Portico
Developer Guide

Version 2.25

October 2016

Heartland
Payment Systems

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 or payment methods (credit, debit, check, EBT, gift, loyalty, prepaid, GSB, etc.) and various industries (retail, restaurant, mail order/telephone order, lodging, eCommerce, and healthcare). Portico also provides integrators and merchants with several options for securing transaction data.

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 2.25. 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:
  PDF 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 titles "Portico Schema" or "posgatewayservice Web Service" appear 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 **Revision History (Section 6.8)** 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.
  NOTE: 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; Discover, including JCB, CUP, Carte Blanche, Diner's Club, and PayPal; American Express; Debit or EBT. This requirement does not apply to Wright Express (WEX), FleetCor, Fleet One, 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 HPS 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 (SSL v3.0 or TLS v1.0/1.1/1.2) 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 (Section 2)** for additional information).

Heartland provides an SSL dial back-up (DBU) using the Point-to-Point Protocol (PPP). This DBU can be defined as a "dial internet connection". The POS makes a connection identical to an ISP dial provider. From this point, the POS can keep using the same URL as if they were on a high speed connection. The maximum possible connection speed for DBU is 56K baud and the format is 8N1.

Note: SSL v3.0 and TLS 1.0 will be phased out 06/30/16. TLS 1.1 is the new minimum requirement for certification.

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 (Section 6.2)** for additional information.

Portico Credentials

To identify a unique device and determine the permissions of the user on that device, Portico requires a valid LicenseID, SiteID, DeviceID, UserName, and Password. The license ID is used to chain multiple sites together for reporting and administration. The site ID is the location and is tied to a specific Merchant Identification Number (MID). The device ID indicates a unique device 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.

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.

Note: 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.

For transactions using either encryption type, 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. The supported encryption versions and required data items are defined below.

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	The EncryptionData element must be provided with the Version set to "02". In addition, the EncryptedTrackNumber element must be

Version	Encryption Type	When Encrypting PAN	When Encrypting Track Data
		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.	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 CardNbr and CVV2 provided must only include the encrypted PAN and encrypted CVV2 parsed by the POS from the E3/Voltage device output stream.	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 by the POS from the E3/Voltage device output stream.

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.

Supported services for tokenization are as follows:

Application Service	Request a Token	Use a Token
CreditAccountVerify	Yes	Yes
CreditAuth	Yes	Yes

Application Service	Request a Token	Use a Token
CreditOfflineAuth	No	Yes
CreditOfflineSale	No	Yes
CreditReturn	No	Yes
CreditReversal	Yes	Yes
CreditSale	Yes	Yes
PrePaidAddValue	Yes	Yes
PrePaidBalanceInquiry	Yes	Yes
RecurringBilling	Yes	Yes

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.

2.2.1 Requesting a Token

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 TokenDataRsp. Portico attempts to request the account number and expiration date associated with the provided token from the tokenization service. If the TokenDataRsp included 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 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 (Section 6.1)**.

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.

Note: 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

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 (Section 6.2)** 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 (Section 6.4)** for additional information.

Timeouts

For transactions, clients should allow 15 seconds for Portico to respond. Transactions are typically on Heartland systems for less than 500ms, but Portico waits up to 10 seconds for other back-end systems to reply.

For searching and reports, clients should allow 60 seconds or more for Portico to respond. Actual response times depend on the amount of data and the type of report or search being done. To improve response times, adjust the criteria being used to obtain a smaller result set.

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.

Note: 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.

4 Transactions

The following list contains all the available Portico transactions with links to their detailed documentation and code examples.

Transaction	Schema Documentation	Description
AddAttachment	Request / Response	AddAttachment can be used to store and associate data (e.g. images, documents, signature capture, etc.) to a prior transaction.
AltPaymentAuth	Request / Response	AltPaymentAuth takes a unique Session Id and performs an Authorization transaction.
AltPaymentCapture	Request / Response	AltPaymentCapture takes an existing Order or Auth and captures some portion of the original transaction and adds that portion to the open batch.
AltPaymentCreateAuth	Request / Response	AltPaymentCreateAuth takes a previously approved Alternate Payment transaction and creates an Authorization from it.
AltPaymentCreateSession	Request / Response	AltPaymentCreateSession creates a unique Session for Electronic Commerce Alternate Payment Processing. This service must be called first to perform Alternate payment processing.
AltPaymentOrder	Request / Response	AltPaymentOrder takes a unique Session Id and performs an Order transaction.
AltPaymentReturn	Request / Response	AltPaymentReturn takes a previously Add To Batch transaction and performs a return against it.
AltPaymentSale	Request / Response	AltPaymentSale takes a unique Session Id and performs a Sale transaction.
AltPaymentSessionInfo	Request / Response	AltPaymentSessionInfo takes a unique Session Id and returns information about the session.
AltPaymentVoid	Request / Response	AltPaymentVoid takes a GatewayTxnId and performs a void against that 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. 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.

