ORBITAL GATEWAY XML

INTERFACE SPECIFICATION

DEVELOPERS GUIDE

August 2013

Version 5.8

Orbital Gateway XML Interface Specification

Version 5.8

August 2013

Copyright © 2013 Chase Paymentech Solutions, LLC. All rights reserved.

Not for Disclosure outside Chase Paymentech Solutions, L.L.C. or its customers.

This publication is for information purposes only, and its content does not represent a contract in any form. Furthermore, this publication shall not be deemed to be a warranty of any kind, either express or implied. Chase Paymentech expressly disclaims, and you expressly waive, any and all warranties, including without limitation those of merchantability and fitness for a particular purpose. Chase Paymentech reserves the right to alter product specifications without notice. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage or retrieval system, without Chase Paymentech's permission.

All brand names and product names used in this document are trade names, service marks, or registered trademarks of their respective owners.

Last Revised: 8/19/2013 6:16 PM

Change Control Log

Date	Action	Description
09/01/06	Rewrite	Orbital Gateway Version 4.0 is a brand new schema that requires the specification to be rewritten
11/01/06	Updated	Added Bill Me Later in Schema version 4.1
12/01/06	Updated	Added PINless Debit
02/01/08	Updated	Updated for Schema 4.3. Added Managed Billing, Auth Recycling
02/01/08	Updated	Added Return via TxRefNum
02/01/08	Updated	Clarified Address Verification wording, added AVS format table
02/01/08	Updated	Added note to Purchasing Card section about Salem P-card edits and rejected batches
02/01/08	Updated	Added AVS Country Code, EU DD, Soft Descriptor support to Profile sections.
02/01/08	Updated	Changed *FlexCache* to *Gift Card* wherever possible
05/15/08	Updated	Expanded MFC Response to include new elements
12/15/08	Updated	Changed format of document. Added Inquiry message details. Added Reversal Retry Number element to Reversal message.
02/03/09	Updated	Added Connection Username/Password information in Authentication section; updated Message Definitions as well
5/18/09	Updated	Put into new template and edited for style and formatting
6/15/09	Updated	Added Reversal and Account Verification information. Updated Response Codes, AVS Response Codes, ProcStatus Codes.
4/27/10	Updated	Updated for Schema 4.9 Added Account Updater. Updated MFC, Gift Card, & Profile descriptions. Updated Message Definitions and ProcStatus Codes.

8/10/10	Updated	Updated for Schema 5.0
		Added Partial Auth (Both BINs) and Country Code Fraud Support (Salem Only).
		Clarified notes on ECP. Updated reference info for P-Card 2/3 & ISOCountryCodes.
		Updated Message Definitions and Response Codes.
3/14/11	Updated	Updated for Schema 5.1
		Added Account Updater Eligibility flag
05/17/11	Updated	Updated for Schema 5.2
		Added support for International Maestro
		Added support for EUDD Customer Profiles
		Added support for Gift Card Block Deactivations and Block Reactivations
08/16/11	Updated	Updated for Schema 5.3
		Added support for ECP for Bin 000002
		Added support for Extended ECP Action Codes and new ECP Auth Methods
10/31/11	Updated	Updated for Schema 5.4
		Added support for Safetech Fraud Analysis for Bin 000001
		Updated info on recurring ECP Authorization Methods
3/30/12	Updated	Added additional clarifications on Safetech Service
6/26/12	Updated	Updated for Schema 5.6
		Added support for Account Verification on International Maestro
		Added support for Purchasing Card 2/3 data for Discover for Bin 000001
		Clarified notes on UK Maestro and International Maestro
		Clarified notes on Security and Authentication
		Clarified notes on Purchasing Cards to reflect Commercial Card support
10/3/12	Updated	Updated various response code and proc status descriptions.
		Updated various grammatical clarifications and typos.
4/23/13	Updated	Updated for Schema 5.7
		Added support for Card Indicators / Enhanced Authorizations
		Updated various sections for additional clarification.
8/18/13	Updated	Updated for Schema 5.8
		Updates various sections for additional clarification.

Table of Contents

List of Examples

List of Tables

Chapter 1   Introduction

Chase Paymentech's Orbital Gateway is a proprietary XML Internet Processing System.

The XML Interface is supported for customers processing through the Salem and Tampa (PNS) platforms. The functionality of the interface is limited to what is possible based on each endpoint.

Chase Paymentech maintains two proprietary Authorization and Deposit platforms. The PNS platform, which is sometimes referred to as *the Tandem* or *Tampa*, is primarily targeted to Retail and smaller customers. The Salem platform, sometimes referred to as *the Stratus*, is primarily targeted to Card-Not-Present and larger customers. Despite the names, both systems are collocated in both Tampa, Florida and Salem, New Hampshire. Each platform has unique processing features, and, since Orbital supports both, the features available to merchants are based on the platform they are set up on.

The Gateway processes to both platforms using identical transaction information as presented in this specification, with the exception of any features that may only be available on one of the two platforms. Throughout this document, there are references to *BIN 000001* (Salem Platform) or *BIN 000002* (PNS Platform). Please contact your Technical Analyst or Relationship Manager if you are unsure which Platform your merchant account resides on.

The Chase Paymentech Orbital Gateway described in this document operates on the basis that a merchant initially instructs the Gateway to perform an operation on the merchant's behalf. Assuming that the initial operation is successful, the Gateway returns information that the merchant must use for all subsequent operations on the transaction in question. The Gateway manages the *transaction state* on behalf of the merchant. The merchant moves the transaction between the various possible states using the messages and fields defined in this document.

1.1   Virtual Terminal

The XML Interface is simply one of the optional interfaces into the Gateway. All transactions processed through the XML Interface will be visible, identifiable, and adjustable via the Virtual Terminal. All transactions processed this way will be identified with a source of XML in the Order History.

1.2   Certification

Before aggregators, software vendors, or merchants can process using this interface, the implementation must go through the appropriate certification process with Chase Paymentech. Please work with your Chase Paymentech Representative to schedule testing and certification as necessary.

Chapter 2 Processing Interface Description

2.1 Introduction

The Chase Paymentech Orbital Gateway API uses XML (Extensible Markup Language) to make eCommerce payment requests using HTTPS (Hypertext Transfer Protocol Secure). The Orbital Gateway XML Interface allows you to submit all transaction types supported by the Orbital Gateway, such as authorization, authorization and capture, prior authorization, capture, refund, void, inquiry, and an end of day (batch).

2.2 Address

Orbital Gateway certification system:

Primary: `orbitalvar1.paymentech.net/authorize` on port 443

Secondary: `orbitalvar2.paymentech.net/authorize` on port 443

Orbital Gateway production system:

Primary: `orbital1.paymentech.net/authorize` on port 443

Secondary: `orbital2.paymentech.net/authorize` on port 443

NOTES   Chase Paymentech exposes redundant hostname/port network endpoints to ensure high availability for the Orbital Gateway. To maximize availability, Developers should code to detect connectivity issues and HTTP errors, and temporarily switch to a failover URL. Failover to the secondary hostname/port must be automatic and completely transparent to the end-user. Communication with the primary hostname/port should be attempted periodically while in a state of failover.

Caching IP Addresses of Orbital Gateway servers is strongly discouraged. For load balancing and redundancy reasons, the Orbital Gateway processing is divided amongst multiple data centers. Therefore, the DNS service should be used to determine the destination IP address for each transaction.

While the certification system is available for testing at all hours, it is only monitored for availability during business hours (8:00am EST – 5:30pm EST Monday – Friday). In addition, the hardware in place is designed primarily for certification testing, not load testing. If there is a need to ensure uptime outside of normal business hours, please advise your Certification Analyst of the testing requirements.

2.3 Security

Given the inherent risks associated with processing transactions over the Internet, the Orbital Gateway requires both encrypted traffic to prevent interception of the payload and authentication of the source request generation. The next two sections define how the system manages that security.

2.3.1 Secure Sockets Layer Implementation Requirement

The XML Gateway URL must be accessed using the `https` protocol so that private information is transferred securely. This requires the client to use a SSL implementation. There are SSL implementations available for most programming languages.

It is the client's responsibility to gain the necessary expertise and technology to properly open a secure channel to the Gateway (unless the client uses one Chase Paymentech's available SDKs).

Interfacing to the Orbital Gateway using SSL does not require the client to have a certificate. The Orbital Gateway uses a non-authenticated SSL session, meaning the client is not authenticated using a digital certificate as a component of the SSL negotiation. See section *2.3.2* for information on how Chase Paymentech authenticates client traffic.

Non-SSL postings should never be made across a network that is external or not totally controlled and secure. If a clear text request is made to one of the Orbital Gateway URLs, the Gateway will return an error condition (an HTTP 403 error) with the accompanying XML payload containing a `ProcStatus 20403` error.

2.3.2 Authentication

The Orbital Gateway supports Connection Username/Password authentication for incoming requests. This means:

- The Username and Password are passed in the message payload. Each must match what is registered on the Orbital Gateway in order to process transactions in the Test or Production environments.

- An HTTP 412 error is returned for all activity wherein the Connection Username/Password is not registered in the Orbital Gateway. The accompanying XML payload contains a ProcStatus 20412 error (See *Table 15   Process Status and Process Status Message values* for more information).

- In addition, the Connection Username must be affiliated with the Client's Merchant IDs:

  - This allows Third-Party Hosting service organizations presenting on behalf of other merchants to submit transactions. However, each time a new customer is added, the merchant or third-party hosting organization must ensure that the new Merchant IDs or Chain IDs are affiliated with the hosting company's Connection Username.

  - If the merchant expects to have more than one merchant account with the Orbital Gateway, it should have its Connection Username affiliated at the Chain-level hierarchy within the Orbital Gateway.
    Each time a new Merchant ID (MID) is added, as long as it is placed within the same Chain, it will simply work. If it is not placed within the same Chain, the additional MIDs must be affiliated with the Connection Username. For example, we generally affiliate all Salem accounts (BIN 000001) with their Company Number (formerly called *MA #*), so all MIDs or Divisions under that Company are automatically affiliated.

- MID-Association Failures

  - If a Connection Username is registered, but the client presents a MID that has NOT been associated with the Username, the Orbital Gateway will return a `ProcStatus 20412`.

2.3.2.1   Connection Username/Password Format

The Orbital Connection Username and Password must be registered on the Orbital Gateway. Each are submitted within the message payload, under these corresponding elements:

- `<OrbitalConnectionUsername>`
- `<OrbitalConnectionPassword>`

The Connection Username and Password must follow specific formatting rules. Both Username and Password:

- Must be between 8–32 characters.
- Must contain at least 1 number.
- Must contain only standard English letters or digits (a-z, A-Z, 0-9).
- Cannot contain embedded spaces.

Additionally, the Connection Password is case-sensitive, while the Connection Username is not.

If additional information is needed, please contact your Technical Analyst or Account Representative.

NOTE   For existing merchants using IP-based authentication, please be advised that IP-based authentication and Connection Username/Password authentication are exclusive of each other. If a merchant is set up for both IP-based authentication and Connection Username/Password authentication, request messages are authenticated based on whether the Connection Username and/or Connection Password elements exist within the payload.

If either element does exist, the Orbital Gateway will attempt to validate the Username/Password values. If the authentication fails (for example, due to an invalid Password), the Orbital Gateway will NOT revert to IP-based authentication.

2.4   Message Specifications

2.4.1 Communication Protocol

The Chase Paymentech Gateway supports one method of communication: HTTPS. This method provides a *single-threaded* (or synchronous) model in which a merchant makes an HTTPS request to the Gateway and then blocks until the Gateway sends back the HTTPS response. While HTTPS is single-threaded, a single interface can make multiple HTTPS requests at once.

2.4.1.1   Posting to a URL

The Orbital Gateway will only provide responses to HTTP `POST` requests. The `POST` method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the `Request-URI` in the `Request-Line`. Orbital Gateway does not support `GET` requests.

2.4.2 XML Schema

The Orbital Gateway accepts and returns XML documents using XML Schema Definitions (XSD) that are defined by Chase Paymentech. The latest XSD published for interfacing with the Orbital Gateway is **PTI58**. There are separate request and response XSDs: `Request_PTI58.xsd` and `Response_PTI58.xsd`.

CAUTION   Versions PTI40 and above **are not backwards compatible** with XML documents created in DTD version PTI34 and earlier. All prior DTD versions are still supported, but require the `MIME-Header` to identify the version as PTI34 or lower. Any new functionality exposed after PTI34 requires coding to the new XSD specification.

This allows Chase Paymentech requests and responses to be easily interpreted and manipulated using the W3C (World Wide Web Consortium) DOM (Document Object Model) or SAX (Simple API for XML) APIs.

Additionally, errors or unexpected behaviors can result if any characters in the request payload do not match the character encoding specified in the request.

Most messages specify "UTF-8" encoding and contain ASCII characters. The Orbital Gateway also supports "ISO-8859-1" encoding. Commonly referred to as the Latin-1 character set, messages containing French, Spanish, or other special characters may require ISO-8859-1 encoding instead.

2.4.3　MIME Header

MIME (Multipurpose Internet Mail Extensions) is a mechanism for specifying and describing the format of Internet message bodies. The Orbital Gateway supports both the HTTP/1.0 and HTTP/1.1 MIME Header specifications for describing the message payload along with other information that allows it to process the incoming transaction request, as well as the outgoing reply.

2.4.3.1　Request MIME-Header Definition

Table 1 lists the elements within the `MIME-Header` for Orbital Gateway requests. The element names are NOT case-sensitive; the values associated to each element ARE. Further details for some of the elements are given in the sections below the table.

Table 1　MIME-Header elements for requests

Element	Description	Required*
MIME-Version	Should always be `1.0` or `1.1`.	M
Content-type	Defines the XML version number. See below for more details.	M
Content-length	This value defines the length of the Request XML Document.	M
Content-transfer-encoding	Defines the encoding of the associated XML document. Recommended encoding is `text`.	M
Request-number	Should always be `1`.	M
Document-type	Defines whether this is a Request or Response. This value should always be `Request`.	M
Trace-number	Retry Trace Number. See below for more details.	C
Interface-Version	Optional MIME-Header element that can be used by Chase Paymentech in production support. See below for more details.	O

*　M = Mandatory, C = Conditional, O = Optional.

2.4.3.1.1　POST/AUTHORIZE HTTP/1.0 Element

Although the request line is not part of the `MIME-Header` element, this value is static and always should be presented as `POST/AUTHORIZE HTTP/1.0`. The details are described as:

- HTTP Post: The Orbital Gateway will only provide responses to HTTP `POST` requests.
- URI: The Request URI for the Orbital Gateway will always be `Authorize`.
- HTTP version number: Provide the HTTP version number `1.0` or `1.1`.

2.4.3.1.2　Content-type Element

This `MIME-Header` element is used by the Client to identify which DTD version is being used for the XML Payload.

- The format for data for this element is `application/`*<XSD Version>*.
- The latest Version and recommended value is `PTI58`.
- As such, the recommended value for this field is `application/PTI58`.

CAUTION　Versions PTI40 and above **are not backwards compatible** with XML documents created in DTD version PTI34 and earlier. All prior DTD versions are still supported, but require the `MIME-Header` to identify the version as PTI34 or lower. Any new functionality exposed after PTI34 requires coding to the new XSD specification.

2.4.3.1.3   Retry Trace Number

This `MIME-Header` element is used in combination with the Merchant ID as the key transaction identifiers as related to Retry Logic. The Retry Trace Number element rules are:

- Data Type = Numeric
- Minimum Length = 1
- Maximum Length = 16
- Valid Values are from 1–9999999999999999
- Submitting an invalid value will result in an XML Quick Response with a `procStatus` Code of `9714`

2.4.3.1.4   Interface-Version

This `MIME-Header` element is used by the client to identify information about their implementation to assist Chase Paymentech in providing production support. This information will be logged distinctly for research purposes.

An example of the usage of this element would be that any Third-Party Software Provider should log their software name and version number in this field so that Chase Paymentech knows how the interface is being managed. Another example would be that a merchant could place information about their development version and implementation language in this element. Please work with your Certification Analyst to best identify what values should be used in this field.

2.4.3.2   Response MIME-Header Definition

Table 2 lists a sample of the elements within the `MIME-Header` for Orbital Gateway responses. This is not the all-inclusive list of `MIME-Header` response elements—**do not** code your system to support only these elements. Further details for some of the elements are given in the sections below the table.

Table 2   MIME-Header elements for responses

Element	Description	Required*
HTTP	See below for more details.	M
Date	Returns the Server Date and Time stamp; for example: `Fri, 27 Oct 2000 20:29:58 GMT`.	M
MIME-Version	Will always be `1.1`.	M
Content-type	Defines the XML version number. This will be an echo of what is submitted in the request.	M
Content-length	This value defines the length of the Response XML Document.	M
Content-transfer-encoding	Defines the encoding of the associated XML document.	M
Request-number	Should always be `1`.	M
Document-type	Defines whether this is a Request or Response. This value should always be `Response`.	M
Retry-Count	Identifies the number of times a response is returned. See below for more details.	C

Element	Description	Required*
Last-Retry-Attempt	Identifies the last previous retry response sent. The format of the data is: `YYYYMMDDhh(24)mmss` See below for more details.	C

* M = Mandatory, C = Conditional, O = Optional.

2.4.3.3 HTTP Responses

When successfully interacting with the Orbital Gateway, the HTTP value returned will always be a 200 response, such as `HTTP/1.0 200 OK`. All other responses indicate some sort of connection problem.

A HTTP 200 response in and of itself does not constitute a good response—it simply means that the connection has successfully been established with the Orbital Gateway.

SEE ALSO Please refer to RFC #2616 at www.w3.org/Protocols/rfc2616/rfc2616.txt for more information on the variety of HTTP responses that could be returned and their meaning.

2.4.3.4 Retry-Count

The purpose of this `MIME-Header` response element is to expose how frequently the Gateway has returned a particular response to your system. The first time a transaction is submitted to our system, the Retry-Count will be `0`. The first time a transaction is retried, the Retry-Count will be `1`.

If a value greater than `1` is returned, the Gateway is returning the same result many times for the same transaction. This can be an indicator that a customer is unintentionally replaying the same transaction or having trouble reading the result.

2.4.3.5 Last-Retry-Attempt

This `MIME-Header` response element is returned if the Retry Count ≥ 2. In other words, it will be returned as soon as a second Retry Response is sent and all others thereafter. It identifies the date and time of the last time a Retry Response for the associated Retry Trace Number and Merchant ID was returned. It is provided as an additional mechanism to ensure that the Retry function is behaving as expected.

Chapter 3   Functional Processing

This chapter defines the base transactions types of the XML Interface. More detailed definition of these transactions, data elements, and examples are provided in the XML message definitions.

3.1   Transaction Types

3.1.1 New Order

New Order is the transaction type for processing new orders. The following actions are permitted:

Authorization (Auth Only)   Authorize the supplied information, but do NOT create a settlement item. This transaction type should be used for deferred billing transactions.

Any transactions approved in this manner must be *marked for capture* in order to be settled. This can be done in the VT manually or via a Mark for Capture transaction.

SEE ALSO   See *3.1.4 Mark for Capture (MFC)* for information.

Authorization and Capture (Sale)   Authorize the supplied information and mark it as captured for next settlement cut. This transaction should be used for immediate fulfillment.

Force and Capture   Force transactions do not generate new authorizations. A *good* response simply indicates that the request has been properly formatted. The Orbital Gateway will settle the captured force during the next settlement event.

Refund (Return/Credit)   Instruct the Gateway to generate a refund based on the supplied information.

Refund via Transaction Reference Number   A Refund can be generated for a previous charge using the `TxRefNum` of the original transaction. If no amount is sent, the original transaction amount is refunded. If an amount is sent, that amount must be equal to or less than the original amount.

SEE ALSO   See *Chapter 4 Message Definition* for more details.

Complex Type Name

New Order Request   =   `NewOrder`

New Order Response   =   `NewOrderResp`

3.1.1.1   Profile Transactions in New Orders

The following are the Profile actions that can be executed in a New Order Transaction:

- Using Profiles for a New Order
  - One of the key transaction types is using a Profile to process a transaction.
  - Overriding Profile Data: Almost any data set in the Profile can be overridden (except card type) during a transaction that is using the Profile.

    For instance, if a Profile included a fixed amount, but a particular transaction was for a different amount, it could be changed for that transaction by including a specific amount in the request.

- Adding Profiles as part of a New Order transaction

  Given that, in many circumstances, an authorization needs to be performed the first time a customer is set up, the Orbital Gateway has extended the traditional Authorization transaction to enable adding a Profile in the same request.
  - Add profiles can be included with all New Order transaction types.

SEE ALSO   See *3.3.2 Profiles and Managed Billing* for more information.

3.1.2   Gift Card Transaction Types (formerly FlexCache)

Instead of using the New Order transaction type for creating new Gift Card transactions, the `FlexCache` transaction type must be used.

The following Gift Card transactional capabilities are supported:

- Card Activation:
  - Single Card Activation (including Prior Activation for PNS Merchants)
  - Block Activation
  - Block Deactivation (PNS Merchants only)
  - Block Reactivation (PNS Merchants only)
  - Deactivate
  - Reactivate
- Add Value (including Prior Add Value for PNS Merchants)
- Authorization
- Redemption (including Prior Redemptions for PNS Merchants)
- Redemption Completion
- Refund
- Balance Inquiry
- Void

Gift Card transactions can also be voided by submitting a Reversal transaction request. See *3.1.5 Reversal (Void a Previous Transaction)* for further details.

Complex Type Name

FlexCache Request	=	`FlexCache`
FlexCache Response	=	`FlexCacheResp`

3.1.3 Profile Transaction Types

This transaction type allows for the following profile actions (see *3.3.2 Profiles and Managed Billing* for details):

- ⬡ Add a Profile
- ⬡ Delete a Profile
- ⬡ Update a Profile
- ⬡ Retrieve a profile

Complex Type Name

Profile Requests   =   `Profile`

Profile Response   =   `ProfileResp`

3.1.4 Mark for Capture (MFC)

Mark a previously authorized transaction as being ready to be submitted for clearing. The Mark for Capture transaction type is present for future fulfillment models. A transaction can be authorized now and marked for capture at any time in the next four months.

CAUTION Authorization of certain payment options will age off after a number of days. Visa applies a window of 7 days, and MasterCard, Discover, and Amex each apply a window of 30 days. Gateway will perform an automatic re-authorization at the time of settlement if an auth is aged off.

The Mark for Capture can be for any amount less than or equal to the original authorization. If the amount is less than the original auth, this is treated as a split transaction.

The split transaction also results in the creation of a new order for the balance left over from the original authorization. Adjustments to the original transaction, such as Level 2 and 3 data or amount, are also made, as required. Upon marking a portion or the remainder of the split transaction, the system will automatically attempt to obtain a new authorization for the new order.

This concept is illustrated in Example 1.

Complex Type Name

Mark for Capture Request   =   `MarkForCapture`

Mark for Capture Response   =   `MarkForCaptureResp`

Example 1   Split Shipment flow

TRANSACTION AMOUNT

$20	$20	$20	$20	$20

1. Original Authorization Request Sent by Merchant $100 USD

1a.There is a Marked for Capture or an Unmarked transaction for $100

2. Merchant sends Marked for Capture (MFC) for $20

2b. System Authorization Reversal (Visa Only): $80

2a. Original $100 Trans. MFC for $20

2c. New *Unmarked* order systemically created for remainder of original order amount: $80

3. Merchant sends MFC for $30

3c. New *Unmarked* order systemically created for remainder of split: $50

3a. System performs Auth request for $30

3b. Unmarked $80 transaction now MFC for $30

4. Merch. sends MFC for $10

4c. New *Unmarked* order systemically created for remainder of split: $40

4a. Syst. Performs Auth for $10

4b. Unmkd $50 now MFC for $10

5. Merchant sends MFC for $40

5a. System performs new Auth request for $40

5b. Unmarked $40 now MFC for $40

TRANSACTION KEY:

- **- Authorization Request**
- **- Marked Transaction**
- **- Mark for Capture [MFC] Request**
- **- Unmarked Transaction**

3.1.5 Reversal (Void a Previous Transaction)

This transaction is for voiding a previous transaction, either in the full amount or partial amount. It can be extended to also reverse the original authorization at the issuer.

A void, in and of itself, does not reverse the original authorization for any card type other than Gift Card and PINless Debit. When extending the void request to include an authorization reversal, the hold on the accountholder's open-to-buy (line-of-credit), which was reserved by the original authorization, is freed up. It is important to note that it is at the Issuer's discretion whether or not to remove the hold.

Merchants have two options for processing an authorization reversal.

- The first option allows merchants to control when an authorization reversal is performed by submitting the Online Reversal Indicator element in the Reversal message. A value of `N` or `NULL` indicates that a void is being requested. A value of `Y` extends the void request to also include the authorization reversal.

    CAUTION   In the event a message contains the Online Reversal Indicator and the authorization reversal does not succeed, the transaction will remain in its prior open state.

- The second option is to allow the Gateway to submit the indicator on behalf of the merchant by setting a flag on the Administrative menu in Virtual Terminal. When a Reversal request is received, the Gateway will attempt an authorization reversal wherever applicable. In the event the original authorization doesn't meet the requirements for an authorization reversal or an error occurs while attempting an authorization reversal, the Gateway will perform a void instead.

    WARNING   Submitting the Online Reversal Indicator within a Reversal message will override the Gateway setting.

The following requirements must be met in order to perform a void:

- Transaction must not have been settled.
- Transaction Reference Number from the response message of the original request must be provided. If the Transaction Reference Number is not known, merchants can submit in its place the Retry Trace Number of the original request within the `<ReversalRetryNumber>` element.
- Full or a partial amount must be submitted. A void for a partial amount creates a split of the original transaction into two components. A voided transaction in the amount of the partial void request and the remainder of the previous transaction in the same state the full amount was previously in (Authorized or Marked for Capture).

The following authorization reversal requirements are in addition to (or override) the void requirements:

- Original authorization must have been obtained through Chase Paymentech, or the transaction will decline.
- Original authorization cannot be greater than 72 hours old.
- Reversal must be for full amount that was received in the authorization.
- Authorization Reversals for *BIN 000001* and *BIN 000002* is supported by:
  Visa, MasterCard, MasterCard Diners, Discover

SEE ALSO   For more information about the implementation of Retry Trace Numbers, please see *3.3.3 Retry Logic*.

Complex Type Name

Void Request   = Reversal

Void Response   = ReversalResp

3.1.6 End of Day

An *End of Day* request/response instructs the Gateway to submit all transactions previously marked for capture (including all successful refunds) for clearing.

Alternative End of Day methodologies include:

- **Auto-Settle** At a Merchant ID level, an account can be set up to settle automatically at any given 15-minute increment during the day and in any US-based time zone.
- **Virtual Terminal** End of Day settlement can be triggered using the Orbital Virtual Terminal as many times as desired. Please see the *Virtual Terminal User Manual* for instructions.

Complex Type Name

End of Day Request   =   EndOfDay

End of Day Response =   EndOfDayResp

3.1.7 Inquiry

An Inquiry transaction returns the response of any specified request. This is useful when a merchant needs to know the result of a transaction in the case of, for example, a communication error or unexpected result. An InquiryRetryNumber value, which corresponds to the Retry Trace Number of the originating transaction, must be passed in the Inquiry request message in order to obtain the response. If there is no matching result, an error message is returned. Similar to the Retry Trace Number, the Inquiry Retry Number is valid within a 48-hour window from the time of the original transaction.

The basic process flow for an Inquiry is as follows:

1. A transaction is submitted with a Retry Trace Number and Merchant ID in the request.

2. The merchant does not receive a response and subsequently submits an inquiry using the Retry Trace Number (as the Inquiry Retry Number) and Merchant ID.

3. The Gateway validates the Inquiry Retry Number and Merchant ID to determine if it has processed a transaction using that value pair within a 48-hour window.

4. The Gateway returns the transaction response details for the original request, if the transaction was found.

SEE ALSO   For more information about the implementation of Retry Trace Numbers, please see *3.3.3 Retry Logic*.

Complex Type Name

Inquiry Request   = Inquiry

Inquiry Response = InquiryResp

3.1.8 Quick Response

When a transaction has an error condition, such as a time out condition or a poorly formed message request, the gateway will generate a quick error message back to the requestor. This error response takes the form of a "Quick Response".

Complex Type Name

Quick Response   = `QuickResp`

3.1.9 Account Updater

This transaction is used to supplement the Account Updater service for customer profiles on a one-off exception basis. Please see section *3.3.4 Account Updater* for more details.

Complex Type Name

Account Updater Request   =   `AccountUpdater`

Account Updater Response =   `AccountUpdaterResp`

3.1.10 Safetech Fraud Analysis

This transaction is used to submit a standalone Fraud Analysis request to the Safetech service, without submitting the transaction to the customer's issuing bank for financial approval.

Please see section *3.3.6 Safetech Fraud Tools* for more details.

Complex Type Name

Fraud Analysis Request   =   `SafetechFraudAnalysis`

Fraud Analysis Response   =   `SafetechFraudAnalysisResp`

3.2   Methods of Payment

3.2.1 Credit Card

3.2.1.1   Cardholder Authentication (Card Not Present)

3.2.1.1.1   Address Verification

Address Verification, also known as *AVS*, is a cardholder authentication mechanism available to merchants. In addition to providing merchants with an additional risk management tool, it is required by Visa and MasterCard to qualify for the lowest interchange rates and protects against certain chargeback conditions. As such, it is highly recommended by Chase Paymentech that all transactions include this information.

Some key points regarding AVS are:

- The minimum required data for AVS is the cardholder's billing postal code.
- AVS is only supported by credit cards issued in the United States, Canada, and the United Kingdom.
- For both Salem and PNS/Tampa-routed accounts (BINs 000001 and 000002), the Orbital Gateway accepts postal codes formatted as alpha-numeric with a length between 1 and 10 bytes. These postal codes are forwarded to the respective authorization hosts for approval.

Table 3   ZIP/Postal Code formats

U.S. ZIP Code	Canadian Postal Code*	U.K. Postal Code*
NNNNN NNNNN-NNNN	ANA NAN ANANAN	AN NAA ANA NAA ANN NAA AAN NAA AANN NAA AANA NAA

*   N = numeric; A = alphabetic

Table 4   Cards supporting AVS

U.S. AVS	Canadian AVS	U.K. AVS
Visa MasterCard MasterCard Diners American Express Discover	Visa MasterCard MasterCard Diners American Express	Visa UK Maestro/Solo American Express

3.2.1.1.2   Card Verification Numbers

The Orbital Gateway supports the submission of Card Verification Numbers for the methods of payment for which this feature is available.

Guidelines for Populating Card Security Fields

The two fields used for submitting Card Security information in the XML interface are:

- `CardSecValInd`
- `CardSecVal`

Visa CVV2/MasterCard CVC2/Discover CID Programs

The Orbital Gateway supports Visa's CVV2 (Card Verification Value 2), MasterCard's CVC2 (Card Validation Code 2) and Discover's CID (Card ID) fraud reduction programs. This section provides some background information on supporting these programs.

The value for these cards is 3 digits. It can be found on the signature panel on the reverse side of the credit card and is represented by the three digits following the account number.

This value **cannot be stored** at all—not even for future transactions—as it is against regulations to do so.

The use of this value provides an important security check because only the individual in possession of the actual credit card can provide the value to the merchant. Statistics validate that those individuals who may know the account number, but are not in possession of the actual credit card, perpetrate much of the fraud occurring in the non-face-to-face environment.

When a merchant collects this value and passes it in the authorization request, Chase Paymentech passes this data through the authorization system to the card issuer. In the authorization response, the card issuer validates the accuracy of the CVV2/CVC2/Discover CID value for the specific card. Used in conjunction with the valid expiration date, this service provides a valuable tool for assessing whether the true cardholder has placed the order with the merchant for their services or product.

American Express CID Merchant Processing Requirements

American Express provides a similar program to Visa, MasterCard, and Discover, but with a few key differences:

- The value for these cards is 4 digits and is printed, not embossed, on the front of all cards. On the American Express card it appears on the right border of the card. On Optima cards, however, it appears on the left border of the card.
- In situations where the CID value is invalid, American Express could respond with an authorization decline message.

Gift Card Requirements (formerly FlexCache)

The Chase Paymentech Gift Card program (formerly known as FlexCache™) supports CVD2 (Card Verification Data 2), which is also known as a PIN, as an optional feature determined by the merchant. The four-digit value may be imprinted on the back of the stored value card and can be used to facilitate a secure Card-Not-Present transaction when the consumer wishes to use a Gift Card as their method of payment.

3.2.1.1.3   Account Verification

Account Verification provides the ability to verify accounts without financially impacting the accountholder's open-to-buy. Address Verification Service (AVS) and Card Security Value can be verified along with the account number.

Some key points regarding Account Verification messages are:

- New Order request must be used.
- Transaction type must be an Authorization Only.

- Amount must be `0`.
- AVS Zip is mandatory for American Express, otherwise optional.
- Card Security Value is optional.
- All existing mandatory fields must be submitted.

Supported Currencies

Account Verification is supported in all currencies

Platforms

BIN 000001 (Salem): Visa, MasterCard, MasterCard Diners, International Maestro

BIN 000002 (Tampa): Visa, MasterCard, MasterCard Diners, Discover, American Express

3.2.1.1.4   Verified by Visa/MasterCard SecureCode Programs

Verified by Visa and MasterCard SecureCode are both solutions designed to authenticate cardholders when paying online. These products offer a mechanism for securing the Internet channel by strongly authenticating the cardholder at the point of interaction by providing a unique transaction-specific token that provides evidence that the cardholder originated the transaction.

How it Works

Verified by Visa

Verified by Visa® is based on the 3-D Secure Protocol, which uses Secure Sockets Layer (SSL) encryption to collect and protect payment card information transmitted via the Internet. It uses three domains for the authentication process:

- **Issuer Domain**   Where the Issuer is responsible for determining whether authentication is available for the card account presented in a purchase.
- **Acquirer Domain**   Where the Acquirer accepts Internet transaction data from the merchant and passes it to Visa.
- **Interoperability/Visa Domain**   This is operated by Visa, where transaction information is exchanged and stored using 3-D Secure as the common protocol.

Transaction Flow

1. The cardholder shops at participating Internet Merchants with no changes to the shopping or checkout. The cardholder selects the merchandise to be purchased and proceeds to the checkout. At the checkout, the cardholder may complete the purchase and payment information in a variety of ways, including self-entered and electronic wallet, Merchant one-click, or using other checkout capabilities.

2. After the purchase and payment information is entered, the cardholder selects the *buy* button. This activates the Merchant Server Plug-In (MPI) software application, which checks its local cache to determine if the Visa Issuer BIN participates in Verified by Visa.

    - If the BIN is participating, the MPI generates an inquiry to the Visa Directory Server to determine if the cardholder's account is enrolled in Verified by Visa. The Visa Directory Server sends a Verify Enrollment Request message to the Issuer Access Control Server (ACS) to determine if authentication is available for the cardholder's account number. The Visa Directory Server sends the Issuer ACS response to the MPI.

        - If authentication is not available, the merchant server receives an `authentication not available` message and returns the transaction to the merchant's commerce server to proceed with a standard Authorization request.

- ▪ If authentication is available, the message response provides the URL for the Issuer ACS where the cardholder can be authenticated. The MPI sends a message and script directing the cardholder's browser to establish a pop up session with the Issuer ACS.

3. The browser directs the transaction to the URL specified for the Issuer ACS, creating an SSL session. The Issuer ACS displays an inline Web page to the cardholder. The page includes Issuer-specific and Visa branding, transaction details (including Merchant name and sale amount), and prompts the cardholder to enter their password.

- ◆ The cardholder is allowed a limited number of password attempts, typically 3–5, as defined by the Issuer ACS.
  - ▪ If unable to correctly enter the password, the cardholder may access the password hint that was established during the registration.
  - ▪ If the password is entered correctly, the transaction continues.
- ◆ If the cardholder is not registered, the ACS briefly displays a processing window and the transaction continues as an attempted authentication.
- ◆ If the password is incorrectly entered more times than the Issuer limit, the failed Payer Authentication Response is returned to the merchant.

4. The Issuer ACS retrieves the authentication information and compares it against the data that was registered during the initial registration process. If the data matches, a success page is presented to the cardholder, and the Issuer ACS sends a message through the browser to the merchant, thus providing evidence of cardholder authentication. Using the Issuer's encryption keys and transaction data, the Issuer server calculates the Cardholder Authentication Verification Value (CAVV), which will be included with the Electronic Commerce Indicator (ECI), as provided at the time of authentication by the MPI, in the response to the merchant.

5. The Issuer ACS creates, digitally signs, and sends a Payer Authentication Response to the cardholder's browser and sends transaction information to the Visa Authentication History Server (AHS) for storage. All Payer Authentication Response messages—successful, unable to authenticate, failed, and attempted authentications—are transmitted and stored in the AHS. The browser routes the Payer Authentication Response back to the MPI, which validates the digital signature in the response, verifying that it is from a valid participating Issuer. If the digital signature is verified and the Issuer has sent an approved Payer Authentication Response, the cardholder is deemed authenticated and the MPI returns the transaction to the storefront software. The merchant starts processing the order, determining whether it can be fulfilled and calculating taxes and shipping for the total transaction amount.

6. The merchant sends the CAVV and an ECI of 5 (`authenticated transaction`) or 6 (`attempted authentication`) to the Orbital Gateway. The CAVV must be sent in Base 64 encoding within the XML Document. If the CAVV is not submitted in Base 64 encoding or if the CAVV is sent with a non-eCommerce transaction, a response code of 37 will be returned in the XML `<RespCode>` element.

7. Chase Paymentech passes the CAVV and ECI along to Visa with the authorization request. These fields are used during authorization processing to verify that authentication, or attempted authentication, was performed and to qualify for the eCommerce Customer Payment Services.

8. The Issuer receives the authorization request, validates the CAVV, and responds with a CAVV Response Code (or `<CAVVRespCode>` within the XML response document), as well as an approval or a decline of the authorization. If the CAVV does not match, the Issuer should decline the transaction.

Visa has not implemented any new decline codes for Verified by Visa. The standard decline codes should apply.

NOTE   A merchant may not submit for authorization a purchase transaction that has failed authentication.

MasterCard SecureCode

MasterCard SecureCode® is a solution designed to authenticate cardholders when paying online. SecureCode offers a mechanism for securing the Internet channel by strongly authenticating the cardholder at the point of interaction by providing a unique transaction-specific token that provides evidence that the cardholder originated the transaction.

- SecureCode uses MasterCard's Universal Cardholder Authentication Field (UCAF) infrastructure to communicate the authentication information among the cardholder, Issuer, merchant, and Acquirer.

- MasterCard SecureCode supports the 3-D Secure Protocol (same as Verified by Visa). MasterCard SecureCode requires merchants to install a 3-D Secure v1.0.2-compliant Merchant Server Plug-in (MPI) software.

NOTE   For additional information on using MasterCard SecureCode with International Maestro transactions, please also see *section 3.2.8 International Maestro*

Transaction Flow

1. The cardholder shops at a participating SecureCode Internet Merchant with no changes to the shopping or checkout. The cardholder selects the merchandise to be purchased and proceeds to the checkout. At the checkout, the cardholder may complete the purchase and payment information in a variety of ways, including self-entered and electronic wallet, Merchant one-click, or using other checkout capabilities.

2. After the purchase and payment information is entered, the cardholder selects the *buy* button. The customer shopping experience is the same for both of the Issuer platforms up until the time that the Merchant Order Confirmation page is displayed.

3. The MPI activates and checks its local cache and the MC Directory Server to determine if the customer card number is part of a participating MasterCard SecureCode BIN range.

   - If so, a Verify Enrollment Request message is sent from the MPI to the MC Directory Server and forwarded to the Issuer Access Control Server (ACS) to determine if authentication is available for the cardholder's account number. The MC Directory Server sends the ACS response to the MPI.

     - If authentication is available, the message response provides the Web address for the Issuer ACS where the cardholder can be authenticated.

     - If authentication is not available, the merchant server receives an `authentication not available` message and returns the transaction to the merchant's commerce server to proceed with a standard Authorization Request. Similar to Verified by Visa, there is an `attempted SecureCode` transaction type (`ECI = 6`).

4. The MPI sends a message and script directing the cardholder's browser to establish an inline Web page session with the Issuer ACS. The window displays Issuer-specific and MasterCard branding, transaction details, including merchant name and amount, and prompts the cardholder to enter their SecureCode (password).

   - The cardholder is allowed a limited number of password attempts, typically 3–5, as defined by the Issuer ACS.

     - If the password is entered correctly, the transaction continues.

- ▪ If unable to correctly enter the password, the cardholder may access the password hint that was established during the registration.
  - ◆ If the password is incorrectly entered more times than the Issuer limit, a failed Payer Authentication Response is returned to the merchant.

5. The Issuer ACS retrieves the authentication information and compares it against the data that was registered during the initial cardholder registration process. If the data matches, a success page is presented to the cardholder and the Issuer ACS sends a message through the browser to the merchant providing evidence of cardholder authentication, including a 28-byte Account AAV. This AAV is generated cryptographically using Issuer-specific secret keys that are synchronized with keys at the Issuer's authorization platform.

6. The merchant then sends the transaction to Chase Paymentech, along with the 28-byte AAV in Base 64 encoding, within the Orbital Gateway XML Interface Specification.
   - ◆ If the AAV is not submitted in Base 64 encoding or if the AAV is sent with a non-eCommerce transaction, a response code of `37` will be returned in the XML `<RespCode>` element.
   - ◆ If the Merchant has not tested and certified with Chase Paymentech to participate in MasterCard SecureCode and an AAV is sent with the e-Commerce transaction, a response code of `38` will be returned in the XML `<RespCode>` element, which indicates the merchant should contact their Chase Paymentech Representative to become SecureCode enabled.

7. Chase Paymentech forwards the transaction, including the AAV in the MC authorization request. The Issuer receives the authorization request, validates the AAV, and responds with an approval or a decline of the authorization. If the AAV does not match, the Issuer should decline the transaction.

