present messages to a host processing system.

T

TDES
Triple Data Encryption System. In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm. It is so named because it applies the Data Encryption Standard (DES) cipher

algorithm three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.

Terminal
See POS system.

Terminal Batch Close
A system where the merchant's transactions are stored within the terminal's memory. The terminal stores the transactions until the merchant closes the batch.

TID
Terminal Identification Number. A number assigned to the physical terminal device to identify its attributes to the processor. Each terminal within a merchant location has a separate TID.

TIN
Taxpayer Identification Number. An identification number assigned to taxpayers by the IRS. The TIN for individuals is their social security number. The TIN for businesses is the employer identification number.

TLS
Transport Layer Security. A cryptographic protocol designed to provide communication security over the Internet.

TLV
Type-length-value. Optional information that may be encoded in a data communication protocol.

TPPs
Third Party Processors. An independent processor that is contracted with by a Bank or Processor to conduct a part of transaction processing.

Trace Number
Number identifying original transaction.

Track Data
Track Data is the information encoded within the magnetic strip on the back of a credit card which is read by the electronic reader within the terminal or point-of-sale (POS) system.

Transaction
A set of messages to complete a processing action.

Transaction Fee
A fee charged to a merchant each time a transaction is processed, which dials into the authorization system, such as a sale or authorization only.

Transaction Header
A header is to be built for each transaction. This is used for authentication and validation.

Transit Routing Number
Every bank is assigned a unique 9-digit number for identification purposes. This routing number appears as the first 9 digits across the bottom of a check. (See also Bank Routing Number).

TRSM
Tamper Resistant Security Module. Key encryption.

TSYS
Total System Services. Vital. Back-end processor.

U

UAT
User Acceptance Test. Testing for business users to attempt to make a system fail, taking into account the type of organization it will function in. It is checking and verifying the system in the context of the business environment it will operate in.

UTC
Coordinated Universal Time. Also known as Greenwich Mean Time.

V

VAR
Value Added Reseller. A company that adds features or services to an existing product and resells it (usually to end-users) as an integrated product or complete turn-key solution.

Version
May refer to a document version or software version. Each time a new document or software revision is released, a revision version number is incremented.

VIP
VISANet Integrated Payment System. Visa's main transaction processing system.

VNP
VISANet Processors. An entity that is directly connected to Visa through a VisaNet Extended Access Server (VEAS).

Voice Authorization
The process of obtaining an authorization by telephone, typically as a back-up procedure. When an authorization cannot be obtained through an electronic credit card terminal or POS device.

Void
An attendant initiated transaction request to cancel a recently completed transaction.

VSAT
Very Small Aperture Terminal. The hardware and software located at a merchant’s location that allows POS communications by satellite.

W

webTOP
Terminal Option Page. Boarding merchants through web options.

WEP
Wired Equivalent Privacy. Standard for data security. Up to four keys are available using 64-bit or 128-bit encryption.

Wi-Fi
Wireless Fidelity. Another name for the 802.11b wireless networking standard developed by the IEEE.

9 Index