Transaction	Schema Documentation	Description
CheckVoid	Request / Response	CheckVoid is used to cancel a previously successful CheckSale transaction.
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.
CreditAddToBatch	Request / Response	CreditAddToBatch is primarily used to add a previously approved open authorization (CreditAuth, CreditOfflineAuth, or OverrideFraudDecline) 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. Incremental authorizations are only allowed for lodging merchants.
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.
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 /	CreditSale authorizes a credit card transaction. These authorizations

Transaction	Schema Documentation	Description
	Response	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 OverrideFraudDecline.
DebitAddValue	Request / Response	DebitAddValue increases the amount on a stored value card.
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.
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.
DebitSale	Request / Response	DebitSale authorizes a debit card transaction.
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 EBT Food Stamps.
EBTFSReturn	Request / Response	EBTFSReturn is used to credit previously debited funds to an EBT Food Stamps account for merchandise returned.
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.

Transaction	Schema Documentation	Description
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.
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.
GiftCardTip	Request / Response	GiftCardTip is used to add tip to an existing GiftCardSale.
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.
InvalidateAuthentication	Request / Response	InvalidateAuthentication is for internal use only.

Transaction	Schema Documentation	Description
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.
OverrideFraudDecline	Request / Header response only	OverrideFraudDecline is for internal use only. It is used to process a CreditSale, CreditReturn or CreditAuth that was previously declined due to fraud. An override causes the fraud concerns to be ignored. The use of this function on a client should require management approval. This can only be done once, and for the original auth amount.
ParameterDownload	Request / Response	ParameterDownload is used to initiate an EMV parameter download by clients interfacing to an EMV device.
PrePaidAddValue	Request / Response	PrePaidAddValue is used to increase the balance associated with a prepaid card.
PrePaidBalanceInquiry	Request / Response	PrePaidBalanceInquiry returns the available balance for a prepaid card.
RecurringBilling	Request / Response	RecurringBilling authorizes a one-time or scheduled recurring transaction.
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 device if needed.
ReportBatchDetail	Request / Response	ReportBatchDetail returns information on each transaction currently associated to the specified batch. This report is for the site and device referenced in the header.
ReportBatchHistory	Request / Response	ReportBatchHistory returns information about previous batches over a period of time. This report is for the site 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 site and device 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 site referenced in the header.
ReportSearch	Request / Response	ReportSearch returns transaction information for a specified time period.
ReportTxnDetail	Request / Response	ReportTxnDetail returns detailed information about a single transaction. This report is for the site and device referenced in the header.
SendReceipt	Request /	SendReceipt is for internal use only. It allows a client to send a receipt

Transaction	Schema Documentation	Description
	Response	from a prior transaction out to specific destinations. The prior transaction must belong to the site and device referenced in the header.
TestCredentials	Request / Response	TestCredentials validates the credentials passed in the header, but does not perform an action.

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
CreditOfflineAuth	Request	Response
CreditOfflineSale	Request	Response
CreditReturn	Request	Response
CreditReversal	Request	Response
CreditSale	Request	Response
CreditTxnEdit	Request	Response
CreditVoid	Request	Response
OverrideFraudDecline	Request	Header response only
RecurringBilling (one-time payment)	Request	Response

4.2 Debit Card Transactions

The following table provides links to the debit card transactions.

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

4.5 EBT Transactions

The following table provides links to the EBT transactions.

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

4.6 Gift Card Transactions

The following table provides links to the gift card transactions.

Transaction Name	Request	Response
GiftCardActivate	Request	Response
GiftCardAddValue	Request	Response

Transaction Name	Request	Response
GiftCardAlias	Request	Response
GiftCardBalance	Request	Response
GiftCardCurrentDayTotals	Request	Response
GiftCardDeactivate	Request	Response
GiftCardPreviousDayTotals	Request	Response
GiftCardReplace	Request	Response
GiftCardReversal	Request	Response
GiftCardReward	Request	Response
GiftCardSale	Request	Response
GiftCardVoid	Request	Response

4.7 PrePaid Card Transactions

The following table provides links to the prepaid card transactions.

Transaction Name	Request	Response
PrePaidAddValue	Request	Response
PrePaidBalanceInquiry	Request	Response

4.8 Utility Transactions

The following table provides links to some utility function transactions.

Transaction Name	Request	Response
AddAttachment	Request	Response
FindTransactions	Request	Response
GetAttachments	Request	Response
ManageTokens	Request	Header response only
ParameterDownload	Request	Response
TestCredentials	Request	Response

4.9 Batch Transactions

The following table provides links to the batch transactions.

Transaction Name	Request	Response

BatchClose	Request	Response

4.10 Report Transactions

The following table provides links to the report transactions.

Transaction Name	Request	Response
ReportActivity	Request	Response
ReportBatchDetail	Request	Response
ReportBatchHistory	Request	Response
ReportBatchSummary	Request	Response
ReportOpenAuths	Request	Response
ReportSearch	Request	Response
ReportTxnDetail	Request	Response

4.11 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 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.

5.1 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.

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	American Express
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 and address match	Y	Y	X	X
5 digit zip and address match	Y	Y	Y	Y
5 digit zip code match, address does not match	Z	Z	Z	Z
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)

Application Service	VISA	Discover/JCB	MasterCard	American Express
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 Street address not verified due to incompatible formats (international address)	P	P	(N/A)	(N/A)

5.2 Adjustments

The original transaction can be adjusted using CreditAddToBatch and 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 (Section 5.9)**.