MasterCard has not implemented any new decline codes for SecureCode. Standard decline codes apply.

Merchant Requirements

Merchant Plug-in Software

Install a Certified 3-D Secure Merchant Plug-in Software Application or code to the 3-D Secure Protocol.

Verify that the Merchant Plug-in will provide the CAVV and or AAV in Base 64 encoding before sending to Chase Paymentech. If not, merchants must convert to Base 64 before sending to Chase Paymentech.

Business Rules

There are a number of business rules related to when a CAVV and/or AAV should be presented on aged transactions, reauthorizations, split transactions, and so on. The Orbital Gateway abstracts your interface from many of these issues. Table 5 outlines what these rules are and what is necessary to understand from an interface perspective.

Table 5   Business rules

Rule subject	Description
Authorizations	▪ Merchants are required to request authorization for all Verified by Visa and MasterCard SecureCode eCommerce transactions. ▪ Merchants must supply the CAVV and ECI on all Visa authorization attempts and the AAV on all MasterCard Authorization attempts.
Failed Authentications	▪ Merchants are prohibited from submitting transactions for authorization that have failed authentication.
Late Fulfillment	▪ When a participating merchant splits the shipment of an order, each authorization component may be submitted with the authentication data (ECI of 5 or 6 and the CAVV or AAV) of the original purchase. ▪ In the event of a dispute, the Acquirer must be able to establish that the authorization requests were related to a single customer authenticated purchase. ▪ Furthermore, if a deposit/settlement record is sent for the subsequent shipment, the authorization will already have been tagged as *used*. Therefore, in order to receive the full benefit of Verified by Visa and MC SecureCode, a merchant must send the authentication data with the subsequent deposit/settlement record so that, when Chase Paymentech reauthorizes, the authentication data can be sent as well. **MasterCard SecureCode** ▪ Initial SecureCode authorization requests with AAVs older than 30 calendar days may be declined by the Issuer.
Recurring Transactions	▪ When a participating merchant offers services of an ongoing nature to a cardholder for which the cardholder pays on a recurring basis (for example, insurance premiums, subscriptions, Internet service provider fees, membership fees, tuition, or utility charges), the cardholder payments are considered recurring payments. ▪ If the first payment originated as an Electronic Commerce Transaction via the Internet, it must be submitted with the appropriate Electronic Commerce Indicator (ECI) value, including Verified by Visa or MasterCard Secure Code authentication data (CAVV or AAV respectively), if applicable. ▪ All subsequent payments must be submitted as Recurring transactions. The merchant must not store and submit the CAVV with any subsequent transaction.
Currencies Supported	All Currencies.

Chargeback Liability Shift Exclusions

Verified by Visa

The exclusions from the Chargeback provisions related to attempted authentications are:

- All Visa Commercial Cards (Visa Business, Visa Purchasing and Visa Corporate Cards), anonymous Prepaid Cards (such as gift cards), and transactions from new channels (such as mobile devices) are excluded from chargeback protections for attempted authentications.

  If these cards are enrolled in Verified by Visa and the Issuer authenticates the cardholder, the Issuer is not permitted to submit a chargeback for unauthorized usage disputes (reason codes 23, 61, 75, and 83).

Either the Issuer ACS or Visa may designate excluded transactions; however, the Visa Directory Server will override excluded responses from an Issuer ACS if the BINs are not also designated as excluded BINs in the Visa Directory. The designation of BINs as Commercial or anonymous Prepaid Cards must be consistent with VisaNet.

🌀 Transactions conducted in new channels (such as mobile or wireless devices).

Merchants named in the Global Merchant Chargeback Monitoring Program are not eligible for Chargeback protection for attempted authentications during the time that they are required to participate in the program and three months thereafter. Visa will work with Acquirers to ensure compliance with this requirement. There are no additional steps for Issuers regarding this provision.

3.2.1.2   Level 2 and Level 3 Data

These additional data fields are typically used in a business-to-business environment. Merchants have the ability to collect funds in conjunction with the settlement of procurement credit card transactions, while providing consumers with line item detail. This affords a cleaner process for both the merchant and the consumer.

The Orbital Gateway supports the processing of procurement cards, including enhanced data required by various card associations.

🌀 Salem and PNS merchants:

Visa and MasterCard: Level 2 and Level 3 Data

🌀 Additionally for Salem merchants:

Discover Level 2 and Line Item Detail

American Express Level 2 and Transaction Advice Addenda (TAA)

NOTE   Level 2 and Level 3 data sets were initially supported for the subset of procurement cards known as Purchasing Cards. Orbital Gateway expanded that support to include the superset of procurement cards known as Commercial Cards. Purchasing and Commercial Cards should not vary with respect to Level 2 and Level 3 requirements. To maintain support of legacy integrations, Level 2 and Level 3 data elements are referenced in this API as Purchasing Card data.

3.2.1.2.1   Edit Checks

The Orbital Gateway performs edit checks on incoming data to ensure necessary information is present. In the event necessary information is missing from a transaction, the transaction will result in an error. Data fields that are edited by Chase Paymentech have been marked as *Conditionally Required* in *Chapter 4 Message Definitions*. Additionally, there are some special edit checks specific to each host described below.

PNS

There are two key mathematical data validations specific to PNS processing for Level 3 Processing:

🌀 The amount field (`<PC3Dtllinetot>`) of every line item must equal the Unit Cost (`<PC3DtlUnitCost>`) multiplied by the quantity (`<PC3DtlQty>`) less any discounts (`<PC3DtlDisc>`). If it does not, then this transaction will receive an error.

♦ `<PC3Dtllinetot>` = (`<PC3DtlUnitCost >` * `< PC3DtlQty >`) - `< PC3DtlDisc >`

🌀 Additionally, the sum of all the Line Item totals (`<PC3Dtllinetot>`) cannot exceed the transaction amount (`<Amount>`) submitted for an order.

♦ `<PC3Dtllinetot>` ≤ `<Amount>`

Salem

There is no mathematical validation for Level 2 or 3 for Salem customers.

However, it should be noted that the Salem host requires that transactions with attached Level 3 data must actually be Commercial Cards or Purchasing Cards. The Salem host will reject any transaction at settlement if Level 3 data is submitted on an unsupported card.

3.2.1.2.2   BIN Ranges

The BIN range assigned by the card associations can identify purchasing cards or commercial cards. BIN ranges are subject to change at the discretion of the card associations.

3.2.1.2.3   Processing

Level 2 or Level 3 data can either be sent with the original auth (via an Auth or Auth-Capture) or appended to the transaction via the Mark for Capture request, if it was not originally supplied in the authorization request.

There are different rules for adding and adjusting the data via the Mark for Capture, based on whether it is simply Level 2 data or if it is Level 3 data.

Level 2 can be sent with Sales and Refunds for both Salem and PNS merchants. Level 3 can be sent with Sales and Refunds for Salem merchants, but only on Sale transactions by PNS merchants.

MFC Adjustment of Level 2 Data

Level 2 data is supplied on either the Authorization request, in the Mark for Capture (MFC) request, or adjusted via the MFC request. The following describes four options and the associated behaviors:

- Level 2 data is only submitted with the Authorization:
    - At settlement, the Orbital Gateway uses the data presented with the Auth request.
- Level 2 Data is submitted with both the Authorization and a Mark for Capture (MFC) request for the full amount of the Authorization:
    - The data submitted with the MFC supersedes the data in the Auth in its entirety.
- Level 2 Data is submitted with both the Authorization and a Mark for Capture (MFC) request for a partial amount of the Authorization:
    - A split transaction is generated. By default, the data submitted in the first MFC is used on all subsequent splits. Each additional MFC may supersede this data with relevant Level 2 data if desired.
- Level 2 Data is only submitted with the MFC
    - At settlement, the Orbital Gateway uses the data presented with the MFC request.
    - If the amount of the MFC is less than in the authorized amount, as described above, a split transaction is generated. By default, the data submitted in the first MFC is used on all subsequent splits. Each additional MFC may supersede this data with relevant Level 2 data if desired.

MFC Adjustment of Level 3 Data

Just as with Level 2 Data, Level 3 data may be supplied on the Authorization request, in the Mark for Capture (MFC) request, or adjusted via the MFC request. The same scenarios apply as listed above.

Additionally, PNS based amount validations are still applied when Level 3 data is supplied on MFC, and when a transaction using Level 3 data is split. Split transactions must have Level 3 data modified accordingly, or the Mark for Capture request fails.

Additional Information

Each card brand has subtle differences in the data requirements to properly qualify for Level 2 and Level 3 transactions. There are also a few differences in data formats between our Salem and PNS hosts. These are identified in the Chapter 4 message definitions, and in the Appendix summary tables. Please see *5.3.3Appendix C: Level 2 & 3 Data Reference* for further information.

Virtual Terminal

All of the functionality supported through this interface for Level 2 and 3 is additionally available through the Orbital Gateway Virtual Terminal.

3.2.2   European Direct Debit

European Direct Debit (EU DD) is a popular method of payment for merchants marketing in Europe. While any merchant may want to accept direct debit payments, it is most important and cost effective for those merchants collecting recurring payments. Unlike in the US, many EU customers prefer to pay for recurring services by direct debit to their bank accounts. This is especially true in Germany, where almost 40% of all electronic payments are made by direct debit.

3.2.2.1   How it Works

In Europe, each country operates its own direct debit network. Merchants wishing to accept direct debit throughout Europe would face the requirement to establish banking relationships and technical integration for each country in which they wish to market. Chase Paymentech Solutions has created a single technical interface for direct debit processing for multiple countries.

3.2.2.2   Processing Requirements

Merchants must contract with Chase Paymentech Solutions for acceptance of European Direct Debit. The Merchant Descriptor is defined on the vendor's system. Sending the Merchant Descriptor record does not alter the descriptor on the accountholder's statement.

The purpose of this document is to outline how a developer can code to take advantage of this method of payment within the Orbital Gateway, both in terms of the message layout and the business rules.

3.2.2.3   Virtual Terminal

All of the functionality supported through this interface for European Direct Debit is additionally available through the Orbital Gateway Virtual Terminal.

3.2.2.4   Platforms

The Orbital Gateway only supports the European Direct Debit method of payment through the Salem host platform (BIN 000001). This method of payment is not supported on the PNS host (BIN 00002).

3.2.3   Gift Card (formerly FlexCache)

The Orbital Gateway supports Chase Paymentech's proprietary Gift Card product (previously called FlexCache™) for both Salem and PNS customers.

3.2.3.1   Transaction Types

This section defines all the Gift Card transaction types supported by the Orbital Gateway.

NOTE   While the official name of the product is no longer FlexCache, certain XML tags and messages may still reference FlexCache for the time being.

3.2.3.1.1   Card Activation

Table 6   Card Activation transaction types

Transaction Type	Description
Activate	This transaction is used to activate one individual card for the first time.
	Merchants processing to the PNS Host can process Prior Activation transactions by additionally passing the correct prior approval code. If the valid Prior Approval code is not passed, it is treated as a new Activation request.
	Salem Merchants attempting to process a Prior Activation receive an error response.
Block Activate	Block activation provides for the ability to activate more than one card at a time. The maximum number of cards that can be activated at a time is 100. Within the Activate request, the card number of the first card in a series is defined, plus the number of additional sequential cards.
	If a Block Activation fails, none of the cards in the block are activated. The first card number that caused the Block Activation failure will be returned in the response.
	The Virtual Terminal supports the ability to perform a Block Activation of 10,000 in a single request. However, as indicated above, the online interface maximum is only 100 cards per request.
Deactivate	This transaction is for the deactivation of a live card. Passing an amount is not required for this transaction type.
Block Deactivate	Block deactivation provides for the ability to deactivate more than one card at a time. The maximum number of cards that can be activated at a time is 100. Within the Deactivate request, the card number of the first card in a series is defined, plus the number of additional sequential cards.
	If a Block Deactivation fails, none of the cards in the block are deactivated. The first card number that caused the Block Deactivation failure will be returned in the response.
	The Virtual Terminal supports the ability to perform a Block Deactivation of 10,000 in a single request. However, as indicated above, the online interface maximum is only 100 cards per request.
	Block Deactivations are only supported on the PNS host at this time. Salem Merchants attempting to process a Block Deactivation receive an error response.
Reactivate	There are two mechanisms for reactivating a card once it has been deactivated: ▪ Reversing the deactivation transaction. This returns the card to the same balance prior to the deactivation transaction. ▪ The card can be reactivated. In a reactivation transaction, a dollar amount must be passed, indicating how much the card should be reactivated for.

Block Reactivation	Block reactivation provides for the ability to reactivate more than one card at a time. The maximum number of cards that can be activated at a time is 100. Within the Reactivate request, the card number of the first card in a series is defined, plus the number of additional sequential cards.
	If a Block Reactivation fails, none of the cards in the block are reactivated. The first card number that caused the Block Reactivation failure will be returned in the response.
	The Virtual Terminal supports the ability to perform a Block Reactivation of 10,000 in a single request. However, as indicated above, the online interface maximum is only 100 cards per request.
	Block Reactivations are only supported on the PNS host at this time. Salem Merchants attempting to process a Block Reactivation receive an error response.

NOTE   The Orbital Gateway supports $0 activation transactions for PNS (BIN 000002).

3.2.3.1.2   Add Value

This transaction type adds value to an active card. If an Add Value is performed on an inactive card, it both activates the card and performs the add value action.

Merchants processing to the PNS Host can process Prior Add Value Transactions by additionally passing the correct prior approval code. If the valid Prior Approval code is not passed, it is treated as a new Add Value request.

Prior Add Value transactions are not supported on the Salem system; therefore, Salem merchants attempting to process a Prior Add Value will receive an error response.

3.2.3.1.3   Purchase and Refund Transactions

The following transaction types are for purchases and refunds. There are two different transaction combinations available for purchases:

- Authorization, followed by a Redemption Completion. This transaction combination is only valid for Salem-based customers.
- Redemption.

These two combinations allow for different purchase processing behavior on Gift Cards. The following sections define how each transaction type functions.

Authorization

Almost all Gift Card transaction types immediately affect the card balance, meaning they add or reduce the funds based on the result. In some circumstances, there might be a desire to perform a sale wherein an authorization is performed, and the funds are not actually moved. One reason for this, for example, might be a deferred shipment of goods.

The Authorization transaction does exactly that. It reduces the *Available to Buy* amount without reducing the actual funds.

Once the item has been shipped, performing a Redemption Completion can complete the transaction.

Generally speaking, an authorization holds the requested funds for seven days, after which the funds will be available again.

As stated above, this functionality is only available to merchants processing through the Salem Platform.

There are two different optional behaviors when managing Redemption Completions: Partial Redemption and Redemption Completion, as described below.

Partial Redemption

The Chase Paymentech Gift Card solution supports a functionality called *Partial Redemption*. If, for any reason, the amount of the original authorization exceeds the available balance when the Redemption Completion is submitted, the merchant has two options on how to treat this transaction, which is managed by submitting the element `<FlexPartialRedemptionInd>`.

If the available balance on the card is less than the Redemption Completion Amount:

- The transaction can be declined with no amount redeemed from the card. If this is the desired behavior on a particular transaction, either do not submit this element or null-fill it.

- The transaction can be approved, with the maximum amount of the Redemption Completion fulfilled, even though it is less. The response in this circumstance would include both the requested amount and the actual redeemed amount. The behavior can be implemented by passing the `<FlexPartialRedemptionInd>` element with a value of `Y`.

Redemption Completion

As stated above, a Redemption Completion is to complete an authorization. A Transaction Reference Number (`<TxRefNum>`), which references the original transaction, is returned. Assuming the authorization approved, then a Redemption Completion `FlexAction` is submitted, including the original authorization's transaction reference number and the amount to be settled (this amount can be equal to or less than the original authorization). When an amount is less than the original amount, the hold on the entire original balance is removed, and the new amount is redeemed from the card.

As stated above, this functionality is only available to merchants processing through the Salem Platform.

Redemption

As opposed to an Authorization followed by a Redemption Completion, a Redemption request is the mechanism to perform an immediate redemption. Once completed, Redemptions can only be reversed.

Merchants processing to the PNS Host can process Prior Redemption transactions by additionally passing the correct prior approval code. If the valid Prior Approval code is not passed, it is treated as a new Redemption request.

Prior Redemption transactions are not supported on the Salem system; therefore, Salem merchants attempting to process a Prior Redemption will receive an error response.

For security reasons, most Gift Card programs require the four-digit CVD (CardSecVal) printed on the front of the card to be included with the redemption request.

Refund

This transaction type is for initiating refunds to a Gift Card. It is essentially the same as an Add Value transaction.

3.2.3.1.4   Reversals

All transaction types, excluding Balance Inquiries, can be reversed, thus returning a transaction to the state it was in prior to the action being reversed. There are two restrictions as it relates to processing Reversals:

- For Salem customers, the reversal must be performed within seven days of the original transaction.

- For PNS-based customers, the reversal must be performed before the next batch close. Batch closes for Gift Cards are usually performed automatically by the Tampa host system at 5:00A.M. EST, regardless of what the Auto-Settle time is on the Gateway.

- For all customers, reversals assume that another action has not occurred that makes the reversal impossible.

  For example, an active card can no longer have an activation reversed once a transaction has been processed. The card can only be deactivated at that point, if desired.

A reversal is accomplished by simply processing a *Void* Gift Card transaction type using the merchant information and the Transaction Reference Number of the original transaction. This is true of all reversal transaction types.

The response on a Reversal provides the same information as any other response (Current Balance, Previous Balance, Response Codes, and so on). In addition, it identifies specifically what transaction type is being reversed, such as `Auth` or `Redemption` in the `<FlexAction>` tag.

3.2.3.1.5   Balance Inquiry

This transaction simply returns the Gift Card balance.

For security reasons, most Gift Card programs require the four-digit CVD (CardSecVal) printed on the front of the card to be included with the Balance Inquiry request.

3.2.3.2   Responses

The basic authorization response for all Gift Card transactions is the same. In other words, all responses are returned in the same basic format, with the same base minimum data elements. The transactions types that include more information are:

- Block Activations (if they fail)
- Redemption Completions with the Partial Redemption Flag

3.2.3.3   Settlement

Since transactions affect the balance of a card in real time, Gift Card transactions are not affected by the End of Day process options. Instead, transactions automatically fall into one of two buckets when viewed through the Virtual Terminal:

- Open Gift Card items (this includes all un-settled activity):
  - Authorizations that have not been redeemed (Redemption Completion)
  - Declined transactions
  - Errors
- All Redeemed items (viewable in the Review section of the Virtual Terminal).

  These items are grouped on a daily basis on the same timing that the Chase Paymentech Gift Card System reports activity, which is 5A.M.–5A.M.

3.2.3.4   Reporting

All standard Gift Card reporting is available from the Gift Card system, including Resource Online. Any questions about available reports should be directed to your Account Manager.

The Virtual Terminal should not be used for Gift Card reconciliation.

3.2.4   PINless Debit

Customers can use their ATM/Debit cards as an alternative method of payment from cash, check, or credit card to pay for goods or services.

Debit transactions are always authorized on a *real-time* basis, with the actual authorization resulting in the debit of the customer's bank account. These transactions must still be captured and settled to Chase Paymentech to support funding, reporting, and associated reconciliation.

The Orbital Gateway presently offers PINless Debit Processing as an option for Salem (BIN 000001) customers.

3.2.4.1   Introduction

PINless Debit is more commonly known as *Debit Bill Payment*. This is a debit transaction where neither the magnetic stripe contents nor the PIN is part of the authorization message.

PINless Debit is supported by the Accel, Star, NYCE, and Pulse debit networks.

The debit network rules for PINless Debit programs are strict, and the networks that support these transactions must approve the merchant prior to their accepting PINless Debit transactions. As a result, PINless Debit processing is only available to merchants in select industries, specifically utilities, telephone companies, cable TV providers, some insurance companies, government entities, and financial institutions. This list could change, so you should check with your Account Manager for availability rules.

Merchants assume 100% liability for PINless Debit payments. Please refer to the *Debit Bill Payment User Manual* for card association and debit network regulations.

3.2.4.2   Processing Requirements

As a result of the specific processing rules associated with PINless Debit, the Orbital Gateway enforces specific behavior as it relates to PINless Debit:

- Only Authorization-Capture, Refund, and Void transaction types are allowed. This means:
  - No Auth Only (future fulfillment) transactions
  - No Mark for Capture
  - No Splits
  - No Force transactions
- All Merchant IDs (Transaction Divisions) enabled for PINless Debit must have Auto-Settle enabled.
- PINless Debit BIN Ranges are very dynamic.

  The Orbital Gateway imports and stores the most up-to-date PINless Card ranges. If a card is submitted as PINless Debit (as identified by the required card mnemonic) and it is not in an eligible card range, a `procStatus` error code of `9797` (`PINless Debit: Card Number Not Eligible for PINless Debit Processing`) is returned.
- A PINless Debit transaction can be reversed using the Void transaction type and must be performed within 90 minutes of the original request. After 90 minutes, a Refund must be issued.
  - Reversals are recommended in the event of an unexpected result.
  - A Retry Trace Number is required for PINless Debit reversals. This helps manage unexpected results.

SEE ALSO   For more information about the implementation of Retry Trace Numbers, please see *3.3.3 Retry Logic*.

🔵 PINless Refunds are supported by all four debit networks. The request is the same as a PINless Sale, with the exception that the transaction type is R.

🔵 Industry types of MOTO (MO), eCommerce (EC), Recurring (RC), and IVR (IV) are allowed for the PINless Debit method of payment.

🔵 Approved PINless Debit transactions may return a Blank or N/A authorization code.

3.2.4.3   Profiles and Managed Billing

Profiles now have the ability to store and use PINless Debit information. The Biller Reference Number is required for all profiles using PINless Debit as a method of payment. The expiration date is optional.

There are two types of eligibility verification that are done against new and existing profiles that contain PINless Debit information:

🔵 When updating a profile containing PINless Debit method of payment, the Gateway checks against the most current eligibility file to verify that the card information is still eligible.

   ◆ If so, the profile is updated.

   ◆ If it is no longer eligible, a check is performed against the Auto Update option, which, if selected, automatically converts a non-eligible PINless debit card to Visa/MasterCard Debit.

      ▪ If the merchant has opted YES for Auto Update, the card information is converted to Visa/MasterCard Debit.

      ▪ If the merchant has opted NO for Auto Update, an error message is returned stating that the update was unsuccessful.

🔵 Each time the Gateway obtains the most current eligibility file, a check is done against all existing PINless Debit profiles.

   ◆ If the Auto Update flag is set to YES, those profiles that are no longer eligible to process as PINless Debit are converted to Visa/MasterCard Debit.

   ◆ If the profiles are not able to be updated to Visa/MasterCard Debit or the Auto Update flag is set to NO, the status of those profiles is changed to Auto Suspend-PINless. Merchants will not be able to process Sale transactions against profiles that are in this status, and Refund attempts will generate decline error messages.

Merchants can convert the card information for existing profiles from PINless Debit to Visa/MasterCard (and vice versa) by performing a profile update.

For Profiles containing Managed Billing information, PINless Debit is only supported for Recurring Profiles. Per Visa/MasterCard Association rules, Installment or Deferred profiles do not support PINless Debit.

3.2.4.4   Supported Currencies

U.S. Currency

3.2.4.5   Virtual Terminal

The Orbital Virtual Terminal can display and report PINless Debit transactions. Other functionalities include:

🔵 Ability to run PINless Debit transactions.

- Ability to adjust existing PINless Debit transactions.
- E-mail triggers that fire e-mails to cardholders when a PINless Debit card is no longer eligible.
- Profile and Managed Billing capability.
- Reports that provide PINless Debit information, including:
  - Suspended Profile Report
  - PINless Debit Status Change Report
  - Managed Billing Activity Report
  - Scheduled Profile Activity Report

  NOTE   PINless Debit information is not included on the Auth Recycle Report.

  SEE ALSO   Please review the *Orbital Virtual Terminal Users Manual* for further details.

3.2.5   Electronic Check

The Orbital Gateway supports Electronic Check Processing (ECP) for eligible merchants. Key to processing is the Bank Routing Number, also known as ABA# or Receiving Depository Financial Institution (RDFI). It is 9 bytes for US merchants. For Canadian merchants, it is 8 bytes. There should be no spaces " " or dashes "-" in the Canadian Bank Routing Number, and the proper formatting is:

    FFFBBBBB

where

    FFF refers to Financial Institution

    BBBBB refers to Branch Number

3.2.5.1   Standard Processing Requirements

Standard ECP processing makes use of the `transType` element to determine the type of transaction required by the merchant in a 'New Order' request. The `ECPActionCode` element should be left empty or NULL for all of the transaction types below in Table 6.

Table 7   Actions that can be performed under ECP

Action	Description
Authorization (A)	An Authorization request is equivalent to check validation. The following operations are performed at this time: 1. A check against the Notification of Change file to see if Chase Paymentech Solutions has been alerted to new account information about this transaction. 2. The Federal Reserve File is checked to verify that the ABA Routing is valid. 3. A check is made against the Chase Paymentech Solutions internal negative database to determine if the account is listed as *bad*. Additionally, US checking accounts undergo verification against an additional negative file at this time. *NOTE* An approved ECP Authorization must eventually be followed by a Mark for Capture request in order to complete the transaction. If a capture is not performed, the transaction will not get funded at the time of settlement.

Action	Description
Authorization and Capture (AC)	An Authorization and Capture request will perform the same operation as an Authorization, and will also prepare the transaction to be included with the next settlement if the Authorization is successful.
Force and Capture (FC)	A Force and Capture request prepares a transaction for settlement without submitting a validation or verification request at the time of the request.
Refund (R)	Refund requests prepare a return of the funds to a consumer's account for settlement. Authorization is not performed, but validation is still done at settlement.

All ECP activity must pass a second validation process at the time of settlement for funding to occur. This process includes the internal negative file, Notification of Change file, and Thompson file verifications. Salem merchants whose transactions fail these checks will see the transactions listed in the Rejected Batch of the Virtual Terminal. (see the *Orbital Virtual Terminal Users Manual* for further details).

3.2.5.2   Extended ECP Processing Requirements

Extended ECP processing makes use of both the `MessageType` and `ECPActionCode` elements to extend standard ECP processing to include all action codes the Salem and Tampa host platforms support. Use of this functionality is optional to process ECP transactions.

Table 8   Extended Actions that can be performed under ECP

Action	ECP Action	Description
Authorization (A)	**Validate (LO)**	A Validate request is an ECP equivalent to $0.00 account verification for Credit Cards. This message is available for Canadian and US merchants.
		The following operations are performed at this time:
		1. A check against the Notification of Change file to see if Chase Paymentech Solutions has been alerted to new account information about this transaction.
		2. The Federal Reserve File is checked to verify that the ABA Routing is valid.
		3. Finally, a check is made against the Chase Paymentech Solutions internal negative database to determine if the account is listed as *bad*.
		NOTE An approved ECP Validate (LO) is always for $0.00 and therefore may not be followed by a Mark for Capture request in order to complete the transaction. To capture funds, a corresponding Force & Capture (FC) or Refund (R) with a valid amount must be performed.

Action	ECP Action	Description
Authorization (A)	Validate & Verify (VO)	A Validate & Verify request is an ECP equivalent to $0.00 account verification for Credit Cards. This message is available for US merchants only. The following operations are performed at this time: 1. A check against the Notification of Change file to see if Chase Paymentech Solutions has been alerted to new account information about this transaction. 2. The Federal Reserve File is checked to verify that the ABA Routing is valid. 3. A check against the Chase Paymentech Solutions internal negative database to determine if the account is listed as *bad*. 4. Finally, a verification against an additional negative file is performed at this time. NOTE An approved ECP Validate & Verify (VO) is always for $0.00 and therefore may not be followed by a Mark for Capture request in order to complete the transaction. To capture funds, a corresponding Force & Capture (FC) or Refund (R) with a valid amount must be performed.
Force and Capture (FC)	Validate, Verify, and Deposit (VD)	A Validate, Verify, and Deposit request prepares a transaction for settlement and deposit without submitting a validation or verification request at the time of the request. NOTE All settled ECP activity which does not include an ECP action code performs a Validate and Deposit request at settlement. An additional Verification is performed when a Validate, Verify, and Deposit (VD) transaction is settled.
Force and Capture (FC)	Validate, Verify, and Prenote (VP)	A Validate, Verify, and Prenote request prepares a prenote transaction for settlement. A validate and verify is not performed at the time of request, instead happening at settlement. See *section 3.2.5.2.1* for information on Prenotifications.
Force and Capture (FC)	Validate and Prenote Debit (ND)	A Validate and Prenote Debit request prepare a prenote transaction for the purposes of a future deposit of funds from a consumer's account for settlement. Authorization is not performed, but validation is still done at settlement. See *section 3.2.5.2.1* for information on Prenotifications.
Refund (R)	Validate and Prenote Credit (NC)	A Validate and Prenote Credit request prepares a prenote transaction for the purposes of a future refund of funds to a consumer's account for settlement. Authorization is not performed, but validation is still done at settlement. See *section 3.2.5.2.1* for information on Prenotifications.

3.2.5.2.1 Prenotification Transactions

Prenotification is a zero dollar ($0) transaction which is treated somewhat like a deposit. A prenote request is submitted without an initial Authorization. Upon settlement, the transaction is validated (NC or ND) or validated & verified (VP). Validations or Verifications which are approved are then submitted by the settlement process to the consumer's bank. The account and routing information is then checked to ensure they exist and are accurate. The balance of funds in the consumer's account is *not* checked.

The post-settlement success or failure of a prenotification is not reported back to the Orbital Gateway. This information must be obtained from financial reporting available from Paymentech Online for Salem merchants, or from Resource Online for Tampa merchants. Contact your Account Executive for more information on these tools.

Once a Prenote request has confirmed the consumer's account is valid, a live (non-zero) transaction will be required to collect any funds from the consumer.

WARNING Per ECP regulations, six days must pass before processing a non-zero dollar deposit on a pre-noted bank account.

3.2.5.3 ECP Authorization Methods

A merchant can receive authorization from a consumer to process an ECP transaction through several different environments. Each authorization environment has certain rules and transaction data required for processing.

NOTE Standard ECP Processing supports all ECP Authorization Methods.

Table 9 ECP Authorization Methods

Authorization Method	Description
Pre-arranged Payment and Debit (Written)	A single or recurring credit or debit initiated by a merchant after the Consumer has provided a one-time or standing authorization to allow an electronic funds transfer from a checking or savings account. Supported ECP action codes: LO, VO, VD, VP, NC, ND Supported for US and Canadian merchants Customer name is required.
Internet (Web)	A single or recurring debit made over the Internet via a website Supported ECP action codes: LO, VO, VD, VP, NC, ND Supported for US and Canadian merchants Customer name is required.
Telephone (Tel)	A single or recurring debit authorized over the telephone drawn on a consumer account. Supports ECP action codes: LO, VO, VD, VP, NC, ND Supported for US and Canadian merchants Customer name is required

Authorization Method	Description
Accounts Receivable (ARC)	A single, one-time debit received via lockbox, drop box, or business mail box.
	Supports ECP action codes: LO, VO, VD, VP
	Supported for US merchants only.
	Check serial number is required. Image reference number and customer name are optional.
Point of Purchase (POP)	A single, one time debit made in person at a point of sale for a consumer purchase.
	Supports ECP action codes: LO, VO, VD, VP
	Supported for US merchants only.
	Check serial number is required. Image reference number, Terminal City, Terminal State, and customer name are optional.

An additional value of "Empty" is also supported for Salem (Bin 000001) merchants only. This value will instruct the downstream host to use whatever default value it has stored.

A merchant may be enabled for a default value on the Orbital Gateway. If this element is left NULL, that default will be used. If no default is stored, the auth method will revert to Telephone.

3.2.6   UK Maestro/Solo

Chase Paymentech Solutions offers processing of Great Britain's UK Maestro®/Solo™ debit cards for Salem merchants (BIN 000001) through the Orbital Gateway. UK Maestro/Solo functionality must be enabled at the merchant level in order to process this method of payment. Please contact your Chase Paymentech Solutions Account Representative if you wish to accept UK Maestro/Solo.

NOTE   As of June 2012, the International Maestro method of payment absorbed UK Maestro / Solo. Merchants who wish to accept these cards going forward should code to process International Maestro transactions.

Legacy users of the Web Services API are not required to re-certify for International Maestro. As of the above date, any details specific to the UK Maestro / Solo data elements are no longer documented.

3.2.7   Bill Me Later

Bill Me Later® is an innovative and secure payment solution for Card-Not-Present merchants. The Bill Me Later method of payment is a non-plastic issued credit vehicle that manages the consumer payment function by providing a transactional credit decision in lieu of the standard predetermined credit line and associated authorization process. Bill Me Later allows consumers to make online/mail order purchases without inputting credit card information.

3.2.7.1   How it works

Using proprietary credit scoring and fraud detection capabilities, Bill Me Later, Inc. (formerly known as I4Commerce) screens each Bill Me Later transaction in real time, instantly decisioning all Bill Me Later requests made by customers.

3.2.7.2   Processing Requirements

Merchants must contract with Bill Me Later, Inc. for acceptance of Bill Me Later.

The Orbital Gateway enforces the following data requirements for Sale (Authorization, Authorization-Capture) transaction types:

Required:

- Account Number
- Bill To Address (`AVS...` elements)
- Ship To Address (`AVSDest...` elements)
- Shipping Cost (`BMLShippingCost`)
- Terms and Conditions Version (`BMLTNCVersion`)
- Customer Registration Date (`BMLCustomerRegistrationDate`)
- Customer Type Flag (`BMLCustomerTypeFlag`)
- Item Category (`BMLItemCategory`)
- Customer Birth Date (`BMLCustomerBirthDate`)
- Customer Social Security Number (`BMLCustomerSSN`)
- Product Delivery Method (`BMLProductDeliveryType`)

Optional:

- Customer Source IP (`BMLCustomerIP`)
- Customer E-mail (`BMLCustomerEmail`)
- Pre-approval Invitation Number (`BMLPreapprovalInvitationNum`)
- Promotional Code (`BMLMerchantPromotionalCode`)
- Customer Annual Income (`BMLCustomerAnnualIncome`)
- Customer Resident Status (`BMLCustomerResidenceStatus`)
- Customer Checking Account (`BMLCustomerCheckingAccount`)
- Customer Saving Account (`BMLCustomerSavingsAccount`)

NOTE   Please contact your Bill Me Later Integration Analyst during the requirements definition phase prior to development to determine required fields.

3.2.7.2.1   Currencies

US Dollar Only

3.2.7.3   Other

3.2.7.3.1   Virtual Terminal

All of the functionality supported through this interface for Bill Me Later is additionally available through the Orbital Gateway Virtual Terminal.

3.2.7.3.2   Platforms

The Orbital Gateway only supports the Bill Me Later method of payment through the Salem host platform (BIN 000001). This method of payment is not supported on the PNS host (BIN 00002).

3.2.8   International Maestro

The International Maestro® payment solution provides Maestro cardholders with an easy, secure way to make Internet purchases using their Maestro cards online. MasterCard is expanding this payment functionality across Europe to give consumers the same ease-of-access to deposit accounts for their Internet purchases that they currently experience with Maestro cards for other purchases. Please contact your Chase Paymentech Solutions Account Representative if you wish to accept International Maestro.

3.2.8.1   Processing Requirements

Orbital gateway supports International Maestro for the following requests:

- All New Order message types
- Mark for Capture messages
- Voids (Including Online Reversals)
- Inquiries
- All Profile messages

International Maestro card numbers are between 13 and 19 digits. International Maestro also supplies a standard expiration date on all cards.

Associations support AVS validation for United Kingdom (UK) issued International Maestro cards only. CVV validation is supported for all International Maestro cards where a CVV is printed on the card. Response codes and rules are identical to MasterCard credit transactions.

3.2.8.1.1   MasterCard SecureCode (MCSC)

Merchants who accept International Maestro are strongly encouraged to offer MasterCard Securecode validation. The first time a customer uses an International Maestro transaction, MCSC validation should be attempted, and an AAV value should be included in the transaction. MCSC Validations are also needed on subsequent transactions, unless one of the two exceptions below are applicable.

A European merchant may enroll in two International Maestro programs, *Maestro Advanced Registration Program (MARP)* or *Maestro Recurring Payment Program (MRPP).* Both programs allow enrolled merchants to accept Maestro cards for eCommerce transactions without using MasterCard SecureCode for every transaction.

Maestro Advanced Registration Program (MARP)

An enrolled MARP merchant is provided with a static Accountholder Authentication Value (AAV) for use with transactions that are processed without SecureCode authentication. Once a merchant has registered in the MARP program all accountholders must go through the SecureCode process again, regardless of whether the accountholder has gone through SecureCode prior to the merchant's registration. After the accountholder has gone through SecureCode process and has been approved, the accountholder is not required to go through SecureCode for subsequent transactions.

Maestro Recurring Payment Program (MRPP)

MRPP operates in a similar fashion to the MARP as described above. At time of enrollment, a static AAV value is provided. The first transaction is processed as a standard eCommerce

transaction. Subsequent transactions are submitted as recurring payments along with the static AAV value. At the present time the MRPP program only supports recurring transactions. Mail order and installment billings are not permitted.

The static AAV value may be stored in the Orbital Gateway. To apply the static AAV stored by the Gateway to a transaction, set the `useStoredAAVInd` element to `Y`. Otherwise, the AAV must be provided in the request message. For more information, please see *3.2.1.1.4 Verified by Visa/MasterCard SecureCode Programs*

3.2.8.2   Profiles and Managed Billing

Profiles have the ability to store and use International Maestro information. The card number is required for all profiles using International as a method of payment. The expiration date is optional.

For Profiles containing Managed Billing information, International Maestro is supported for Recurring Billings. A Static AAV value must be kept on file with the Gateway to include Managed Billing information in an International Maestro profile.

Per Association rules, International Maestro profiles do not support deferred or installment billings.

3.2.8.3   Other

3.2.8.3.1   Virtual Terminal

All of the functionality supported through this interface for International Maestro is additionally available through the Orbital Gateway Virtual Terminal.

Management of a merchant's Static AAV value is done through the General Admin page in the Virtual Terminal. Please refer to the Virtual Terminal user guide for more information.

3.2.8.3.2   Platforms

The Orbital Gateway only supports the International Maestro method of payment through the Salem host platform (BIN 000001). This method of payment is not supported on the PNS host (BIN 00002).

3.3   Available Processing Functionalities

3.3.1 Soft Descriptors

The Soft Descriptor Records are used to define the merchant name/product description that will appear on the consumer's statement. It allows the merchant greater flexibility in describing the consumer's purchase. Soft Descriptors are supported for Visa, MasterCard, MasterCard Diners, and ECP.

It is subject to issuer discretion whether this descriptor will be displayed on the cardholder statement.

NOTE   Although only some of the Soft Descriptor records can be populated with data in any given combination, all of the Soft Descriptor elements must be submitted in the transaction request. Any element that is not populated should be null-filled.

3.3.1.1   Soft Descriptor Support

Support for Soft Descriptors is not globally available to all customers using the Orbital Gateway.

Salem (BIN 000001)

The Orbital Gateway supports Soft Descriptors into the Salem Host. However:

- Prior Risk Department approval is required.
- The Merchant ID/Terminal ID must be enabled for Soft Descriptors on the Orbital Gateway.

PNS (BIN 000002)

The Orbital Gateway supports Soft Descriptors into the PNS Host. However:

- It is only supported for Chase Paymentech Canada customers.
- The Merchant ID/Terminal ID must be enabled for Soft Descriptors on the Orbital Gateway.
- The behavior is different from that of the Salem Interface. See *3.3.1.3 PNS/Tampa Support* for more details.

NOTE   Please contact your Chase Paymentech Representative for setup information for either host.

3.3.1.2   Salem Support

3.3.1.2.1   Rules and Guidelines—Credit Card

Chase Paymentech will not generate or segregate reports by the Soft Descriptor. If the merchant wishes to see Salem reports segregated by product, the merchant must set up specific reporting divisions and deposit those transactions under that division number.

For those merchants who need to roll up several merchant names under one corporation, please contact your Chase Paymentech Representative for details on the use and regulation of the Soft Descriptors.

The description in the merchant name field should be what is most recognizable to the cardholder. It should consist of the company name and/or trade name combined with some type of description of the product or service that was purchased.

The Merchant Name can be one of 3 different lengths:

- 3 bytes
- 7 bytes

⭕ 12 bytes

In addition, the Product Description can be appended based on the length of the Merchant Name, such that they are a combined length of 21 bytes. In other words, the options are:

⭕ 18 bytes

⭕ 14 bytes

⭕ 9 bytes

Additional notes:

⭕ The Merchant City field allows the merchant to identify the business location or provide the cardholder with a Customer Service Phone Number or URL. This is a requirement to qualify for Visa's lowest Direct Marketing interchange rate.

⭕ If the merchant submits a backslash (\) in the merchant descriptor, it is converted to a hyphen (-) on the cardholder statement. If the merchant submits a question mark (?) in the merchant descriptor, it is converted to a space on the cardholder statement.

⭕ There are certain American Express card types/programs that ignore the descriptors sent using Soft Descriptors. The Optima card is one of these types. The merchant should contact their American Express representative for more details.

⭕ Non-eCommerce transactions sent with a URL do not qualify for the best interchange.

⭕ For MasterCard MOTO and Recurring Industry Types, if the City/Phone field at the division level is not a Customer Service Phone Number, then a Customer Service Phone Number must be populated in the Merchant City/Customer Phone Number field, or the transaction will error with Response Reason Code BP (Customer Service Phone reqd. for MOTO and Recurring. MC Only).

⭕ The Orbital Gateway will apply the asterisks (*) in the necessary locations. Please do not add these to the request.

3.3.1.2.2   Rules and Guidelines—ECP

The Automated Clearing House (ACH) uses two fields to describe the transaction to the consumer. The Merchant Name (15 bytes) will always appear on the consumer's statement, and the Entry Description (10 bytes) will appear on the consumer's statement a majority of the time. Both are required fields.

Chase Paymentech recommends using the Doing Business As (DBA) description/value in the Merchant Name field and the product information in the Product Description field.