5.3 Alternate Payments

A merchant has the option to accept alternate forms of payment. At present, PayPal is the only form of alternate payment, but more will be supported in time. Once other alternate payment types are available, this process will be modified to reflect all options.

The ability to accept PayPal payment through Portico is available with a plug in.

The process flow for Portico to process alternate payments is:

AltPaymentCreateSession—Portico API call that is required to initially start sending transactions to PayPal. Portico's service has implemented the SetEC API call from PayPal. The Payment Type (Sale, Order or Authorization) within the CreateSession data drives the subsequent API call.
NOTE: After AltPaymentCreateSession, the returned RedirectUrl must be used to log into Paypal's sandbox site and confirm the payment. This requires a buyer account to be created on the sandbox. The ID (numbers/letters) created from the ID is used in the SoapUI tests after the Session is created.

AltPaymentSale—Minimal call to complete an Ecommerce transaction with PayPal. Portico has implemented the DoEC API call from PayPal and sends the Payment Action field (in the paypal request) as Sale.

AltPaymentAuth—Call to send an authorization transaction to PayPal. PayPal authorizes and adjusts the buyer's open to buy. Portico has implemented the DoEC API call from PayPal and sends the Payment Action field (in the paypal request) as Authorization. This transaction requires the AltPaymentCapture to be completed against it.

AltPaymentOrder—Call to send an order transaction to PayPal. PayPal does not authorize or adjust the Buyer's open to buy. Portico has implemented the DoEC API call from PayPal and sends the Payment Action field (in the paypal request) as Order. This transaction requires the AltPaymentCapture to be completed against it.

AltPaymentCapture—Call to send a capture transaction to PayPal. Portico has implemented the DoCapture API call from PayPal. This transaction is run against an existing Order or Auth and captures some portion of the original transaction and adds that portion to the open batch. This transaction moves money.

AltPaymentReturn—Call to send a Return transaction to PayPal. Portico has implemented the RefundTransaction API call from PayPal. This transaction is run against an existing Sale or an existing Capture against an Order or Auth. Portico adds the return to the open batch. This transaction moves money.

AltPaymentVoid—Call to send a Void transaction to PayPal. Portico has implemented the DoVoid API call from PayPal.

This transaction is run against an existing Order or Auth. This transaction cancels future captures against an Auth or Order. Existing captures are unaffected.

AltPaymentSessionInfo—Call to send a Session inquiry transaction to PayPal. Portico has implemented the GetEC API call from PayPal. This transaction is run against an existing SessionId. This transaction is inquiry only and does not affect any transactions.

AltPaymentCreateAuth—Call to create a stand-alone authorization from an existing Order. Portico has implemented the DoAuthorization API call from PayPal. This transaction is run against an existing Order transaction. This transaction requires the AltPaymentCapture to be completed against it.

AltPaymentReversal—Call to reverse a Sale, Capture, Auth or Order, that has not been successfully recorded on Portico. If Portico has only ever recorded a timeout for a Sale or Capture, send a Return to PayPal. If Portico has only ever recorded a timeout for an Auth or Order, send a Void transaction to PayPal.

- **Alternate Service NameValuePair Request Fields (Section 5.3.1)**
- **Alternate Service Request Field Usage Detail (Section 5.3.2)**
- **Alternate Service NameValuePair Response Fields (Section 5.3.3)**
- **Alternate Service Response Field Usage Detail (Section 5.3.4)**

5.3.1 Alternate Service NameValuePair Request Fields

Group	NameValuePair name	Required	Edit	Length	Used by
Buyer	CancelUrl	Yes	Start with Http: or Https: Https preferred	2048	AltPaymentCreateSession
	ReturnUrl	Yes	Start with Http: or Https: Https preferred	2048	AltPaymentCreateSession
	BuyerId	Yes	Valid ascii	100	AltPaymentSale, Auth and Order
	EmailAddress		Valid ascii	20	AltPaymentCreateSession
	FundingSource		Credit. Default is non-credit.	N/A	AltPaymentCreateSession
	MerchantLogoUrl		Start with Http: or Https: Https preferred	2000	AltPaymentCreateSession
Payment	ItemAmount		Decimal, 12,2 with decimal point. Total of LineItem Amounts.	N/A	AltPaymentSale, Auth, Order and CreateAuth
	ShippingAmount		Decimal, 12,2 with decimal point.	N/A	AltPaymentSale, Auth, Order and CreateAuth
	ShippingAmountDiscount		Decimal, 12,2 with decimal point. Requires negative amount.	N/A	AltPaymentCreateSession, Auth, Sale and Order
	TaxAmount		Decimal, 12,2 with decimal point.	N/A	AltPaymentSale, Auth, Order and CreateAuth
	NOTE*		ItemAmount, Shipping Amount, Tax Amount must equal Amt of the transaction.		AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	PaymentType		Order, Authorization or Sale. Default is Sale.	N/A	AltPaymentCreateSession