When utilizing the Soft Descriptor for ECP transactions, both the Merchant Name and the Product Description are mandatory.

3.3.1.2.3   Soft Descriptor Examples

Example 2   Soft Descriptor section for a 3 byte Merchant Descriptor with Phone number

```
<SDMerchantName>XYZ</SDMerchantName>
<SDProductDescription>PAYMENT1OF3</SDProductDescription>
<SDMerchantCity/>
<SDMerchantPhone>888-888-8888</SDMerchantPhone>
<SDMerchantURL/>
<SDMerchantEmail/>
```

Example 3   Soft Descriptor section for a 12 byte Merchant Descriptor with E-mail

```
<SDMerchantName>XYZCOMPANY</SDMerchantName>
<SDProductDescription>PYMT1OF3</SDProductDescription>
<SDMerchantCity/>
<SDMerchantPhone/>
<SDMerchantURL/>
<SDMerchantEmail>suppt@xyz.com</SDMerchantEmail>
```

NOTE   Phone, URL, and email fields can be a maximum of 13 characters therefore care should be given when supplying this data so that consumers can understand the information on their statements.

Example 4   Soft Descriptor section for ECP

```
<SDMerchantName>XYZCOMPANY12345</SDMerchantName>
<SDProductDescription>PRODUCT123</SDProductDescription>
<SDMerchantCity/>
<SDMerchantPhone/>
<SDMerchantURL/>
<SDMerchantEmail/>
```

3.3.1.3   PNS/Tampa Support

3.3.1.3.1   Rules and Guidelines

Again, the support for Soft Descriptors via the PNS Host is only for customers processing through Chase Paymentech Canada.

Unlike Salem, the only value passed on to the cardholder statement is the Merchant Name field, which, for these customers, is a maximum of 25 bytes of data.

All other Soft Descriptor fields can optionally be sent, but will not be submitted to the settlement host and will not display on the cardholder statement.

3.3.1.3.2   Soft Descriptor Example

Example 5   PNS Soft Descriptor section

```
<SDMerchantName>XYZPAYMENT1OF3</SDMerchantName>
<SDProductDescription/>
<SDMerchantCity/>
<SDMerchantPhone/>
<SDMerchantURL/>
<SDMerchantEmail/>
```

3.3.2   Profiles and Managed Billing

The Orbital Gateway includes functionality called *Customer Profile Management*, which allows cardholder data to be stored with the Orbital Gateway. A merchant can process transactions by simply passing a token value that represents that cardholder.

Once a Profile is created, transactions can be processed, using either the online interface or the Orbital Virtual Terminal (VT), simply by referencing the Customer Profile and filling in any additional information not stored in the profile. This feature is only available to merchants using the Chase Paymentech Orbital Interface.

Released in March of 2008, Managed Billing extends the capabilities of Profiles to include Recurring, Installment, and Deferred billing. Using this feature, merchants can configure future payments that the Orbital Gateway will initiate on the desired date.

3.3.2.1   Supports both Recurring and Non-Recurring Charges

By default, Profiles do not provide a full recurring service. Although the Orbital Gateway stores all the relevant information for processing a transaction, it will not automatically process it. When using standard Profiles, merchants are required to initiate a Profile request to the Orbital Gateway and retrieve the result of that request.

Profiles can also be configured to bill automatically via a process known as Managed Billing. Merchants wishing to use Managed Billing to support recurring, installment, or deferred charges must have the Managed Billing feature enabled for their account. A Merchant Contract Addendum is required to enable this feature, so interested merchants should contact their Sales Representative or Account Executive.

SEE ALSO   See *3.3.2.4.6 Managed Billing Profiles* for more information.

Additionally, please reference the supplemental document *Managed Billing 101* for more information about the overall product, its features, and how merchants can use the Managed Billing features.

3.3.2.2   Benefits

There are a number of potential benefits when using the Profiles feature:

- It simplifies transaction processing. When making a transaction request, one simply references the Customer Reference Number and fills in any of the missing information.
- It eliminates risk. Since it eliminates the need to store sensitive information about a merchant's customer on their database, merchants can focus on their business, and Chase Paymentech can focus on securely processing their transactions.
- It can eliminate data entry errors when using the Virtual Terminal. By retrieving a pre-existing Profile and validating the data, it eliminates the risk of *keying* the wrong customer information such as Order Number (which may equate to a Membership ID) or credit card number.

3.3.2.3   Setup Information

For any Orbital Gateway Merchant ID to support Profiles, it must be configured on the Orbital System to do so. There are several different configuration aspects that must be set up.

- **Enablement**   First the Merchant ID must be configured to allow Profile functionality. Any Merchant ID that is not configured to use Customer Profiles and attempts to process a Profile Action will receive an error—a Profile Error Code of `9578` (or `Merchant-Bin combination is not allowed to perform profile transactions`).
- **Customer Profile Hierarchy Support**   Each Merchant ID must be configured to support Profiles at the Chain ID (Company) level or Merchant ID level.

  NOTE   Managed Billing requires that Profiles be configured at the Merchant ID level.

- **Virtual Terminal Users**   If your organization will utilize Profiles on the VT in addition to the XML interface, there are a few important considerations, as described in the next section.

3.3.2.3.1 Profile User Management

🔸 **Profile Administration**   For any VT User to administer Profiles (add, delete, update), that user must be provided the *right* to administer Profiles. Any existing user can be granted this additional user permission.

🔸 **Profile Usage**   For any VT User to use Profiles for processing a transaction, permission needs be granted to use profiles. Any existing user can be granted this additional User permission. The user will not be able to administer profiles, just use existing ones.

🔸 **Profile Access Disabled**   If the VT User is not enabled for any Profile access level, they will not see any of the functionality. Profiles can be disabled for one user and enabled for another user.

3.3.2.3.2 General Access Rights

🔸 **Card Masking**   The same card masking rules that currently apply to any card number viewing in the VT apply to Profile management or usage:

- ◆ If a user's permission allows the viewing of the credit card number, then, during usage or management, that user will be allowed to see any credit card number whether maintaining a profile or using it.

- ◆ Conversely, if a user's permission level does not allow the number to be viewed, then it cannot be viewed whether they have the right to maintain a profile or use it. However, the card can be changed or updated regardless of masking.

🔸 **Access Levels**   All existing access levels are not impacted, regardless of Profile user rights. For instance, if a user cannot submit credits, they will not be able to submit credits using Profiles.

3.3.2.4 Business Rules

3.3.2.4.1 How it works

The first step is to create a Profile. This can be done in two different fashions:

🔸 Adding a Profile as a distinct action.

🔸 Adding Profile as a part of an authorization request.

Once that Profile exists, it can be utilized to complete a sale or refund with any of the data elements stored in the profile. Additionally, any part of the Profile can be overridden during the subsequent transactions.

Finally, the Profile can be updated (or even deleted) at any point.

3.3.2.4.2 Customer Reference Number Options

The Customer Reference Number is the referential data element to a Profile.

Key Customer Reference Number facts:

🔸 Must be unique (either by Merchant ID or Chain ID)

🔸 Can be from 1 to 22 bytes in length

🔸 Valid characters are:

```
abcdefghijklmnopqrstuvwxyz
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