Group	NameValuePair name	Required	Edit	Length	Used by
	FullyCapuredFlag		True or False	N/A	AltPaymentCapture
	InvoiceNbr		Valid ascii. Must be unique per Session.	256	AltPaymentSale, Auth, Order and CreateAuth
	InstantPaymentOnly		True or False	N/A	AltPaymentCreateSession
Shipping	ShipName		Valid ascii	128	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipAddress		Valid ascii	100	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipAddress2		Valid ascii	100	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipCity		Valid ascii	40	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipState		Valid ascii. Valid state.	40	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipZip		Valid ascii. Validated against state and city and only US addresses.	20	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipCountryCode		Valid ascii. Valid two character country.	2	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipPhoneNbr		Valid ascii	20	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	ShipAllowAddressOverride		True or False. Default is True.	N/A	AltPaymentCreateSession
LineItem	Name		Valid ascii	127	
	Description		Valid ascii	127	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	Amount		Decimal, 12,2 with decimal point. Allows Negative sign.	N/A	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	Quantity		Up to 10 digits numeric	N/A	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	NOTE*		Quantity times Amount rolls up to Payment/ItemAmount.		

Group	NameValuePair name	Required	Edit	Length	Used by
	Number		Valid ascii	127	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	TaxAmount		Decimal, 12,2 with decimal point. Allows negative sign.	N/A	AltPaymentCreateSession, Auth, Sale, Order and CreateAuth
	NOTE*		Quantity times TaxAmount rolls up to Payment/TaxAmount.		
Return	ReturnType		Full or Partial	N/A	AltPaymentReturn
	InvoiceNbr		Valid ascii. Must be unique per Session.	127	AltPaymentReturn

5.3.2 Alternate Service Request Field Usage Detail

Field Name	Usage
PaymentType	Indicates payment type. PayPal is the only valid value.
Amt	Amount of request.
SessionId	Session Id that is returned from a Create Session response.
GatewayTxnId	Unique Portico Transaction Id. Returned in Common header.
CancelUrl	Redirect provided by Merchant. Used if Buyer cancels order from PayPal UI.
ReturnUrl	Redirect provided by Merchant. Used if Buyer accepts order from PayPal UI.
BuyerId	Buyer payer id. Indicates who the PayPal buyer is.
EmailAddress	Buyer Email Address.
FundingSource	Indicates funding source.
MerchantLogoUrl	Logo URL to be displayed when Buyer confirms payment.
ItemAmount	Total Item Amount.
ShippingAmount	Total Shipping Amount.
TaxAmount	Total Tax Amount.
PaymentType	Indicates what type of Payment needs to be created during Create Session. Set this value to the intended follow-up service call.
FullyCapuredFlag	Indicates during Capture if this is the final capture.
InvoiceNbr	Invoice Number. Must be unique per session id.
ShipName	Shipping name
ShipAddress	Shipping Address
ShipAddress2	Shipping Address2
ShipCity	Shipping City

Field Name	Usage
ShipState	Shipping State
ShipZip	Shipping Zip
ShipCountryCode	Shipping Country Code
ShipPhoneNbr	Shipping Phone Number
ShipAllowAddressOverride	Indicates if Buyer can alter shipping information on Pay Pal Site. Use during Create Session.
Name	Item Name
Description	Item Description
Amount	Item Amount
Quantity	Item Quantity
Number	Item SKU
TaxAmount	Item Tax Amount
ReturnType	Indicates full or partial return.
InstantPaymentOnly	Indicates the merchant expects Instant payment only responses for this transaction.
ShippingAmountDiscount	Indicates a Payment level shipping discount.

5.3.3 Alternate Service NameValuePair Response Fields

Group	NameValuePair Name	Used By
Session	SessionId	AltPaymentCreateSession
	RedirectUrl	AltPaymentCreateSession
Buyer	InvoiceNbr	AltPaymentSessionInfo
	EmailAddress	AltPaymentSessionInfo
	BuyerId	AltPaymentSessionInfo
	Status	AltPaymentSessionInfo
	CountryCode	AltPaymentSessionInfo
	BusinessName	AltPaymentSessionInfo
	FirstName	AltPaymentSessionInfo
	LastName	AltPaymentSessionInfo
	PhoneNumber	AltPaymentSessionInfo
Shipping	ShipName	AltPaymentSessionInfo
	ShipAddress	AltPaymentSessionInfo
	ShipAddress2	AltPaymentSessionInfo
	ShipCity	AltPaymentSessionInfo

Group	NameValuePair Name	Used By
	ShipState	AltPaymentSessionInfo
	ShipZip	AltPaymentSessionInfo
	ShipCountryCode	AltPaymentSessionInfo
Payment	Amt	AltPaymentSessionInfo
	ItemAmount	AltPaymentSessionInfo
	ShippingAmount	AltPaymentSessionInfo
	TaxAmount	AltPaymentSessionInfo
LineItem	Name	AltPaymentSessionInfo
	Description	AltPaymentSessionInfo
	Amount	AltPaymentSessionInfo
	Number	AltPaymentSessionInfo
	Quantity	AltPaymentSessionInfo
	TaxAmount	AltPaymentSessionInfo
Processor	Code	All Services
	Message	All Services
	Type	All Services