```
0123456789
```

```
-,$@&
```

and the space character

- ◆ Please note that, although lowercase characters can be submitted, all alphabetic characters in this field are stored in uppercase by the Orbital system. Users cannot use uppercase and lowercase values to differentiate Customer Reference Numbers.

- ◆ Because the ampersand (&) has unique properties within XML, an ampersand must be sent as `&`

Setting the Customer Reference Number

The merchant can either set or request that the Orbital Gateway set the Customer Reference Number.

The `<CustomerProfileFromOrderInd>` element controls this behavior as follows:

A Auto-generate the Customer Reference Number. In other words, the Orbital Gateway will assign the Customer Reference Number and return it in the response.

S The Orbital Gateway will use the value passed in the `<CustomerRefNum>` element as the Customer Reference Number.

O This option only relates to when a Profile is added as a part of an authorization request. In this circumstance, the value passed in the `<OrderID>` element is used as the Customer Reference Number. For example, this would be used in circumstances wherein the Order ID also represents your customer's identification in your system, such as a Policy Number for an insurance company.

D This option only relates to when a Profile is added as a part of an authorization request. In this circumstance, the value passed in the `<Comments>` element is used as the Customer Reference Number.

NOTE When using a Profile, set this field to `EMPTY` or null-fill:
`<CustomerProfileFromOrderInd>EMPTY</CustomerProfileFromOrderInd>`

This value is NOT case-sensitive.

Using the Customer Reference Number to Set Other Data Elements

The Orbital Gateway has configuration options for the Profile setup to determine how the Customer Reference Number is leveraged to populate other data sets using the `<CustomerProfileOrderOverrideInd>` value.

The options are:

NO No mapping to order data.

OI Pre-populate `<OrderID>` with the Customer Reference Number.

OD Pre-populate the `<Comments>` field (this field is called Order Description in the Virtual Terminal) with the Customer Reference Number.

The relevance of this feature is on the PNS platform (BIN 000002), where the `<Comments>` field populates the Customer-Definable Data. This data can then be made available on certain Resource Online Reports. Any questions about your reports should be directed to your Relationship Manager.

OA Pre-populate the `<OrderId>` and `<Comments>` fields with the Customer Reference Number.

3.3.2.4.3   Customer Reference Number Hierarchy Setup and Usage

As stated earlier, Profiles can be created at the Merchant ID level or at the Chain level.

If a MID is configured to use Profiles at a Chain ID level, any profiles set up by any Merchant ID are available to be used by any other Merchant IDs tied to that chain. However, if the MID is set up to manage Profiles at the merchant level, any Profile set up by that Merchant ID can only be used by that Merchant ID.

For example:

Let's assume there is a single customer with two merchant IDs on the Orbital Gateway, `111111` and `222222`, and that these two merchant IDs are tied to the same chain ID, `333333`. Then, merchant ID 111111 sets up a new customer profile, `ABC`.

- If both merchant ID `111111` and merchant ID `222222` are set up to manage profiles at a chain level, then merchant ID `222222` will be able to use profile `ABC`.

- If either one of them is not, then merchant ID `222222` will not be able to use profile `ABC`.

Additional notes:

- All Merchant Profile configurations are performed at a Merchant ID level, so this cross Chain ID sharing can only be facilitated via Orbital Setup.

- In addition, given that all setup and usage of Profile IDs is done using a specific Merchant ID, the Chain ID must be known to take advantage if this feature.

  As long as all the Merchant IDs are properly linked to the same chain, it will simply work. If the Merchant IDs are not correctly mapped to the same Chain ID, Merchant IDs can be remapped to new Chain IDs easily. If this feature will be used, it is recommended that the correct chaining be validated prior to going live.

- Whatever level is defined as the storage level, there can only be one version of a Customer Reference Number.

  If two Merchant IDs have different customers who share the same customer identification, it is recommended that the Profile storage and usage be maintained at the Merchant ID level, as opposed to the Chain level. If the second store tried to establish the same Customer Reference Number and the setup dictated Chain level storage, then a `Duplicate Customer Reference Number` error (`<ProfileProcStatus>` error code of `9582`) would be generated.

- Again, Managed Billing is not available for profiles configured at the Chain level.

Salem Hierarchy

For Salem Orbital Gateway customers, the Orbital Gateway hierarchy closely emulates the Salem hierarchy:

- Your Orbital Gateway MID will be the same as your Salem Division (or TD) number.

- Your Orbital Gateway Chain ID will be the same value as your Company Number (formerly known as the *MA*).

If the Salem Division numbers are all linked to a specific Company number, then that is how it will be set up on the Orbital Gateway.

PNS Hierarchy

For PNS Orbital Gateway customers, the Orbital Gateway hierarchy is tied to the PNS Authorization Host hierarchy. As such:

- Your Orbital Gateway MID will be the same as your PNS Authorization Merchant ID (MID) – Terminal ID (TID).

- ⟳ However, there is no PNS Chain value. Therefore the Orbital Gateway assigns the next available chain value when setting up accounts for the first time.

If an organization has multiple Merchant IDs, there is no guarantee that all of those Orbital Gateway Merchant IDs will be linked under a single Chain ID. However, Merchant IDs can be moved under one chain to take advantage of this feature.

3.3.2.4.4   Profile Methods of Payment

Profiles may be associated with any one of a number of payment options. Customer details will vary based on the Method of Payment chosen. It is possible to modify a profile from one payment option to another.

Profiles may use the following payment options: Credit Card, Pinless Debit, Electronic Check (ECP), European Direct Debit (EUDD), and International Maestro.

3.3.2.4.5   Profile Transaction Types

There are a number of transaction types associated with Profiles. Some of these are extensions of existing transaction types, and some are new to Profiles. This section describes how to support all Profile transaction types and some of the specific rules associated with each of them. Again, all of the functionality identified within this document is possible through the Virtual Terminal as well.

Managing Profiles

There is a set of transactions specifically set up for managing the Profile—for adding, updating, deleting, and retrieving the information.

Adding Profiles

First and foremost, a profile needs to be added to the Orbital Gateway. There are two different transaction actions that can be performed to add a profile.

Adding a Profile as a Stand-Alone Transaction

The simplest mechanism to add a Profile is to simply make a Profile Add Request. This document includes both the definition of the values necessary to complete this transaction (*4.9*) and an example template of an Add Profile Request (*5.1.3*).

There are new response data elements that need to be interpreted to determine the success of this Add request.

Adding Profiles during an Authorization

Since an authorization must often be performed the first time a customer is set up, the Orbital Gateway has extended the traditional Authorization transaction to enable adding a Profile in the same request.

- ⟳ Any data included in the Authorization that can be saved as a part of the profile will be.
- ⟳ The minimum data to create a profile must be included, or no profile will be created.
- ⟳ The result of the authorization is separate from the result of the profile add step. On the same transaction, the authorization can be successful, while the Profile-Add component is not, and vice-versa. These results are mutually exclusive and should be interpreted from a response management process as such.
- ⟳ Add Profiles functionality can only be included with Auth Only, Auth-Capture, Prior Auth (Force), and Refund transactions. It cannot be completed as a part of a Void or Mark for Capture.

Information Saved in a Profile

Whether a Profile is created via a Profile Add transaction, added on-the-fly via an Authorization transaction, or updated later via a Profile Update transaction, the following list defines what data elements can be saved as part of the Profile:

- Customer Reference Number   Required and uneditable (also referred to as Profile ID)
- Customer Name
- Customer E-mail

  NOTE   Only available for Profile Add or Update transactions. This value is not yet available for on-the-fly Profile Adds within Authorization transactions.

- Address Information:
  - Address 1
  - Address 2
  - City
  - State
  - ZIP
  - AVS Country Code
  - Phone
- Amount
- Order Description

  This can be set in two ways:
  - By sending a specific description message in the `<Comments>` tag.
  - By setting the `<CustomerProfileOrderOverrideInd>` to populate the `<Comments>` tag.
- Order ID

  This can be accomplished by setting the `<CustomerProfileOrderOverrideInd>` to populate the `<OrderID>` tag
- Payment Information
  - Credit Card
    - Card Number
    - Expiration Date
  - ECP (Salem Host Only: BIN 000001)
    - DDA Account Number
    - R/T (Bank Routing Number)
    - Account Type
    - Payment Delivery Method
  - PINless Debit
    - Card Number
    - Biller Reference Number

Information NOT Saved in a Profile

There are a number of data elements that are not added to a Profile, regardless of how it is done, including, but is not limited to:

- Level 2 and Level 3 Data

- Card Verification Number (CVV2, CVC2, and CID).

  Card Association rules forbid storing of this information. It must be requested from a cardholder on a transaction-by-transaction basis.

- Verified by Visa and MasterCard SecureCode Data

Updating Profiles

Once a Profile has been added, any information about the Profile can be modified, except the key Profile values (which include the Customer Reference Number, Merchant ID, and BIN). This is accomplished by sending a Profile Update transaction.

Some important keys to performing an Update:

- All Profile Update requests must include the correct Profile key values, or an error message will be returned. A list of the error messages can be found in *Table 16* in *Appendix A*.

- An update requires the tags to be sent for both:

  - The data that should be changed.

  - Any fields that should be cleared.

- To clear any legacy data, the XML tag is submitted with nothing but a tilde (~), as in the example below:

  `<CCExpireDate>~</CCExpireDate>`

- If the Customer Profile includes an amount and an update is sent with the `<Amount>` tag present, but filled with a tilde character, the amount stored in the profile is changed to `NULL` in the database.

- If an XML tag is sent with a Null value (such as `<CCExpireDate></CCExpireDate>`), it is ignored as a part of the update process (that is, no update would occur on the `CCExpireDate` value).

- When changing Card Types, such as from an ECP to a Credit Card, the requirements are:

  - Send the XML tag representing the new card type.

  - Submit the appropriate data for that card type.

  - Null-fill the old card type data elements using the tilde process described above.

    For example, changing from an ECP transaction type to a Credit Card type, the Profile Update message should:

    - Have the Card Type defined as Credit.

    - Include the Credit Card Number and Expiration Date.

    - Send a tilde for the four ECP data elements (DDA, R/T, Account Type, and Payment Delivery Method).

Retrieving a Profile

At any given time, there may be a need to retrieve the data on an existing Profile. The Retrieve Profile transaction type is available to perform this action.

Deleting a Profile

Any Profile can be deleted at any time with a Delete Profile transaction type.

Even though a Profile has been deleted, the Customer Profile Reference Number may not be used again.

Using Profiles

One of the key functionalities is to use a Profile to process a transaction. This is accomplished by inserting the Customer Reference Number in one of the existing message types. All data that can be pre-populated by the Profile will be.

- Any relevant data, such as CVD for eCommerce transactions, should be included in the request.
- The transaction request should be completed per the normal spec in terms of which tags are mandatory. If the data exists in the Profile and the tag is mandatory, simply null-fill the tag.
- The correct values should be used based on the card type of the profile. For example, if the card type of a Profile is a credit card, then the base credit card message structure should be used to use the profile. The credit card data, again, should be null-filled.

Overriding Profile Data

Almost any data set in the Profile can be overridden during a transaction that is using the Profile. For instance, if a Profile includes a fixed amount, but a particular transaction is for a different amount, it could be changed for that transaction by including a specific amount in the Use Profile request.

The one exception to the override rule is that the payment type, such as Credit Card versus ECP, cannot be overridden. If the payment type is different, then the Profile should either be updated (if that change is permanent) or not used (if it is temporary).

By the same token, if the payment type is the same, but the data is different, it can be overridden on a single transaction, if desired.

Finally, overriding Profile data does not update the profile. If the change is permanent, an Update Profile request should be sent in.

Overriding an Expiration Date

One scenario to take into consideration when overriding data has to do with the usage of expiration dates. As defined in the spec, for a Salem customer, a null expiration date is one mechanism to submit transactions for authorization when the expiration date is unknown. By the same token, an expiration date is required for credit card transactions and must be present when using a Profile. It must also be null-filled to not override the expiration date that might be set in the Profile.

As such, if an expiration date is saved in a Profile and the desire is to override it but submit nothing because the new expiration date is unknown, the transaction should use one of the following mechanisms for supporting unknown expiration dates:

- Send four spaces: `<CCExpireDate>    </CCExpireDate>`
- Zero-fill the XML Element: `<CCExpireDate>0000</CCExpireDate>`

Transaction Types

Profiles may be used on the following types of transactions:

- Authorization
- Authorization-Capture
- Prior Authorizations
- Refund
- Safetech Fraud Analysis

Profile usage is not functional (or necessary) for:

- Voids/Reversals
- Mark for Capture
- End of Day

Note Regarding Mark for Capture Transactions

Previously, the Orbital Gateway DTD mandated the presence of the card number XML element, even though the Credit Card or Maestro Solo Mark for Capture ([*MFC*) transaction never really required it from a business perspective. To meet this requirement, many customers have been sending either the actual or a dummy credit card number or null-filling this tag.

Effective with the release of Profile Management, the Orbital Gateway has corrected this design and **no longer mandates** this tag to be a part of the MFC request. This was done to ensure that a customer using a Profile could complete a MFC without having to include this tag.

Industry Types

All the Industry Types that are supported by the Orbital Gateway (eCommerce, Mail Order, Recurring, Installment and Interactive Voice Response) are supported within Profiles.

Currencies

All currencies supported by the Orbital Gateway are supported as a part of Profiles. Simply set the correct currency code and exponent on the transaction being processed (see *Table 22 Currency codes and exponents* in Appendix A).

3.3.2.4.6   Managed Billing Profiles

Managed Billing enables merchants to configure Profiles so that Chase Paymentech will automatically run transactions in the future. Managed Billing supports Recurring, Installment, and Deferred Billings.

NOTE   A merchant account can only be configured for one type of Managed Billing at a time.

Recurring Billings

Recurring billings bill cardholders for future payments according to a predefined schedule. Recurring billings can be configured to happen on a weekly, monthly, or yearly basis. Attributes such as Start Date, End Date, and Recurring Frequency must be set so that the Managed Billing system can schedule payments.

Also, since Chase Paymentech will be initiating the future transaction instead of the merchant, a choice must be made regarding Order ID generation.

Installment Billings

Installment billings are handled exactly like Recurring, except that the End Billings trigger is configured using the `<MBRecurringMaxBillings>` tag. However, this behavior is not enforced by the Orbital Gateway.

Deferred Billings

Deferred Billings are one-time billings that occur on a future date. The key element that needs to be set for a Deferred Billing is the Deferred Billing date.

As with Recurring Billings, since Chase Paymentech will be initiating the future transaction instead of the merchant, a choice must be made regarding Order ID generation.

Setting a Managed Billing Frequency Pattern

Frequency patterns for Managed Billing are configured using a subset of a standard `CRON` expression, comprising 3 fields separated by a white space.

Table 10   Managed Billing frequency pattern fields

Field Name	Allowed Values*	Allowed Special Characters*
Day-of-Month	1–31	, – * / ? L W
Month	1–12 or JAN–DEC	, – * /
Day-of-Week	1–7 or SUN–SAT	, – * / ? L #

*   Not case-sensitive

Notes on frequency pattern special characters:

- The comma (**,**) character is used to specify additional values. For example, **MON,WED,FRI** in the `Day-of-Week` field means *the days Monday, Wednesday, and Friday*.

- The dash (**–**) character is used to specify ranges. For example, **10–12** in the `Month` field means *the months October, November, and December*.

- The asterisk (*****) character is used to specify *all values*. For example, ***** in the `Month` field means *every month*.

- The forward slash (**/**) character is used to specify increments. For example, **1/3** in the `Day-of-Month` field means *every three days starting on the first day of the month*.

- The question mark (**?**) character is allowed for the `Day-of-Month` and `Day-of-Week` fields. It is used to specify *no specific value* for the given field. This is useful when you need to specify something in two of the fields but not the third. See Table 11 for clarification.

- The capital **L** character is allowed for the `Day-of-Month` and `Day-of-Week` fields. This character is short-hand for *last*, but it has a different meaning in each of the two fields.

  - The value **L** in the `Day-of-Month` field means *the last day of the month* (day 31 for January, day 28 for February on non leap years, and so on).

  - If used in the `Day-of-Week` field by itself, it simply means 7 or SAT.

  - If used in the `Day-of-Week` field after another value, it means *the last xxx day of the month* (for example, **6L** means *the last Friday of the month*).

  CAUTION   When using the L option, do not specify lists or ranges of values, as you will get confusing results.

- The capital **W** character is allowed for the `Day-of-Month` field. This character is used to specify *the weekday (Monday-Friday) nearest the given day*.

  As an example, if you were to specify **15W** as the value for the `Day-of-Month` field, the meaning is *the nearest weekday to the 15th of the month*.

  - If the 15th is a Saturday, the billing will occur on Friday the 14th.
  - If the 15th is a Sunday, the billing will occur on Monday the 16th.
  - If the 15th is a Tuesday, then the billing will occur on Tuesday the 15th.

  However, if you specify **1W** as the value for `Day-of-Month` and the 1st is a Saturday, the billing will occur on Monday the 3rd, as it will not *jump over* the boundary of a month's days.

  The W character can only be specified when the `Day-of-Month` is a single day, not a range or list of days.

- The **L** and **W** characters can also be combined for the `Day-of-Month` expression to yield **LW**, which translates to *last weekday of the month*.

🔶 The number sign (**#**) character is allowed for the `Day-of-Week` field. This character is used to specify *the nth xxx day of the month*.

For example, the value **6#3** means *the third Friday of the month* (day `6` = Friday and `#3` = the 3rd one of the month).

Other examples: **2#1** means *the first Monday of the month*, and **4#5** means *the fifth Wednesday of the month*.

CAUTION   If you specify **#5** and there are not five occurrences of that day in the given month, no billings will occur that month.

Table 11   Managed Billing frequency pattern examples

Recurrence Pattern Needed	Corresponding CRON Expression[*]
Weekly	
Every Wednesday in the month of March	`? MAR WED` or `? 3 WED` or `? 3 4`
Every Sunday, June through August	`? JUN-AUG SUN`
Every Monday	`? * MON`
Every 5th Monday	`? */5 MON`
Monthly	
First day of each month	`1 * ?`
First day of every three months starting January	`1 1/3 ?`
First day of every other month (odd months)	`1 1,3,5,7,9,11 ?`
First day of every other month (even months)	`1 2,4,6,8,10,12 ?`
15th day of every month	`15 * ?`
Last day of every month	`L * ?`
Last Friday of every month	`? * 6L` or `? * FRIL`
Third Friday of every month	`? * 6#3`
Nearest weekday to the first of the month	`1W * ?`
Last weekday of the month	`LW * ?`
Yearly	
1st of January	`1 JAN ?`
1st weekday of January	`1W JAN ?`
Last day of May, every year	`L MAY ?` or `L 5 ?`

* These are examples only—there are multiple ways to express most patterns.

3.3.2.4.7   Retry Logic Usage

Retry Logic, the function that allows transactions to be processed without risk of duplicating them **is not supported** for Profile Management transactions (Adds, Deletes, Retrieves, and Updates).

However, if an unknown result occurs when performing a Profile Management transaction, simply replay that transaction.

- If the prior transaction was a success, the second attempt will simply result in a duplicate response, which will not cause any harm.
- If the original request was not successful, the second attempt will create the desired result.

While Retry is not supported for Profile Management transactions, there is no harm in placing the Trace-ID values associated with Retry Logic in the `MIME-Header` of these request items. In these circumstances, the trace value will simply be ignored.

NOTE   When using a Profile during an Authorization, Retry Logic is fully supported as defined in the message specification.

3.3.3   Retry Logic

Retry Logic is a function available from the Orbital Gateway for client interfaces to reprocess transactions when there is an unknown result on a XML transaction request. It is available to any merchant interfacing to the Orbital Gateway using XML by simply adding two new values to the `MIME-Header`: the Merchant ID and a transaction Retry Trace Number. The Orbital Gateway uses this combination of values to determine the uniqueness of a transaction in determining how to process the transaction.

The result is that any Client properly utilizing Retry Logic can safely reprocess transactions with an unknown result while avoiding:

- Risk of double-authorizing a transaction against a cardholder's available balance.
- Duplication (or more) of settlement items.

The basic process flow of Retry Logic is as follows:

1. A request is submitted with a Retry Trace Number and Merchant ID in the `MIME-Header`.

2. The Gateway validates the Retry Trace Number and Merchant ID to determine if it has processed a transaction using that value pair within the past 48-hour window.

3. If the transaction was declined or generated an error on the initial response, the next request is treated as a new request.

4. If it has not processed the pair, the Gateway treats that transaction as a new request and processes it accordingly.

5. If it has processed the pair and the request has either already been processed (the initial response is an approval) or is in process, the Orbital Gateway will immediately echo back the exact response from the initial request.

   If the initial request is still in process, the Orbital Gateway will block and wait until that original response is completed. As soon as that is done, it will then echo back the same response as the original request.

The following sections outline the detailed business rules and implementation considerations associated with Retry Logic.

3.3.3.1 Retry Timing

The Orbital Gateway only retains an original Retry Trace Number/Merchant ID pair for 48 hours after submission. Any transaction that reuses these values more than 48 hours after the original transaction was submitted will be treated as a new request.

Therefore, if there is an unknown result for a transaction, that transaction must be reattempted within 48 hours or the original result must be determined through the Virtual Terminal Interface prior to regenerating the transaction.

3.3.3.2 Request Validation on Duplicate Trace Numbers

The following is a description of the message validation of the request when a retry attempt is made that matches a prior Retry Trace Number/Merchant ID combination.

- The following conditions result in an error, even if the Retry Trace Number/Merchant ID combination is a match:
  - There is no XML Document present.
  - That XML Document does not pass schema validation based on the version number passed in the `MIME-Header`.
  - The Merchant ID in the XML Document does not match the Merchant ID in the `MIME-Header`.
  - The request type (Auth versus Auth Capture versus Refund, and so on) must be the same.

    If the request type changes between transactions, a Quick Response is returned with a `ProcStatus` of `9715`, even if the Retry Trace Number/Merchant ID combination is a match.

- No other validation is associated with the XML Document of this request—beyond the request type and Retry Trace Number/Merchant ID, no other data between requests is matched.

  If, for example, two requests with the same Retry Trace Number and Merchant ID but different card numbers are submitted within 48 hours, the second request will still be treated as a duplicate.

CAUTION It is very important when implementing Retry Logic that the Retry Trace Number process is implemented correctly. Otherwise, the same result could be returned for different requests multiple times.

WARNING If the Retry Trace Number/Merchant ID pair **does not match** a prior transaction in the previous 48-hour window, the Orbital Gateway will treat that new message as a new request and process it accordingly, even if it is a *duplicate* transaction.

3.3.3.3 Transaction Types Supported

The Retry Logic for initial transactions and retry attempts can be used for all transaction types.

3.3.3.4 Retry Error Responses

When an error occurs resulting from the client's implementation of Retry Logic:

- That request is not processed.
- An error is returned, just as other Orbital Gateway errors are returned.

3.3.3.5   Concurrency

There is no limit to the number of Retry attempts on a transaction, as long as they all occur within the 48-hour window.

However, no more than two concurrent transactions with the same Retry Trace Number/Merchant ID value pair can be in process with the Orbital Gateway at any given time. If more than two transactions are sent while the Orbital Gateway is in the midst of processing the first two, it will immediately respond with an error code of 9711 (`Too many transactions to process`).

If this occurs, it might be an indicator of a Client problem. There would never be a reason to have more than two concurrent requests in queue with the same Retry Trace Number on a particular MID. As such, receiving this response code could indicate that the Retry Trace Number is not always being generated uniquely when it should be or that your system is not waiting long enough for responses.

3.3.3.6   Merchant ID

Retry Logic requires that the Merchant ID be submitted in the `MIME-Header` in addition to the XML Document. The Merchant IDs submitted in the `MIME-Header` and the XML Document must be the same or the Orbital Gateway will return an error in the form of a Quick Response with a `ProcStatus` of 9713, (`Invalid mime header - Merchant ID in mime does not match XML message`).

3.3.3.7   Retry Attempt Time Out

As indicated above, when a retry attempt is made while the original request is still in process, the Orbital Gateway will block and wait for that original response to be created with the intent to echo that completed response in the Retry response. However, the Orbital Gateway must return a result to the Client on all requests in no more than 90 seconds, including a retry attempt. Therefore, there is a time limit on how long the retry attempt will block and wait. If the original request response is not complete prior to this window, a Quick Response `ProcStatus` of 9710 (`Timed out waiting for transaction to complete`) will be returned.

If this occurs, the correct action is to make a second retry attempt of the transaction with the original request's Retry Trace Number/Merchant ID pair.

3.3.4 Account Updater

Fully managed Account Updater for Profiles is available to Salem (BIN 000001) merchants using customer profiles. The functionality is specifically designed to update merchant or chain level profiles housed on the gateway utilizing the Salem Account Updater process.   Visa and MasterCard approval is required for participation. Please contact your account representative for additional details.

Once enabled, update requests are submitted to Visa and MasterCard according to a merchant selected schedule. Visa and MasterCard typically respond to requests within three days, inclusive of the submission day. Visa and MasterCard responses may contain information regarding new card account numbers, expiration dates, account closures, etc. Based upon the actionable information returned, the Gateway automatically updates customer profiles. A scheduled report is available that lists profiles that were updated as a part of the process.

NOTE   If the card account number contained within a profile is invalid or not eligible for the Transaction Division's Account Updater setup on the host, the Account Updater request triggers a host reject.

NOTE   If the card account number is invalid or the card account is closed, an associated profile is automatically suspended, preventing unsuccessful future auth or capture attempts. As with any suspended profile, the status can easily be changed to active as new information becomes available

CAUTION   An Account Updater change of account number update to a profile is suppressed if the merchant initiates a change to the account number after the request is initiated and prior to the update.

The Account Updater transaction type facilitates an additional account updater request for a specific profile, outside of the selected schedule. The request is included in the next Account Updater submission unless sent with a future scheduled date (Use `<ScheduledDate>` to do so). A successful Account Updater transaction returns a message stating the profile is scheduled for Account Updater. Subsequent information provided by Visa or MasterCard is used for a profile update. This information is not returned via an XML response.

3.3.4.1   Designated Profiles

In some situations, merchants may have the need to exclude a subset of customer profiles from automatic scheduling of Account Updater requests. Fully managed Account Updater may be set up to support Designated Profiles. Please see the Virtual Terminal user's manual for information on enabling this setup.

When Account Updater for Designated Profiles Only is enabled, only profiles which are specifically flagged will be submitted according to the merchant's selected schedule. This is managed through the *Account Updater Eligibility flag* of the `NewOrder` complex type, or the `Profile` complex type when Updating or Creating a profile. Omitting this element is equivalent to setting the element to `N`.

The Account Updater Eligibility flag has no bearing on requests of the Account Updater transaction type.

3.3.5 Partial Authorization Support

A Partial Authorization occurs when the cardholder's issuing bank returns an approval for an amount less than the original requested amount. This is most common with customers who use branded pre-paid cards (such as Visa or Mastercard), but may happen under other circumstances as well.

The Orbital Gateway supports partial authorizations on New Order requests only. Partial authorizations are supported for both Salem (BIN 000001) and Tampa (BIN 000002) merchants. All merchants must communicate support for partial approvals in the request message to receive partial authorization response messages.

The `<PartialAuthInd>` element in the New Order message indicates support for partial authorizations.   For Tampa merchants, populating the element with a Y indicates a request for a partial authorization if the full amount cannot be authorized. Salem merchants can rely on host settings by sending populating the element with an S, or override the host settings by sending a Y or an N. Please see section *4.1 New Order Request Elements* for further details.
Partial Authorizations are not supported by New Order messages using specifications prior to *PTI50,* or with a NULL `<PartialAuthInd>` value.

WARNING Salem clients who have host system settings for Amex cards and do not indicate support for partial approvals may receive a partial approval response from Amex. The Orbital Gateway will respond to this by overriding the partial approval with a decline, returning a respcode value of 'M2'

3.3.6   Safetech Fraud Tools

The Orbital Gateway supports the Safetech™ Fraud Tools service. This advanced fraud scoring technology is offered to Salem (Bin 000001) merchants, enabling the detection of fraud patterns that are more difficult to identify through traditional fraud management tools.

Merchants create a custom fraud analysis strategy for their business using the Safetech Agent Web Console. The Safetech service applies this strategy to provide the following benefits:

- Minimize lost sales and the associated costs of combating fraud
- Control levels of fraud exposure with customizable tools
- Maximize order conversion, increasing your revenue

The Safetech service is fully integrated with Orbital Gateway processing. Whether including additional information in an authorization request, or sending a stand-alone request, the basic process remains the same:

- A consumer navigates to the payment page to complete a purchase or bill payment.
- The Safetech Fraud Tools seamlessly capture location and device data from the consumer.
- The merchant sends an authorization request or standalone Fraud Analysis request, including any additional or optional elements available, to the Orbital Gateway.
- The Safetech service returns fraud score information in the response message to the request.
  - A dynamic suite of detectors are utilized to perform real-time checks on over 200 variables, to produce a 'score' from 1 to 99 – a higher fraud score indicates a higher risk.
- Based on the response, the merchant determines whether to complete or reject the transaction.

Please contact your Account Representative for more information on the program, including how to obtain a Safetech Merchant ID (used in addition to the merchant ID number) and the assignment of a risk analyst.

The risk analyst:

- Provides ongoing monitoring of rule strategy effectiveness, including modification of rules as needed
- Assists with creation of fraud strategy and establishment of respective custom fraud rules

3.3.6.1   Fraud Analysis Requests

Fraud scoring information may be requested from the Safetech service through either an authorization (most `newOrder` or `flexCache` messages) or a standalone Fraud Analysis request (a `SafetechFraudAnalysis` message).

All data elements submitted in the transaction are included in the fraud scoring process performed by the Safetech service, so the overall value of the fraud score result is directly related to the transaction data included in the request.

Fraud analysis requests indicate one of two available formats. The format is designated by the `fraudScoreIndicator` element in the request and echoed in the response. The two fraud scoring formats are defined below:

Fraud Score 1 (FS1)

This is the short form fraud analysis request. It limits the information supplied, as well as the information returned in the response.

Fraud Score 2 (FS2)

This is the long form fraud analysis request. It extends both the number of data fields that may be submitted, as well as the volume of data returned in the response.

The Safetech service also allows for additional shopping cart data and user defined fields to be passed on a transaction by transaction basis. These data sets may be submitted through the `KTTVersionNumber`, `KTTDataLength`, and `KTTDataString` elements in the request message. See *5.1.4 Safetech Fraud Analysis Request* to see an example of this information.

3.3.6.2 Fraud Analysis Responses

Safetech Fraud Tools is a solution which enables a merchant to better determine the risk involved with a transaction. The Fraud Score is a numerical representation of the relative risk of each transaction that is screened. The information returned can be used to enhance any current risk program, or to develop a customized approach to risk management.

The Orbital Gateway provides the response information provided by the Safetech service; however it is the merchant's decision to proceed or not to proceed with a transaction.

Key items to remember when handling transactions which include Fraud Analysis:

- The authorization returned by the issuer and the Fraud Score response from the Safetech service are two separate and distinct values.

- The fraud score information does not impact the Merchant Selectable Response functionality provided by the Orbital Gateway. A fraud score value cannot trigger the Gateway to override an approval with a decline.

- When a transaction receives a fraud score a merchant deems unacceptable, the merchant should submit a corresponding Void or Reversal request to the Gateway to prevent the transaction from going out in settlement.

3.3.6.3 Other

Neither Level 2 and Level 3 data, nor Soft Descriptors, are supported by the Safetech service.

The Safetech service can utilize address data for countries which do not support AVS; however AVS responses are only provided by the customer's issuing bank.

Orbital Gateway supports the use of customer profiles to perform a Fraud Analysis request; however profiles may not be created as part of a standalone request to the Safetech service.

The Safetech Service is also available through the Orbital Gateway Virtual Terminal. Please see the Virtual Terminal user guide for more information.

3.3.7 Card Type Indicators: Enhanced Authorizations

Card Type Indicators are enhanced authorization data elements available to merchants who utilize the Salem (Bin 000001) platform. Card Type Indicators (sometimes abbreviated as CTI) are designed to capture valuable data that helps merchants make better payment decisions – both at the time of the transaction and afterward.

This enhanced authorization data can assist with:

- Targeting special communications to preferred customers.

- Minimizing recurring payment declines.

- Reducing fraud from specific countries.

- Providing better customer service.

All businesses can identify key data points that can drive payment decisions. Examples of the information returned by Card Type Indicators include:

- Affluent cardholders, which generally have no pre-set spending limit.
- Commercial cards, which support level 2 and possibly level 3 data.
- Prepaid cards, which are less likely to support recurring payments.
- Signature Debit cards, which are backed by a checking account of some sort.
- The Country of Issuance is also returned.

3.3.7.1   CTI Requests and Responses

All New Orders for BIN 000001 merchants may request Card Type Indicators. The `CardIndicators` element should be set to `Y` for all such transactions.

Orbital Gateway performs validations when this value is present. Those validations include:

- The Bin supports Card Type Indicators
- The Message Type is supported
  - Supported Message Types: A, AC
- The Method of Payment is supported
  - Supported MOPs: Visa, MasterCard, Discover, Diners, JCB, International Maestro

The `CardIndicators` element is ignored if any of the above validations fail – a corresponding proc status error is not returned.

Additional response values are returned when `CardIndicators` is set to `Y` on supported transactions. In addition to the issuing country, each indicator is returned as a separate response element. Response indicators contain a `Y`, `N`, or `X` value, where `X` indicates the indicator is Not Applicable.

3.3.7.2   Virtual Terminal

All of the functionality supported through this interface for Card Type Indicators is additionally available through the Orbital Gateway Virtual Terminal.

Merchants may request Enhanced Authorization data on a transaction by transaction basis, or for all Virtual Terminal transactions through the General Admin screen. Please refer to the Virtual Terminal user guide for more information.

Chapter 4   Message Definitions

This chapter contains tables describing the elements of the possible request and response messages, including:

- *New Order Request Elements*
- *New Order Response Elements*
- *Mark for Capture Request Elements*
- *Mark for Capture Response Elements*
- *Reversal (Void) Request Elements*
- *Reversal (Void) Response Elements*
- *End of Day Request Elements*
- *End of Day Response Elements*
- *Inquiry Request Elements*
- *Inquiry Response Elements*
- *Profile Request Elements*
- *Profile Response Elements*
- *Gift Card (FlexCache) Request Elements*
- *Gift Card (FlexCache) Response Elements*
- *Quick Response Elements*
- *Account Updater Request Elements*
- *Account Updater Response Elements*
- *Fraud Analysis Request Elements*
- *Fraud Analysis Response Elements*

Notes on Columns in the Tables

Required	M = Mandatory	
	C = Conditional	
	O = Optional	
Field Type	A = Alphanumeric	
	N = Numeric	

4.1 New Order Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
NewOrder	Request	**XML tag that defines the transaction as a New Order request**	M	N/A	N/A
OrbitalConnectionUsername	NewOrder	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	NewOrder	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
IndustryType	NewOrder	**Industry Type of the Transaction** MO Mail Order transaction RC Recurring Payment (not a valid choice for Canadian merchants) EC eCommerce transaction IV IVR (PINless Debit Only) IN Installment	M	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MessageType	NewOrder	**The transaction New Order Transaction Type** A Authorization request AC Authorization and Mark for Capture FC Force-Capture request R Refund request	M	2	A
BIN	NewOrder	**Transaction Routing Definition** Assigned by Chase Paymentech. 000001 Salem 000002 PNS	M	6	N
MerchantID	NewOrder	**Gateway merchant account number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number ▪ BIN 000002: 12-digit PNS Merchant ID	M	12	N
TerminalID	NewOrder	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to 001. ▪ PNS Terminal IDs: between 001 and 999; typically 001.	M	3	N
CardBrand	NewOrder	**Card Type/Brand for the Transaction** Required for: BL Bill Me Later DP PINless Debit (Generic Value Used in Requests) EC Electronic Check ED European Direct Debit IM International Maestro	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AccountNum	NewOrder	**Card Number Identifying the Customer** ▪ Should be NULL for electronic check processing and Profile Transactions. ▪ Can be NULL for Refund transactions, provided that the TxRefNum field is filled appropriately. ▪ For Bill Me Later transactions, should be populated with either the customer's Bill Me Later account number or a Bill Me Later Bank Identification Number (BIN) followed by ten zeros (dummy account number). For example: 5049900000000000 The consumer's 16-byte Bill Me Later account number will be returned on all approved transactions.	C	19	N
Exp	NewOrder	**Card Expiration Date** ▪ Format: MMYY ▪ Mandatory for all card types, except ECP, European Direct Debit, Bill Me Later, and PINless Debit. ▪ Can be NULL for Refund transactions, provided that the TxRefNum field is filled appropriately. ▪ Salem (BIN 000001) allows a *blank* to be submitted when no known expiration date exists. There are three valid mechanisms for submitting a *Blank* expiration date to the Salem Host using Orbital: - null-fill this XML element: `<Exp/>` - Send four spaces: `<Exp>    </Exp>` - Zero-fill this XML element: `<Exp>0000</Exp>` NOTE Please discuss this feature with your certification analyst before implementing.	C	4	N
CurrencyCode	NewOrder	**Transaction Currency Code** ▪ The ISO-assigned code for the currency of the transaction. ▪ Bin 000002 supports only U.S. Dollar (840) and Canadian Dollar (124). See *Table 22* in Appendix A for a list of currency codes.	M	3	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CurrencyExponent	NewOrder	**Exponent for the Transaction Currency** See *Table 22* in Appendix A for a list of currency code exponents.	M	6	N
CardSecValInd	NewOrder	**Card Security Presence Indicator** ▪ If you are trying to collect a Card Verification Number (CardSecVal) for a Visa or Discover transaction, pass one of these values: 1 Value is Present 2 Value on card but illegible 9 Cardholder states data not available ▪ If the transaction is not a Visa or Discover transaction: - Null-fill this attribute **OR** - Do not submit the attribute at all.	C	1	N
CardSecVal	NewOrder	**Card Verification Number** ▪ Visa CVV2 3 bytes ▪ MasterCard CVC2 3 bytes ▪ American Express CID 4 bytes ▪ Discover CID 3 bytes *WARNING* It is against regulations to store this value.	O	4	N
BCRtNum	NewOrder	**Bank Routing and Transit Number for the Customer** Conditionally required for Electronic Check processing. **NOTES:** ▪ All US Bank Routing Numbers are 9 digits. ▪ All Canadian Bank Routing Numbers are 8 digits. - Formatted FFFBBBBB where F is Financial Institution and B is Branch Number - Cannot include spaces " " or dashes "-"	C	9	N
CheckDDA	NewOrder	**Customer DDA Account Number** Conditionally required for Electronic Check processing.	C	17	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BankAccountType	NewOrder	**Deposit Account Type** Conditionally required for Electronic Check processing: C Consumer Checking (US or Canadian) S Consumer Savings (US Only) X Commercial Checking (US Only) *NOTE* If this tag is missing, the host will default the value to 'C' – Consumer Checking	C	1	A
ECPAuthMethod	NewOrder	**ECP Authorization Method** ▪ Code used to identify the method used by consumers to authorize debits to their accounts. ▪ Valid values: W Written I Internet (Web) – default T Telephone A Accounts Recievable (ARC) – US Merchants only P Point of Purchase (POP) – US Merchants only ▪ If no value submitted, we will default this value. See *3.2.5.3 ECP Authorization Methods* for more information.	O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BankPmtDelv	NewOrder	**ECP Payment Delivery Method** ▪ Conditionally required for Electronic Check processing. ▪ This field indicates the preferred manner to deposit the transaction: B Best Possible Method (US Only) Chase Paymentech utilizes the method that best fits the situation. If the RDFI is not an ACH participant, a facsimile draft is created. This should be the default value for this field. A ACH (US or Canadian) Deposit the transaction by ACH only. If the RDFI is not an ACH participant, the transaction is rejected. F Facsimile Draft This is a document created by CPS per merchant request or if the receiving bank is not a participant of the ACH association. The facsimile draft flows through the Federal Reserve's check clearing process rather than the ACH network	C	1	A
AVSzip	NewOrder	**Cardholder Billing Address Zip Code** ▪ All AVS Requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	10	A
AVSaddress1	NewOrder	**Cardholder Billing Address line 1** ▪ Should not include any of the following characters: % | ^ \ / ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	30	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVSaddress2	NewOrder	**Cardholder Billing Address line 2** ▪ Should not include any of the following characters: `%	^ \ /` ▪ Required for Bill Me Later sale transactions.	O	30	A
AVScity	NewOrder	**Cardholder Billing City** ▪ Should not include any of the following characters: `%	^ \ /` ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	20	A
AVSstate	NewOrder	**Cardholder Billing State** ▪ Should not include any of the following characters: `%	^ \ /` ▪ Required for Bill Me Later sale transactions.	C	2	A
AVSphoneNum	NewOrder	**Cardholder Billing Phone Number** `AAAEEENNNNXXXX`, where `AAA` = Area Code `EEE` = Exchange `NNNN` = Number `XXXX` = Extension Required for Bill Me Later sale transactions.	C	14	A
AVSname	NewOrder	**Cardholder Billing Name** Required for Bill Me Later sale transactions and all Electronic Check transactions, and all European Direct Debit (EU DD) transactions.	C	30	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVScountryCode	`NewOrder`	**Cardholder Billing Address Country Code** Valid values: `US` United States `CA` Canada `GB` Great Britain `UK` United Kingdom Conditionally required for Bill Me Later sale transactions.	C	2	A
AVSDestzip	`NewOrder`	**Bill Me Later Cardholder Destination Address Zip Code** ▪ All AVS Requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ Required for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service.	C	10	A
AVSDestaddress1	`NewOrder`	**Bill Me Later Cardholder Destination Address line 1** ▪ Should not include any of the following characters: `%	^ \ / –` ▪ Required for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service.	C	30	A
AVSDestaddress2	`NewOrder`	**Bill Me Later Cardholder Destination Address Line 2** ▪ Should not include any of the following characters: `%	^ \ / –` ▪ Optional for Bill Me Later Transactions. Also supported on non-BML transactions which use the Safetech service.	O	28	A
AVSDestcity	`NewOrder`	**Bill Me Later Cardholder Destination Billing City** ▪ Should not include any of the following characters: `%	^ \ / –` ▪ Required for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service.	C	20	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVSDeststate	NewOrder	**Bill Me Later Cardholder Destination Billing State** ▪ Should not include any of the following characters: `%  |  ^  \  /  -` ▪ Required for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service.	C	2	A
AVSDestphoneNum	NewOrder	**Bill Me Later Cardholder Destination Phone Number** `AAAEEENNNNXXXX`, where `AAA` = Area Code `EEE` = Exchange `NNNN` = Number `XXXX` = Extension ▪ Optional for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service. ▪ International phone numbers are restricted to 14 bytes therefore U.S. formats may not be applicable	O	14	A
AVSDestname	NewOrder	**Bill Me Later Cardholder Destination Billing Name** Required for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service.	C	30	A
AVSDestcountryCode	NewOrder	**Bill Me Later Cardholder Destination Address Country Code** ▪ Valid values: `US` United States `CA` Canada `GB` Great Britain `UK` United Kingdom `" "` Blank for all other countries ▪ Required for Bill Me Later sale transactions. Also supported on non-BML transactions which use the Safetech service.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

CustomerProfileFromOrderInd	NewOrder	**Method to use to Generate the Customer Profile Number**
		
		▪ When Customer Profile Action Type = Create, defines what the Customer Profile Number will be:
		  A Auto-Generate the CustomerRefNum
		  S Use CustomerRefNum field
		  O Use OrderID field
		  D Use Comments field
			C	5	A

CustomerRefNum	NewOrder	**Sets the Customer Reference Number that will be used to utilize a Customer Profile on all future Orders**
		
		▪ Mandatory if:
		Customer Profile Action Type = Create and CustomerProfileFromOrderInd = **S** (Use CustomerRefNum Element).
		
		▪ If CustomerProfileFromOrderInd = **A**, the Customer Reference Number will be defined by the Gateway, and any value passed in this element will be ignored.
		
		▪ The valid characters include:
		  - abcdefghijklmnopqrstuvwxyz
		  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
		  - 0123456789
		  - – , $ @ & and a space character, though the space character **cannot** be the leading character
		  - Please note that all alphabetic characters in this field are stored in uppercase by the Orbital system. Uppercase and lowercase values cannot be used to differentiate Customer Reference Numbers.
		
		▪ This value cannot be changed through a Profile Update action.
			C	22	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerProfileOrderOverrideInd	NewOrder	**Defines if any Order Data can be pre-populated from the Customer Reference Number (`CustomerRefNum`)** ▪ Mandatory if Customer Profile Action Type = `Create`. NO No mapping to order data OI Use `<CustomerRefNum>` for `<OrderID>` OD Use `<CustomerReferNum>` for `<Comments>` OA Use `<CustomerRefNum>` for `<OrderID>` and `<Comments>`	C	2	A
Status	NewOrder	**Profile Status Flag** This field is used to set the status of a Customer Profile. A Active I Inactive MS Manual Suspend	C	Var	A
AuthenticationECIInd	NewOrder	**The Transaction Type** Conditionally required for Verified by Visa and MasterCard SecureCode transactions. 5 Verified by Visa/MasterCard SecureCode – Authenticated Transaction 6 Verified by Visa/MasterCard SecureCode – Attempted Authentication	C	1	N
CAVV	NewOrder	**Cardholder Authentication Verification Value (CAVV)** ▪ Conditionally required for Verified by Visa. ▪ This number must be Base 64 Encoded. ▪ Cryptographic value derived with an algorithm that applies the Issuer's private key to the combination of the Cardholder account number, the Transaction Identifier (`XID`), and other data.	C	40	A
XID	NewOrder	**Transaction ID used in Verified by Visa Transactions** ▪ This number must be Base 64 Encoded. ▪ Unique tracking number set by the Merchant and sent to the Issuer Authentication/Service in the Authentication Request message. (Optional)	O	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PriorAuthID	`NewOrder`	**Defines the Transaction Type as a Prior Authorization** ▪ When this value is present, the request is considered a Force Authorization. ▪ No online authorization will be generated to the Host systems.	O	6	A
OrderID	`NewOrder`	**Merchant-Defined Order Number** ▪ Field defined and supplied by the auth originator and echoed back in response. ▪ The first 8 characters should be unique for each transaction. The valid characters include: ▪ `abcdefghijklmnopqrstuvwxyz` ▪ `ABCDEFGHIJKLMNOPQRSTUVWXYZ` ▪ `0123456789` ▪ `-` , `$` `@` `&` and a space character, though the space character **cannot** be the leading character ▪ PINless Debit transactions can only use uppercase and lowercase alpha (A-Z, a-z) and numeric (0-9) characters—NO special characters. For BIN 000002 merchants: ▪ If `IndustryType` = `EC`, first 16 bytes are passed to the Host Processing System ▪ If `IndustryType` = `MO`, first 9 bytes are passed to the Host Processing System	M	22	A
Amount	`NewOrder`	**Transaction Amount** Implied decimal, including those currencies that are a zero exponent. For example, both $100.00 (an exponent of 2) and ¥100 (an exponent of 0) should be sent as `<Amount>`**10000**`</Amount>`.	C	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Comments	NewOrder	**Free-form comments** ▪ Merchant can fill in this field, and the information will be stored with the transaction details. ▪ For PNS customers, this field will populate the Customer Defined Data field, which is displayed in Resource Online.	O	64	A
ShippingRef	NewOrder	**Shipping Tracking Reference Number** Merchant can fill in this field, and the information will be stored with the transaction details.	O	40	A
TaxInd	NewOrder	**Level 2 Data- Tax Type** Conditionally required for Level 2 Data. 0 Not provided 1 Included 2 Non-Taxable See *Level 2 & 3 Data Reference* for further details.	C	1	N
Tax	NewOrder	**Level 2 Data- Tax Amount for the Purchase** ▪ Conditionally required for Level 2 Data. ▪ Implied decimal, including those currencies that are a zero exponent. See *Level 2 & 3 Data Reference* for further details.	C	12	N
AMEXTranAdvAddn1	NewOrder	**Amex Purchasing Card Data – Transaction Advice Addendum #1** ▪ The TAA Record is used to further identify the purchase associated with the charge to the cardholder. ▪ It is also used in Purchasing/Procurement card transactions to provide specific details about the transaction to the cardholder for tracking purposes. ▪ TAAs should be as concise as possible, while still providing adequate information. For example, a TAA of `Merchandise` would not be acceptable. ▪ Salem Only/Conditionally required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AMEXTranAdvAddn2	`NewOrder`	**Amex Purchasing Card Data – Transaction Advice Addendum #2** Salem Only/Conditionally required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	40	A
AMEXTranAdvAddn3	`NewOrder`	**Amex Purchasing Card Data – Transaction Advice Addendum #3** Salem Only/Conditionally required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	40	A
AMEXTranAdvAddn4	`NewOrder`	**Amex Purchasing Card Data – Transaction Advice Addendum #4** Salem Only/Conditionally required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	40	A
AAV	`NewOrder`	**Accountholder Authentication Value for MasterCard SecureCode** ▪ Conditionally required for MasterCard SecureCode transactions. ▪ This number must be Base 64 Encoded. ▪ Unique transaction token generated by the issuer and presented to the merchant each time a cardholder conducts an electronic transaction using MasterCard SecureCode. AAV incorporates elements specific to the transaction and effectively binds the cardholder to a transaction at a merchant for a given sales amount.	C	32	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

SDMerchantName	NewOrder	**Soft Descriptor Merchant Name**
		▪ Conditionally required for Soft Descriptors.
		▪ The Merchant Name field should be what is most recognizable to the cardholder (Company name or trade name). The actual length of this field is conditionally tied to Host and the Size of the `<SDProductDescription>` field used.
		Salem:
		▪ CREDIT – Three options, which conditionally affect the `SDProductDescription`:
		  - Max 3 bytes
		  - Max 7 bytes
		  - Max 12 bytes
		▪ ECP:
		  - Max 15 bytes
		PNS:
		▪ Max 25 bytes
			C	25	A

SDProductDescription	NewOrder	**Soft Descriptor Product Description**
		▪ Conditionally required for Soft Descriptors.
		▪ Provides an accurate product description.
		Salem:
		▪ CREDIT:
		  - If `SDMerchantName` = 3 bytes, then Max = 18 bytes
		  - If `SDMerchantName` = 7 bytes, then Max = 14 bytes
		  - If `SDMerchantName` = 12 bytes, then Max = 9 bytes
		▪ ECP:
		  - 10 bytes Max
		PNS:
		▪ This field will not show on Cardholder statements for PNS Merchants.
			C	18	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SDMerchantCity	`NewOrder`	**Soft Descriptor Merchant City** ▪ Tag conditionally required for Soft Descriptors. ▪ Merchant City for Retail. Field required, but should be null-filled if any Soft Descriptor data is submitted.	C	13	A
SDMerchantPhone	`NewOrder`	**Soft Descriptor Merchant Phone** ▪ Tag conditionally required for Soft Descriptors. ▪ Only one of the location Soft Descriptor values should be sent (Phone, URL, or E-mail); all others should be null-filled. ▪ This field will not show on Cardholder statements for PNS Merchants. Valid Formats: ▪ `NNN-NNN-NNNN` ▪ `NNN-AAAAAAA` *NOTE* For MasterCard MOTO and Recurring, if the City/Phone field at the division level is not a Customer Service Phone Number, then a Customer Service Phone Number must be populated or the transaction will reject with Response Reason Code `BP` (`Missing Customer Service Phone`).	C	12	A
SDMerchantURL	`NewOrder`	**Soft Descriptor Merchant URL** ▪ Tag conditionally required for Soft Descriptors (can be null-filled). ▪ Only one of the location Soft Descriptor values should be sent (Phone, URL, or E-mail); all others should be null-filled. ▪ This field will not show on Cardholder statements for PNS Merchants.	C	13	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SDMerchantEmail	NewOrder	**Soft Descriptor Merchant E-mail** ▪ Field conditionally required for Soft Descriptors. ▪ Only one of the location Soft Descriptor values should be sent (Phone, URL, or E-mail); all others should be null-filled. ▪ This field will not show on Cardholder statements for PNS Merchants.	C	13	A
RecurringInd	NewOrder	**Recurring indicator** This tag is conditionally required for merchants that are: ▪ Located in Canada ▪ And processing on BIN 000002 ▪ And processing recurring transactions This field should not be sent when the IndustryType field is recurring. In Canada, the objective is to define the initial transaction collection method. Valid values: RF First Recurring Transaction RS Subsequent Recurring Transactions	C	2	A
EUDDCountryCode	NewOrder	**European Direct Debit Country Code** ▪ Customer's Country Code. ▪ Valid country codes: AT Austria BE Belgium DE Germany FR France GB United Kingdom NL Netherlands ▪ Conditionally required for European Direct Debit.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

EUDDBankSortCode		**European Direct Debit Bank Sort Code**
		▪ Customer's Bank Sort code.
		▪ Mandatory for the following Country Codes:
		  AT Austria
		  DE Germany
		  FR France
		  GB United Kingdom
			C	10	A

EUDDRibCode	NewOrder	**European Direct Debit RIB** ▪ Bank Account checksum. ▪ Used in France only.	C	2	A
BMLCustomerIP	NewOrder	**Customer's IP Address** Optional for Bill Me Later sale transactions.	O	45	A
BMLCustomerEmail	NewOrder	**Customer E-mail Address** Optional for Bill Me Later sale transactions.	O	50	A
BMLShippingCost	NewOrder	**Total Shipping Cost of Consumer's Order** Mandatory for Bill Me Later sale transactions.	C	8	N
BMLTNCVersion	NewOrder	**Terms and Conditions Number** ▪ The Terms and Conditions Number to which the consumer agreed. ▪ Mandatory for Bill Me Later sale transactions.	C	5	N
BMLCustomerRegistrationDate	NewOrder	**Customer Registration Date** ▪ The date a customer registered with the merchant. ▪ Mandatory for Bill Me Later sale transactions.	C	8	N

BMLCustomerTypeFlag	NewOrder	**Customer Type Flag**
		▪ New or Existing Customer to the Merchant (not Bill Me Later):
		  N New
		  E Existing
		▪ Optional for Bill Me Later sale transactions.
			O	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BMLItemCategory	`NewOrder`	**Item Category** ▪ Product Description Code assigned by Bill Me Later, Inc. ▪ Mandatory for Bill Me Later sale transactions.	C	4	N
BMLPreapprovalInvitationNum	`NewOrder`	**Pre-Approval Invitation Number** ▪ Indicates whether the consumer has been pre-approved for Bill Me Later. - Pre-approval from a credit bureau should include the 16-digit pre-approval number. This will allow the pre-approval to be matched with the first consumer order. - Internal pre-approval should have `1` as the leftmost digit. - Pre-approvals cannot include all zeros or be blank-filled. ▪ Optional for Bill Me Later sale transactions.	O	16	A
BMLMerchantPromotionalCode	`NewOrder`	**Merchant Promotional Code** Optional for Bill Me Later sale transactions.	O	4	A
BMLCustomerBirthDate	`NewOrder`	**Customer Date of Birth** ▪ Format: `YYYYMMDD` ▪ Mandatory for Bill Me Later sale transactions.	C	8	N
BMLCustomerSSN	`NewOrder`	**Customer Social Security Number** ▪ Either the full 9 digits or last 4 digits of the customer's Social Security Number. ▪ Mandatory for Bill Me Later sale transactions.	C	9	N
BMLCustomerAnnualIncome	`NewOrder`	**Gross Household Annual Income** ▪ Implied decimal. For example, $100,000.00 should be sent as: `<BMLCustomerAnnualIncome>10000000</BMLCustomerAnnualIncome>` ▪ Optional for Bill Me Later sale transactions.	O	10	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

BMLCustomerResidenceStatus	NewOrder	**Customer Residence Status**
		
		Valid values:
		  O Own
		  R Rent
		  X Other
		
		Optional for Bill Me Later sale transactions.
			O	1	A

BMLCustomerCheckingAccount	NewOrder	**Customer Checking Account Indicator**
		
		Valid values:
		  Y Yes, customer has a checking account
		  N No, customer does not have a checking account
		
		Optional for Bill Me Later sale transactions.
			O	1	A

BMLCustomerSavingsAccount	NewOrder	**Customer Savings Account Indicator**
		
		Valid values:
		  Y Yes, customer has a savings account
		  N No, customer does not have a savings account
		
		Optional for Bill Me Later sale transactions.
			O	1	A

BMLProductDeliveryType	NewOrder	**Delivery Type Indicator**
		
		Valid values:
		  CNC Cash and Carry
		  DIG Digital Goods
		  PHY Physical Delivery Required
		  SVC Service
		  TBD To Be Determined
		
		Optional for Bill Me Later sale transactions.
			C	3	A

BillerReferenceNumber	NewOrder	**Biller Reference Number (PINless Debit Only)** ▪ Reference Number the Biller (merchant) uses on their system to identify this customer. ▪ Conditionally required for PINless Debit.	C	25	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBType	NewOrder	**Managed Billing Type** ▪ Indicates the type of Managed Billing the merchant is participating in: R Recurring D Deferred ▪ The value submitted must be in agreement with the type of Managed Billing the merchant is configured for at Chase Paymentech. ▪ This field serves to notify the Orbital system that the transaction is a Managed Billing transaction. If this field is not sent with a Managed Billing transaction, all other Managed Billing fields are ignored.	C	1	A
MBOrderIdGenerationMethod	NewOrder	**Managed Billing Order ID Generation Method** ▪ This value is used to set the method that Orbital will use to generate the Order ID for any Managed Billing transactions. ▪ This field does NOT influence the Order ID for stand-alone transactions initiated by the merchant, VT transactions, and so on. ▪ Valid values: IO Use the Customer Reference Number (Profile ID). This value is made up of the capital letters I and O, not numbers. DI Dynamically generate the Order ID. This value is made up of the capital letters D and I, no numbers.	C	2	A
MBRecurringStartDate	NewOrder	**Managed Billing Recurring Start Date** ▪ Defines the future date that Orbital will begin a recurring billing cycle to the associated Profile. ▪ To allow the Managed Billing engine to properly calculate and schedule all billings, this date must be at least one day after the request date (a recurring billing cycle can never begin on the date that the request message is sent to the Orbital system). ▪ Format: MMDDYYYY	C	8	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBRecurringEndDate	NewOrder	**Managed Billing Recurring End Date** ▪ Defines the future date that Orbital will end a recurring billing cycle to the associated Profile. ▪ Format: MMDDYYYY ▪ This is the first of three possible recurring end triggers. Only one end trigger can be submitted per request message.	C	8	N

MBRecurringNoEndDateFlag	NewOrder	**Managed Billing 'No End Date' Indicator**
		
		▪ Valid values:
		  Y Schedule recurring transactions for an infinite amount of time. A Y in this field overrides the value, if any, in the MBRecurringEndDate field.
		  N (or blank) Orbital will use the value of the MBRecurringEndDate field to define the recurring end date.
		
		▪ This is the second of three possible recurring end triggers. Only one end trigger can be submitted per request message.
			C	1	A

MBRecurringMaxBillings	NewOrder	**Managed Billing Max Number of Billings** ▪ This value defines the maximum number of billings that will be allowed for a recurring billing cycle. ▪ Valid values: 1–999999 ▪ This is the third of three possible recurring end triggers. Only one end trigger can be submitted per request message.	C	6	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBRecurringFrequency	`NewOrder`	**Managed Billing Recurring Frequency Pattern** This pattern is a subset of a standard `CRON` expression, comprising 3 fields separated by white space: <table><tr><th>Field</th><th>Allowed Values</th><th>Allowed Special Chars</th></tr><tr><td>Day-of-month</td><td>`1–31`</td><td>`, – * ? / L W`</td></tr><tr><td>Month</td><td>`1–12` or `JAN–DEC`</td><td>`, – * /`</td></tr><tr><td>Day-of-week</td><td>`1–7` or `SUN–SAT`</td><td>`, – * ? / L #`</td></tr></table> *SEE ALSO* For a full discussion of these three fields, the usage of the special characters, and multiple example values, see *3.3.2 Profiles and Managed Billing*.	C	Var	A
MBDeferredBillDate	`NewOrder`	**Managed Billing Deferred Billing Date** ▪ Defines the future date that Orbital will trigger a one-time billing to the associated Profile. ▪ This date must be at least one day after the request date (a deferred billing can never take place on the date that the request message is sent to the Orbital system). ▪ Format: `MMDDYYYY`	C	8	N
TxRefNum	`NewOrder`	**Gateway Transaction Reference Number** A unique value is assigned by the Gateway for each transaction. ▪ The only time this field is used in a New Order is to complete a **Return** (Refund, Credit) transaction on the card used in the original transaction from which the `TxRefNum` was issued. If this field is submitted with any other type of New Order transaction, it is ignored. ▪ If this field is submitted with a Return, the card number and expiration date are no longer required. ▪ If no amount is sent, the original amount is refunded. ▪ If an amount is sent, it must be less than or equal to the original amount.	O	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PCOrderNum	NewOrder	**PO Number or Order Number from Customer** Required for Level 2 Data. Do not include the following characters: `<>?;':"[]\{}|` `=~!@#%^&*()_+` See *Level 2 & 3 Data Reference* for further details.	C	17	A
PCDestZip	NewOrder	**Shipping Destination Zip Code for the Purchase** ▪ Required for Level 2 and Level 3 Data. ▪ For Zip Code + 4, please separate with a hyphen (-). ▪ Required for best interchange rate. ▪ Cannot be all zeros or all nines. See *Level 2 & 3 Data Reference* for further details.	C	10	A
PCDestName	NewOrder	**Amex Purchasing Card Data - Cardholder Ship To: Name** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	30	A
PCDestAddress1	NewOrder	**Amex Purchasing Card Data - Cardholder Ship To: Address line 1** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	30	A
PCDestAddress2	NewOrder	**Amex Purchasing Card Data - Cardholder Ship To: Address line 2** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	30	A
PCDestCity	NewOrder	**Amex Purchasing Card Data – Cardholder Ship To: City** Salem Only/Required for Amex Purchasing Card Data See *Level 2 & 3 Data Reference* for further details.	C	20	A
PCDestState	NewOrder	**Amex Purchasing Card Data – Cardholder Ship To: State** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3FreightAmt	NewOrder	**Level 3 Freight Amount for Shipment** Total freight or shipping and handling charges. Implied decimal. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3DutyAmt	NewOrder	**Level 3 Duty Amount for Shipment** Total charges for any import and/or export duties included in this transaction. Implied decimal. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3DestCountryCd	NewOrder	**Level 3 Destination Country Code** ▪ The ISO-assigned code of the country to which the goods are shipped. ▪ Required for all Level 3 transactions. ▪ If no value is submitted, defaults to the United States (USA). See *Table 18 ISO country codes* in Appendix A. See *Level 2 & 3 Data Reference* for further details.	C	3	A
PC3ShipFromZip	NewOrder	**Level 3 Ship From Zip Code** ▪ The zip/postal code of the location from which the goods are shipped. ▪ Required for best interchange rate. ▪ Cannot be all zeros or all nines. See *Level 2 & 3 Data Reference* for further details.	C	10	A
PC3DiscAmt	NewOrder	**Level 3 Discount Amount from Order** ▪ The total amount of discount applied to the transaction by the merchant. Used by the merchant when a price break is given on an entire transaction rather than on unit prices. Typically, this is shown as a credit on a detailed invoice. ▪ Implied decimal. ▪ Optional. For Visa only; should not be sent for MasterCard. See *Level 2 & 3 Data Reference* for further details.	O	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3VATtaxAmt	NewOrder	**Level 3 Total Amount of VAT or Other Tax** ▪ The total amount of VAT or other tax included in this transaction. ▪ Implied decimal. ▪ Optional. For Visa only; should not be sent for MasterCard. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3VATtaxRate	NewOrder	**Level 3 Rate of VAT or Other Tax** ▪ The total amount of VAT or other tax included (expressed in percentage terms) for this line item. ▪ 2 decimal implied. For example, `0001` = 1%. ▪ Optional. For Visa only; should not be sent for MasterCard. See *Level 2 & 3 Data Reference* for further details.	O	4	N
PC3AltTaxInd	NewOrder	**Level 3 Alternate Tax ID** ▪ Tax ID number for the alternate tax associated with this transaction. ▪ Optional, but required if an amount is sent in `PC3AltTaxAmt`. ▪ For MasterCard only; should not be sent for Visa. See *Level 2 & 3 Data Reference* for further details.	O	15	N
PC3AltTaxAmt	NewOrder	**Level 3 Alternate Tax Amount** ▪ Total Amount of alternate tax associated with this transaction. ▪ Implied decimal. ▪ Optional, but required if a value is sent in `PC3AltTaxID`. ▪ For MasterCard only; should not be sent for Visa. See *Level 2 & 3 Data Reference* for further details.	O	9	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3LineItemCount	NewOrder	**Level 3 Number of Line Items** ▪ The number of Level 3 Line Item Detail items included with this transaction. ▪ The maximum number of line items is 98. ▪ At least 1 line item must be included to submit Level 3 data. ▪ Required for Level 3 Data.	C	2	N
PC3LineItemArray	NewOrder	**Level 3 Detail Header** Required parent tag for Level 3 Line Item Detail components.	C	N/A	N/A
PC3LineItem	PC3LineItemArray	**Parent XML Tag for Individual Level 3 Line Item Details** This XML element is the parent for each Line Item Detail included in this transaction. It should be repeated for each item up to the value of PC3LineItemCount.	C	N/A	N/A
PC3DtlIndex	PC3LineItem	**Level 3 Line Item Index** ▪ The sequential number (1–98) of this Line Item Detail within the PC3LineItemArray included with this transaction. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	2	N
PC3DtlDesc	PC3LineItem	**Level 3 Line Item Detail Element – Description** ▪ Text description of the item purchased. ▪ Cannot be all zeros. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	35	A
PC3DtlProdCd	PC3LineItem	**Level 3 Line Item Detail Element – Product Code** ▪ Product code of the item purchased. ▪ Cannot be all zeros. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	12	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlQty	PC3LineItem	**Level 3 Line Item Detail Element – Number of Units** ▪ Number of units of the item purchased. ▪ Cannot be all zeros. ▪ Implied decimal of 4. ▪ Required for Level 3 Data. See *Level 2 & 3 Data Reference* for further details. NOTE The Salem host (BIN 000001) requires a minimum quantity of one. Orbital will round this up for Salem merchants if the quantity is less than one.	C	13	N
PC3DtlUOM	PC3LineItem	**Level 3 Line Item Detail Element – Unit of Measurement** ▪ The unit of measure or unit of measure code used for this line item. ▪ Required for Level 3 Data. See *Table 19 Unit of measure codes* in Appendix A. Only known values are accepted. See *Level 2 & 3 Data Reference* for further details.	C	3	A
PC3DtlTaxAmt	PC3LineItem	**Level 3 Line Item Detail Element – Tax Amount** ▪ The tax amount for this item. ▪ Implied decimal. ▪ Required for Level 3 Data. See *Level 2 & 3 Data Reference* for further details.	C	13	N
PC3DtlTaxRate	PC3LineItem	**Level 3 Line Item Detail Element – Tax Rate** ▪ Tax rate applied for this item. ▪ Implied decimal of 3 as a percentage. For example: an interest rate of 6.25% should be sent as `06250`. ▪ Required for Level 3 Data. See *Level 2 & 3 Data Reference* for further details.	C	5	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

PC3Dtllinetot	PC3LineItem	**Level 3 Line Item Detail Element – Line Item Total**
		
		▪ For PNS customers:
		  - This field must equal the Unit Cost (PC3DtlUnitCost) multiplied by the quantity (PC3DtlQty) less any discounts (PC3DtlDisc). If it does not, then this transaction will receive an error.
		  - Additionally, the sum of all the Line Item totals (that is, the sum of all these fields) cannot exceed the transaction amount (<Amount>) submitted for this order.
		▪ Implied decimal.
		▪ Cannot be all zeros for either PNS or Salem.
		▪ Required for Level 3 Data.
		See Level 2 & 3 Data Reference for further details.
			C	13	N

PC3DtlDisc	PC3LineItem	**Level 3 Line Item Detail Element – Discount Amount for Line Item** ▪ Amount of the discount applied to the line item. ▪ Implied decimal. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	13	N
PC3DtlCommCd	PC3LineItem	**Level 3 Line Item Detail Element – Commodity Code for Line Item** ▪ The commodity code used to classify the item purchased. ▪ Required for Visa Level 3 Data; should not be sent for MasterCard. *See Level 2 & 3 Data Reference for further details.*	C	12	N
PC3DtlUnitCost	PC3LineItem	**Level 3 Line Item Detail Element – Unit Cost of Item Purchased** ▪ Unit Cost of the unit purchased. ▪ Implied decimal of 4. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	13	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlGrossNet	PC3LineItem	**Level 3 Line Item Detail Element – Gross/Net Indicator** ▪ Indicates whether tax amount is included in the item amount: Y Item amount includes tax amount N Item amount does not include tax amount ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	1	A
PC3DtlTaxType	PC3LineItem	**Level 3 Line Item Detail Element – Type of Tax Being Applied** Type of tax being applied. *See Level 2 & 3 Data Reference for further details.*	O	4	A
PC3DtlDiscInd	PC3LineItem	**Level 3 Line Item Detail Element – Discount Indicator** ▪ Indicates whether the amount is discounted: Y Amount is discounted N Amount is not discounted ▪ If value = Y and Discount Amount Field (PC3DtlDisc) is blank or zero-filled, Chase Paymentech will change this field indicator to **N** before sending the data. ▪ Required for MasterCard only; should not be sent for Visa. *See Level 2 & 3 Data Reference for further details.*	C	1	A
PC3DtlDebitInd	PC3LineItem	**Level 3 Line Item Detail Element – Item Debit/Credit Indicator** Valid values: D Item extended amount is a debit. C Item extended amount is a credit. Required for Level 3 Data for PNS (BIN 000002) Merchants. Should not be submitted by Salem (BIN 000001) merchants. *See Level 2 & 3 Data Reference for further details.*	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlDiscountRate	PC3LineItem	**Level 3 Line Item Detail Element – Discount Rate** ▪ The Discount Rate for this item. ▪ Implied decimal, four places. ▪ Only for Discover; Should not be sent for Visa or MasterCard ▪ Conditionally required for Level 3 Data for Salem (BIN 000001) merchants *See Level 2 & 3 Data Reference for further details.*	C	5	N
PartialAuthInd	NewOrder	**Partial Auth Support Indicator** This element must be populated to indicate the web application can support a partial authorization. Valid values: Y Specify the issuer should return a partial auth if needed. N Specify the issuer should not return a partial auth. S ***Salem (BIN 000001) only***: Indicates a partial auth can be supported without attempting to override host settings. Supported for Visa, MasterCard, Amex, and Discover only.	O	1	A
AccountUpdaterEligibility	NewOrder	**Account Updater Eligibility Flag** This element is used to designate if a customer profile created as part of a New Order should be eligible for Account Updater. • This field only applies to Salem (Bin 000001) merchants using the "Designated Profiles" Account Updater setup option. Valid values: Y Account Updater requests for this profile may be processed. N Account Updater requests for this profile will not be processed.	O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
UseStoredAAVInd	NewOrder	**Use Stored AAV Indicator** This element is conditionally required on recurring payments for International Maestro. Valid values: Y Submit the Static AAV stored by Gateway with this transaction. This should not be submitted if the **AAV** element is populated.	C	1	A
ECPActionCode	NewOrder	**ECP Action Code** This element is conditionally required to extend the MessageType for additional ECP processing methods. Valid values: LO Validate Only VO Validate & Verify VD Validate, Verify, and Deposit VP Validate, Verify, and Prenote ND Validate and Prenote (Debit) NC Validate and Verify (Credit) Supported for electronic check processing only. See *3.2.5.2 Extended ECP Processing Requirements* for more information.	C	2	A
ECPCheckSerialNumber	NewOrder	**ECP Check Serial Number** This value corresponds to the check number on a physical check supplied by the consumer. This value is 9 digits for BIN 000001 merchants and 6 digits for BIN 000002. Must be NULL unless CardBrand = EC and ECPAuthMethod = A or P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	Var	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ECPTerminalCity	NewOrder	**ECP Terminal City** This value corresponds to the city of the point of sale the check is processed at. Must be NULL unless CardBrand = EC and ECPAuthMethod = P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	4	A
ECPTerminalState	NewOrder	**ECP Terminal State** This value corresponds to the city of the point of sale the check is processed at. Must be NULL unless CardBrand = EC and ECPAuthMethod = P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	2	A
ECPImageReferenceNumber	NewOrder	**ECP Check Image Reference Number** Image reference number associated with a check. Must be NULL unless CardBrand = EC and ECPAuthMethod = P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	32	A/N
CustomerAni	NewOrder	**Customer Automatic Number Identification** The ANI specified phone number that the customer used to place the order. Recommended for transactions utilizing Safetech Fraud Tools.	O	10	N
AVSPhoneType	NewOrder	**Customer Telephone Type Indicator** Valid values: D Day H Home N Night W Work This value is defaulted to H if any phone number is present and this element is either not present or null filled.	O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVSDestPhoneType	NewOrder	**Bill Me Later Cardholder Destination Telephone Type Indicator** Valid values: D Day H Home N Night W Work This value is defaulted to H if any phone number is present and this element is either not present or null filled.	O	1	A
CustomerEmail	NewOrder	**Customer Email Address** The customer's contact email address.	O	50	A
EmailAddressSubtype	NewOrder	**Customer Email Address Subtype** Used to indicate the type of email address in the CustomerEmail element. Valid values: B Bill To/Buyer Email Address G Giftee Email Address This value is defaulted to B if an email address is present and this element is not present or null filled.	O	1	A
CustomerIpAddress	NewOrder	**Customer IP Address** The single source IP address used by the customer to request a payment. Supports IPv4 or IPv6 formats. Punctuation marks are allowed.	O	45	A/N
CustomerBrowserName	NewOrder	**Customer Browser Type** Used to indicate the type of web browser used by the customer to initiate the request. Example: MOZILLA/4.0 (COMPATIBLE; MSIE 5.0; WINDOWS 95)	O	60	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

ShippingMethod	NewOrder	**Method of Shipping To A Customer**
		
		Valid values:
		  C Lowest Cost
		  D Carrier Designated by Customer
		  E Electronic Delivery*
		  G Ground*
		  I International
		  M Military
		  N Next Day or Overnight*
		  O Other
		  P Store Pickup*
		  S Same Day*
		  T Two Day Service*
		  W Three Day Service*
		
		For American Express, use only values marked with an asterisk.
			O	1	A

FraudAnalysis	NewOrder	**Parent XML Tag for Safetech Fraud Analysis Elements**	O	N/A	N/A

FraudScoreIndicator	FraudAnalysis	**Fraud Analysis Type Indicator**
		
		Used to request the type of fraud analysis performed on the transaction. The value in this field directly determines the scope of elements returned in the response message.
		
		Valid values:
		  1 Short Form Request
		  2 Long Form Request
			C	1	N

RulesTrigger	FraudAnalysis	**Fraud Analysis Rules Return Trigger**
		
		Determines whether the Agent Web Console (AWC) rules are returned.
		
		Valid values:
		  Y Triggered rules are returned
		  N Triggered rules are not returned
			O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SafetechMerchantID	FraudAnalysis	**Safetech Merchant ID** A value assigned by Chase Paymentech when a merchant is enabled for the Safetech service. This is not the same value as Transaction Division number found in the `MerchantID` element. If no value is present, a default value will be used if available. If no default is stored, the request will generate an error.	O	6	A/N
KaptchaSessionID	FraudAnalysis	**Kaptcha Session ID** A merchant generated session ID for this fraud scoring request. The Safetech system recommends this value be unique for 30 days, or the Fraud Score results may not be accurate.	O	32	A
WebsiteShortName	FraudAnalysis	**Short Name for the Merchant's Website** This value is used by the Safetech service for fraud score rules.	O	8	A
CashValueOfFencibleIterms	FraudAnalysis	**Cash Value of Fencible Items** The cash value of any fencible items in the order. This element should only be sent when the `FraudScoreIndicator` element is set to 2.	O	12	N
CustomerDOB	FraudAnalysis	**Customer Date of Birth** Format: *YYYY-MM-DD* (Including dashes) This element should only be sent when the `FraudScoreIndicator` element is set to 2.	O	10	A/N

CustomerGender	FraudAnalysis	**Customer Gender**
		
		Valid values:
		  `F` Female
		  `M` Male
		
		This element should only be sent when the `FraudScoreIndicator` element is set to 2.
			O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerDriverLicense	FraudAnalysis	**Customer Driver's License Number** U.S. Driver's License number only. The Safetech service recommends this value for fraud scoring of Electronic Check (ECP) requests. This element should only be sent when the FraudScoreIndicator element is set to 2.	O	32	A
CustomerID	FraudAnalysis	**Customer ID** A merchant generated ID for a specific customer. This element should only be sent when the FraudScoreIndicator element is set to 2.	O	32	A
CustomerIDCreationTime	FraudAnalysis	**Customer ID Creation Time** The time the value used in the CustomerID element was created by the merchant. Format: Unix Epoc This element should only be sent when the FraudScoreIndicator element is set to 2.	O	10	N
KTTVersionNumber	FraudAnalysis	**User Defined and Shopping Cart Format Indicator** This element must contain a value of "1" as of the release of this specification if the KTTDataLength and KTTDataString elements are populated.	C	1	N
KTTDataLength	FraudAnalysis	**User Defined or Shopping Cart Format Data Length** Indicates the length of the value of the KTTDataString element. This must be a 4 digit number no less than 0001 and no greater than 0999.	C	4	N
KTTDataString	FraudAnalysis	**User Defined or Shopping Cart Format Data String** This field can be populated with user-defined Agent Web Console rules, Shopping Cart Data, or both. Please see *Special notes on KTT elements* for additional information.	C	Var	A/N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CardIndicators	NewOrder	**Enhanced Authorization: Card Type Indicators** This element is optionally available to BIN 000001 merchants, to request additional response information. This value is ignored on unsupported transactions. See *3.3.7.1* for more information. Valid values: Y Card Indicators should be returned, if available. N Card Indicators should not be returned	O	1	A

4.2   New Order Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required XML Parent Tag**	M	N/A	N/A
NewOrderResp	`Response`	**XML Tag that Defines the Transaction as a New Order Response**	M	N/A	N/A
IndustryType	`NewOrderResp`	**Industry Type of the Transaction** This tag returns `null` results.	M	2	A
MessageType	`NewOrderResp`	**Transaction New Order Transaction Type** Echoes the Message Type passed in the request.	M	2	A
MerchantID	`NewOrderResp`	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	M	12	N
TerminalID	`NewOrderResp`	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID passed in the request.	M	3	N
CardBrand	`NewOrderResp`	**Card Type/Brand for the Transaction** Echoes the Card Type/Brand passed in the request, except: ▪ If no `CardBrand`, such as Visa or MasterCard, was sent in the request (when optional), the specific Card Brand mnemonic is returned. ▪ For PINless Debit transactions, the *request* Card Brand is `DP` (which is a generic PINless mnemonic). However, the *response* Card Brand will be one of the four supported PINless Debit Card Brands: `NP` NYCE PINless Debit `PP` Pulse PINless Debit `SP` Star PINless Debit `AP` Accel PINless Debit	M	2	A
AccountNum	`NewOrderResp`	**Account Number** ▪ Value is conditionally returned for approved Bill Me Later transactions.	M	19	N
OrderID	`NewOrderResp`	**Merchant-Defined Order Number** Echoes the Order Number passed in the request.	M	22	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TxRefNum	NewOrderResp	**Gateway Transaction Reference Number** A unique value for each transaction, which is required to adjust any transaction in the Gateway (such as Mark for Capture or Void).	M	40	A
TxRefIdx	NewOrderResp	**Gateway Transaction Index** ▪ Used to identify the unique components of transactions adjusted more than one time. ▪ Required on Void transactions; not for Mark for Captures.	M	4	A
ProcStatus	NewOrderResp	**Process Status** ▪ The first element that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A
ApprovalStatus	NewOrderResp	**Approval Status** Conditional on Process Status returning a 0 (or successful) response. If so, the Approval Status identifies the result of the authorization request to the host system: 0 Declined 1 Approved 2 Message/System Error	C	1	N
RespCode	NewOrderResp	**Response Code** Normalized authorization response code issued by the host system (Salem/PNS), which identifies an approval (00) or the reason for a decline or error. See *Table 13* in Appendix A for values.	C	2	A
AVSRespCode	NewOrderResp	**Address Verification Request Response** Conditional on AVS request being sent. See *Table 14* in Appendix A for values.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CVV2RespCode	`NewOrderResp`	**Card Verification Value Request Response** Conditional on card verification request being sent. See *Table 17* in Appendix A for values.	C	1	A
AuthCode	`NewOrderResp`	**Issuer Approval Code** Unique transactional-level code issued by the bank or service establishment for approvals. PINless Debit transactions could return blanks or `N/A`.	C	6	A
RecurringAdviceCd	`NewOrderResp`	**Recurring Payment Advice Code** Valid values: 01 New account information available. Obtain new account information. 02 Try again later. Recycle transaction in 72 hours. 03 Do not try again. Obtain another type of payment from customer.	C	2	N
CAVVRespCode	`NewOrderResp`	**Response Code to Verified by Visa Requests** See *Table 20* in Appendix A for values.	C	1	A
StatusMsg	`NewOrderResp`	**Text Message Associated with `RespCode` Value**	C	Var	A
RespMsg	`NewOrderResp`	**Message Associated with `HostRespCode`** May not be populated for transactions not requiring an authorization such as Force or Refunds	C	80	A
HostRespCode	`NewOrderResp`	**Actual Host Response Code** ▪ Exact response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	3	A
HostAVSRespCode	`NewOrderResp`	**Actual Host Address Verification Response Code** ▪ Exact address verification response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
HostCVV2RespCode	NewOrderResp	**Actual Host Card Verification Response Code** ▪ Exact card verification response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	1	A
CustomerRefNum	NewOrderResp	**Customer Reference Number** If Customer Profile Action Type = `Create` and `CustomerProfileFromOrderInd` = `S`, this field will echo the Customer Reference Number sent in the Profile Request.	C	22	A
CustomerName	NewOrderResp	**Customer Billing Name** Echoes value from the request.	C	30	A
ProfileProcStatus	NewOrderResp	**Result Status of Profile Management** Communicates the success or failure of a Profile Management request: `0` Success `>0` An error condition, see *Table 16* in Appendix A for values	C	6	A
CustomerProfileMessage	NewOrderResp	**Verbose Text Description associated with `ProfileProcStatus`**	C	Var	A
BillerReferenceNumber	NewOrderResp	**Biller Reference Number (PINless Debit Only)** Echoes value from request.	C	25	A
RespTime	NewOrderResp	**Time the Transaction was Processed by Gateway** Format: `hh24mmss`	M	6	N
PartialAuthOccured	NewOrderResp	**Indicates if a Partial Approval was returned** This tag will be NULL unless a Partial Authorization has been returned.	C	1	A
RequestedAmount	NewOrderResp	**Requested Transaction Amount** Indicates the requested amount as returned in the response from the host.	C	Var	N
RedeemedAmount	NewOrderResp	**Redeemed Transaction Amount** Indicates the amount returned in the response from the host.	C	Var	N
RemainingBalance	NewOrderResp	**Remaining Card Balance** Indicates the amount remaining on the card when returned in the response from the issuer.	C	Var	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CountryFraudFilterStatus	NewOrderResp	**Country Fraud Filter Status** If the transaction is sent to the Salem (BIN 000001) host for a merchant who has enrolled in Country based Fraud filtering, the Salem host may send back a response message for this field. This will always be **NULL** for Tampa (BIN 000002) merchants Please contact your Account Executive for questions on fraud filtering.	C	1	A
IsoCountryCode	NewOrderResp	**ISO Country Code** Corresponds with the CountryFraudFilterStatus element, indicating the country where the consumer's card was issued. This will always be **NULL** for Tampa (BIN 000002) merchants. Please contact your Account Executive for questions on fraud filtering. Please see *Appendix 5.3.3A.11 - Fraud Filter Country Codes* for valid values.	C	2	A
FraudScoreProcStatus	NewOrderResp	**Process Status of Fraud Score request** ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks related specifically to Fraud Analysis messages: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	Var	N
FraudScoreProcMsg	NewOrderResp	**Verbose Text Description associated with `FraudScoreProcStatus`**	C	Var	A
FraudAnalysisResponse	NewOrderResp	**Parent Element of Fraud Analysis Response Data**	M	N/A	N/A
FraudScoreIndicator	FraudAnalysis Response	**Echoes `FraudScoreIndicator` from the request message.**	M	1	N
FraudStatusCode	FraudAnalysis Response	**Fraud Status Code** The response code returned by the Safetech service to indicating the status of the fraud analysis.	C	4	A
RiskInquiryTransactionId	FraudAnalysis Response	**Risk Inquiry Transaction ID** A unique ID used to identify the fraud assessment.	C	32	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AutoDecisionResponse	FraudAnalysis Response	**Auto Decision Response** The auto decision response code returned by the Safetech service. The following is a list of valid values. A Approved D Decline E Manager Review R Review This list may expand in the future.	O	1	A
RiskScore	FraudAnalysis Response	**Risk Score** This element may be returned as null if the Safetech service was not successful in generating a fraud score.	C	2	N
KaptchaMatchFlag	FraudAnalysis Response	**Kaptcha Match Flag** Indicates if a request to the Safetech service has a corresponding Kaptcha record.	O	1	A
WorstCountry	FraudAnalysis Response	**Worst Country** The two character ISO 3166 country code associated with this customer in the last 14 days. This element is only returned with a Fraud Score Indicator of 2.	C	2	A
CustomerRegion	FraudAnalysis Response	**Customer Region** The estimated region of the customer. The Safetech service will use lower case letters to represent a state or province, while uppercase letters indicate a county. This element is only returned with a Fraud Score Indicator of 2.	C	2	A
PaymentBrand	FraudAnalysis Response	**Payment Brand** The payment method (brand) identified by the Safetech service during Fraud Analysis. This element is only returned with a Fraud Score Indicator of 2.	O	4	A
FourteenDayVelocity	FraudAnalysis Response	**Fourteen Day Velocity** The total number of prior sales by this customer within the last 14 days. This element is only returned with a Fraud Score Indicator of 2.	O	2	A/N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SixHourVelocity	`FraudAnalysis Response`	**Six Hour Velocity** The total number of prior sales by this customer in any six hour window over the last 14 days. This element is only returned with a Fraud Score Indicator of 2.	O	2	A/N
CustomerNetwork	`FraudAnalysis Response`	**Customer Network Type indicator** A single character designation of the type of network used by the customer to initiate the transaction. Some possible values can include: `A` Anonymous `L` Library `H` High School `N` Normal `P` Prison `S` Satellite This element is only returned with a Fraud Score Indicator of 2.	O	1	A
NumberOfDevices	`FraudAnalysis Response`	**Number of Devices with Transaction** The number of devices associated with the transaction, as recorded by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	3	N
NumberOfCards	`FraudAnalysis Response`	**Number of Cards with Transaction** The number of cards associated with the transaction, as recorded by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	3	N
NumberOfEmails	`FraudAnalysis Response`	**Number of Emails with Transaction** The number of emails associated with the transaction, as recorded by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	3	N
DeviceLayers	`FraudAnalysis Response`	**Device Layer Description** A period-delimited description of the Network, Flash, JavaScript, HTTP, and Browser layers of the device used by the customer to initiate the transaction, as determined by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	54	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
DeviceFingerprint	FraudAnalysis Response	**Device Fingerprint** A hash of system identifiers determined by the Safetech service to be constants for the device used by the customer. This element is only returned with a Fraud Score Indicator of 2.	O	32	A
CustomerTimeZone	FraudAnalysis Response	**Customer Time Zone** The time zone where the customer resides, as an offset from GMT. This element is only returned with a Fraud Score Indicator of 2.	O	4	N
CustomerLocalDateTime	FraudAnalysis Response	**Customer Local Date & Time** The local timestamp of the customer's device. Format: YYYY-MM-DD HH:MM This element is only returned with a Fraud Score Indicator of 2.	O	16	N
DeviceRegion	FraudAnalysis Response	**Device Region** Indicates the region or state where the customer's device resides. The Safetech service will use lower case letters to represent a state or province, while uppercase letters indicate a county. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
DeviceCountry	FraudAnalysis Response	**Device Country** The ISO 3166 Country code which indicates the country where the customer's device resides. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
ProxyStatus	FraudAnalysis Response	**Proxy Status Indicator** Indicates if the device used by the customer is using a proxy network. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
JavascriptStatus	FraudAnalysis Response	**JavaScript Status Indicator** Indicates if the device used by the customer allows use of JavaScript. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
FlashStatus	FraudAnalysis Response	**Flash Status Indicator** Indicates if the device used by the customer allows Flash. This element is only returned with a Fraud Score Indicator of 2.	O	1	A

New Order Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CookiesStatus	`FraudAnalysis Response`	**Cookies Status Indicator** Indicates if the device used by the customer allows use of cookies. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
BrowserCountry	`FraudAnalysis Response`	**Browser Country** The ISO 3166 Country code which indicates the country where the customer's browser resides. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
BrowserLanguage	`FraudAnalysis Response`	**Browser Language** The ISO 639-1 standard code which indicates the language of the customer's browser. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
MobileDeviceIndicator	`FraudAnalysis Response`	**Mobile Device Indicator** Indicates if the device used by the customer is a mobile device. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
MobileDeviceType	`FraudAnalysis Response`	**Mobile Device Type** A description of the type of mobile device used by the customer. This element is only returned with a Fraud Score Indicator of 2.	O	32	A
MobileWirelessIndicator	`FraudAnalysis Response`	**Mobile Wireless Indicator** Indicates if the device used by the customer has wireless capabilities. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
VoiceDevice	`FraudAnalysis Response`	**Voice Device Indicator** Indicates if the device used by the customer is voice controlled. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
PCRemoteIndicator	`FraudAnalysis Response`	**PC Remote Indicator** Indicates if the device used by the customer is a remotely controlled computer. This element is only returned with a Fraud Score Indicator of 2.	O	1	A

New Order Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
RulesDataLength	`FraudAnalysis Response`	**Rules Trigger Reply Data Length** Indicates the length of the data contained in the RulesData element. Values in this element are no less than 0005 and no greater than 0999. Returned only if the `RulesTrigger` element is set to 'Y' on the request message.	O	4	N
RulesData	`FraudAnalysis Response`	**Rules Trigger Reply Data** A comma-delimited list of the rules triggered in the Safetech service by the transaction request. For more information on the data contained in this element, please see *Special Notes on Rules Trigger response data.*	O	Var	A/N
CTIAffluentCard	`NewOrderResp`	**Card Indicator: Affluent Category** Affluent cards have very high pre-set spending limits, if any. Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTICommercialCard	`NewOrderResp`	**Card Indicator: Commercial Card** See *Level 2 and Level 3 Data* for more information. Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTIDurbinExemption	`NewOrderResp`	**Card Indicator: Durbin** Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTIHealthcareCard	`NewOrderResp`	**Card Indicator: Healthcare Card** Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTILevel3Eligible	`NewOrderResp`	**Card Indicator: Level 3 Data Eligibility** See *Level 2 and Level 3 Data* for more information. Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTIPayrollCard	`NewOrderResp`	**Card Indicator: Payroll Card** Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTIPrepaidCard	`NewOrderResp`	**Card Indicator: Prepaid Card** Returned only for BIN 000001 merchants on applicable transactions.	O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CTIPINlessDebitCard	NewOrderResp	**Card Indicator: PINless Debit Eligibility** See *PINless Debit* for more information. Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTISignatureDebitCard	NewOrderResp	**Card Indicator: Signature Debit Eligibility** Signature Debit refers to processing a debit card as a credit card. Returned only for BIN 000001 merchants on applicable transactions.	O	1	A
CTIIssuingCountry	NewOrderResp	**Card Indicator: Issuing Country** Used to distinguish a domestic or international customer. Format: 3 alphanumeric character ISO country code. Returned only for BIN 000001 merchants on applicable transactions.	O	3	A

4.3   Mark for Capture Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
MarkForCapture	Request	**XML tag that defines the transaction as a Mark for Capture request**	M	N/A	N/A
OrbitalConnectionUsername	MarkForCapture	**Orbital Connection Username set up on Orbital Gateway** Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
OrbitalConnectionPassword	`MarkForCapture`	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
OrderID	`MarkForCapture`	**Merchant-Defined Order Number** Must match the `OrderID` of the original request.	M	22	A
Amount	`MarkForCapture`	**Amount to be Captured** Keys: ▪ Implied decimal including those currencies that are a zero exponent. For example, both $100.00 (an exponent of 2) and ¥100 (an exponent of 0) should be sent as `<Amount>`**10000**`</Amount>`. ▪ Amount must be less than or equal to the amount of the original transaction being marked for capture. If the amount submitted is less than the original transaction, the New Order will be split.	C	12	N
TaxInd	`MarkForCapture`	**Level 2 Data- Tax type** Required for Level 2 Data. 0 Not provided 1 Included 2 Non-Taxable—not valid for Visa Level 2 qualification See *Level 2 & 3 Data Reference* for further details.	O	1	N
Tax	`MarkForCapture`	**Level 2 Data- Tax Amount for the Purchase** ▪ Required for Purchasing Card Level 2 Data. ▪ Implied decimal, including those currencies that are a zero exponent. See *Level 2 & 3 Data Reference* for further details.	O	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BIN	`MarkForCapture`	**Transaction Routing Definition** Assigned by Chase Paymentech. `000001`　　Salem `000002`　　PNS	M	6	N
MerchantID	`MarkForCapture`	**Gateway Merchant Account Number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number ▪ BIN 000002: 12-digit PNS Merchant ID	M	15	N
TerminalID	`MarkForCapture`	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to `001`. ▪ PNS Terminal IDs: between `001` and `999`; typically `001`.	M	3	N
TxRefNum	`MarkForCapture`	**Gateway transaction Reference Number** A unique value for each transaction, which is required to adjust any transaction in the Gateway, such as Mark for Capture or Void.	M	40	A
PCOrderNum	`MarkForCapture`	**Level 2 Data- PO Number from Customer** Required for Level 2 Data. Do not include the following characters: <>?;':"[]\{}|`=~!@#%^&*()_+ *See Level 2 & 3 Data Reference for further details.*	O	17	A
PCDestZip	`MarkForCapture`	**Level 2 Data- Shipping Destination Zip Code for the Purchase** ▪ Required for Level 2 Data. ▪ For Zip Code + 4, please separate with a hyphen (-). *See Level 2 & 3 Data Reference for further details.*	O	10	A
PCDestName	`MarkForCapture`	**Amex Purchasing Card Data - Cardholder Ship To: Name** Salem Only/Required for Amex Purchasing Card Data. *See Level 2 & 3 Data Reference for further details.*	O	30	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PCDestAddress1	MarkForCapture	**Amex Purchasing Card Data - Cardholder Ship To: Address line 1** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	C	30	A
PCDestAddress2	MarkForCapture	**Amex Purchasing Card Data - Cardholder Ship To: Address line 2** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	O	30	A
PCDestCity	MarkForCapture	**Amex Purchasing Card Data – Cardholder Ship To: City** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	O	20	A
PCDestState	MarkForCapture	**Amex Purchasing Card Data – Cardholder Ship To: State** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	O	2	A
AMEXTranAdvAddn1	MarkForCapture	**Amex Purchasing Card Data - Transaction Advice Addendum #1** ▪ The TAA Record is used to further identify the purchase associated with the charge to the cardholder. ▪ It is also used in Purchasing/Procurement card transactions to provide specific details about the transaction to the cardholder for tracking purposes. ▪ TAAs should be as concise as possible, while still providing adequate information. For example, a TAA of `Merchandise` would not be acceptable. ▪ Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	O	40	A
AMEXTranAdvAddn2	MarkForCapture	**Amex Purchasing Card Data - Transaction Advice Addendum #2** Salem Only/Required for Amex Purchasing Card Data See *Level 2 & 3 Data Reference* for further details.	O	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AMEXTranAdvAddn3	MarkForCapture	**Amex Purchasing Card Data - Transaction Advice Addendum #3** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	O	40	A
AMEXTranAdvAddn4	MarkForCapture	**Amex Purchasing Card Data - Transaction Advice Addendum #4** Salem Only/Required for Amex Purchasing Card Data. See *Level 2 & 3 Data Reference* for further details.	O	40	A
PC3FreightAmt	MarkForCapture	**Level 3 Freight Amount for Shipment** Total freight or shipping and handling charges. Implied decimal. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3DutyAmt	MarkForCapture	**Level 3 Duty Amount for Shipment** Total charges for any import and/or export duties included in this transaction. Implied decimal. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3DestCountryCd	MarkForCapture	**Level 3 Destination Country Code** ▪ The ISO-assigned code of the country to which the goods are shipped. ▪ Required for all Level 3 transactions. ▪ If no value is submitted, defaults to the United States (USA). See *Table 18* in Appendix A for country codes. See *Level 2 & 3 Data Reference* for further details.	C	3	A
PC3ShipFromZip	MarkForCapture	**Level 3 Ship from Zip** ▪ The zip/postal code of the location from which the goods are shipped. ▪ Required for best interchange rate. ▪ Cannot be all zeros or nines. See *Level 2 & 3 Data Reference* for further details.	C	10	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DiscAmt	MarkForCapture	**Level 3 Discount Amount from Order** ▪ The total amount of discount applied to the transaction by the merchant. Used by the merchant when a price break is given on an entire transaction rather than on unit prices. Typically, this is shown as a credit on a detailed invoice. ▪ Implied decimal. ▪ Optional. For Visa only; should not be sent for MasterCard. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3VATtaxAmt	MarkForCapture	**Level 3 Total Amount of VAT or Other Tax** ▪ The total amount of VAT or other tax included in this transaction. ▪ Implied decimal. ▪ Optional. For Visa only; should not be sent for MasterCard. See *Level 2 & 3 Data Reference* for further details.	O	12	N
PC3VATtaxRate	MarkForCapture	**Level 3 Rate of VAT or Other Tax** ▪ The total amount of VAT or other tax included (expressed in percentage terms) for this line item. ▪ 2 decimal implied. For example, `0001` = 1%. ▪ Optional. For Visa only; should not be sent for MasterCard. See *Level 2 & 3 Data Reference* for further details.	O	4	N
PC3AltTaxID	MarkForCapture	**Level 3 Alternate Tax ID** ▪ Tax ID number for the alternate tax associated with this transaction. ▪ Optional. For MasterCard only; should not be sent for Visa. ▪ Required if an amount is sent in `PC3AltTaxAmt`. See *Level 2 & 3 Data Reference* for further details.	O	15	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3AltTaxAmt	MarkForCapture	**Level 3 Alternate Tax Amount** § Total Amount of alternate tax associated with this transaction. § Implied decimal. § Optional. For MasterCard only; should not be sent for Visa. § Required if a value is sent in PC3AltTaxInd. See *Level 2 & 3 Data Reference for further details.*	O	9	N
PC3LineItemCount	MarkForCapture	**Level 3 Number of Line Items** § The number of Level 3 Line Item Detail items included with this transaction. § The maximum number of line items is 98. § At least 1 line item must be included to submit Level 3 Data. § Required for Level 3 Data.	C	2	N
PC3LineItemArray	MarkForCapture	**Level 3 Detail Header** Required parent tag for Level 3 Line Item Detail components.	C	N/A	N/A
PC3LineItem	PC3LineItemArray	**Parent XML Tag for Individual Level 3 Line Item Details** This XML element is the parent for each Line Item Detail included in this transaction. It should be repeated for each item up to the value of PC3LineItemCount.	C	N/A	N/A
PC3DtlIndex	PC3LineItem	**Level 3 Line Item Index** § The sequential number (1–98) of this Line Item Detail within the PC3LineItemArray included with this transaction. § Required for Level 3 Data. See *Level 2 & 3 Data Reference for further details.*	C	2	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlDesc	PC3LineItem	**Level 3 Line Item Detail Element – Description** ▪ Text description of the item purchased. ▪ Cannot be all zeros. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	35	A
PC3DtlProdCd	PC3LineItem	**Level 3 Line Item Detail Element – Product Code** ▪ Product code of the item purchased. ▪ Cannot be all zeros. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	12	A
PC3DtlQty	PC3LineItem	**Level 3 Line Item Detail Element – Number of Units** ▪ Number of units of the item purchased. ▪ Cannot be all zeros. ▪ Implied decimal of 4. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.* *NOTE* The Salem host (BIN 000001) requires a minimum quantity of one. Orbital will round this up for Salem merchants if the quantity is less than one.	C	13	N
PC3DtlUOM	PC3LineItem	**Level 3 Line Item Detail Element – Unit of Measurement** ▪ The unit of measure or unit of measure code used for this line item. ▪ Required for Level 3 Data. See *Table 19 Unit of measure codes* in Appendix A. Only known values are accepted. *See Level 2 & 3 Data Reference for further details.*	C	3	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlTaxAmt	PC3LineItem	**Level 3 Line Item Detail Element – Tax Amount** ▪ The tax amount for this item. ▪ Implied decimal. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	13	N
PC3DtlTaxRate	PC3LineItem	**Level 3 Line Item Detail Element – Tax Rate** ▪ Tax rate applied for this item. ▪ Implied decimal of 3 as a percentage. For example: an interest rate of 6.25% should be sent as 06250. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	5	N
PC3Dtllinetot	PC3LineItem	**Level 3 Line Item Detail Element – Line Item Total** ▪ For PNS customers: - This field must equal the Unit Cost (PC3DtlUnitCost) multiplied by the quantity (PC3DtlQty) less any discounts (PC3DtlDisc). If it does not, then this transaction will receive an error. - Additionally, the sum of all the Line Item totals (that is, the sum of all these fields) cannot exceed the transaction amount (<Amount>) submitted for this order. ▪ Implied decimal. ▪ Cannot be all zeros for either PNS or Salem. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	13	N
PC3DtlDisc	PC3LineItem	**Level 3 Line Item Detail Element – Discount Amount for Line Item** ▪ Amount of the discount applied to the line item. ▪ Implied decimal. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	13	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlCommCd	PC3LineItem	**Level 3 Line Item Detail Element – Commodity Code for Line Item** ▪ The commodity code used to classify the item purchased. ▪ Required for Visa; should not be sent for MasterCard. *See Level 2 & 3 Data Reference for further details.*	C	12	N
PC3DtlUnitCost	PC3LineItem	**Level 3 Line Item Detail Element – Unit Cost of Item Purchased** ▪ Unit Cost of the unit purchased. ▪ Implied decimal of 4. ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	13	N
PC3DtlGrossNet	PC3LineItem	**Level 3 Line Item Detail Element – Gross/Net Indicator** ▪ Indicates whether tax amount is included in the item amount: Y Item amount includes tax amount N Item amount does not include tax amount ▪ Required for Level 3 Data. *See Level 2 & 3 Data Reference for further details.*	C	1	A
PC3DtlTaxType	PC3LineItem	**Level 3 Line Item Detail Element – Type of Tax Being Applied** Type of tax being applied. *See Level 2 & 3 Data Reference for further details.*	O	4	A
PC3DtlDiscInd	PC3LineItem	**Level 3 Line Item Detail Element – Discount Indicator** ▪ Indicates whether the amount is discounted: Y Amount is discounted N Amount is not discounted ▪ If value = Y and Discount Amount Field (PC3DtlDisc) is blank or zero-filled, Chase Paymentech will change this field indicator to **N** before sending the data. ▪ Required for MasterCard only; should not be sent for Visa. *See Level 2 & 3 Data Reference for further details.*	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
PC3DtlDebitInd	PC3LineItem	**Level 3 Line Item Detail Element – Item Debit/Credit Indicator** Valid values: D Item extended amount is a debit. C Item extended amount is a credit. Required for Level 3 Data for PNS (BIN 00002) Merchants. See *Level 2 & 3 Data Reference* for further details.	C	1	A
PC3DtlDiscountRate	PC3LineItem	**Level 3 Line Item Detail Element – Discount Rate** ▪ The Discount Rate for this item. ▪ Implied decimal, four places. ▪ Only for Discover; Should not be sent for Visa or MasterCard ▪ Conditionally required for Level 3 Data for Salem (BIN 000001) merchants See *Level 2 & 3 Data Reference* for further details.	C	5	N

4.4 Mark for Capture Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required XML Parent Tag**	M	N/A	N/A
MarkForCaptureResp	Response	**XML Tag that Defines the Transaction as a Mark for Capture Response**	M	N/A	N/A
MerchantID	MarkForCaptureResp	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the account number passed in request.	M	12	N
TerminalID	MarkForCaptureResp	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID passed in request.	M	3	N
OrderID	MarkForCaptureResp	**Merchant-Defined Order Number** Echoes the Order Number passed in request.	M	22	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TxRefNum	MarkForCaptureResp	**Gateway Transaction Reference Number** Echoes the Transaction Reference Number passed in request.	M	40	A
TxRefIdx	MarkForCaptureResp	**Gateway Transaction Index** ▪ Used to identify the unique components of transactions adjusted more than one time. ▪ Required on Void transactions; not for Mark for Captures.	C	4	A
Amount	MarkForCaptureResp	**Transaction Amount** Echoes the Amount passed in request.	M	12	N
ProcStatus	MarkForCaptureResp	**Process Status** ▪ The first data set that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A
StatusMsg	MarkForCaptureResp	**Text Message Associated with `RespCode` Value**	C	Var	A
RespTime	MarkForCaptureResp	**Time the Transaction was Processed by Gateway** Format: `hh24mmss`	M	6	N
ApprovalStatus	MarkForCaptureResp	**Approval Status** Conditional on Process Status returning a 0 (or successful) response. If so, the Approval Status identifies the result of the authorization request to the host system: 0 Declined 1 Approved 2 Message/System Error	C	1	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
RespCode	`MarkForCaptureResp`	**Response Code** Normalized authorization response code issued by the host system (Salem/PNS), which identifies an approval (`00`) or the reason for a decline or error. See *Table 13* in Appendix A for values.	C	2	A
AVSRespCode	`MarkForCaptureResp`	**Address Verification Request Response** Conditional on AVS request being sent. See *Table 14* in Appendix A for values.	C	2	A
AuthCode	`MarkForCaptureResp`	**Issuer Approval Code** Unique transactional-level code issued by the bank or service establishment for approvals. PINless Debit transactions could return blanks or `N/A`.	C	6	A
RespMsg	`MarkForCaptureResp`	**Text Message Associated with `HostRespCode`**	C	80	A
HostRespCode	`MarkForCaptureResp`	**Actual Host Response Code** ▪ Exact response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	3	A
HostAVSRespCode	`MarkForCaptureResp`	**Actual Host Address Verification Response Code** ▪ Exact address verification response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	2	A

4.5   Reversal (Void) Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
Reversal	`Request`	**XML tag that defines the transaction as a Reversal request**	M	N/A	N/A
OrbitalConnectionUsername	`Reversal`	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	`Reversal`	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
TxRefNum	`Reversal`	**Gateway transaction Reference Number** ▪ A unique value for each transaction, which is required to adjust any transaction in the Gateway, such as Mark for Capture or Void. ▪ If reference number is not known, use `ReversalRetryNumber` tag.	C	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TxRefIdx	Reversal	**Gateway Transaction Index** ▪ Used to identify the unique components of transactions adjusted more than one time. ▪ Submit this tag as NULL when voiding a transaction which has not been adjusted more than once. ▪ To Void the un-captured remainder of a split transaction (partial capture), submit this tag as NULL. ▪ To Void a specific partial capture, `TxRefIdx` = value returned in response for that partial capture.	C	4	N
AdjustedAmt	Reversal	**Transaction Amount** ▪ When a specific amount is included with this field, that amount will be voided (assuming that the amount is not greater than the transaction amount remaining). ▪ The absence of this tag on a Void transaction will perform a full Reversal. ▪ Implied decimal, including those currencies that are a zero exponent. For example, both $100.00 (an exponent of 2) and ¥100 (an exponent of 0) should be sent as `<AdjustedAmt>`**10000**`</AdjustedAmt>`.	C	12	N
OrderID	Reversal	**Merchant-Defined Order Number** Must match the `orderID` of the original transaction being Reversed.	M	22	A
BIN	Reversal	**Transaction Routing Definition** Assigned by Chase Paymentech. `000001` Salem `000002` PNS	M	6	N
MerchantID	Reversal	**Gateway Merchant Account Number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number ▪ BIN 000002: 12-digit PNS Merchant ID	M	15	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TerminalID	`Reversal`	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to `001`. ▪ PNS Terminal IDs: between `001` and `999`; typically `001`.	M	3	N
ReversalRetryNumber	`Reversal`	**Retry Trace Number from Original Transaction Request** Provide the Retry Trace Number from the transaction that needs to be voided (in the event the Transaction Reference Number is not known).	C	16	N
OnlineReversalInd	`Reversal`	**Online Reversal Indicator** Indicates whether an authorization reversal or a void is being requested. This value will override the Orbital Gateway setting on the host, if any. `Y` Authorization Reversal `N` Void `NULL` Void For information on card types which accept online reversals, please see *Reversal (Void a Previous Transaction)*	C	1	A

4.6   Reversal (Void) Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required XML Parent Tag**	M	N/A	N/A
ReversalResp	`Response`	**XML Tag that Defines the Transaction as a Reversal Response**	M	N/A	N/A
MerchantID	`ReversalResp`	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	M	12	N
TerminalID	`ReversalResp`	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID passed in the request.	M	3	N
OrderID	`ReversalResp`	**Merchant-Defined Order Number** Echoes the Order Number passed in the request.	M	22	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TxRefNum	ReversalResp	**Gateway Transaction Reference Number** Echoes the Transaction Reference Number passed in the request.	M	40	A
TxRefIdx	ReversalResp	**Gateway Transaction Index** ▪ Used to identify the unique components of transactions adjusted more than one time. ▪ Required on Void transactions; not for Mark for Captures.	C	4	A
OutstandingAmt	ReversalResp	**Remaining Non-voided Amount for Partial Voids**	C	12	N
ProcStatus	ReversalResp	**Process Status** ▪ The first data set that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 　0　Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A
StatusMsg	ReversalResp	**Text Message Associated with `ProcStatus` Value**	C	Var	A
RespTime	ReversalResp	**Time the Transaction was Processed by Gateway** Format: MMDDYYYY`hh24mmss`	M	6	N

Reversal (Void) Response Elements

Release Date: August 2013　　Page 134 of 283

4.7   End of Day Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
EndOfDay	Request	**XML Tag that Defines the Transaction as a Batch/EOD Request**	M	N/A	N/A
OrbitalConnectionUsername	EndOfDay	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	EndOfDay	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
BIN	EndOfDay	**Transaction Routing Definition** Assigned by Chase Paymentech. 000001 Salem 000002 PNS	M	6	N
MerchantID	EndOfDay	**Gateway Merchant Account Number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number ▪ BIN 000002: 12-digit PNS Merchant ID	M	15	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TerminalID	`EndOfDay`	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to `001`. ▪ PNS Terminal IDs: between `001` and `999`; typically `001`.	M	3	N

4.8   End of Day Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
EndOfDayResp	`Response`	**XML Tag that Defines the Transaction as a Batch/EOD Response**	M	N/A	N/A
MerchantID	`EndOfDayResp`	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	M	12	N
TerminalID	`EndOfDayResp`	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID passed in the request.	M	3	N
BatchSeqNum	`EndOfDayResp`	**Batch Sequence Number** A sequence value that references a Settlement Batch.	M	32	A
ProcStatus	`EndOfDayResp`	**Process Status** ▪ The first data set that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A
StatusMsg	`EndOfDayResp`	**Text Message Associated with `ProcStatus` Value**	C	Var	A
RespTime	`EndOfDayResp`	**Time the Transaction was Processed by Gateway** Format: `hh24mmss`	M	6	N

4.9 Inquiry Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
Inquiry	Request	**XML Tag that Defines the Transaction as an Inquiry Request**	M	N/A	N/A
OrbitalConnectionUsername	Inquiry	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	Inquiry	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
BIN	Inquiry	**Transaction Routing Definition** Assigned by Chase Paymentech. 000001 Salem 000002 PNS	M	6	N
MerchantID	Inquiry	**Gateway merchant account number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number ▪ BIN 000002: 12-digit PNS Merchant ID	M	15	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TerminalID	Inquiry	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to `001`. ▪ PNS Terminal IDs: between `001` and `999`; typically `001`.	M	3	N
OrderID	Inquiry	**Merchant-Defined Order Number** Must match the `OrderID` of the original request.	C	22	A
InquiryRetryNumber	Inquiry	**Retry Trace Number from Original Transaction Request** ▪ Provide the Retry Trace Number from the original request in this tag to return the original response. ▪ If the original transaction was not processed successfully, the Gateway will return an error message.	M	16	N

4.10 Inquiry Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
InquiryResp	Response	**XML Tag that Defines the Transaction as an Inquiry Response**	M	N/A	N/A
IndustryType	InquiryResp	**Industry Type of the Transaction** This tag returns `null` results.	M	2	A
MessageType	InquiryResp	**Transaction New Order Transaction Type** Echoes the Message Type passed in the request.	M	2	A
MerchantID	InquiryResp	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant Account Number passed in the request.	M	12	N
TerminalID	InquiryResp	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID passed in the request.	M	3	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CardBrand	InquiryResp	**Card Type/Brand for the Transaction** Echoes the Card Type/Brand passed in the request, except: ▪ If no CardBrand, such as Visa or MasterCard, was sent in the request (when optional), the specific Card Brand mnemonic is returned. ▪ For PINless Debit transactions, the *request* Card Brand is DP (which is a generic PINless mnemonic). However, the *response* Card Brand will be one of the four supported PINless Debit Card Brands: NP NYCE PINless Debit PP Pulse PINless Debit SP Star PINless Debit AP Accel PINless Debit	C	2	A
AccountNum	InquiryResp	**Card Number Identifying the Customer** Echoes the Account Number passed in the request.	C	19	N
OrderID	InquiryResp	**Merchant-Defined Order Number** Echoes the Order Number passed in the request.	M	22	A
TxRefNum	InquiryResp	**Gateway Transaction Reference Number** Echoes the Transaction Reference Number passed in the request.	M	40	A
TxRefIdx	InquiryResp	**Gateway Transaction Index** Used to identify the unique components of transactions adjusted more than one time. Required for Void transactions.	C	4	A
ProcStatus	InquiryResp	**Process Status** ▪ The first data set that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ApprovalStatus	InquiryResp	**Approval Status** Conditional on Process Status returning a `0` (or successful) response. If so, the Approval Status identifies the result of the authorization request to the host system: `0` Declined `1` Approved `2` Message/System Error	C	1	N
RespCode	InquiryResp	**Response Code** Normalized authorization response code issued by the host system (Salem/PNS), which identifies an approval (`00`) or the reason for a decline or error. See *Table 13* in Appendix A for values.	C	2	A
AVSRespCode	InquiryResp	**Address Verification Request Response** Conditional on AVS request being sent. See *Table 14* in Appendix A for values.	C	2	A
CVV2RespCode	InquiryResp	**Card Verification Value Request Response** Conditional on card verification request being sent. See *Table 17* Appendix A for values.	C	1	A
AuthCode	InquiryResp	**Issuer Approval Code** Unique transactional-level code issued by the bank or service establishment for approvals. PINless Debit transactions could return blanks or `N/A`.	C	6	A
RecurringAdviceCd	InquiryResp	**Recurring Payment Advice Code (MasterCard Only)** Valid values: `01` New account information available. Obtain new account information. `02` Try again later. Recycle transaction in 72 hours. `03` Do not try again. Obtain another type of payment from customer.	C	2	N
CAVVRespCode	InquiryResp	**CAVV Response Code for VbV Transactions** See *Table 20* in Appendix A for values.	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
StatusMsg	InquiryResp	**Text Message Associated with `RespCode` Value**	C	Var	A
RespMsg	InquiryResp	**Text Message Associated with `HostRespCode` Value**	C	80	A
HostRespCode	InquiryResp	**Actual Host Response Code** ▪ Exact response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	3	A
HostAVSRespCode	InquiryResp	**Actual Host Address Verification Response Code** ▪ Exact address verification response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	2	A
HostCVV2RespCode	InquiryResp	**Actual Host Card Verification Response Code** ▪ Exact card verification response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	1	A
CustomerRefNum	InquiryResp	**Customer Reference Number** If Customer Profile Action Type = `Create` and `CustomerProfileFromOrderInd` = `S`, this field will echo the Customer Reference Number sent in the Profile Request.	C	22	A
CustomerName	InquiryResp	**Customer Billing Name** Echoes value from the request.	C	30	A
ProfileProcStatus	InquiryResp	**Result Status of Profile Management** Communicates the success or failure of a Profile Management request: `0` Success `>0` An error condition, see *Table 16* in Appendix A for values.	C	6	A
CustomerProfileMessage	InquiryResp	**Verbose Text Description associated with `ProfileProcStatus`**	C	Var	A
BillerReferenceNumber	InquiryResp	**Biller Reference Number (PINless Debit Only)** Echoes value from request.	C	25	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
RespTime	InquiryResp	**Time the Transaction was Processed by Gateway** Format: `hh24mmss`	M	6	N

4.11   Profile Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
Profile	Request	**XML Tag that Defines the Transaction as a Profile Request**	M	N/A	N/A
OrbitalConnectionUsername	Profile	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	Profile	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

CustomerBin	Profile	**Transaction Routing Definition**
		▪ Assigned by Chase Paymentech.
		  000001 Salem
		  000002 PNS
		▪ This value cannot be changed through a Profile Update action.
		▪ This is the equivalent to the `<BIN>` element used on transactional requests.
			M	6	N

CustomerMerchantID	Profile	**Gateway merchant account number assigned by Chase Paymentech**
		▪ This account number will match that of your host platform:
		  - BIN 000001: 6-digit Salem Division Number
		  - BIN 000002: 12-digit PNS Merchant ID
		▪ This value cannot be changed through a Profile Update action.
		▪ This is the equivalent to the `<MerchantID>` element used on transactional requests.
			M	15	N

CustomerName	Profile	**Customer Billing Name** ▪ Conditionally required for Electronic Check profiles. ▪ This is the equivalent to the `<AVSname>` element used on transactional requests.	C	30	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

CustomerRefNum	Profile	**Sets the Customer Reference Number that will be used to utilize a Customer Profile on all future Orders**
		
		▪ Mandatory if:
		  - `CustomerProfileAction` = **R** or **U** or **D** (Read, Update, or Delete)
		  OR
		  - `CustomerProfileAction` = **C** (Create) AND the `customerProfileFromOrderInd` option = **S** (use the `CustomerRefNum` field).
		
		▪ If `customerProfileFromOrderInd` = **A**, the Customer Reference Number will be defined by the Orbital Gateway, and any value passed in this element will be ignored.
		
		▪ Given that this value can be the same as the Order Number, the valid characters for this field follow the same convention as the Order ID element and include:
		  - `abcdefghijklmnopqrstuvwxyz`
		  - `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
		  - `0123456789`
		  - `-` `,` `$` `@` `&` and a space character, though the space character **cannot** be the leading character
		  - Please note that all alphabetic characters in this field are stored in uppercase by the Orbital system. Uppercase and lowercase values cannot be used to differentiate Customer Reference Numbers.
		
		▪ This value cannot be changed through a Profile Update action.
			C	22	A

CustomerAddress1	Profile	**Cardholder Billing Address line 1** ▪ Optional if `CustomerProfileAction` = **C** or **U** (Create or Update). ▪ This is the equivalent to the `<AVSaddress1>` element used on transactional requests.	O	30	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerAddress2	`Profile`	**Cardholder Billing Address line 2** ▪ Optional if `CustomerProfileAction` = **C** or **U** (Create or Update). ▪ This is the equivalent to the `<AVSaddress2>` element used on transactional requests.	O	30	A
CustomerCity	`Profile`	**Cardholder Billing City** ▪ Optional if `CustomerProfileAction` = **C** or **U** (Create or Update). ▪ This is the equivalent to the `<AVScity>` element used on transactional requests.	O	20	A
CustomerState	`Profile`	**Cardholder Billing State** ▪ Optional if `CustomerProfileAction` = **C** or **U** (Create or Update). ▪ This is the equivalent to the `<AVSstate>` element used on transactional requests.	O	2	A
CustomerZIP	`Profile`	**Cardholder Billing Address Zip Code** ▪ All AVS requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ Conditionally required if `CustomerProfileAction` = **C** (Create). ▪ This is the equivalent to the `<AVSzip>` element used on transactional requests.	C	10	A
CustomerEmail	`Profile`	**Cardholder E-mail Address** ▪ Optional if `CustomerProfileAction` = **C** or **U** (Create or Update).	O	50	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerPhone	Profile	**Cardholder Telephone Number** AAAEEENNNNXXXX, where AAA = Area Code EEE = Exchange NNNN = Number XXXX = Extension ▪ Optional if CustomerProfileAction = C or U (Create or Update). ▪ This is the equivalent to the \<AVSphonenum\> element used on transactional requests.	O	14	A
CustomerCountryCode	Profile	**Cardholder Billing Address Country Code** ▪ Valid values: US United States CA Canada GB Great Britain UK United Kingdom ▪ This is the equivalent to the \<AVScountryCode\> element used on transactional requests.	C	2	A
CustomerProfileAction	Profile	**Defines the Customer Profile Action Desired** ▪ Valid values: C Create a Customer Profile U Update a Customer Profile R Retrieve a Customer Profile's Attributes D Delete a Customer Profile ▪ This element is only used for Customer Profile Management actions.	M	6	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerProfileOrderOverrideInd	Profile	**Defines if any Order Data can be pre-populated from the Customer Reference Number (CustomerRefNum)** ▪ Mandatory if CustomerProfileAction = **C** (Create). ▪ Optional if CustomerProfileAction = **U** (Update). ▪ Valid Values NO No mapping to order data OI Use <CustomerRefNum> for <OrderID> OD Use <CustomerRefNum> for <Comments> OA Use <CustomerRefNum> for <OrderID> and <Comments>	C	2	A
CustomerProfileFromOrderInd	Profile	**Customer Profile Number Generation Options** ▪ When CustomerProfileAction = **C** (Create), defines what the Customer Profile Number will be: A Auto-Generate the CustomerRefNum S Use CustomerRefNum element	C	5	A
OrderDefaultDescription	Profile	**Order Description** ▪ Optional if CustomerProfileAction = **C** or **U** (Create or Update). ▪ If CustomerProfileOrderOverrideInd = **OA**, do not set this value, since this defaults the Order Description to the Customer Reference Number. ▪ This is the equivalent to the <Comments> element used on transactional requests.	O	64	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
OrderDefaultAmount	`Profile`	**Transaction Amount** ▪ Optional if `CustomerProfileAction` = **C** or **U** (Create or Update). ▪ This is the equivalent to the `<Amount>` element used on transactional requests. Keys: ▪ Implied decimal including those currencies that are a zero exponent. For example, both $100.00 (an exponent of 2) and ¥100 (an exponent of 0) should be sent as `<OrderDefaultAmount>`**10000**`</OrderDefaultAmount>`. ▪ Given that each Orbital Gateway Merchant ID is restricted to one currency, the Currency Code (and exponent) is defaulted based on the Merchant ID in which a transaction is presented.	O	12	N
CustomerAccountType	`Profile`	**Customer's Payment Type to save in the Profile** ▪ Mandatory if `CustomerProfileAction` = **C** (Create). ▪ Optional if `CustomerProfileAction` = **U** (Update). ▪ Valid Values 　`CC`　Credit Card 　`DP`　PINless Debit 　`EC`　Electronic Check 　`ED`　European Direct Debit 　`IM`　International Maestro	C	2	A
Status	`Profile`	**Profile Status Flag** This field is used to set the status of a Customer Profile. 　`A`　Active 　`I`　Inactive 　`MS`　Manual Suspend	C	Var	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CCAccountNum	Profile	**Customer Credit Card Number** ▪ Mandatory if `CustomerProfileAction` = **C** (Create) AND `CustomerAccountType` is not 'EC'. ▪ Optional if `CustomerProfileAction` = **ʊ** (Update) AND `CustomerAccountType` is not 'EC'. ▪ This is the equivalent to the `<AccountNum>` element used on transactional requests.	C	19	N

CCExpireDate	Profile	**Customer Credit Card Expiration Date**
		
		▪ Mandatory if `CustomerProfileAction` = **C** (Create) AND `CustomerAccountType` = **CC**
		
		▪ Optional if `CustomerProfileAction` = **ʊ** (Update) AND `CustomerAccountType` = **CC**
		
		▪ Format: `MMYY`
		
		▪ Salem (BIN 000001) allows a *blank* to be submitted when no known expiration date exists. There are three valid mechanisms for submitting a *Blank* expiration date to the Salem Host using Orbital:
		
		- Null-fill the element:
		`<CCExpireDate/>`
		
		- Send four spaces:
		`<CCExpireDate>    </CCExpireDate>`
		
		- Zero-fill the element:
		`<CCExpireDate>0000</CCExpireDate>`
		
		▪ This is the equivalent to the `<Exp>` element used on transactional requests.
		
		NOTE Please discuss this feature with your certification analyst before implementing.
			C	4	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ECPAccountDDA	Profile	**ECP (DDA) Account Number** ▪ Mandatory if `CustomerProfileAction` = **C** (Create) AND `CustomerAccountType` = **EC** (Electronic Check). ▪ Optional if `CustomerProfileAction` = **U** (Update) AND `CustomerAccountType` = **EC** (Electronic Check). ▪ This is the equivalent to the `<CheckDDA>` element used on transactional requests.	C	17	A

ECPAccountType	Profile	**Deposit Account Type**
		
		▪ Valid values:
		  C Consumer Checking (US or Canadian)
		  S Consumer Savings (US Only)
		  X Commercial Checking (US Only)
		
		▪ Mandatory if `CustomerProfileAction` = **C** (Create) AND `CustomerAccountType` = **EC** (Electronic Check).
		
		▪ Optional if `CustomerProfileAction` = **U** (Update) AND `CustomerAccountType` = **EC** (Electronic Check).
		
		▪ This is the equivalent to the `<BankAccountType>` element used on transactional requests.
			C	1	A

ECPAccountRT	Profile	**Bank Routing and Transit Number for the Customer**
		
		▪ Mandatory if `CustomerProfileAction` = **C** (Create) AND `CustomerAccountType` = **EC** (Electronic Check).
		
		▪ Optional if `CustomerProfileAction` = **U** (Update) AND `CustomerAccountType` = **EC** (Electronic Check).
		
		▪ This is the equivalent to the `<BCRtNum>` element used on transactional requests.
		
		NOTES:
		▪ All US Bank Routing Numbers are 9 digits.
		▪ All Canadian Bank Routing Numbers are 8 digits.
		  - Formatted FFFBBBBB where F is Financial Institution and B is Branch Number
		  - Cannot include spaces " " or dashes "-"
			C	9	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ECPBankPmtDlv	Profile	**ECP Payment Delivery Method** ▪ This field indicates the preferred manner to deposit the transaction: B Best Possible Method (US Only) Chase Paymentech utilizes the method that best fits the situation. If the RDFI is not an ACH participant, a facsimile draft is created. This should be the default value for this field. A ACH (US or Canadian) Deposit the transaction by ACH only. If the RDFI is not an ACH participant, the transaction is rejected. ▪ Mandatory if CustomerProfileAction = **C** (Create) AND CustomerAccountType = **EC** (Electronic Check). ▪ Optional if CustomerProfileAction = **U** (Update) AND CustomerAccountType = **EC** (Electronic Check). ▪ This is the equivalent to the <BankPmtDelv> element used on transactional requests.	C	1	A
MBType	Profile	**Managed Billing Type** ▪ Indicates the type of Managed Billing the merchant is participating in: R Recurring D Deferred ▪ The value submitted must be in agreement with the type of Managed Billing the merchant is configured for at Chase Paymentech. ▪ This field serves to notify the Orbital system that the transaction is a Managed Billing transaction. If this field is not sent with a Managed Billing transaction, all other Managed Billing fields are ignored.	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBOrderIdGenerationMethod	Profile	**Managed Billing Order ID Generation Method** ▪ This value is used to set the method that Orbital will use to generate the Order ID for any Managed Billing transactions. ▪ This field does NOT influence the Order ID for stand-alone transactions initiated by the merchant, VT transactions, and so on. ▪ Valid values: IO Use the Customer Reference Number (Profile ID). This value is made up of the capital letters I and O, not numbers. DI Dynamically generate the Order ID. This value is made up of the capital letters D and I, no numbers.	C	2	A
MBRecurringStartDate	Profile	**Managed Billing Recurring Start Date** ▪ Defines the future date that Orbital will begin a recurring billing cycle to the associated Profile. ▪ To allow the Managed Billing engine to properly calculate and schedule all billings, this date must be at least one day after the request date (a recurring billing cycle can never begin on the date that the request message is sent to the Orbital system). ▪ Format: MMDDYYYY	C	8	N
MBRecurringEndDate	Profile	**Managed Billing Recurring End Date** ▪ Defines the future date that Orbital will end a recurring billing cycle to the associated Profile. ▪ Format: MMDDYYYY ▪ This is the first of three possible recurring end triggers. Only one end trigger can be submitted per request message.	C	8	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBRecurringNoEndDateFlag	`Profile`	**Managed Billing 'No End Date' Indicator** ▪ Valid values: `Y` — Schedule recurring transactions for an infinite amount of time. A `Y` in this element overrides the value, if any, in the `MBRecurringEndDate` field. `N` (or blank) — Orbital will use the value of the `MBRecurringEndDate` field to define the recurring end date. ▪ This is the second of three possible recurring end triggers. Only one end trigger can be submitted per request message.	C	1	A
MBRecurringMaxBillings	`Profile`	**Managed Billing Max Number of Billings** ▪ This value defines the maximum number of billings that will be allowed for a recurring billing cycle. ▪ Valid values: `1–999999` ▪ This is the third of three possible recurring end triggers. Only one end trigger can be submitted per request message.	C	6	N
MBRecurringFrequency	`Profile`	**Managed Billing Recurring Frequency Pattern** This pattern is a subset of a standard `CRON` expression, comprising 3 fields separated by white space: **Field / Allowed Values / Allowed Special Chars** Day-of-month — `1–31` — `,  -  *  ?  /  L  W` Month — `1–12` or `JAN–DEC` — `,  -  *  /` Day-of-week — `1–7` or `SUN–SAT` — `,  -  *  ?  /  L  #` *SEE ALSO* For a full discussion of these three fields, the usage of the special characters, and multiple example values, see *3.3.2 Profiles and Managed Billing*.	C	Var	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBDeferredBillDate	`Profile`	**Managed Billing Deferred Billing Date** ▪ Defines the future date that Orbital will trigger a one-time billing to the associated Profile. ▪ This date must be at least one day after the request date (a deferred billing can never take place on the date that the request message is sent to the Orbital system). ▪ Format: `MMDDYYYY`	C	8	N
MBCancelDate	`Profile`	**Managed Billing Cancel Date** ▪ Used to cancel a single future billing that is already scheduled. ▪ The exact date of the scheduled billing must be submitted. ▪ Format: `MMDDYYYY`	C	8	N
MBRestoreBillingDate	`Profile`	**Managed Billing Restore Billing Date** ▪ Used to reinstate a cancelled billing. ▪ The exact date of the previously scheduled billing must be submitted. ▪ Format: `MMDDYYYY`	C	8	N
MBRemoveFlag	`Profile`	**Managed Billing Remove Flag** Valid values: `Y` This value is used to remove all Managed Billing settings from the associated Profile. The Profile becomes a *Standard* Profile, and any scheduled future billings are removed from the Orbital system and will not occur. `N` (or blank) This value has no effect on the Profile.	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
EUDDCountryCode	`Profile`	**European Direct Debit Country Code** ▪ Mandatory if `CustomerProfileAction` = **C** (Create) AND `CustomerAccountType` = **ED** (European Direct Debit). ▪ Optional if `CustomerProfileAction` = **U** (Update) AND `CustomerAccountType` = **ED** (European Direct Debit). ▪ Customer's Country Code. ▪ Valid country codes: `AT` Austria `BE` Belgium `DE` Germany `FR` France `GB` United Kingdom `NL` Netherlands	C	2	A
EUDDBankSortCode	`Profile`	**European Direct Debit Bank Sort Code** ▪ Customer's Bank Sort code. ▪ Mandatory for the following Country Codes: `AT` Austria `DE` Germany `FR` France `GB` United Kingdom	C	10	A
EUDDRibCode	`Profile`	**European Direct Debit RIB** ▪ Bank Account checksum. ▪ Used in France only.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SDMerchantName	Profile	**Soft Descriptor Merchant Name** ▪ Conditionally required for Soft Descriptors. ▪ The Merchant Name field should be what is most recognizable to the cardholder (Company name or trade name). The actual length of this field is conditionally tied to Host and the Size of the <SDProductDescription> element used. Salem: ▪ CREDIT – Three options, which conditionally affect the SDProductDescription: - Max 3 bytes - Max 7 bytes - Max 12 bytes ▪ ECP: - Max 15 bytes PNS: ▪ Max 25 bytes.	C	25	A
SDProductDescription	Profile	**Soft Descriptor Product Description** ▪ Conditionally required for Soft Descriptors. ▪ Provides an accurate description. Salem: ▪ CREDIT: - If SDMerchantName = 3 bytes, then Max = 18 bytes - If SDMerchantName = 7 bytes, then Max = 14 bytes - If SDMerchantName = 12 bytes, then Max = 9 bytes ▪ ECP: - 10 bytes Max PNS: ▪ This field will not show on Cardholder statements for PNS Merchants.	C	18	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SDMerchantCity	`Profile`	**Soft Descriptor Merchant City** ▪ Tag conditionally required for Soft Descriptors. ▪ Merchant City for Retail. Field required, but should be null-filled if any Soft Descriptor data is submitted.	C	13	A
SDMerchantPhone	`Profile`	**Soft Descriptor Merchant Phone** ▪ Tag conditionally required for Soft Descriptors. ▪ Only one of the location Soft Descriptor values should be sent (Phone, URL, or E-mail); all others should be null-filled. ▪ This field will not show on Cardholder statements for PNS Merchants. Valid Formats: ▪ `NNN-NNN-NNNN` ▪ `NNN-AAAAAAA` *NOTE* For BIN 000001 merchants processing MasterCard (MOTO and Recurring), if the City/Phone field at the division level is not a Customer Service Phone Number, then a Customer Service Phone Number must be populated or the transaction will reject with Response Reason Code `BP` (`Missing Customer Service Phone`).	C	12	A
SDMerchantURL	`Profile`	**Soft Descriptor Merchant URL** ▪ Tag conditionally required for Soft Descriptors. ▪ Only one of the location Soft Descriptor values should be sent (Phone, URL, or E-mail); all others should be null-filled. ▪ This field will not show on Cardholder statements for PNS Merchants.	C	13	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
SDMerchantEmail	Profile	**Soft Descriptor Merchant E-mail** ▪ Tag conditionally required for Soft Descriptors. ▪ Only one of the location Soft Descriptor values should be sent (Phone, URL, or E-mail); all others should be null-filled. ▪ This field will not show on Cardholder statements for PNS Merchants.	C	13	A
BillerReferenceNumber	Profile	**Biller Reference Number (PINless Debit Only)** ▪ Reference Number the Biller (merchant) uses on their system to identify this customer. ▪ Conditionally required for PINless Debit.	C	25	A
AccountUpdaterEligibility	Profile	**Account Updater Eligibility Flag** This field is used to designate if the customer profile should be eligible for Account Updater. • This field only applies to Salem (Bin 000001) merchants using the "Designated Profiles" Account Updater setup option. Valid values: Y Account Updater requests may be processed. N Account Updater requests will not be processed.	O	1	A

4.12 Profile Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required Parent XML Tag**	M	N/A	N/A
ProfileResp	Response	**XML Tag that Defines the Transaction as a Profile Response**	M	N/A	N/A
CustomerBin	ProfileResp	**Transaction Routing Definition** Echoes the BIN passed in the request.	M	6	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerMerchantID	ProfileResp	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	M	15	N
CustomerName	ProfileResp	**Customer Billing Name** Echoes the Customer Name passed in the request.	M	30	A
CustomerRefNum	ProfileResp	**Customer Reference Number**	M	22	A
CustomerProfileAction	ProfileResp	**Customer Profile Action that was Requested**	M	6	A
ProfileProcStatus	ProfileResp	**Result Status of Profile Management** Communicates the success or failure of a Profile Management request: `0`　　Success `>0`　　An error condition, see *Table 16* in Appendix A for values.	M	6	A
CustomerProfileMessage	ProfileResp	**Text Message Associated with `ProfileProcStatus` Value**	C	Var	A