5.3.4 Alternate Service Response Field Usage Detail

Name	Usage
RspCode	Response code to validate the Alternate Payers processing. 0 equals Success. 1 equals failure.
RspMessage	Alternate Payers processing message.
Status	Alternate Payers status of request.
StatusMessage	Alternate Payers status message of request.
SessionId	PayPal's session id. Returned from Create Session.
RedirectUrl	Redirect URL with Session Id. Use by Merchant to redirect Buyer.
Code	PayPal Code for additional Response information.
Message	PayPal Message for additional Response information.
Type	PayPal Type for additional Response information.
ReturnAmt	Return Amount for transction.
TotalReturnAmt	Total Return amount of original. Multiple return scenarios.

5.4 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

Note: 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.

Note: 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.

5.5 Batch Processing

Portico is a host capture system. This means that Portico is the system of record for transactions, batches, and settlement details. 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.

Batches are maintained at the device level. If a site (merchant) has multiple devices, each is closed individually. If a device does not have an open batch, the next transaction will create a new open batch.

Batch information will be removed from Portico after 90 days.

5.5.1 Settlement

Portico supports auto and manual batch close options. The POS can use either or both of these options.

5.5.1.1 Auto-close

Each device can be configured with a specific auto-close time at boarding. Portico uses this setting to determine when to automatically close the device's batch each day. This 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. 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. 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.

5.5.1.2 Manual Entry

Information must be manually keyed into the application when 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.

5.6 Card Not Present Transactions

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

5.7 Card Present Transactions

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

5.8 Card Verification Value (CVV2)

The CVV2 number enhances fraud protection for transactions in order to qualify for the proper interchange rates. It helps to validate the following two things:

- The customer has the credit card in their possession.
- The credit card number is legitimate.

The following table describes how each credit card association implements CVV2 protection.

Card Brand	CVV2 Name	CVV2 Location
VISA	Card Verification Value	Three-digit number printed in the signature space on the back of the card
MasterCard	Card Validation Code	Three-digit number printed in the signature space on the back of the card
American Express	Card Verification Value	Four-digit number on front of card It is printed, not embossed like the card number.
Discover	Card Member ID	Three-digit number printed in the signature space on the back of the card

CVV2 protection takes place when a transaction is being processed and the card is not present. For example, when a cardholder makes a purchase over the telephone or on the Internet. The merchant asks the cardholder to read the CVV2 code from the card. The merchant adds this code to the transaction being sent to Portico. Entering CVV2 information along with Address Verification Service (AVS) should result in fewer chargebacks and lower Interchange rates.

CVV2/CID is highly encouraged, but not required for card not present transactions. Discover Card charges $0.50 per keyed transaction if CID is not present at the time of authorization.

Some Issuers may decline the sale if the CVV code does not match what is on file for the cardholder. Others may approve the transaction. If the transaction is approved, the merchant needs to make a decision to go forward with the sale based upon the CVV response. It is strongly recommended that the merchant ask the cardholder for another form of payment if the CVV code does not match ("N" response).

CVV protects the merchant against chargebacks if the response code is returned as a match and later the transaction is found to be fraudulent.

The following are the possible CVV2/CID response codes returned by Portico:

Value	Description
M	CVV Match
N	CVV No Match
P	Not Processed
S	Should Have Been Present
U	Issuer is not certified and/or Issuer has not provided Visa with the CVV2 encryption keys

5.9 Corporate Cards

A merchant has the option to participate in Corporate Purchase Card (CPC) transactions. These are also known as "Level II" 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, or RecurringBilling transaction. If the Issuer identifies the associated card as a Corporate Purchase Card, the response message will contain a value in the CPCInd field indicating the specific card type of business, corporate, or purchasing card. 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 is also supported, but when it is used a CreditCPCEdit cannot be used as it does not apply.

CPCData can also be included directly in the RecurringBilling transaction. In this case, the subsequent call to CreditCPCEdit is not required.

5.10 Duplicate Checking

Duplicate Checking logic checks for duplicate transactions submitted by a device. 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 device. 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 to the caller.

5.10.1 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

Note: 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.

5.10.2 Override Duplicate Checking

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

5.10.3 Portico Services Supporting Duplicate Checking

The following Services provide Duplicate Checking support:

- ChipCardDecline
- CreditAdditionalAuth
- CreditAuth
- CreditOfflineAuth
- CreditOfflineSale
- CreditReturn
- CreditSale
- DebitAddValue
- DebitReturn
- DebitSale
- EBTCashBackPurchase
- EBTCashBenefitWithdrawal
- EBTFSPurchase
- EBTFSReturn
- EBTVoucherPurchase
- OverrideFraudDeclineService
- PrePaidAddValueService
- RecurringBillingService

5.11 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.

Portico generates a merchant name by concatenating a configurable, ShortDBAName with the TxnDescriptor field provided on CreditSale or CreditAuth request transactions. The generated Merchant Name is passed to the card issuers to display on cardholder statements. Portico returns the generated Merchant Name including TxnDescriptor in the CreditSale or CreditAuth response. Merchants can display this generated Merchant Name on printed or online receipts, so customers are notified how the transaction appears on their statement.