CustomerAddress1	ProfileResp	**Cardholder Billing Address line 1**	C	30	A
CustomerAddress2	ProfileResp	**Cardholder Billing Address line 2**	C	30	A
CustomerCity	ProfileResp	**Cardholder Billing City**	C	20	A
CustomerState	ProfileResp	**Cardholder Billing State**	C	2	A
CustomerZIP	ProfileResp	**Cardholder Billing Address Zip Code**	C	10	A
CustomerEmail	ProfileResp	**Cardholder E-mail Address**	C	50	A
CustomerPhone	ProfileResp	**Cardholder Telephone Number** `AAAEEENNNNXXXX`, where 　`AAA` = Area Code 　`EEE` = Exchange 　`NNNN` = Number 　`XXXX` = Extension	C	14	A
CustomerCountryCode	ProfileResp	**Cardholder Address Country Code**	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerProfileOrderOverrideInd	ProfileResp	**Whether any Order Data can be pre-populated from the Customer Reference Number (CustomerRefNum)** NO No mapping to order data OI Use \<CustomerRefNum> for \<OrderID> OD Use \<CustomerRefNum> for \<Comments> OA Use \<CustomerRefNum> for \<OrderID> and \<Comments>	C	2	A
OrderDefaultDescription	ProfileResp	**Order Description**	C	64	A
OrderDefaultAmount	ProfileResp	**Defaulted Transaction Amount** Implied decimal.	C	12	N
CustomerAccountType	ProfileResp	**Card Type/Brand for the Transaction** Echoes the Card Type/Brand passed in the request, except: ▪ If no CardBrand, such as Visa or MasterCard, was sent in the request (when optional), the specific Card Brand mnemonic is returned. ▪ For PINless Debit transactions, the *request* Card Brand is DP (which is a generic PINless mnemonic). However, the *response* Card Brand will be one of the four supported PINless Debit Card Brands: NP NYCE PINless Debit PP Pulse PINless Debit SP Star PINless Debit AP Accel PINless Debit	C	2	A
Status	ProfileResp	**Current Status of the Profile** A Active I Inactive MS Manual Suspend	C	Var	A
CCAccountNum	ProfileResp	**Customer Credit Card Number**	C	19	N
CCExpireDate	ProfileResp	**Customer Credit Card Expiration Date**	C	4	N
ECPAccountDDA	ProfileResp	**ECP (DDA) Account Number**	C	17	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ECPAccountType	ProfileResp	**Deposit Account Type** C Consumer Checking (US or Canadian) S Consumer Savings (US Only) X Commercial Checking (US Only)	C	1	A
ECPAccountRT	ProfileResp	**Bank Routing and Transit Number for the Customer**	C	9	N

ECPBankPmtDlv	ProfileResp	**ECP Payment Delivery Method**
		The preferred manner to deposit the transaction:
		B Best Possible Method (US Only)
		      Chase Paymentech utilizes the method that best fits the situation. If the RDFI is not an ACH participant, a facsimile draft is created. This should be the default value for this field.
		A ACH (US or Canadian)
		      Deposit the transaction by ACH only. If the RDFI is not an ACH participant, the transaction is rejected.
			C	1	A

MBType	ProfileResp	**Managed Billing Type** R Recurring D Deferred	C	1	A
MBOrderIdGenerationMethod	ProfileResp	**Managed Billing Order ID Generation Method** IO Use the Customer Reference Number (Profile ID). DI Dynamically generate the Order ID.	C	2	A
MBRecurringStartDate	ProfileResp	**Managed Billing Recurring Start Date** ▪ Defines the date that Orbital began/will begin a recurring billing cycle to the associated Profile. ▪ Format: MMDDYYYY	C	8	N
MBRecurringEndDate	ProfileResp	**Managed Billing Recurring End Date** ▪ Defines the date that Orbital ended/will end a recurring billing cycle to the associated Profile. ▪ Format: MMDDYYYY	C	8	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MBRecurringNoEndDateFlag	`ProfileResp`	**Managed Billing 'No End Date' Indicator** `Y` Recurring transactions are scheduled for an infinite amount of time. A `Y` in this element overrides the value, if any, in the `MBRecurringEndDate` element. `N` (or blank) Orbital is using the value of the `MBRecurringEndDate` element to define the recurring end date.	C	1	A
MBRecurringMaxBillings	`ProfileResp`	**Managed Billing Max Number of Billings** ▪ The maximum number of billings that will be allowed for a recurring billing cycle. ▪ Valid values: `1-999999`	C	6	N
MBRecurringFrequency	`ProfileResp`	**Managed Billing Recurring Frequency Pattern** This pattern is a subset of a standard `CRON` expression, comprising 3 fields separated by white space. *SEE ALSO* For a full discussion of these three fields, the usage of the special characters, and multiple example values, see *3.3.2 Profiles and Managed Billing.*	C	Var	A
MBDeferredBillDate	`ProfileResp`	**Managed Billing Deferred Billing Date** Format: `MMDDYYYY`	C	8	N
MBCustomerStatus	`ProfileResp`	**Managed Billing Customer Status** Text message indicating the status of a Managed Billing request.	C	Var	N
EUDDCountryCode	`ProfileResp`	**European Direct Debit Country Code** `AT` Austria `BE` Belgium `DE` Germany `FR` France `GB` United Kingdom `NL` Netherlands	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

EUDDBankSortCode	ProfileResp	**European Direct Debit Bank Sort Code**
		▪ Mandatory for the following Country Codes:
		  AT Austria
		  DE Germany
		  FR France
		  GB United Kingdom
			C	10	A

EUDDRibCode	ProfileResp	**European Direct Debit RIB** ▪ Bank Account checksum. ▪ Used in France only.	C	2	A
SDMerchantName	ProfileResp	**Soft Descriptor Merchant Name**	C	25	A
SDProductDescription	ProfileResp	**Soft Descriptor Product Description**	C	18	A
SDMerchantCity	ProfileResp	**Soft Descriptor Merchant City**	C	13	A
SDMerchantPhone	ProfileResp	**Soft Descriptor Merchant Phone**	C	12	A
SDMerchantURL	ProfileResp	**Soft Descriptor Merchant URL**	C	13	A
SDMerchantEmail	ProfileResp	**Soft Descriptor Merchant E-mail**	C	13	A
BillerReferenceNumber	ProfileResp	**Biller Reference Number (PINless Debit Only)** Echoed from Request.	C	25	A
RespTime	ProfileResp	**Time the Transaction was Processed by Gateway** Format: hh24mmss	M	6	N

4.13 Gift Card (FlexCache) Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required XML Parent Tag**	M	N/A	N/A
FlexCache	`Request`	**XML Tag that Defines the Transaction as a Gift Card Request**	M	N/A	N/A
OrbitalConnectionUsername	`FlexCache`	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	`FlexCache`	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
BIN	`FlexCache`	**Transaction Routing Definition** Assigned by Chase Paymentech. `000001` Salem `000002` PNS	M	6	N
MerchantID	`FlexCache`	**Gateway Merchant Account Number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number ▪ BIN 000002: 12-digit PNS Merchant ID	M	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TerminalID	`FlexCache`	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to `001`. ▪ PNS Terminal IDs: between `001` and `999`; typically `001`.	M	3	N
AccountNum	`FlexCache`	**Card Number identifying the Gift Card Customer** Required for all `FlexAction` types, except Block Activations, Block Deactivations, and Block Reactivations (which use `StartAccountNum`).	C	19	N
OrderID	`FlexCache`	**Merchant-Defined Order Number** ▪ Field defined and supplied by the auth originator and echoed back in response. ▪ The first 8 characters should be unique for each transaction. The valid characters include: ▪ `abcdefghijklmnopqrstuvwxyz` ▪ `ABCDEFGHIJKLMNOPQRSTUVWXYZ` ▪ `0123456789` ▪ `-` , `$` `@` `&` and a space character, though the space character **cannot** be the leading character For BIN 000002 merchants: ▪ If `IndustryType = EC`, first 16 bytes are passed to the Host Processing System ▪ If `IndustryType = MO`, first 9 bytes are passed to the Host Processing System	M	22	A
Amount	`FlexCache`	**Transaction Amount** ▪ Implied decimal, including those currencies that are a zero exponent. For example, both $100.00 (an exponent of 2) and ¥100 (an exponent of 0) should be sent as `<Amount>`**10000**`</Amount>`.	C	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CardSecVal	FlexCache	**Card Verification Data (CVD)/PIN** While the CVD value can be submitted on any transaction type, the Gift Card Host will only validate the value on the following transaction types: ▪ Authorize ▪ Redemption ▪ Balance Inquiry NOTE Most gift card programs require the presence of this value in the above transaction types.	O	4	N
Comments	FlexCache	**Free-form comments** Merchant can fill in this field, and the information will be stored with the transaction details.	O	64	A
ShippingRef	FlexCache	**Shipping Tracking Reference Number** Merchant can fill in this field, and the information will be stored with the transaction details.	O	40	A
IndustryType	FlexCache	**Industry Type of the Transaction** MO Mail Order transaction RC Recurring Payment (not a valid choice for Canadian merchants) EC eCommerce transaction	M	2	A
FlexAutoAuthInd	FlexCache	**Reserved for Future Use** Set the value for this tag to **N**.	M	1	A
FlexPartialRedemptionInd	FlexCache	**Whether Partial Redemptions are Allowed** ▪ Trigger to allow an approval for a Redemption Completion FlexAction if the available balance is less than the requested amount: Y Approve Redemption Completion N Do Not Approve Redemption Completion ▪ 'Y' is only supported for Salem Merchants.	M	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
FlexAction	FlexCache	**Transaction (or Action) Type** Valid values: ACTIVATE REDEMPTION DEACTIVATE REDEMPTIONCOMPLETION REACTIVATE REFUND ADDVALUE BALANCEINQUIRY AUTH VOID NOTE To perform a Block Activation, use the **ACTIVATE** FlexAction, and supply values with the StartAccountNum and ActivationCount tags. Block Deactivations and Block Reactivations follow the same pattern	M	30	A
StartAccountNum	FlexCache	**The First Card Number in a Block Request Sequence** ▪ Should only used when the FlexAction = **ACTIVATE, DEACTIVATE, or REACTIVATE**. ▪ Should be used in conjunction with the ActivationCount.	C	19	N
ActivationCount	FlexCache	**The Number of Cards in Addition to the First Card Number in the Sequence** ▪ The maximum number of cards that can be activated at one time is 100. As such, the maximum number for this field is 99. ▪ Required if FlexAction = **ACTIVATE, DEACTIVATE, OR REACTIVATE** and a value is submitted in the StartAccountNum element.	C	2	N
TxRefNum	FlexCache	**Gateway Transaction Reference Number** A unique value for each transaction, which is required to adjust any transaction in the Gateway, such as a Redemption Completion or Reversal.	C	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
FlexEmployeeNumber	FlexCache	**Employee Number** ▪ Optionally available field to pass an Employee Number on the transaction. This will appear in FlexCache-generated (not Orbital Gateway) reports. ▪ Only supported for PNS Merchants.	O	15	A
PriorAuthID	FlexCache	**Prior Authorization Code** If a prior authorization code is available, it should be sent in this tag. ▪ Only supported for PNS Merchants.	O	6	A

NOTE **All further elements of the FlexCache complex type are only used by the Safetech Fraud Analysis service.**

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVSzip	FlexCache	**Cardholder Billing Address Zip Code** ▪ All AVS Requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	10	A
AVSaddress1	FlexCache	**Cardholder Billing Address line 1** ▪ Should not include any of the following characters: % | ^ \ / ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	30	A
AVSaddress2	FlexCache	**Cardholder Billing Address line 2** ▪ Should not include any of the following characters: % | ^ \ / ▪ Required for Bill Me Later sale transactions.	O	30	A

AVSCity	`FlexCache`	**Cardholder Billing City** ▪ Should not include any of the following characters: `%   |   ^   \   /` ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	20	A
AVSstate	`FlexCache`	**Cardholder Billing State** ▪ Should not include any of the following characters: `%   |   ^   \   /` ▪ Required for Bill Me Later sale transactions.	C	2	A
AVSphonenum	`FlexCache`	**Cardholder Billing Phone Number** `AAAEEENNNNXXXX`, where `AAA` = Area Code `EEE` = Exchange `NNNN` = Number `XXXX` = Extension Required for Bill Me Later sale transactions.	C	14	A
AVSname	`FlexCache`	**Cardholder Billing Name** Required for Bill Me Later sale transactions and all Electronic Check transactions, and all European Direct Debit (EU DD) transactions.	C	30	A
AVScountryCode	`FlexCache`	**Cardholder Billing Address Country Code** Valid values: `US` United States `CA` Canada `GB` Great Britain `UK` United Kingdom Conditionally required for Bill Me Later sale transactions.	C	2	A
AVSDestZip	`FlexCache`	**Cardholder Destination Address Zip Code** ▪ All AVS Requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ Required for Bill Me Later sale transactions.	C	10	A

AVSDestaddress1	FlexCache	**Cardholder Destination Address line 1** ▪ Should not include any of the following characters: `% | ^ \ / –` ▪ Required for Bill Me Later sale transactions.	C	30	A
AVSDestaddress2	FlexCache	**Cardholder Destination Address Line 2** ▪ Should not include any of the following characters: `% | ^ \ / –` ▪ Optional for Bill Me Later Transactions.	O	28	A
AVSDestcity	FlexCache	**Cardholder Destination Billing City** ▪ Should not include any of the following characters: `% | ^ \ / –` ▪ Required for Bill Me Later sale transactions.	C	20	A
AVSDeststate	FlexCache	**Cardholder Destination Billing State** ▪ Should not include any of the following characters: `% | ^ \ / –` ▪ Required for Bill Me Later sale transactions	C	2	A
AVSDestphoneNum	FlexCache	**Cardholder Destination Phone Number** `AAAEEENNNNXXXX`, where `AAA` = Area Code `EEE` = Exchange `NNNN` = Number `XXXX` = Extension ▪ Optional for Bill Me Later sale transactions. ▪ International phone numbers are restricted to 14 bytes therefore U.S. formats may not be applicable	O	14	A
AVSDestname	FlexCache	**Cardholder Destination Billing Name** Required for Bill Me Later sale transactions.	C	30	A

AVSDestcountryCode	FlexCache	**Cardholder Destination Address Country Code**
		▪ Valid values:
		  US United States
		  CA Canada
		  GB Great Britain
		  UK United Kingdom
		▪ Required for Bill Me Later sale transactions.
			C	2	A

CustomerAni	FlexCache	**Customer Automatic Number Identification** The ANI specified phone number that the customer used to place the order. Recommended for transactions utilizing Safetech Fraud Tools.	O	10	N

AVSPhoneType	FlexCache	**Customer Telephone Type Indicator**
		Valid values:
		  D Day
		  H Home
		  N Night
		  W Work
		This value is defaulted to H if any phone number is present and this element is either not present or null filled.
			O	1	A

AVSDestPhoneType	FlexCache	**Bill Me Later Cardholder Destination Telephone Type Indicator**
		Valid values:
		  D Day
		  H Home
		  N Night
		  W Work
		This value is defaulted to H if any phone number is present and this element is either not present or null filled.
			O	1	A

CustomerEmail	FlexCache	**Customer Email Address** The customer's contact email address.	O	50	A
CustomerIpAddress	FlexCache	**Customer IP Address** The single source IP address used by the customer to request a payment. Supports IPv4 or IPv6 formats. Punctuation marks are allowed.	O	45	A/N

EmailAddressSubtype	FlexCache	**Customer Email Address Subtype**
		
		Used to indicate the type of email address in the `CustomerEmail` element.
		
		Valid values:
		  B Bill To/Buyer Email Address
		  G Giftee Email Address
		This value is defaulted to B if an email address is present and this element is not present or null filled.
			O	1	A

CustomerBrowserName	FlexCache	**Customer Browser Type** Used to indicate the type of web browser used by the customer to initiate the request. Example: `MOZILLA/4.0 (COMPATIBLE; MSIE 5.0; WINDOWS 95`	O	60	A

ShippingMethod	FlexCache	**Method of Shipping To A Customer**
		Valid values:
		  C Lowest Cost
		  D Carrier Designated by Customer
		  E Electronic Delivery*
		  G Ground*
		  I International
		  M Military
		  N Next Day or Overnight*
		  O Other
		  P Store Pickup*
		  S Same Day*
		  T Two Day Service*
		  W Three Day Service*
		For American Express, use only values marked with an asterisk.
			O	1	A

FraudAnalysis	FlexCache	**Parent XML Tag for Safetech Fraud Analysis Elements**	C	N/A	N/A

FraudScoreIndicator	`FraudAnalysis`	**Fraud Analysis Type Indicator**	C	1	N
		Used to request the type of fraud analysis performed on the transaction. The value in this field directly determines the scope of elements returned in the response message. Valid values: 1 Short Form Request 2 Long Form Request			
RulesTrigger	`FraudAnalysis`	**Fraud Analysis Rules Return Trigger**	O	1	A
		Determines whether the Agent Web Console (AWC) rules are returned. Valid values: Y Triggered rules are returned N Triggered rules are not returned			
SafetechMerchantID	`FraudAnalysis`	**Safetech Merchant ID**	O	6	A/N
		A value assigned by Chase Paymentech when a merchant is enabled for the Safetech service. This is not the same value as Transaction Division number found in the `MerchantID` element. If no value is present, a default value will be used if available. If no default is stored, the request will generate an error.			
KaptchaSessionID	`FraudAnalysis`	**Kaptcha Session ID**	O	32	A
		A merchant generated session ID for this fraud scoring request. The Safetech system recommends this value be unique for 30 days, or the Fraud Score results may not be accurate.			
WebsiteShortName	`FraudAnalysis`	**Short Name for the Merchant's Website**	O	8	A
		This value is used by the Safetech service for fraud score rules.			
CashValueOfFencibleIterms	`FraudAnalysis`	**Cash Value of Fencible Items**	O	12	N
		The cash value of any fencible items in the order. This element should only be sent when the `FraudScoreIndicator` element is set to 2.			
CustomerDOB	`FraudAnalysis`	**Customer Date of Birth**	O	10	A/N
		Format: *YYYY-MM-DD* (Including dashes) This element should only be sent when the `FraudScoreIndicator` element is set to 2.			

Gift Card (FlexCache) Request Elements

CustomerGender	FraudAnalysis	**Customer Gender**
		Valid values:
		  F Female
		  M Male
		
		This element should only be sent when the FraudScoreIndicator element is set to 2.
			O	1	A

CustomerDriverLicense	FraudAnalysis	**Customer Driver's License Number** U.S. Driver's License number only. The Safetech service recommends this value for fraud scoring of Electronic Check (ECP) requests. This element should only be sent when the FraudScoreIndicator element is set to 2.	O	32	A
CustomerID	FraudAnalysis	**Customer ID** A merchant generated ID for a specific customer. This element should only be sent when the FraudScoreIndicator element is set to 2.	O	32	A
CustomerIDCreationTime	FraudAnalysis	**Customer ID Creation Time** The time the value used in the CustomerID element was created by the merchant. Format: Unix Epoc This element should only be sent when the FraudScoreIndicator element is set to 2.	O	10	N
KTTVersionNumber	FraudAnalysis	**User Defined and Shopping Cart Format Indicator** This element must contain a value of "1" as of the release of this specification if the KTTDataLength and KTTDataString elements are populated.	C	1	N
KTTDataLength	FraudAnalysis	**User Defined or Shopping Cart Format Data Length** Indicates the length of the value of the KTTDataString element. This must be a 4 digit number no less than 0001 and no greater than 0999.	C	4	N

Gift Card (FlexCache) Request Elements   **Release Date:** August 2013   Page 174 of 283

KTTDataString	`FraudAnalysis`	**User Defined or Shopping Cart Format Data String** This field can be populated with user-defined Agent Web Console rules, Shopping Cart Data, or both. Please see *Special notes on KTT elements* for more information.	C	Var	A/N

4.14   Gift Card (FlexCache) Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required XML Parent Tag**	M	N/A	N/A
FlexCacheResp	`Response`	**XML Tag that Defines the Transaction as a Gift Card Response**	M	N/A	N/A
MerchantID	`FlexCacheResp`	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID sent in request.	M	12	N
TerminalID	`FlexCacheResp`	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID sent in request.	M	3	N
OrderID	`FlexCacheResp`	**Merchant-Defined Order Number** Field defined and supplied by the authorization originator and echoed back in response.	M	22	A
AccountNum	`FlexCacheResp`	**Gift Card Account Number** Echoes the Account Number sent in request, except for Block Activations.	C	19	N
StartAccountNum	`FlexCacheResp`	**The First Card Number in a Block Activation Sequence** Echoes the initial Account Number sent in a Block Activation request.	C	19	N
BatchFailedAcctNum	`FlexCacheResp`	**Card Number in a Block Activation Sequence that caused a Block Activation Failure** Conditionally returned on a Block Activation failure.	C	19	N
FlexRequestedAmount	`FlexCacheResp`	**Transaction Amount Submitted in the Request** ▪ Implied decimal.	C	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
FlexRedeemedAmt	FlexCacheResp	**Actual Amount Redeemed on a Redemption Completion** ▪ Implied decimal. ▪ Conditionally returned. Regardless of whether the amount redeemed is less than or equal to the requested amount, it will be identified in this tag.	C	12	N
FlexHostTrace	FlexCacheResp	**Gateway Transaction Reference Number** A unique value for each transaction, which is required to adjust any Gift Card transaction in the Gateway (such as Redemption Completion or Void/Reversal).	C	40	N
FlexAction	FlexCacheResp	**Transaction (or Action) Type Performed in the Request** Echoes the Action sent in request.	M	30	A
FlexAcctBalance	FlexCacheResp	**Current Balance of the Gift Card** The Balance after the result of the request transaction. This information is returned in all Gift Card response messages.	C	12	N
FlexAcctPriorBalance	FlexCacheResp	**Prior Balance of the Gift Card** Balance prior to the result of the request transaction. This information is returned in all Gift Card response messages.	C	12	N
FlexAcctExpireDate	FlexCacheResp	**Gift Card Expiration Date** ▪ The Expiration Date of the Gift Card, if any, is returned in all response messages. ▪ Format: `MMYY`	C	6	N
CardBrand	FlexCacheResp	**Request Card Type** Mnemonic representing the of the request card type: `FC` FlexCache	M	2	A
TxRefNum	FlexCacheResp	**Gateway Transaction Reference Number** A unique value for each transaction, which is required to Void (Reverse) a transaction.	M	40	A
TxRefIdx	FlexCacheResp	**Gateway Transaction Index** ▪ Used to identify the unique components of transactions adjusted more than one time. ▪ Required for Void transactions.	C	4	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ProcStatus	FlexCacheResp	**Process Status** ▪ The first data set that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A
StatusMsg	FlexCacheResp	**Text Message Associated with `RespCode` Value**	M	Var	A

ApprovalStatus	FlexCacheResp	**Approval Status**
		
		Conditional on:
		▪ Process Status returning a 0 or successful response.
		▪ Only returned if performing a MFC on a Gift Card Type.
		If present, the approval status identifies the result of the authorization request to the host system:
		  0 Decline
		  1 Approved
		  2 Message/System Error
			C	1	N

AuthCode	FlexCacheResp	**Issuer Approval Code** Unique transactional-level code issued by the bank or service establishment for approvals.	C	6	A
RespCode	FlexCacheResp	**Response Code** ▪ Normalized authorization response code issued by the host system (Salem/PNS), which identifies an approval (00) or the reason for a decline or error. ▪ Conditionally returned when `ProcStatus` = 0. See *Table 13* in Appendix A for values.	C	2	A
CVV2RespCode	FlexCacheResp	**Card Verification Value Request Response** Conditional on card verification request being sent. See *Table 17* in Appendix A for values.	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
RespTime	`FlexCacheResp`	**Time the Transaction was Processed by Gateway** Format: `hh24mmss`	M	6	N
FraudScoreProcStatus	`FlexCacheResp`	**Process Status of Fraud Score request** ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks related specifically to Fraud Analysis messages: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	Var	N
FraudScoreProcMsg	`FlexCacheResp`	**Verbose Text Description associated with `FraudScoreProcStatus`**	C	Var	A
FraudAnalysisResponse	`FlexCacheResp`	**Parent Element of Fraud Analysis Response Data**	M	N/A	N/A
FraudScoreIndicator	`FraudAnalysis Response`	**Echoes `FraudScoreIndicator` from the request message.**	M	1	N
FraudStatusCode	`FraudAnalysis Response`	**Fraud Status Code** The response code returned by the Safetech service to indicating the status of the fraud analysis.	C	4	A
RiskInquiryTransaction Id	`FraudAnalysis Response`	**Risk Inquiry Transaction ID** A unique ID used to identify the fraud assessment.	C	32	A

AutoDecisionResponse	`FraudAnalysis Response`	**Auto Decision Response**
		
		The auto decision response code returned by the Safetech service.
		
		The following is a list of valid values.
		
		  A Approved
		  D Decline
		  E Manager Review
		  R Review
		This list may expand in the future.
			O	1	A

RiskScore	`FraudAnalysis Response`	**Risk Score** This element may be returned as null if the Safetech service was not successful in generating a fraud score.	C	2	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
KaptchaMatchFlag	`FraudAnalysis Response`	**Kaptcha Match Flag** Indicates if a request to the Safetech service has a corresponding Kaptcha record.	O	1	A
WorstCountry	`FraudAnalysis Response`	**Worst Country** The two character ISO 3166 country code associated with this customer in the last 14 days. This element is only returned with a Fraud Score Indicator of 2.	C	2	A
CustomerRegion	`FraudAnalysis Response`	**Customer Region** The estimated region of the customer. The Safetech service will use lower case letters to represent a state or province, while uppercase letters indicate a county. This element is only returned with a Fraud Score Indicator of 2.	C	2	A
PaymentBrand	`FraudAnalysis Response`	**Payment Brand** The payment method (brand) identified by the Safetech service during Fraud Analysis. This element is only returned with a Fraud Score Indicator of 2.	O	4	A
FourteenDayVelocity	`FraudAnalysis Response`	**Fourteen Day Velocity** The total number of prior sales by this customer within the last 14 days. This element is only returned with a Fraud Score Indicator of 2.	O	2	A/N
SixHourVelocity	`FraudAnalysis Response`	**Six Hour Velocity** The total number of prior sales by this customer in any six hour window over the last 14 days. This element is only returned with a Fraud Score Indicator of 2.	O	2	A/N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

CustomerNetwork	`FraudAnalysis Response`	**Customer Network Type indicator**
		
		A single character designation of the type of network used by the customer to initiate the transaction.
		
		Some possible values can include:
		  `A` Anonymous
		  `L` Library
		  `H` High School
		  `N` Normal
		  `P` Prison
		  `S` Satellite
		This element is only returned with a Fraud Score Indicator of 2.
			O	1	A

NumberOfDevices	`FraudAnalysis Response`	**Number of Devices with Transaction** The number of devices associated with the transaction, as recorded by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	3	N
NumberOfCards	`FraudAnalysis Response`	**Number of Cards with Transaction** The number of cards associated with the transaction, as recorded by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	3	N
NumberOfEmails	`FraudAnalysis Response`	**Number of Emails with Transaction** The number of emails associated with the transaction, as recorded by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	3	N
DeviceLayers	`FraudAnalysis Response`	**Device Layer Description** A period-delimited description of the Network, Flash, JavaScript, HTTP, and Browser layers of the device used by the customer to initiate the transaction, as determined by the Safetech service. This element is only returned with a Fraud Score Indicator of 2.	O	54	A
DeviceFingerprint	`FraudAnalysis Response`	**Device Fingerprint** A hash of system identifiers determined by the Safetech service to be constants for the device used by the customer. This element is only returned with a Fraud Score Indicator of 2.	O	32	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerTimeZone	`FraudAnalysis Response`	**Customer Time Zone** The time zone where the customer resides, as an offset from GMT. This element is only returned with a Fraud Score Indicator of 2.	O	4	N
CustomerLocalDateTime	`FraudAnalysis Response`	**Customer Local Date & Time** The local timestamp of the customer's device. Format: YYYY-MM-DD HH:MM This element is only returned with a Fraud Score Indicator of 2.	O	16	N
DeviceRegion	`FraudAnalysis Response`	**Device Region** Indicates the region or state where the customer's device resides. The Safetech service will use lower case letters to represent a state or province, while uppercase letters indicate a county. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
DeviceCountry	`FraudAnalysis Response`	**Device Country** The ISO 3166 Country code which indicates the country where the customer's device resides. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
ProxyStatus	`FraudAnalysis Response`	**Proxy Status Indicator** Indicates if the device used by the customer is using a proxy network. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
JavascriptStatus	`FraudAnalysis Response`	**JavaScript Status Indicator** Indicates if the device used by the customer allows use of JavaScript. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
FlashStatus	`FraudAnalysis Response`	**Flash Status Indicator** Indicates if the device used by the customer allows Flash. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
CookiesStatus	`FraudAnalysis Response`	**Cookies Status Indicator** Indicates if the device used by the customer allows use of cookies. This element is only returned with a Fraud Score Indicator of 2.	O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BrowserCountry	`FraudAnalysis Response`	**Browser Country** The ISO 3166 Country code which indicates the country where the customer's browser resides. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
BrowserLanguage	`FraudAnalysis Response`	**Browser Language** The ISO 639-1 standard code which indicates the language of the customer's browser. This element is only returned with a Fraud Score Indicator of 2.	O	2	A
MobileDeviceIndicator	`FraudAnalysis Response`	**Mobile Device Indicator** Indicates if the device used by the customer is a mobile device. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
MobileDeviceType	`FraudAnalysis Response`	**Mobile Device Type** A description of the type of mobile device used by the customer. This element is only returned with a Fraud Score Indicator of 2.	O	32	A
MobileWirelessIndicator	`FraudAnalysis Response`	**Mobile Wireless Indicator** Indicates if the device used by the customer has wireless capabilities. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
VoiceDevice	`FraudAnalysis Response`	**Voice Device Indicator** Indicates if the device used by the customer is voice controlled. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
PCRemoteIndicator	`FraudAnalysis Response`	**PC Remote Indicator** Indicates if the device used by the customer is a remotely controlled computer. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
RulesDataLength	`FraudAnalysis Response`	**Rules Trigger Reply Data Length** Indicates the length of the data contained in the RulesData element. Values in this element are no less than 0005 and no greater than 0999. Returned only if the `RulesTrigger` element is set to 'Y' on the request message.	O	4	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
RulesData	`FraudAnalysis Response`	**Rules Trigger Reply Data** A comma-delimited list of the rules triggered in the Safetech service by the transaction request. For more information on the data contained in this element, please see *Special Notes on Rules Trigger response data*	O	Var	A/N

4.15   Quick Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required XML Parent Tag**	M	N/A	N/A
QuickResp	`Response`	**XML Tag that Defines the Transaction as a Quick Response**	M	N/A	N/A
MerchantID	`QuickResp`	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID sent in request.	M	12	N
TerminalID	`QuickResp`	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID sent in request.	M	3	N
OrderID	`QuickResp`	**Merchant-Defined Order Number** Field defined and supplied by the authorization originator and echoed back in response.	C	22	A
AccountNum	`QuickResp`	**Card Number Identifying the Customer** Echoes the Account Number sent in request.	C	19	N
StartAccountNum	`QuickResp`	**The First Card Number in a Block Activation Sequence** Echoes the initial Account Number sent in a Block Activation request.	C	19	N
TxRefNum	`QuickResp`	**Gateway Transaction Reference Number** A unique value for each transaction, which is required to Void (Reverse) a transaction.	C	40	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
TxRefIdx	`QuickResp`	**Gateway Transaction Index** Used to identify the unique components of transactions adjusted more than one time.	C	4	N
ProcStatus	`QuickResp`	**Process Status** ▪ The first data set that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A
StatusMsg	`QuickResp`	**Text Message Associated with `ProcStatus` Value**	C	Var	A
ApprovalStatus	`QuickResp`	**Approval Status** ▪ Conditional on Process Status returning a 0 or successful response. ▪ If present, the approval status identifies the result of the authorization request to the host system: 0 Decline 1 Approved 2 Message/System Error	C	1	N
CustomerBin	`QuickResp`	**Transaction Routing Definition** Echoes the BIN passed in the request.	C	6	N
CustomerMerchantID	`QuickResp`	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	C	15	N
CustomerName	`QuickResp`	**Customer Billing Name** Echoes the Customer Name passed in the request.	C	30	A
CustomerRefNum	`QuickResp`	**Customer Reference Number**	C	22	A
CustomerProfileAction	`QuickResp`	**Customer Profile Action that was Requested**	C	6	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

ProfileProcStatus	`QuickResp`	**Result Status of Profile Management**
		
		Communicates the success or failure of a Profile Management request:
		  `0` Success
		  `>0` An error condition, see *Table 16* in Appendix A for values.
			C	6	A

CustomerProfileMessage	`QuickResp`	**Text Message Associated with `ProfileProcStatus` Value**	C	Var	A
CustomerAddress1	`QuickResp`	**Cardholder Billing Address line 1**	C	30	A
CustomerAddress2	`QuickResp`	**Cardholder Billing Address line 2**	C	30	A
CustomerCity	`QuickResp`	**Cardholder Billing City**	C	20	A
CustomerState	`QuickResp`	**Cardholder Billing State**	C	2	A
CustomerZIP	`QuickResp`	**Cardholder Billing Address Zip Code**	C	10	A
CustomerEmail	`QuickResp`	**Cardholder E-mail Address**	C	50	A

CustomerPhone	`QuickResp`	**Cardholder Telephone Number**
		
		`AAAEEENNNNXXXX`, where
		  `AAA` = Area Code
		  `EEE` = Exchange
		  `NNNN` = Number
		  `XXXX` = Extension
			C	14	A

CustomerProfileOrderOverrideInd	`QuickResp`	**Whether any Order Data can be pre-populated from the Customer Reference Number (`CustomerRefNum`)**
		
		  `NO` No mapping to order data
		  `OI` Use `<CustomerRefNum>` for `<OrderID>`
		  `OD` Use `<CustomerRefNum>` for `<Comments>`
		  `OA` Use `<CustomerRefNum>` for `<OrderID>` and `<Comments>`
			C	2	A

OrderDefaultDescription	`QuickResp`	**Order Description**	C	64	A
OrderDefaultAmount	`QuickResp`	**Defaulted Transaction Amount** Implied decimal.	C	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerAccountType	`QuickResp`	**Card Type/Brand for the Transaction** Echoes the Card Type/Brand passed in the request, except: ▪ If no `CardBrand`, such as Visa or MasterCard, was sent in the request (when optional), the specific Card Brand mnemonic is returned. ▪ For PINless Debit transactions, the *request* Card Brand is `DP` (which is a generic PINless mnemonic). However, the *response* Card Brand will be one of the four supported PINless Debit Card Brands: `NP` NYCE PINless Debit `PP` Pulse PINless Debit `SP` Star PINless Debit	C	2	A
CCAccountNum	`QuickResp`	**Customer Credit Card Number**	C	19	N
CCExpireDate	`QuickResp`	**Customer Credit Card Expiration Date**	C	4	N
ECPAccountDDA	`QuickResp`	**ECP (DDA) Account Number**	C	17	A
ECPAccountType	`QuickResp`	**Deposit Account Type** `C` Consumer Checking (US or Canadian) `S` Consumer Savings (US Only) `X` Commercial Checking (US Only)	C	1	A
ECPAccountRT	`QuickResp`	**Bank Routing and Transit Number for the Customer**	C	9	N
ECPBankPmtDlv	`QuickResp`	**ECP Payment Delivery Method** The preferred manner to deposit the transaction: `B` Best Possible Method (US Only) Chase Paymentech utilizes the method that best fits the situation. If the RDFI is not an ACH participant, a facsimile draft is created. This should be the default value for this field. `A` ACH (US or Canadian) Deposit the transaction by ACH only. If the RDFI is not an ACH participant, the transaction is rejected.	C	1	A
RespTime	`QuickResp`	**Time the Transaction was Processed by Gateway** Format: `hh24mmss`	M	6	N

4.16   Account Updater Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required Parent XML Tag**	M	N/A	N/A
AccountUpdater	`Request`	**XML Tag that Defines the Transaction as an Account Updater Request**	M	N/A	N/A
OrbitalConnectionUsername	`AccountUpdater`	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces Not case-sensitive	M	32	A
OrbitalConnectionPassword	`AccountUpdater`	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A

CustomerBin	`AccountUpdater`	**Transaction Routing Definition**
		▪ Assigned by Chase Paymentech.
		  `000001` Salem
		  `000002` PNS
		▪ This is the equivalent to the `<BIN>` element used on transactional requests.
			M	6	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

CustomerMerchantID	AccountUpdater	**Gateway merchant account number assigned by Chase Paymentech**
		
		▪ This account number will match that of your host platform:
		
		  - BIN 000001: 6-digit Salem Division Number
		
		  - BIN 000002: 12-digit PNS Merchant ID
		
		▪ This is the equivalent to the `<MerchantID>` element used on transactional requests.
			M	15	N

CustomerRefNum	AccountUpdater	**Sets the Customer Reference Number that will be used to utilize a Customer Profile on all future Orders**
		
		▪ Given that this value can be the same as the Order Number of a transaction, the valid characters for this field follow the same convention as the Order ID element and include:
		
		  - abcdefghijklmnopqrstuvwxyz
		
		  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
		
		  - 0123456789
		
		  - - , $ @ & and a space character, though the space character **cannot** be the leading character
		
		  - Please note that all alphabetic characters in this field are stored in uppercase by the Orbital system. Uppercase and lowercase values cannot be used to differentiate Customer Reference Numbers.
			M	22	A

CustomerProfileAction	AccountUpdater	**Defines the Customer Profile Action Desired** ▪ Must be filled with 'AU' for the profile to be included with the next Account Updater submission	M	6	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ScheduledDate	AccountUpdater	**Defines A Future Date for an Account Updater Submission** ▪ Defines the future date that Orbital will add this profile to the set of Account Updater submissions ▪ Format: MMDDYYYY When this tag is not set, the profile will automatically go into the next AU submission.	O	8	N

4.17 Account Updater Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required Parent XML Tag**	M	N/A	N/A
AccountUpdaterResp	Response	**XML Tag that Defines the Transaction as an Account Updater Response**	M	N/A	N/A
CustomerBin	AccountUpdaterResp	**Transaction Routing Definition** Echoes the BIN passed in the request.	M	6	N
CustomerMerchantID	AccountUpdaterResp	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	M	15	N
CustomerRefNum	AccountUpdaterResp	**Customer Reference Number**	M	22	A
CustomerProfileAction	AccountUpdaterResp	**Customer Profile Action that was Requested**	M	6	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Status	AccountUpdaterResp	**Current Status of the Profile** A Active AS Auto Suspend I Inactive MS Manual Suspend	M	Var	A
ScheduledDate	AccountUpdaterResp	**The Requested Future Date of the AU Submission for this Profile.** **This will be blank if the <ScheduledDate> tag is not filled in the request.**	M	8	N
ProfileProcStatus	AccountUpdaterResp	**Result Status of Profile Management** Communicates the success or failure of a Profile Management request: 0 Success >0 An error condition, see *Table 16* in Appendix A for values.	M	6	A
CustomerProfileMessage	AccountUpdaterResp	**Text Message Associated with ProfileProcStatus Value**	M	Var	A
RespTime	AccountUpdaterResp	**Time the Transaction was Processed by Gateway** Format: YYYYMMDD HH24MMSS	M	15	N

4.18   Fraud Analysis Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Request	N/A	**Required Parent XML Tag**	M	N/A	N/A
SafetechFraudAnalysis	Request	**XML Tag that Defines the Transaction as a Fraud Analysis Request**	M	N/A	N/A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char[2]	Field Type[2]
OrbitalConnectionUsername	SafetechFraudAnalysis	**Orbital Connection Username set up on Orbital Gateway** Provides the Username associated with this MID. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Not case-sensitive	M	32	A
OrbitalConnectionPassword	SafetechFraudAnalysis	**Orbital Connection Password used in conjunction with Orbital Username** Provides the Password associated with Connection Username. Formats: ▪ Between 8–32 characters (a-z, A-Z, 0-9) ▪ Minimum 1 number ▪ No leading, trailing, or embedded spaces ▪ Password is case-sensitive and must exactly match what is stored on Orbital Gateway	M	32	A
BIN	SafetechFraudAnalysis	**Transaction Routing Definition** Assigned by Chase Paymentech. `000001` Salem	M	6	N
MerchantID	SafetechFraudAnalysis	**Gateway Merchant Account Number assigned by Chase Paymentech** This account number will match that of your host platform: ▪ BIN 000001: 6-digit Salem Division Number	M	12	N
TerminalID	SafetechFraudAnalysis	**Merchant Terminal ID assigned by Chase Paymentech** ▪ Salem Terminal IDs: presently set to `001`.	M	3	N
BaseElements	SafetechFraudAnalysis	**Parent XML Tag for Individual Transaction Elements**	M	N/A	N/A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
IndustryType	`BaseElements`	**Industry Type of the Transaction** MO Mail Order transaction RC Recurring Payment (not a valid choice for Canadian merchants) EC eCommerce transaction IV IVR (PINless Debit Only) IN Installment	M	2	A
CardBrand	`BaseElements`	**Card Type/Brand for the Transaction** Required for: ED European Direct Debit EC Electronic Check BL Bill Me Later DP PINless Debit (Generic Value Used in Requests) IM International Maestro FC Gift Card	C	2	A
AccountNum	`BaseElements`	**Card Number Identifying the Customer** ▪ Should be `NULL` for electronic check processing and Profile Transactions. ▪ Can be `NULL` for Refund transactions, provided that the `TxRefNum` field is filled appropriately. ▪ For Bill Me Later transactions, should be populated with either the customer's Bill Me Later account number or a Bill Me Later Bank Identification Number (BIN) followed by ten zeros (dummy account number). For example: `5049900000000000` The consumer's 16-byte Bill Me Later account number will be returned on all approved transactions.	C	19	N

Fraud Analysis Request Elements

Release Date: August 2013   Page 192 of 283

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Exp	BaseElements	**Card Expiration Date** ▪ Format: MMYY ▪ Mandatory for all card types, except ECP, European Direct Debit, Bill Me Later, and PINless Debit. ▪ Can be NULL for Refund transactions, provided that the TxRefNum field is filled appropriately. ▪ Salem (BIN 000001) allows a *blank* to be submitted when no known expiration date exists. There are three valid mechanisms for submitting a *Blank* expiration date to the Salem Host using Orbital: - null-fill this XML element: `<Exp/>` - Send four spaces: `<Exp>    </Exp>` - Zero-fill this XML element: `<Exp>0000</Exp>` *NOTE* Please discuss this feature with your certification analyst before implementing.	C	4	N
CurrencyCode	BaseElements	**Transaction Currency Code** ▪ The ISO-assigned code for the currency of the transaction. ▪ Bin 000002 supports only U.S. Dollar (840) and Canadian Dollar (124). See *Table 22* in Appendix A for a list of currency codes.	M	3	N
CurrencyExponent	BaseElements	**Exponent for the Transaction Currency** See *Table 22* in Appendix A for a list of currency code exponents.	M	6	N
CardSecValInd	BaseElements	**Card Security Presence Indicator** ▪ If you are trying to collect a Card Verification Number (CardSecVal) for a Visa or Discover transaction, pass one of these values: 1 Value is Present 2 Value on card but illegible 9 Cardholder states data not available ▪ If the transaction is not a Visa or Discover transaction: - Null-fill this attribute **OR** - Do not submit the attribute at all.	C	1	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CardSecVal	BaseElements	**Card Verification Number** ▪ Visa CVV2 3 bytes ▪ MasterCard CVC2 3 bytes ▪ American Express CID 4 bytes ▪ Discover CID 3 bytes *WARNING* It is against regulations to store this value.	O	4	N
BCRtNum	BaseElements	**Bank Routing and Transit Number for the Customer** Conditionally required for Electronic Check processing. **NOTES:** ▪ All US Bank Routing Numbers are 9 digits. ▪ All Canadian Bank Routing Numbers are 8 digits. - Formatted FFFBBBBB where F is Financial Institution and B is Branch Number - Cannot include spaces " " or dashes "-"	C	9	N
CheckDDA	BaseElements	**Customer DDA Account Number** Conditionally required for Electronic Check processing.	C	17	A
BankAcctType	BaseElements	**Deposit Account Type** Conditionally required for Electronic Check processing: C Consumer Checking (US or Canadian) S Consumer Savings (US Only) X Commercial Checking (US Only) *NOTE* If this tag is missing, the host will default the value to 'C' – Consumer Checking	C	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

ECPAuthMethod	BaseElements	**ECP Authorization Method**
		▪ Code used to identify the method used by consumers to authorize debits to their accounts.
		▪ Valid values:
		  W Written
		  I Internet (Web) – default
		  T Telephone
		  A Accounts Recievable (ARC) – US Merchants only
		  P Point of Purchase (POP) – US Merchants only
		▪ If no value submitted, we will default this value.
		See *3.2.5.3 ECP Authorization Methods* for more information.
			O	1	A

BankPmtDelv	BaseElements	**ECP Payment Delivery Method**
		▪ Conditionally required for Electronic Check processing.
		▪ This field indicates the preferred manner to deposit the transaction:
		  B Best Possible Method (US Only)
		    Chase Paymentech utilizes the method that best fits the situation. If the RDFI is not an ACH participant, a facsimile draft is created. This should be the default value for this field.
		  A ACH (US or Canadian)
		    Deposit the transaction by ACH only. If the RDFI is not an ACH participant, the transaction is rejected.
		  F Facsimile Draft
		    This is a document created by CPS per merchant request or if the receiving bank is not a participant of the ACH association. The facsimile draft flows through the Federal Reserve's check clearing process rather than the ACH network
			C	1	A

AVSzip	BaseElements	**Cardholder Billing Address Zip Code** ▪ All AVS Requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	10	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVSaddress1	BaseElements	**Cardholder Billing Address line 1** ▪ Should not include any of the following characters: `%	^ \ /` ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	30	A
AVSaddress2	BaseElements	**Cardholder Billing Address line 2** ▪ Should not include any of the following characters: `%	^ \ /` ▪ Required for Bill Me Later sale transactions.	O	30	A
AVScity	BaseElements	**Cardholder Billing City** ▪ Should not include any of the following characters: `%	^ \ /` ▪ For BIN 000001, must supply AVSzip, AVSaddress1, and AVScity in order for data to be transmitted to Host Processing System ▪ Required for Bill Me Later sale transactions.	C	20	A
AVSstate	BaseElements	**Cardholder Billing State** ▪ Should not include any of the following characters: `%	^ \ /` ▪ Required for Bill Me Later sale transactions.	C	2	A
AVSphoneNum	BaseElements	**Cardholder Billing Phone Number** `AAAEEENNNNXXXX`, where `AAA` = Area Code `EEE` = Exchange `NNNN` = Number `XXXX` = Extension Required for Bill Me Later sale transactions.	C	14	A
AVSname	BaseElements	**Cardholder Billing Name** Required for Bill Me Later sale transactions and all Electronic Check transactions, and all European Direct Debit (EU DD) transactions.	C	30	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
AVScountryCode	BaseElements	**Cardholder Billing Address Country Code** Valid values: US United States CA Canada GB Great Britain UK United Kingdom Conditionally required for Bill Me Later sale transactions.	C	2	A
AVSDestzip	BaseElements	**Cardholder Destination Address Zip Code** ▪ All AVS Requests must minimally include the 5-digit Zip Code. ▪ If sending Zip Code + 4, separate with a hyphen (-). ▪ Required for Bill Me Later sale transactions.	C	10	A
AVSDestaddress1	BaseElements	**Cardholder Destination Address line 1** ▪ Should not include any of the following characters: % | ^ \ / - ▪ Required for Bill Me Later sale transactions.	C	30	A
AVSDestaddress2	BaseElements	**Cardholder Destination Address Line 2** ▪ Should not include any of the following characters: % | ^ \ / - ▪ Optional for Bill Me Later Transactions.	O	28	A
AVSDestcity	BaseElements	**Cardholder Destination Billing City** ▪ Should not include any of the following characters: % | ^ \ / - ▪ Required for Bill Me Later sale transactions.	C	20	A
AVSDeststate	BaseElements	**Cardholder Destination Billing State** ▪ Should not include any of the following characters: % | ^ \ / - ▪ Required for Bill Me Later sale transactions	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]

AVSDestphoneNum	BaseElements	**Cardholder Destination Phone Number**
		
		AAAEEENNNNXXXX, where
		  AAA = Area Code
		  EEE = Exchange
		  NNNN = Number
		  XXXX = Extension
		▪ Optional for Bill Me Later sale transactions.
		▪ International phone numbers are restricted to 14 bytes therefore U.S. formats may not be applicable
			O	14	A

AVSDestname	BaseElements	**Cardholder Destination Billing Name** Required for Bill Me Later sale transactions.	C	30	A

AVSDestcountryCode	BaseElements	**Cardholder Destination Address Country Code**
		▪ Valid values:
		  US United States
		  CA Canada
		  GB Great Britain
		  UK United Kingdom
		▪ Required for Bill Me Later sale transactions.
			C	2	A

UseCustomerRefNum	BaseElements	**The Customer Reference Number that will be used to populate missing request fields** Conditionally required when Using a Profile during a fraud analysis request.	C	22	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
OrderID	BaseElements	**Merchant-Defined Order Number** ▪ Field defined and supplied by the auth originator and echoed back in response. ▪ The first 8 characters should be unique for each transaction. The valid characters include: ▪ abcdefghijklmnopqrstuvwxyz ▪ ABCDEFGHIJKLMNOPQRSTUVWXYZ ▪ 0123456789 ▪ – , $ @ & and a space character, though the space character **cannot** be the leading character ▪ PINless Debit transactions can only use uppercase and lowercase alpha (A-Z, a-z) and numeric (0-9) characters—NO special characters. For BIN 000002 merchants: ▪ If IndustryType = EC, first 16 bytes are passed to the Host Processing System ▪ If IndustryType = MO, first 9 bytes are passed to the Host Processing System	M	22	A
Amount	BaseElements	**Transaction Amount** Implied decimal, including those currencies that are a zero exponent. For example, both $100.00 (an exponent of 2) and ¥100 (an exponent of 0) should be sent as `<Amount>`**10000**`</Amount>`.	C	12	N
Comments	BaseElements	**Free-form comments** ▪ Merchant can fill in this field, and the information will be stored with the transaction details. ▪ For PNS customers, this field will populate the Customer Defined Data field, which is displayed in Resource Online.	O	64	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
EUDDCountryCode	BaseElements	**European Direct Debit Country Code** ▪ Customer's Country Code. ▪ Valid country codes: AT Austria BE Belgium DE Germany FR France GB United Kingdom NL Netherlands ▪ Conditionally required for European Direct Debit.	C	2	A
EUDDBankSortCode	BaseElements	**European Direct Debit Bank Sort Code** ▪ Customer's Bank Sort code. ▪ Mandatory for the following Country Codes: AT Austria DE Germany FR France GB United Kingdom	C	10	A
EUDDRibCode	BaseElements	**European Direct Debit RIB** ▪ Bank Account checksum. ▪ Used in France only.	C	2	A
BMLCustomerIP	BaseElements	**Customer's IP Address** Optional for Bill Me Later sale transactions.	O	45	A
BMLCustomerEmail	BaseElements	**Customer E-mail Address** Optional for Bill Me Later sale transactions.	O	50	A
BMLShippingCost	BaseElements	**Total Shipping Cost of Consumer's Order** Mandatory for Bill Me Later sale transactions.	C	8	N
BMLTNCVersion	BaseElements	**Terms and Conditions Number** ▪ The Terms and Conditions Number to which the consumer agreed. ▪ Mandatory for Bill Me Later sale transactions.	C	5	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BMLCustomerRegistrationDate	BaseElements	**Customer Registration Date** ▪ The date a customer registered with the merchant. ▪ Mandatory for Bill Me Later sale transactions.	C	8	N
BMLCustomerTypeFlag	BaseElements	**Customer Type Flag** ▪ New or Existing Customer to the Merchant (not Bill Me Later): N New E Existing ▪ Optional for Bill Me Later sale transactions.	O	2	A
BMLItemCategory	BaseElements	**Item Category** ▪ Product Description Code assigned by Bill Me Later, Inc. ▪ Mandatory for Bill Me Later sale transactions.	C	4	N
BMLPreapprovalInvitationNum	BaseElements	**Pre-Approval Invitation Number** ▪ Indicates whether the consumer has been pre-approved for Bill Me Later. - Pre-approval from a credit bureau should include the 16-digit pre-approval number. This will allow the pre-approval to be matched with the first consumer order. - Internal pre-approval should have 1 as the leftmost digit. - Pre-approvals cannot include all zeros or be blank-filled. ▪ Optional for Bill Me Later sale transactions.	O	16	A
BMLMerchantPromotionalCode	BaseElements	**Merchant Promotional Code** Optional for Bill Me Later sale transactions.	O	4	A
BMLCustomerBirthDate	BaseElements	**Customer Date of Birth** ▪ Format: YYYYMMDD ▪ Mandatory for Bill Me Later sale transactions.	C	8	N
BMLCustomerSSN	BaseElements	**Customer Social Security Number** ▪ Either the full 9 digits or last 4 digits of the customer's Social Security Number. ▪ Mandatory for Bill Me Later sale transactions.	C	9	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BMLCustomerAnnualIncome	BaseElements	**Gross Household Annual Income** ▪ Implied decimal. For example, $100,000.00 should be sent as: <BMLCustomerAnnualIncome>10000000</BMLCustomerAnnualIncome> ▪ Optional for Bill Me Later sale transactions.	O	10	N
BMLCustomerResidenceStatus	BaseElements	**Customer Residence Status** Valid values: O Own R Rent X Other Optional for Bill Me Later sale transactions.	O	1	A
BMLCustomerCheckingAccount	BaseElements	**Customer Checking Account Indicator** Valid values: Y Yes, customer has a checking account N No, customer does not have a checking account Optional for Bill Me Later sale transactions.	O	1	A
BMLCustomerSavingsAccount	BaseElements	**Customer Savings Account Indicator** Valid values: Y Yes, customer has a savings account N No, customer does not have a savings account Optional for Bill Me Later sale transactions.	O	1	A
BMLProductDeliveryType	BaseElements	**Delivery Type Indicator** Valid values: CNC Cash and Carry DIG Digital Goods PHY Physical Delivery Required SVC Service TBD To Be Determined Optional for Bill Me Later sale transactions.	C	3	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
BillerReferenceNumber	BaseElements	**Biller Reference Number (PINless Debit Only)** ▪ Reference Number the Biller (merchant) uses on their system to identify this customer. ▪ Conditionally required for PINless Debit.	C	25	A
UseStoredAAVIndicator	BaseElements	**Use Stored AAV Indicator** This element is conditionally required on recurring payments for International Maestro. Valid values: Y Submit the Static AAV stored by Gateway with this transaction. This should not be submitted if the **AAV** element is populated.	C	1	A
ECPCheckSerialNumber	BaseElements	**ECP Check Serial Number** This value corresponds to the check number on a physical check supplied by the consumer. This value is 9 digits for BIN 000001 merchants and 6 digits for BIN 000002. Must be NULL unless CardBrand = EC and ECPAuthMethod = A or P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	Var	A/N
ECPTerminalCity	BaseElements	**ECP Terminal City** This value corresponds to the city of the point of sale the check is processed at. Must be NULL unless CardBrand = EC and ECPAuthMethod = P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	4	A
ECPTerminalState	BaseElements	**ECP Terminal State** This value corresponds to the city of the point of sale the check is processed at. Must be NULL unless CardBrand = EC and ECPAuthMethod = P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	2	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ECPImageReferenceNumber	BaseElements	**ECP Check Image Reference Number** Image reference number associated with a check. Must be NULL unless CardBrand = EC and ECPAuthMethod = P. See *3.2.5.3 ECP Authorization Methods* for more information.	C	32	A/N
CustomerAni	BaseElements	**Customer Automatic Number Identification** The ANI specified phone number that the customer used to place the order. Recommended for transactions utilizing Safetech Fraud Tools.	O	10	N
AVSPhoneType	BaseElements	**Customer Telephone Type Indicator** Valid values: D Day H Home N Night W Work This value is defaulted to H if any phone number is present and this element is either not present or null filled.	O	1	A
AVSDestPhoneType	BaseElements	**Bill Me Later Cardholder Destination Telephone Type Indicator** Valid values: D Day H Home N Night W Work This value is defaulted to H if any phone number is present and this element is either not present or null filled.	O	1	A
CustomerEmail	BaseElements	**Customer Email Address** The customer's contact email address.	O	50	A
CustomerIpAddress	BaseElements	**Customer IP Address** The single source IP address used by the customer to request a payment. Supports IPv4 or IPv6 formats. Punctuation marks are allowed.	O	45	A/N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
EmailAddressSubtype	BaseElements	**Customer Email Address Subtype** Used to indicate the type of email address in the CustomerEmail element. Valid values: B Bill To/Buyer Email Address G Giftee Email Address This value is defaulted to B if an email address is present and this element is not present or null filled.	O	1	A
CustomerBrowserName	BaseElements	**Customer Browser Type** Used to indicate the type of web browser used by the customer to initiate the request. Example: MOZILLA/4.0 (COMPATIBLE; MSIE 5.0; WINDOWS 95	O	60	A
ShippingMethod	BaseElements	**Method of Shipping To A Customer** Valid values: C Lowest Cost D Carrier Designated by Customer E Electronic Delivery* G Ground* I International M Military N Next Day or Overnight* O Other P Store Pickup* S Same Day* T Two Day Service* W Three Day Service* For American Express, use only values marked with an asterisk.	O	1	A
FraudAnalysis	SafetechFraudAnalysis	**Parent XML Tag for Safetech Fraud Analysis Elements**	M	N/A	N/A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
FraudScoreIndicator	FraudAnalysis	**Fraud Analysis Type Indicator** Used to request the type of fraud analysis performed on the transaction. The value in this field directly determines the scope of elements returned in the response message. Valid values: 1 Short Form Request 2 Long Form Request	M	1	N
RulesTrigger	FraudAnalysis	**Fraud Analysis Rules Return Trigger** Determines whether the Agent Web Console (AWC) rules are returned. Valid values: Y Triggered rules are returned N Triggered rules are not returned	O	1	A
SafetechMerchantID	FraudAnalysis	**Safetech Merchant ID** A value assigned by Chase Paymentech when a merchant is enabled for the Safetech service. This is not the same value as Transaction Division number found in the `MerchantID` element. If no value is present, a default value will be used if available. If no default is stored, the request will generate an error.	O	6	A/N
KaptchaSessionID	FraudAnalysis	**Kaptcha Session ID** A merchant generated session ID for this fraud scoring request. The Safetech system recommends this value be unique for 30 days, or the Fraud Score results may not be accurate.	O	32	A
WebsiteShortName	FraudAnalysis	**Short Name for the Merchant's Website** This value is used by the Safetech service for fraud score rules.	O	8	A
CashValueOfFencibleIterms	FraudAnalysis	**Cash Value of Fencible Items** The cash value of any fencible items in the order. This element should only be sent when the `FraudScoreIndicator` element is set to 2.	O	12	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CustomerDOB	FraudAnalysis	**Customer Date of Birth** Format: *YYYY-MM-DD* (Including dashes) This element should only be sent when the FraudScoreIndicator element is set to 2.	O	10	A/N
CustomerGender	FraudAnalysis	**Customer Gender** Valid values: F Female M Male This element should only be sent when the FraudScoreIndicator element is set to 2.	O	1	A
CustomerDriverLicense	FraudAnalysis	**Customer Driver's License Number** U.S. Driver's License number only. The Safetech service recommends this value for fraud scoring of Electronic Check (ECP) requests. This element should only be sent when the FraudScoreIndicator element is set to 2.	O	32	A
CustomerID	FraudAnalysis	**Customer ID** A merchant generated ID for a specific customer. This element should only be sent when the FraudScoreIndicator element is set to 2.	O	32	A
CustomerIDCreationTime	FraudAnalysis	**Customer ID Creation Time** The time the value used in the CustomerID element was created by the merchant. Format: Unix Epoc This element should only be sent when the FraudScoreIndicator element is set to 2.	O	10	N
KTTVersionNumber	FraudAnalysis	**User Defined and Shopping Cart Format Indicator** This element must contain a value of "1" as of the release of this specification if the KTTDataLength and KTTDataString elements are populated.	C	1	N

Fraud Analysis Request Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
KTTDataLength	FraudAnalysis	**User Defined or Shopping Cart Format Data Length** Indicates the length of the value of the `KTTDataString` element. This must be a 4 digit number no less than 0001 and no greater than 0999.	C	4	N
KTTDataString	FraudAnalysis	**User Defined or Shopping Cart Format Data String** This field can be populated with user-defined Agent Web Console rules, Shopping Cart Data, or both. Please see *Special notes on KTT elements* for additional information.	C	Var	A/N

4.19   Fraud Analysis Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
Response	N/A	**Required XML Parent Tag**	M	N/A	N/A
SafetechFraudAnalysisResp	Response	**XML Tag that Defines the Transaction as a Fraud Analysis Response**	M	N/A	N/A
IndustryType	SafetechFraudAnalysisResp	**Industry Type of the Transaction** This tag returns `null` results.	M	2	A
MerchantID	SafetechFraudAnalysisResp	**Gateway Merchant Account Number assigned by Chase Paymentech** Echoes the Merchant ID passed in the request.	M	12	N
TerminalID	SafetechFraudAnalysisResp	**Merchant Terminal ID assigned by Chase Paymentech** Echoes the Terminal ID passed in the request.	M	3	N

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
CardBrand	SafetechFraudAnalysis Resp	**Card Type/Brand for the Transaction** Echoes the Card Type/Brand passed in the request, except: ▪ If no CardBrand, such as Visa or MasterCard, was sent in the request (when optional), the specific Card Brand mnemonic is returned. ▪ For PINless Debit transactions, the *request* Card Brand is DP (which is a generic PINless mnemonic). However, the *response* Card Brand will be one of the three supported PINless Debit Card Brands: NP NYCE PINless Debit PP Pulse PINless Debit SP Star PINless Debit AP Accel PINless Debit	M	2	A
AccountNum	SafetechFraudAnalysis Resp	**Account Number** Echoes the Account Number passed in the request	M	19	N
OrderID	SafetechFraudAnalysis Resp	**Merchant-Defined Order Number** Echoes the Order Number passed in the request.	M	22	A
TxRefNum	SafetechFraudAnalysis Resp	**Gateway Transaction Reference Number** A unique value for each transaction, which is required to adjust any transaction in the Gateway (such as Mark for Capture or Void).	M	40	A
RespTime	SafetechFraudAnalysis Resp	**Time the Transaction was Processed by Gateway** Format: hh24mmss	M	6	N
ProcStatus	SafetechFraudAnalysis Resp	**Process Status** ▪ The first element that should be checked to determine the result of a request. ▪ The only element that is returned in all response scenarios. ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks: 0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	6	A

Fraud Analysis Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
ApprovalStatus	`SafetechFraudAnalysisResp`	**Approval Status** Conditional on Process Status returning a `0` (or successful) response. If so, the Approval Status identifies the result of the request to the host system: `0` Declined `1` Approved `2` Message/System Error	C	1	N
RespCode	`SafetechFraudAnalysisResp`	**Response Code** Normalized authorization response code issued by the host system (Salem/PNS), which identifies an approval (`00`) or the reason for a decline or error. See *Table 13* in Appendix A for values.	C	2	A
StatusMsg	`SafetechFraudAnalysisResp`	**Text Message Associated with `RespCode` Value**	C	Var	A
RespMsg	`SafetechFraudAnalysisResp`	**Message Associated with `HostRespCode`** May not be populated for transactions not requiring an authorization such as Force or Refunds	C	80	A
HostRespCode	`SafetechFraudAnalysisResp`	**Actual Host Response Code** ▪ Exact response sent by host authorization system (non-normalized by the Gateway). ▪ For those systems that have already coded to the Salem/PNS authorization response values, they are available via this tag.	C	3	A
CustomerRefNum	`SafetechFraudAnalysisResp`	**Customer Reference Number** This field will echo the Customer Reference Number sent in the Request, if applicable.	C	22	A
CustomerName	`SafetechFraudAnalysisResp`	**Customer Billing Name** Echoes value from the request.	C	30	A
ProfileProcStatus	`SafetechFraudAnalysisResp`	**Result Status of Profile Management** Communicates the success or failure of a Profile Management request: `0` Success `>0` An error condition, see *Table 16* in Appendix A for values	C	6	A
CustomerProfileMessage	`SafetechFraudAnalysisResp`	**Verbose Text Description associated with `ProfileProcStatus`**	C	Var	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
FraudScoreProcStatus	`SafetechFraudAnalysis Resp`	**Process Status of Fraud Score request** ▪ Identifies whether transactions have successfully passed all of the Gateway edit checks related specifically to Fraud Analysis messages: 　0 Success All other values constitute an error condition. See *Table 15* in Appendix A for definition of these error values.	M	Var	N
FraudScoreProcMsg	`SafetechFraudAnalysis Resp`	**Verbose Text Description associated with `FraudScoreProcStatus`**	C	Var	A
FraudAnalysisResponse	`SafetechFraudAnalysis Resp`	**Parent Element of Fraud Analysis Response Data**	M	N/A	N/A
FraudScoreIndicator	`FraudAnalysisResponse`	**Echoes `FraudScoreIndicator` from the request message.**	M	1	N
FraudStatusCode	`FraudAnalysisResponse`	**Fraud Status Code** The response code returned by the Safetech service to indicating the status of the fraud analysis.	C	4	A
RiskInquiryTransactionId	`FraudAnalysisResponse`	**Risk Inquiry Transaction ID** A unique ID used to identify the fraud assessment.	C	32	A
AutoDecisionResponse	`FraudAnalysisResponse`	**Auto Decision Response** The auto decision response code returned by the Safetech service. The following is a list of valid values. 　A　Approved 　D　Decline 　E　Manager Review 　R　Review This list may expand in the future.	O	1	A
RiskScore	`FraudAnalysisResponse`	**Risk Score** This element may be returned as null if the Safetech service was not successful in generating a fraud score.	C	2	N
KaptchaMatchFlag	`FraudAnalysisResponse`	**Kaptcha Match Flag** Indicates if a request to the Safetech service has a corresponding Kaptcha record.	O	1	A

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
WorstCountry	FraudAnalysisResponse	**Worst Country**	C	2	A
		The two character ISO 3166 country code associated with this customer in the last 14 days.			
		This element is only returned with a Fraud Score Indicator of 2.			
CustomerRegion	FraudAnalysisResponse	**Customer Region**	C	2	A
		The estimated region of the customer.			
		The Safetech service will use lower case letters to represent a state or province, while uppercase letters indicate a county.			
		This element is only returned with a Fraud Score Indicator of 2.			
PaymentBrand	FraudAnalysisResponse	**Payment Brand**	O	4	A
		The payment method (brand) identified by the Safetech service during Fraud Analysis.			
		This element is only returned with a Fraud Score Indicator of 2.			
FourteenDayVelocity	FraudAnalysisResponse	**Fourteen Day Velocity**	O	2	A/N
		The total number of prior sales by this customer within the last 14 days.			
		This element is only returned with a Fraud Score Indicator of 2.			
SixHourVelocity	FraudAnalysisResponse	**Six Hour Velocity**	O	2	A/N
		The total number of prior sales by this customer in any six hour window over the last 14 days.			
		This element is only returned with a Fraud Score Indicator of 2.			
CustomerNetwork	FraudAnalysisResponse	**Customer Network Type indicator**	O	1	A
		A single character designation of the type of network used by the customer to initiate the transaction.			
		Some possible values can include: A Anonymous L Library H High School N Normal P Prison S Satellite This element is only returned with a Fraud Score Indicator of 2.			

Fraud Analysis Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
NumberOfDevices	FraudAnalysisResponse	**Number of Devices with Transaction**	O	3	N
		The number of devices associated with the transaction, as recorded by the Safetech service.			
		This element is only returned with a Fraud Score Indicator of 2.			
NumberOfCards	FraudAnalysisResponse	**Number of Cards with Transaction**	O	3	N
		The number of cards associated with the transaction, as recorded by the Safetech service.			
		This element is only returned with a Fraud Score Indicator of 2.			
NumberOfEmails	FraudAnalysisResponse	**Number of Emails with Transaction**	O	3	N
		The number of emails associated with the transaction, as recorded by the Safetech service.			
		This element is only returned with a Fraud Score Indicator of 2.			
DeviceLayers	FraudAnalysisResponse	**Device Layer Description**	O	54	A
		A period-delimited description of the Network, Flash, JavaScript, HTTP, and Browser layers of the device used by the customer to initiate the transaction, as determined by the Safetech service.			
		This element is only returned with a Fraud Score Indicator of 2.			
DeviceFingerprint	FraudAnalysisResponse	**Device Fingerprint**	O	32	A
		A hash of system identifiers determined by the Safetech service to be constants for the device used by the customer.			
		This element is only returned with a Fraud Score Indicator of 2.			
CustomerTimeZone	FraudAnalysisResponse	**Customer Time Zone**	O	4	N
		The time zone where the customer resides, as an offset from GMT.			
		This element is only returned with a Fraud Score Indicator of 2.			
CustomerLocalDateTime	FraudAnalysisResponse	**Customer Local Date & Time**	O	16	N
		The local timestamp of the customer's device.			
		Format: YYYY-MM-DD HH:MM			
		This element is only returned with a Fraud Score Indicator of 2.			

Fraud Analysis Response Elements

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
DeviceRegion	FraudAnalysisResponse	**Device Region**	O	2	A
		Indicates the region or state where the customer's device resides.			
		The Safetech service will use lower case letters to represent a state or province, while uppercase letters indicate a county.			
		This element is only returned with a Fraud Score Indicator of 2.			
DeviceCountry	FraudAnalysisResponse	**Device Country**	O	2	A
		The ISO 3166 Country code which indicates the country where the customer's device resides.			
		This element is only returned with a Fraud Score Indicator of 2.			
ProxyStatus	FraudAnalysisResponse	**Proxy Status Indicator**	O	1	A
		Indicates if the device used by the customer is using a proxy network.			
		This element is only returned with a Fraud Score Indicator of 2.			
JavascriptStatus	FraudAnalysisResponse	**JavaScript Status Indicator**	O	1	A
		Indicates if the device used by the customer allows use of JavaScript.			
		This element is only returned with a Fraud Score Indicator of 2.			
FlashStatus	FraudAnalysisResponse	**Flash Status Indicator**	O	1	A
		Indicates if the device used by the customer allows Flash.			
		This element is only returned with a Fraud Score Indicator of 2.			
CookiesStatus	FraudAnalysisResponse	**Cookies Status Indicator**	O	1	A
		Indicates if the device used by the customer allows use of cookies.			
		This element is only returned with a Fraud Score Indicator of 2.			
BrowserCountry	FraudAnalysisResponse	**Browser Country**	O	2	A
		The ISO 3166 Country code which indicates the country where the customer's browser resides.			
		This element is only returned with a Fraud Score Indicator of 2.			
BrowserLanguage	FraudAnalysisResponse	**Browser Language**	O	2	A
		The ISO 639-1 standard code which indicates the language of the customer's browser.			
		This element is only returned with a Fraud Score Indicator of 2.			

XML Element Name	XML Parent Element	Description	Required[1]	Max Char	Field Type[2]
MobileDeviceIndicator	FraudAnalysisResponse	**Mobile Device Indicator** Indicates if the device used by the customer is a mobile device. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
MobileDeviceType	FraudAnalysisResponse	**Mobile Device Type** A description of the type of mobile device used by the customer. This element is only returned with a Fraud Score Indicator of 2.	O	32	A
MobileWirelessIndicator	FraudAnalysisResponse	**Mobile Wireless Indicator** Indicates if the device used by the customer has wireless capabilities. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
VoiceDevice	FraudAnalysisResponse	**Voice Device Indicator** Indicates if the device used by the customer is voice controlled. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
PCRemoteIndicator	FraudAnalysisResponse	**PC Remote Indicator** Indicates if the device used by the customer is a remotely controlled computer. This element is only returned with a Fraud Score Indicator of 2.	O	1	A
RulesDataLength	FraudAnalysisResponse	**Rules Trigger Reply Data Length** Indicates the length of the data contained in the RulesData element. Values in this element are no less than 0005 and no greater than 0999. Returned only if the RulesTrigger element is set to 'Y' on the request message.	O	4	N
RulesData	FraudAnalysisResponse	**Rules Trigger Reply Data** A comma-delimited list of the rules triggered in the Safetech service by the transaction request. For more information on the data contained in this element, please see *Special Notes on Rules Trigger response data*	O	Var	A/N

Fraud Analysis Response Elements

Chapter 5   Sample XML Transactions

This chapter contains sample transactions for the various types of requests and responses described earlier in this guide. These samples illustrate the XML format in which the requests must ultimately be presented to the Orbital Gateway and in which the Gateway will present the responses to you.

NOTE   The samples in this chapter do not illustrate all of the possible elements you can include in a request.

5.1   Example Requests

5.1.1   New Order Request