The Maximum characters of the generated Merchant Name is 22 characters. The ShortDBAName may be three, seven, or 12 characters in length. The ShortDBAName is separated from the TxnDescriptor by a "*" in a fixed position based on the ShortDBAName length. The Maximum characters of the TxnDescriptor is based on the length of the ShortDBAName plus the separator.
For example:

- If the ShortDBAName = 3, the separator "*" is fixed in position 4 and the TxnDescriptor Maximum characters is 18 characters.
- If the ShortDBAName = 7, the separator "*" is fixed in position 8 and the TxnDescriptor Maximum characters is 14 characters.
- If the ShortDBAName = 12, the separator "*" is fixed in position 13 and the TxnDescriptor Maximum characters is 9 characters.

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

5.12 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. Currently, the Portico API only supports EMV credit transactions. 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). 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 EMV Integrator Guide.

5.12.1 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)

Service	Tag	Condition
ChipCardDecline	8A	equals Z1 (8A025A31) or Z3 (08A025A33)

5.12.2 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.

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 w/ Track2 and EMV tag data. **Note:** 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, 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.

5.12.3 Services That Support EMV Tags

Services that support passing of EMV tags are below:

Note: 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.

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.

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

5.12.4 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" – one-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 one 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.

5.12.4.1 EMV Request Tags

The following table lists the EMV tags associated with authorization or return requests.

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
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	9F26	M	The 16-character Application Cryptogram contains the cryptogram returned by the

Field Name	Tag	Usage	Description
CRYPTOGRAM			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 four-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 PRIMARY ACCOUNT NUMBER (PAN) SEQUENCE NUMBER	5F34	C	The two-character numeric Application Primary Account Number 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 four-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
APPLICATION USAGE CONTROL	9F07	C	The four-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 four-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 four-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 four-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)

Field Name	Tag	Usage	Description
			Example (2 bytes alphanumeric) => Y1 TLV => 8A025931
CARDHOLDER VERIFICATION METHOD (CVM) RESULTS	9F34	C	The six-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 two-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 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 four-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 two-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). Example (5 bytes binary) => FC-F8-FC-F8-F0 TLV => FFC605FCF8FCF8F0

Field Name	Tag	Usage	Description
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 six-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 four-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 two-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 four-character numeric Transaction Currency Code contains the currency code of the transaction according to ISO 4217. Example (decimal value) => 840 TLV => 5F2A020840
TRANSACTION DATE	9A	M	The six-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 four-character Transaction Status Information contains the functions performed in the transaction. Example (2 binary bytes) => 48-00 TLV => 9B024800
TRANSACTION TIME	9F21	C	The six-character numeric Transaction Time subfield contains the local time that the transaction was authorized. Example (decimal value - HHMMSS) => 123456 TLV => 9F2103123456

Field Name	Tag	Usage	Description
TRANSACTION TYPE	9C	M	The two-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 eight-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 five 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. 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 five 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 eight-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 TLV => 9F6E05123456789A PAYPASS THIRD-PARTY DATA

Field Name	Tag	Usage	Description
			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 ASCII-coded binary format. Example (4 bytes binary) => 01-02-03-04 TLV => 9F6E0401020304
ICC DYNAMIC NUMBER	9F4C	C	The four- 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 TLV => 9F6E0401020304
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 ASCII coded binary format. Conversion from ASCII 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 four- to eight-character numeric (binary) Transaction Sequence Counter uniquely identifies each transaction on a POS terminal. Example (decimal value) => 435 TLV => 9F4104000001B3

C=Conditional
M=Mandatory
O=Optional

5.12.4.2 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 ASCII coded binary format. Conversion from ASCII 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 two- 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 ASCII to coded binary is dependent on the kernel API. Example (10 bytes binary) => 01-02-03-04-05-06-07-08-09-0A TLV => 710A0102030405060708090A

ISSUER SCRIPT TEMPLATE 2	72	O	The two- 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 ASCII to coded binary is dependent on the kernel API. Example (10 bytes binary) => 01-02-03-04-05-06-07-08-09-0A TLV => 7210A0102030405060708090A

C=Conditional
M=Mandatory
O=Optional

5.12.5 EMV Parameter Data Download

Clients that interface with EMV capable terminals are required to accept Parameter Data Downloads when notified. 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.

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).

5.12.5.1 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. **Note:** 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.

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

5.12.5.1.1 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
PARAMETER VERSION or TABLE VERSION	3	A/N	TERM	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

Field Name	Length	Format	Source	Value/Description
				back from the Host in the initial PDL response.
BLOCK SEQUENCE NUMBER	2	N	TERM	Block sequence number. • 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.

5.12.5.1.2 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.

5.12.5.1.2.1 PDL Response 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

Field Name	Length	Format	Source	Value/Description
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

Field Name	Length	Format	Source	Value/Description
NO. of CARD TYPES	2	N	HOST	Number of CARD TYPES supported by the customer.

The following fields will be repeated, dependent upon the number of card types.

Field Name	Length	Format	Source	Value/Description
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	
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

5.12.5.1.2.2 PDL Response Tables 30-60

Note: 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

Field Name	Length	Format	Source	Value/Description
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.

5.12.5.1.2.2.1 PDL Response Table 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 CAPABILITES	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

Field Name	Length	Format	Source	Value/Description
				○ 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. ○ 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.

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

5.12.5.1.2.2.2 PDL Response 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.

Field Name	Length	Format	Source	Value/Description
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 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

Field Name	Length	Format	Source	Value/Description
				○ 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
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 transaction online more frequently (biased random selection).

Field Name	Length	Format	Source	Value/Description
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 LIST (TDOL)	32	HEX	HOST	TDOL to be used for generating the TC Hash Value if the TDOL in the card is not present.
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.

5.12.5.1.2.2.3 PDL Response 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.

Field Name	Length	Format	Source	Value/Description
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 ○ Bit 6 – EBT ○ Bit 5 – Gift ○ Bit 4 – Loyalty ○ Bit 3 – Stored Value ○ Bits 2-1 – RFU • Byte 2 ○ Bits 8-1 – RFU

Field Name	Length	Format	Source	Value/Description
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.
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	10	HEX	HOST	Specifies the acquirer’s conditions that cause a transaction to be

Field Name	Length	Format	Source	Value/Description
ACTION CODE (TAC) – ONLINE				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. **Note:** 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.

5.12.5.1.2.2.4 PDL Response 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.

Field Name	Length	Format	Source	Value/Description
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

Field Name	Length	Format	Source	Value/Description
				• 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.

Field Name	Length	Format	Source	Value/Description
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.

5.12.5.1.2.3 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.

5.13 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.

5.14 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.

5.14.1 Retail

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

5.14.2 Restaurant

A typical restaurant transaction is processed using the CreditAuth transaction type to process the initial purchase amount. This transaction can be followed by a CreditAddToBatch transaction that adjusts 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 CreditSale followed by CreditTxnEdit. CreditAuth+CreditAddToBatch has the advantage of ensuring that no unadjusted transactions are inadvertently settled if the merchant is wanting to use auto-settlement.

Portico supports a specific transaction for the handling of bar tabs: CreditAdditionalAuth.

5.14.3 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

A Check-In transaction authorizes a sale purchased with a credit card. The Check-In transaction utilizes the CreditAuth transaction if the amount is not meant to be settled. However, if the amount should be settled (e.g., if there is an advance deposit or fee to be charged) this can be done with a CreditSale. Also, if all that is needed at check in is to validate the card, a CreditAccountVerify can be used.

Check Out

A Check-Out transaction closes out a Check-In transaction and adds the transaction to the current batch. A Check-Out transaction utilizes the CreditAddToBatch transaction if the Check-In transaction was a CreditAuth and has not yet been added to a batch. Otherwise, a new CreditSale can be run or the Check-In amount can be edited with a CreditTxnEdit transaction. The transaction request includes the GatewayTxnID from the Check-In transaction, and optionally the amount of the
transaction.

Incremental Authorization

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

Note: Once a CreditIncrementalAuth has been run against a transaction, the original transaction cannot be reversed. This is a known issue that will be corrected in a future release. Until this is corrected, the original sale must be reversed prior to running an CreditIncrementalAuth. After an CreditIncrementalAuth is run, you can run a new authorization for the full amount including the incremental amount. The total can be reduced at checkout with a partial reversal or a return. This could increase related transaction fees. There is also an option to use multiple separate auths, but these will appear separately on the customer's statement.

- 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.

Note: 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.

- Additional Charge—To include an additional charge, use the CreditTxnEdit transaction to alter the original transaction.

- No Show—To charge penalties for a No Show, use a CreditSale transaction.

Note: The check in date is the initial authorization date and the stay duration is one day.

5.14.4 Healthcare

Auto-substantiation (Section 5.4) 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.

Note: 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.

5.14.5 MOTO/eCommerce

Mail Order/Telephone Order (MOTO) and eCommerce transactions are handled as "card not present" transactions. These are typically credit transactions.

In Application Payments

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.

This functionality is currently only supported for ApplePay with all four card brands.

3-D Secure Authentication

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 3-D Secure data that is required by the brands and issuers to settle correctly.

Note: An updated HPS policy now requires that merchants process eCommerce transactions on a separate Merchant Identification Number (MID) regardless of their eCommerce sales volume or the percentage of transactions that are processed online. Contact your Heartland representative for more information on setting up your eCommerce MID. When an eCommerce MID is created, you receive a SiteId and DeviceId to process eCommerce transactions on Portico.

5.15 Partial Authorization

A partial authorization is supported for a credit or PIN debit authorization request. The merchant must submit a CreditAuth, CreditSale, or DebitSale 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:

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
5399 Miscellaneous General Merchandise Stores
5411 Grocery Stores, Supermarkets
5499 Miscellaneous Food Stores—Convenience Stores, Markets, Specialty Stores and Vending Machines
5541 Service Stations (with or without Ancillary 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
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.

Note: 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.