```
<?xml version="1.0" encoding="UTF-8"?>
<Request>
    <NewOrder>
        <OrbitalConnectionUsername>TESTUSER123</OrbitalConnectionUsername>
        <OrbitalConnectionPassword>abcd1234</OrbitalConnectionPassword>
        <IndustryType>EC</IndustryType>
        <MessageType>AC</MessageType>
        <BIN>000001</BIN>
        <MerchantID>123456</MerchantID>
        <TerminalID>001</TerminalID>
        <CardBrand></CardBrand>
        <AccountNum>5454545454545454</AccountNum>
        <Exp>0112</Exp>
        <CurrencyCode>840</CurrencyCode>
        <CurrencyExponent>2</CurrencyExponent>
        <AVSzip>25541</AVSzip>
        <AVSaddress1>123 Test Street</AVSaddress1>
        <AVSaddress2>Suite 350</AVSaddress2>
        <AVScity>Test City</AVScity>
        <AVSstate>FL</AVSstate>
        <AVSphoneNum>8004564512</AVSphoneNum>
        <OrderID>8316384413</OrderID>
        <Amount>2500</Amount>
    </NewOrder>
</Request>
```

5.1.2 PINless Debit Request

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Request>
    <NewOrder>
        <OrbitalConnectionUsername>TESTUSER123</OrbitalConnectionUsername>
        <OrbitalConnectionPassword>abcd1234</OrbitalConnectionPassword>
        <IndustryType>EC</IndustryType>
        <MessageType>R</MessageType>
        <BIN>000001</BIN>
        <MerchantID>123456</MerchantID>
        <TerminalID>001</TerminalID>
        <CardBrand>DP</CardBrand>                                    ← DP=PINless Debit
        <AccountNum>9409400000000000</AccountNum>
        <Exp>0112</Exp>
        <CurrencyCode>840</CurrencyCode>
        <CurrencyExponent>2</CurrencyExponent>
        <AVSzip>25541</AVSzip>
        <AVSaddress1>123 Test Street</AVSaddress1>
        <AVSaddress2>Suite 350</AVSaddress2>
        <AVScity>Test City</AVScity>
        <AVSstate>FL</AVSstate>
        <AVSphoneNum>8004564512</AVSphoneNum>
        <AVSname>TestMerchant</AVSname>
        <AVScountryCode>US</AVScountryCode>
        <OrderID>TestOrder458467</OrderID>            ← no spaces in PINless Debit Order ID
        <Amount>2500</Amount>
        <BillerReferenceNumber>Testbiller12355</BillerReferenceNumber>  ← required for PINless
    </NewOrder>
</Request>
```