5.16 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.

Note: 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". **NOTE:** 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>71011111111111111112222222222222222<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>22222222222222221111111111111111</PinBlock>
...
</Block1>
</DebitSale>
```

5.17 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 is read by a proximity reader to capture the card information stored on the magnetic stripe or chip.

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.

5.18 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.

- **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 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.

5.19 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.

6 Appendices

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

6.1 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
```

6.2 Gateway Response Codes

Note: When checking response codes, be sure to check both the Gateway Response Codes and **Issuer Response Codes (Section 6.4)**. See **Validating Response Codes (Section 3.4)** 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

Response Code	Description
+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’s 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.
+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

Response Code	Description
	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-&gt;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.
+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.
+35	Device setting error—This error is returned from SendReceipt if the "AllowEmail" setting is not set to true for the device 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.
+50	Processor System error
+51	Processor Configuration error

6.3 Tokenization-Specific Response Codes

Error Code	Description
0	Tokenization was successful. Note: 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.

6.4 Issuer Response Codes

Note: When checking response codes, be sure to check both the **Gateway Response Codes (Section 6.2)** and Issuer Response Codes. See **Validating Response Codes (Section 3.4)** 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 cardholder has exceeded their allowable credit line.
06	ERROR—merchant closed, no match.
07	HOLD-CALL
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 six digits of the card number are not recognized by the Issuer. Reenter transaction.
19	RE ENTER—reenter transaction. Bad swipe.
41	HOLD-CALL—lost card.

Response Code	Description
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 is 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—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
91	NO REPLY—time out.
96	SYSTEM ERROR
EB	CHECK DIGIT ERR
EC	CID FORMAT ERROR—format error.

Response Code	Description
FR	FRAUD—Transaction declined because possible fraud was detected by Heartland.
N7	CVV2 MISMATCH—incorrect number of CVV2/CID digits sent.
PD	PARAMETER DOWNLOAD—EMV PDL system response. Response text indicates EMV PDL status code.

6.5 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. NOTE: 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

6.6 Status Indicators

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.

Indicator	Status	Description
X	Autovoided	The transaction was voided by Portico's automated process. NOTE: 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 device. There is only one open batch per device.
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.

6.7 HMS Gift Card Certification

The following sections include details about HMS certification.

6.7.1 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.

6.7.1.1 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. **Note:** 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

Amount	Status Code	Status Name
308	400	InvalidCard
500	200	CannotVoid

6.7.2 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.

6.8 Revision History

- The content was separated into two sites to optimize search results by issolating the noise of the generated content:
  Static/manual content 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. Searches performed in this site will provide results for only this site. A PDF of this content is provided.
  Generated/technical content site: This site contains the content generated from the XML Schema. Pages in this site are opened in a new tab in your browser. Searches performed in this site will provide results for only this site. The nature of this content does not lend itself to display in a PDF, so no PDF is provided.

Documentation Section / Topic	Change Description
Managing Tokens (Section 2.2.3)	Added text to the DeleteAttribute, DeleteToken subsection to state that not providing attributes causes a token to be deleted.
Industries	Removed GSB Card Services, as it is no longer supported.
Partial Authorization (Section 5.15)	Removed DebitAuth from the list of supported transactions for partial authorization.
MOTO/eCommerce (Section 5.14.5)	Added paragraphs for "In Application Payments" and "3-D Secure Authorization".
Gateway Response Codes (Section 6.2)	Added response codes +21 and +22.

Schema site	Added support for eCommerce 3-D Secure Authentication and ApplePay InApp for Discover to the SecureECommerceType block.
Schema site	Added note concerning the max number of digits supported for the SurchargeAmtInfo field.
Schema site	Changed list to specifically AMEX instead of just "other" in CreditAccountVerify transaction page.
Schema site	Changed the Amt and AuthAmt field descriptions in CreditReversal.

7Glossary

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 nine-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
Changing the state of a fixed denomination account from "inactive" to "active", enabling a stored value/prepaid card for use.

Activation and Initial Load
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.

ASCII
American Standard Code for Information Interchange. ASCII is a character-encoding scheme based on the ordering of the English alphabet. ASCII codes represent text for computers, communications equipment, and other devices that use text.

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 nine-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
Based on pre-determined criteria, the terminal will submit the details of all transactions that have taken place since the last successful batch.

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 six-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.

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 card holders (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 three-digit or four-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 three- or four-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 (three digits) used by VISA and MasterCard account numbers.
CID (three digits) used by Discover account numbers.
CID (four 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 card holder 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 three- or four-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 three-digit code appearing on the front or back of VISA or MasterCards. CVV2 is used for fraud prevention. For all other bankcards see CVN.

D

DBA
Doing Business As

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.

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 one 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 in 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. 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, 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.

GSB
Give Something Back (GSB) Network^{SM} OneCard. A prepaid card that works like cash. Designed to make charitable giving easy and automatic.

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

H

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.

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 ASCII, non-text attachments, Message bodies with multiple parts, and Header information in non-ASCII 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
NonDisclosure 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.

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 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. A 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.

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 nine-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

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.

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.

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 nine-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.

8 Index