5.1.3 Profile Add Request

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Request>
    <Profile>
        <OrbitalConnectionUsername>TESTUSER123</OrbitalConnectionUsername>
        <OrbitalConnectionPassword>abcd1234</OrbitalConnectionPassword>
        <CustomerBin>000001</CustomerBin>
        <CustomerMerchantID>123456</CustomerMerchantID>
        <CustomerName>Jon Doe</CustomerName>
        <CustomerRefNum>ADDPROFILE 123</CustomerRefNum>
        <CustomerAddress1>123 Test Drive</CustomerAddress1>
        <CustomerAddress2>Suite 123</CustomerAddress2>
        <CustomerCity>Test City</CustomerCity>
        <CustomerState>FL</CustomerState>
        <CustomerZIP>33626</CustomerZIP>
        <CustomerEmail>jondoe@test.com</CustomerEmail>
        <CustomerPhone>2232231234</CustomerPhone>
        <CustomerCountryCode>US</CustomerCountryCode>
        <CustomerProfileAction>C</CustomerProfileAction>
        <CustomerProfileOrderOverrideInd>NO</CustomerProfileOrderOverrideInd>
        <CustomerProfileFromOrderInd>S</CustomerProfileFromOrderInd>
        <OrderDefaultDescription>Sample Order Description</OrderDefaultDescription>
        <OrderDefaultAmount>1500</OrderDefaultAmount>
        <CustomerAccountType>CC</CustomerAccountType>
        <Status>A</Status>
        <CCAccountNum>5454545454545454</CCAccountNum>
        <CCExpireDate>0810</CCExpireDate>
        <MBType>R</MBType>                                          ← Recurring
        <MBOrderIdGenerationMethod>IO</MBOrderIdGenerationMethod>
        <MBRecurringStartDate>11012008</MBRecurringStartDate>
        <MBRecurringNoEndDateFlag>Y</MBRecurringNoEndDateFlag>
        <MBRecurringFrequency>? */5 MON</MBRecurringFrequency>      ← every 5th Monday
    </Profile>
</Request>
```

5.1.4   Safetech Fraud Analysis Request

```
<Request>
<SafetechFraudAnalysis>
        <OrbitalConnectionUsername></OrbitalConnectionUsername>
        <OrbitalConnectionPassword></OrbitalConnectionPassword>
        <BIN>000001</BIN>
        <MerchantID>123456</MerchantID>
        <TerminalID>001</TerminalID>
        <BaseElements>
            <IndustryType>EC</IndustryType>
            <AccountNum>4012888888888886</AccountNum>
            <Exp>1213</Exp>
            <CurrencyCode>840</CurrencyCode>
            <CurrencyExponent>2</CurrencyExponent>
            <CardSecValInd>1</CardSecValInd>
            <CardSecVal>222</CardSecVal>
            <AVSzip>33333</AVSzip>
            <AVSaddress1>4200 test lane</AVSaddress1>
            <AVSaddress2>test lane</AVSaddress2>
            <AVScity>north pole</AVScity>
            <AVSstate>FL</AVSstate>
            <AVSphoneNum>813-555-1234</AVSphoneNum>
            <AVSname>Test Name</AVSname>
            <AVScountryCode>CA</AVScountryCode>
            <AVSDestzip>33333</AVSDestzip>
            <AVSDestaddress1>4200 test lane</AVSDestaddress1>
            <AVSDestaddress2>test lane</AVSDestaddress2>
            <AVSDestcity>north pole</AVSDestcity>
            <AVSDeststate>AZ</AVSDeststate>
            <AVSDestphoneNum>840-555-1111</AVSDestphoneNum>
            <AVSDestname>Test Name</AVSDestname>
            <AVSDestcountryCode>GB</AVSDestcountryCode>
            <OrderID>FA Request</OrderID>
            <Amount>2000</Amount>
            <Comments>FA Request</Comments>
            <CustomerAni>815555555</CustomerAni>
            <AVSPhoneType>D</AVSPhoneType>
            <AVSDestPhoneType>D</AVSDestPhoneType>
            <CustomerEmail>test_user@test_merchant.com</CustomerEmail>
            <CustomerIpAddress>12.12.12.12</CustomerIpAddress>
            <EmailAddressSubtype>G</EmailAddressSubtype>
            <CustomerBrowserName>Mozilla/4.0</CustomerBrowserName>
            <ShippingMethod>C</ShippingMethod>
        </BaseElements>
        <FraudAnalysis>
            <FraudScoreIndicator>2</FraudScoreIndicator>
            <RulesTrigger>N</RulesTrigger>
            <SafetechMerchantID>300002</SafetechMerchantID>
            <KaptchaSessionID>123abc</KaptchaSessionID>
            <WebsiteShortName></WebsiteShortName>
```

```
            <CashValueOfFencibleItems>100</CashValueOfFencibleItems>
            <CustomerDOB>1981-03-24</CustomerDOB>
            <CustomerGender>F</CustomerGender>
            <CustomerDriverLicense>DL987654321</CustomerDriverLicense>
            <CustomerID>99</CustomerID>
            <CustomerIDCreationTime>305641650</CustomerIDCreationTime>
            <KTTVersionNumber>1</KTTVersionNumber>
            <KTTDataLength>0019</KTTDataLength>
            <KTTDataString><![CDATA[UPROMOCODE=X6Y3Z1&|]]></KTTDataString>
        </FraudAnalysis>
    </SafetechFraudAnalysis>
</Request>
```

5.1.4.1   Special notes on KTT elements

Requests made to the Safetech service may extend beyond the standard short or long form request formats. The Safetech service allows for a variable-length data string which can be customized on a transaction by transaction basis. This data is populated in an element called the `KTTDataString`.

The Data String may contain any combination of two types of data:

- User defined Safetech fields
- Shopping cart data

User Defined (UDF) values are custom data elements, defined by the merchant through the Safetech Agent Web Console.

UDF elements are individually passed within the Data String to the Safetech service using a special string of characters. The convention used is to concatenate the following pieces of data:

"U" + Field Name + "=" + Field value + "&|"

For example, let's say a customer used a special promotional coupon, found through a social media promotion. Here is an example of possible UDF fields included for that transaction:

`UPROMOCODE=X6Y3Z1&|UCUSTOMERREFERAL=SocialMedia&|UDISCOUNTGIVEN=10.00&|`

Shopping cart data is intended to provide an itemized receipt of the purchase to the Safetech service. Each line item detail is pipe delimited.

Each line item contains five ampersand-delimited sub elements. The sub elements are defined below:

    T = Type
    I = Item
    D = Description
    Q = Quantity
    P = Price (w/ implied decimal)

For example, let's say a customer wants to buy two tickets and a parking pass to take a date to a baseball game. Here is an example of possible Shopping Cart Data for that transaction:

`T=Tickets&I=FridayNightBaseballGame&D=SeatsBehindHomePlate&Q=2&P=20000&|T=StadiumParking&I=FridayNightBaseBallGame&D=VIPParkingPass&Q=1&P=2000&|`

CAUTION Ampersands, equal signs, and pipe characters may be included as part of a sub element, but **must** be URI Encoded. Never URI encode an actual delimiter.

The total length of all data in the `KTTDataString` element must be submitted in the `KTTDataLength` element. The current maximum length of `KTTDataString` is 999 characters. Please note: the element must be submitted as a four digit number with leading zero(es).

NOTE   While Safetech KTT Data requires the use of ampersands, this character is not conductive to well-formed XML messages. For requests using this field, the concept of CDATA may be necessary.

CDATA is defined as element data wrapped in the following: `<![CDATA[ ]]>`. Escaping these characters will add the "<![CDATA" and "]]>" characters themselves to the data string, which should result in a host decline.

Invalid messages will result in either a DTD error or authentication failure.

5.1.5 Gift Card (FlexCache) Request

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Request>
<FlexCache>
    <OrbitalConnectionUsername></OrbitalConnectionUsername>
    <OrbitalConnectionPassword></OrbitalConnectionPassword>
    <BIN>000002</BIN>
    <MerchantID>700000123456</MerchantID>
    <TerminalID>001</TerminalID>
    <AccountNum>6035718888880000000</AccountNum>
    <OrderID>Gift Card Example</OrderID>
    <Amount>1000</Amount>
    <Comments>Testing GiftCard</Comments>
    <ShippingRef></ShippingRef>
    <IndustryType>EC</IndustryType>
    <FlexAutoAuthInd>N</FlexAutoAuthInd>
    <FlexPartialRedemptionInd>N</FlexPartialRedemptionInd>
    <FlexAction>REDEMPTION</FlexAction>
</FlexCache>
</Request>
```

5.2   Example Responses

5.2.1 New Order Response

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Response>
    <NewOrderResp>
        <IndustryType/>
        <MessageType>AC</MessageType>
        <MerchantID>123456</MerchantID>
        <TerminalID>001</TerminalID>
        <CardBrand>MC</CardBrand>
        <AccountNum>5454545454545454</AccountNum>
        <OrderID>8316384413</OrderID>
        <TxRefNum>48E0E5BC6EAB75C4863A09DFED9804E7EC2E54A1</TxRefNum>
        <TxRefIdx>1</TxRefIdx>
        <ProcStatus>0</ProcStatus>                          ← Successful
        <ApprovalStatus>1</ApprovalStatus>                  ← Approved
        <RespCode>00</RespCode>                             ← Approved
        <AVSRespCode>H </AVSRespCode>             ← Zip Match/Locale match
        <CVV2RespCode> </CVV2RespCode>           ← Not applicable (non-Visa)
        <AuthCode>191044</AuthCode>
        <RecurringAdviceCd/>
        <CAVVRespCode/>
        <StatusMsg>Approved</StatusMsg>
        <RespMsg/>
        <HostRespCode>00</HostRespCode>
        <HostAVSRespCode>Y</HostAVSRespCode>
        <HostCVV2RespCode/>
        <CustomerRefNum/>
        <CustomerName/>
        <ProfileProcStatus/>
        <CustomerProfileMessage/>
        <RespTime>102708</RespTime>
    </NewOrderResp>
</Response>
```

5.2.2 PINless Debit Response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
    <NewOrderResp>
        <IndustryType/>
        <MessageType>R</MessageType>
        <MerchantID>123456</MerchantID>
        <TerminalID>001</TerminalID>
        <CardBrand>DP</CardBrand>
        <AccountNum>9409400000000000</AccountNum>
        <OrderID>Test Order 458467</OrderID>
        <TxRefNum>493D9212BC78349837BE8DB13EB12F6A545453E0</TxRefNum>
        <TxRefIdx>1</TxRefIdx>
        <ProcStatus>0</ProcStatus>                          ← Successful
        <ApprovalStatus>1</ApprovalStatus>                  ← Approved
        <RespCode>00</RespCode>                             ← Approved
        <AVSRespCode>3 </AVSRespCode>                  ← AVS not performed
        <CVV2RespCode> </CVV2RespCode>            ← Not applicable (non-Visa)
        <AuthCode>096836</AuthCode>
        <RecurringAdviceCd/>
        <CAVVRespCode/>
        <StatusMsg>Approved</StatusMsg>
        <RespMsg/>
        <HostRespCode>100</HostRespCode>
        <HostAVSRespCode> </HostAVSRespCode>
        <HostCVV2RespCode>  </HostCVV2RespCode>
        <CustomerRefNum/>
        <CustomerName/>
        <ProfileProcStatus/>
        <CustomerProfileMessage/>
        <RespTime>163058</RespTime>
    </NewOrderResp>
</Response>
```

5.2.3 Profile Add Response

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Response>
    <ProfileResp>
        <CustomerBin>000001</CustomerBin>
        <CustomerMerchantID>123456</CustomerMerchantID>
        <CustomerName>JON DOE</CustomerName>
        <CustomerRefNum>ADDPROFILE 123</CustomerRefNum>
        <CustomerProfileAction>CREATE</CustomerProfileAction>
        <ProfileProcStatus>0</ProfileProcStatus>              ← Profile Action Successful
        <CustomerProfileMessage>Profile Request Processed</CustomerProfileMessage>
        <CustomerAddress1>123 TEST DRIVE</CustomerAddress1>
        <CustomerAddress2>SUITE 123</CustomerAddress2>
        <CustomerCity>TEST CITY</CustomerCity>
        <CustomerState>FL</CustomerState>
        <CustomerZIP>33626</CustomerZIP>
        <CustomerEmail>jondoe@test.com</CustomerEmail>
        <CustomerPhone>2232231234</CustomerPhone>
        <CustomerCountryCode>US</CustomerCountryCode>
        <CustomerProfileOrderOverrideInd>NO</CustomerProfileOrderOverrideInd>
        <OrderDefaultDescription>Sample Order Description</OrderDefaultDescription>
        <OrderDefaultAmount>1500</OrderDefaultAmount>
        <CustomerAccountType>CC</CustomerAccountType>
        <Status>A</Status>                                    ← Active
        <CCAccountNum>5454545454545454</CCAccountNum>
        <CCExpireDate>0810</CCExpireDate>
        <ECPAccountDDA/>
        <ECPAccountType/>
        <ECPAccountRT/>
        <ECPBankPmtDlv/>
        <MBType>R</MBType>
        <MBOrderIdGenerationMethod>IO</MBOrderIdGenerationMethod>
        <MBRecurringStartDate>12092008</MBRecurringStartDate>
        <MBRecurringNoEndDateFlag>Y</MBRecurringNoEndDateFlag>
        <MBRecurringFrequency>00000205W</MBRecurringFrequency>
        <RespTime/>
    </ProfileResp>
</Response>
```

5.2.4 Safetech Fraud Analysis Response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<SafetechFraudAnalysisResp>
    <IndustryType></IndustryType>
    <MerchantID>651117</MerchantID>
    <TerminalID>001</TerminalID>
    <CardBrand>VI</CardBrand>
    <AccountNum>4012888888888886</AccountNum>
    <OrderID>FA Request</OrderID>
    <TxRefNum>4E8F1F941CA2AC859420FCB679532751E1125470</TxRefNum>
    <RespTime>114941</RespTime>
    <ProcStatus>0</ProcStatus>
    <ApprovalStatus>1</ApprovalStatus>
    <RespCode>27</RespCode>
    <StatusMsg>Approved</StatusMsg>
    <RespMsg></RespMsg>
    <HostRespCode>104</HostRespCode>
    <CustomerRefNum></CustomerRefNum>
    <CustomerName></CustomerName>
    <ProfileProcStatus></ProfileProcStatus>
    <CustomerProfileMessage></CustomerProfileMessage>
    <FraudAnalysisResponse>
        <FraudScoreIndicator>2</FraudScoreIndicator>
        <FraudStatusCode>A001</FraudStatusCode>
        <RiskInquiryTransactionID>61HG0W11DRS7                     </RiskInquiryTransactionID>
        <AutoDecisionResponse>R</AutoDecisionResponse>
        <RiskScore>29</RiskScore>
        <KaptchaMatchFlag>N</KaptchaMatchFlag>
        <WorstCountry>US</WorstCountry>
        <CustomerRegion>ny</CustomerRegion>
        <PaymentBrand>VISA</PaymentBrand>
        <FourteenDayVelocity>0 </FourteenDayVelocity>
        <SixHourVelocity>0 </SixHourVelocity>
        <CustomerNetwork>N</CustomerNetwork>
        <NumberOfDevices>1  </NumberOfDevices>
        <NumberOfCards>1  </NumberOfCards>
        <NumberOfEmails>1  </NumberOfEmails>
        <DeviceLayers>....</DeviceLayers>
        <DeviceFingerprint></DeviceFingerprint>
        <CustomerTimeZone></CustomerTimeZone>
        <CustomerLocalDateTime></CustomerLocalDateTime>
        <DeviceRegion></DeviceRegion>
        <DeviceCountry></DeviceCountry>
        <ProxyStatus></ProxyStatus>
        <JavascriptStatus></JavascriptStatus>
        <FlashStatus></FlashStatus>
        <CookiesStatus></CookiesStatus>
        <BrowserCountry></BrowserCountry>
        <BrowserLanguage></BrowserLanguage>
```

```
    <MobileDeviceIndicator></MobileDeviceIndicator>
    <MobileDeviceType></MobileDeviceType>
    <MobileWirelessIndicator></MobileWirelessIndicator>
    <VoiceDevice></VoiceDevice>
    <PCRemoteIndicator></PCRemoteIndicator>
    <RulesDataLength></RulesDataLength>
    <RulesData></RulesData>
  </FraudAnalysisResponse>
</SafetechFraudAnalysisResp>
</Response>
```

5.2.4.1   Special Notes on Rules Trigger response data

Requests to the Safetech service include an element labeled `RulesTrigger`. This element in the request message will ask the Safetech service to return the discreet set of rules or validations applied by the Safetech service for this transaction.

Information on triggered rules is returned in the `RulesData` element of the response message. This element is a specially delimited text string that indicates how many rules were triggered and what those rules were.

NOTE   The setup and management of rules is done through the Safetech Agent Web Console.

The data string returned begins with the number of rules which were triggered by the transaction. This four digit number is always followed by a "=" delimiter, and then a comma delimited list of the rules triggered. There is no delimiter on the end of the string.

An example of this response data is listed below:
```
0003=1234,338,2974642135
```

If no rules are triggered, the data will return as listed below:
```
0000=
```

The length of the string is returned in a separate `RulesDataLength` element. The maximum length of this string is 999 characters. The string will end with a "+" delimiter if the data returned by the Safetech service exceeds this length.

5.2.5 Gift Card (FlexCache) Response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<FlexCacheResp>
<MerchantID>700000001482</MerchantID>
<TerminalID>001</TerminalID>
<OrderID>Gift Card Example</OrderID>
<AccountNum>6035718888880000000</AccountNum>
<FlexRequestedAmount>0</FlexRequestedAmount>
<FlexHostTrace></FlexHostTrace>
<FlexAction>Redemption</FlexAction>
<FlexAcctBalance></FlexAcctBalance>
<FlexAcctPriorBalance></FlexAcctPriorBalance>
<CardBrand>FC</CardBrand>
<TxRefNum>4F524E6B357C4F8A31F621456D57C50F992C5422</TxRefNum>
<TxRefIdx>1</TxRefIdx>
<ProcStatus>0</ProcStatus>
<StatusMsg>Approved</StatusMsg>
<ApprovalStatus>0</ApprovalStatus>
<AuthCode>123456</AuthCode>
<RespCode>00</RespCode>
<CVV2RespCode> </CVV2RespCode>
<RespTime>03032012120132</RespTime>
</FlexCacheResp>
</Response>
```

5.3 Response Handling – Best Practices

Response messages are returned in many complex types. Multiple levels of response codes may be included, based on the source of the response and the type of transaction submitted to the Orbital Gateway. This section includes a number of key points to consider when parsing a response, to ensure that all scenarios are planned for.

WARNING Responses should not be parsed in a fixed positional manner. This specification does not make any guarantees with respect to the spacing between elements.

5.3.1 Gateway Success

The Orbital Gateway runs various validations on every request message, to insure the request is valid in schema, format, and business logic. These validations happen prior to communication with the upstream host, and should therefore be verified first. The **ProcStatus** element is returned in all response types to communicate the result of all validations done by the gateway.

Proc Status errors are often found within the `<QuickResp>` complex type. A proc status of 0 (zero) indicates a success, while any other number indicates the gateway has detected a failure of some kind. The most common exception to this rule is a Profile Proc Status which is specific to customer profile actions and logged separately.

A list of Proc Status messages is available in Appendix A.4 *Process Status Codes and Messages*

Below are examples of common gateway generated errors.

Example 1 – ProcStatus error:
```xml
<?xml version="1.0" encoding="UTF-8" ?>
  <Response>
      <QuickResp>                            ← Indicates an initial Gateway generated error
          <ProcStatus>9717</ProcStatus>              ← The specific Gateway Error Code
          <StatusMsg>Security Information - agent/chain/merchant is missing
          </StatusMsg>                    ← Response Text: A security error was detected
      </QuickResp>
  </Response>
```

Example 2 – ProcStatus error:
```xml
<?xml version="1.0" encoding="UTF-8" ?>
  <Response>
      <QuickResp>                            ← Indicates an initial Gateway generated error
        <TxRefNum>4C05310F121D8809E59DD07BB2D3938B642753B2</TxRefNum>
        <TxRefIdx>0</TxRefIdx>
        <ProcStatus>882</ProcStatus>                ← The specific Gateway Error Code
        <StatusMsg>This transaction is locked down. You cannot mark or unmark
it.</StatusMsg>       ← Response Text: This transaction reference has expired or has already
                                                    been marked for capture

        <ApprovalStatus>2</ApprovalStatus>
      </QuickResp>
  </Response>
```

NOTE   A separate **ProfileProcStatus** element is used when a request initiates action on a customer profile. These are not returned in the QuickResp complex type.

CAUTION New Order responses can contain both a Proc Status and a Profile Proc Status element (for example, when creating a customer profile as part of a sale). The Proc Status is the result of validating the transaction, and Profile Proc Status is the result of the profile action.

Below are two examples of common profile based errors.

Example 3 – ProfileProcStatus error:

```
<?xml version="1.0" encoding="UTF-8"?>
  <Response>
    <ProfileResp>
        <CustomerBin></CustomerBin>
        <CustomerMerchantID></CustomerMerchantID>
        <CustomerName></CustomerName>
        <CustomerRefNum></CustomerRefNum>
        <CustomerProfileAction></CustomerProfileAction>
        <ProfileProcStatus>9579</ProfileProcStatus>        ← Indicates a Gateway generated error
        <CustomerProfileMessage>Profile: Merchant-Bin [123456]:[000001] is not
active.</CustomerProfileMessage>          ← Response text: This MID is not enabled for profiles
        <CustomerAddress1></CustomerAddress1>
        <CustomerAddress2></CustomerAddress2>
        <CustomerCity></CustomerCity>
        <CustomerState></CustomerState>
        <CustomerZIP></CustomerZIP>
        <CustomerEmail></CustomerEmail>
        <CustomerPhone></CustomerPhone>
        <CustomerProfileOrderOverrideInd></CustomerProfileOrderOverrideInd>
        <OrderDefaultDescription></OrderDefaultDescription>
        <OrderDefaultAmount></OrderDefaultAmount>
        <CustomerAccountType></CustomerAccountType>
        <CCAccountNum></CCAccountNum>
        <CCExpireDate></CCExpireDate>
        <ECPAccountDDA></ECPAccountDDA>
        <ECPAccountType></ECPAccountType>
        <ECPAccountRT></ECPAccountRT>
        <ECPBankPmtDlv></ECPBankPmtDlv>
        <RespTime></RespTime>
    </ProfileResp>
  </Response>
```

Example 4 – Profile Error on Successful Transaction:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<NewOrderResp>
<IndustryType></IndustryType>
<MessageType>A</MessageType>
<MerchantID>123456</MerchantID>
<TerminalID>001</TerminalID>
<CardBrand>DI</CardBrand>
<AccountNum>6500000000000002</AccountNum>
<OrderID>831638456</OrderID>
<TxRefNum>4C3213241331117CD265DE7ADA3967A15218542B</TxRefNum>
<TxRefIdx>0</TxRefIdx>                    ← Indicates the request did not ask to capture
<ProcStatus>0</ProcStatus>               ← Indicates Gateway success for the transaction
<ApprovalStatus>0</ApprovalStatus>       ← Does not indicate the transaction was approved
<RespCode>M1</RespCode>                   ← Decline Reason: Merchant Selectable Response
<AVSRespCode>3 </AVSRespCode>
<CVV2RespCode>S</CVV2RespCode>
<AuthCode>tst099</AuthCode>
<RecurringAdviceCd></RecurringAdviceCd>
<CAVVRespCode></CAVVRespCode>
<StatusMsg>Merchant Override Decline</StatusMsg>
<RespMsg></RespMsg>
<HostRespCode>100</HostRespCode>
<HostAVSRespCode></HostAVSRespCode>
<HostCVV2RespCode>S</HostCVV2RespCode>
<CustomerRefNum></CustomerRefNum>
<CustomerName></CustomerName>
<ProfileProcStatus>9582</ProfileProcStatus>       ← Indicates the profile action
                                                      returned an error
<CustomerProfileMessage>Profile: Cannot Create profile. Profile already exists for Cust Ref
Num [TestProfile] and MID:[123456]</CustomerProfileMessage>
<RespTime>164618</RespTime>
<PartialAuthOccurred></PartialAuthOccurred>  ← Indicates the issuer returned a partial approval
<RequestedAmount></RequestedAmount>
<RedeemedAmount></RedeemedAmount>            ← The amount which was actually charged
<RemainingBalance></RemainingBalance>       ← The balance of the order which is still due
<CountryFraudFilterStatus></CountryFraudFilterStatus>
<IsoCountryCode></IsoCountryCode>
</NewOrderResp>
</Response>
```

5.3.2 Host / Issuer Success

Request Complex types can be separated into two categories - messages which return information from the upstream host, and messages which do not.

List of Example Complex Types which return only Gateway response data (not all inclusive):
Profile, AccountUpdater, EndOfDay, Inquiry, MarkForCapture (exceptions listed below)***, Void*** *(w/o Online Reversal)*

List of Example Complex Types which may return host and issuer data (not all inclusive):
NewOrder, FlexCache, MarkForCapture *(on aged orders and split shipments),* ***Void*** *(w/ Online Reversal)*

Multiple data sets are returned when the upstream host responds to a transaction request. Orbital Gateway returns the **ApprovalStatus** element to communicate an overall status, as well as multiple individual response elements such as AVS and CVV response data.

Gateway provides normalized response elements for consistency between the Salem and Tampa upstream hosts. Raw host response elements are also provided for developers who are familiar with the response values of the upstream host.

Example 5 – New Order with AVS and Partial Authorization:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
 <Response>
      <NewOrderResp>
        <IndustryType />
        <MessageType>A</MessageType>
        <MerchantID>700000123456</MerchantID>
        <TerminalID>001</TerminalID>
        <CardBrand>VI</CardBrand>
        <AccountNum>4XXXXXXXXXXX1111</AccountNum>
        <OrderID>844901</OrderID>
        <TxRefNum>4C04887CE799F0BA541FDC447426A7B0F48E27A5</TxRefNum>
        <TxRefIdx>0</TxRefIdx>          ← Indicates the request did not ask to capture
        <ProcStatus>0</ProcStatus>      ← Indicates the request did not ask to capture
        <ApprovalStatus>1</ApprovalStatus>     ← Indicates an overall Issuer Approval
        <RespCode>00</RespCode>             ← The Auth Response Code stored by Gateway
        <AVSRespCode>H</AVSRespCode>         ← The AVS Response Code stored by Gateway
        <CVV2RespCode />              ← Indicates CVV validation was not performed
        <AuthCode>091141</AuthCode>
        <RecurringAdviceCd />
        <CAVVRespCode />
        <StatusMsg>Approved</StatusMsg>
        <RespMsg />
        <HostRespCode>00</HostRespCode>       ← The Auth Response Code stored by Host
        <HostAVSRespCode>Y</HostAVSRespCode>   ← The AVS Response Code stored by Host
        <HostCVV2RespCode />
        <CustomerRefNum />
        <CustomerName />
        <ProfileProcStatus />          ← Indicates a profile action was not requested
        <CustomerProfileMessage />
        <RespTime>001140</RespTime>
        <PartialAuthOccurred>Y</PartialAuthOccurred>   ← Indicates the issuer returned
                                                          a partial approval
        <RequestedAmount>10000</RequestedAmount>
        <RedeemedAmount>7000</RedeemedAmount>        ← The amount which was approved
        <RemainingBalance></RemainingBalance>
        <CountryFraudFilterStatus></CountryFraudFilterStatus>
        <IsoCountryCode></IsoCountryCode>
```

```
        </NewOrderResp>
    </Response>
```

Example 6 – New Order with AVS and CVV:

```
<?xml version="1.0" encoding="UTF-8" ?>
 <Response>
    <NewOrderResp>
      <IndustryType />
        <MessageType>AC</MessageType>
        <MerchantID>123456</MerchantID>
        <TerminalID>001</TerminalID>
        <CardBrand>VI</CardBrand>
        <AccountNum>4XXXXXXX8881</AccountNum>
        <OrderID>00000002</OrderID>
        <TxRefNum>4C04885DDC2478DBE8A8C2731844EF1F90515309</TxRefNum>
        <TxRefIdx>1</TxRefIdx>          ← Indicates this response is for the first Capture
        <ProcStatus>0</ProcStatus>          ← Indicates Gateway Success for the transaction
        <ApprovalStatus>0</ApprovalStatus>          ← Indicates a decline by the Issuer
        <RespCode>05</RespCode>          ← Indicates the decline code stored by Gateway
        <AVSRespCode>F</AVSRespCode>          ← Indicates the AVS code stored by Gateway
        <CVV2RespCode>M</CVV2RespCode>          ← Indicates the CVV code stored by Gateway
        <AuthCode></AuthCode>          ← A NULL AuthCode also indicates a decline or error
        <RecurringAdviceCd />
        <CAVVRespCode />
        <StatusMsg>Approved</StatusMsg>
        <RespMsg />
        <HostRespCode>530</HostRespCode>          ← Indicates the decline code stored by Host
        <HostAVSRespCode>A</HostAVSRespCode>          ← This is the host AVS code
        <HostCVV2RespCode>M</HostCVV2RespCode>          ← This is the host CVV code
        <CustomerRefNum>TestProfile4</CustomerRefNum>
        <CustomerName />
        <ProfileProcStatus>0</ProfileProcStatus>          ← Indicates a profile action succeeded
                                                            separately of the transaction itself
        <CustomerProfileMessage>Profile was created successfully</CustomerProfileMessage>
        <RespTime>001109</RespTime>
        <RequestedAmount></RequestedAmount>
        <RedeemedAmount></RedeemedAmount>
        <RemainingBalance></RemainingBalance>
        <CountryFraudFilterStatus></CountryFraudFilterStatus>
        <IsoCountryCode></IsoCountryCode>

    </NewOrderResp>
 </Response>
```

5.3.3 Safetech Fraud Analysis Data Handling

Safetech fraud scoring can be requested in one of two ways: As part of a transaction; using the *NewOrder* or *FlexCache* complex types and in parallel to the host approval/decline, or as a standalone request; using the *SafetechFraudAnalysis* complex type.

Prior to sending the request information to the Safetech service, the Gateway ensures all the minimally required is present and properly formatted. Orbital Gateway returns the **FraudAnalysisProcStatus** element to indicate if the data passed the necessary validations. A value of zero indicates success. Any other value indicates an error.

If the Fraud Analysis is successful, the Safetech service will return several additional elements to the Orbital Gateway. These elements are contained in a parent element called **FraudAnalysisResponse**, common to each complex type that supports the Safetech service.

The Safetech service may return either a short or long form response message, depending on the **FraudScoreIndicator** provided in the request message.

Fraud Score 1

This is the short form response from the Safetech service. At minimum, a Fraud Status code is returned. Additionally, the following elements may be returned:

- Risk Inquiry Transaction ID
- Fraud Score Auto Decision Response
- Risk Score
- Kaptcha Match Flag
- Rules Triggered

Fraud Score 2

This is the long form response from the Safetech service. All of the short form elements may be returned in the response message. In addition to the response information listed above, the response may include over 25 additional data elements.

For more information on these elements, please refer to ***Error! Reference source not found. Error! Reference source not found.***, or your documentation for the Safetech Agent Web Console.

Appendix A   Codes Reference

This appendix contains tables describing the codes that you might receive in a response message.

A.1   Action Key

Many of the tables in this appendix have an Action column. Table 12 describes what action the values displayed in the Action column indicate that you should take.

Table 12   **Action column key**

Action	Description
Call	Call your Chase Paymentech Customer Service representative for assistance.
Cust.	Try to resolve with customer or obtain alternate payment method.
Fix	There is an invalid value being sent. Fix and resend.
None	No action required.
Resend	Send this transaction back at any time.
Voice	Perform a voice authorization per instructions provided by Chase Paymentech.
Wait	Wait 2–3 days before resending or try to resolve with the customer.

A.2   Response Codes

Table 13 describes the different values for the `<RespCode>` element in a response message.

Table 13   **Response code values**

respCode	Definition	Status	Action[*]	Host Code Salem	Host Code Tampa
00	Approved	Approved	None	100, 102	00, 100, 102
01	Call/Refer to Card Issuer	Decline	Voice	401	01
02	Refer to Card Issuer's Special Conditions	Decline	Voice	N/A	02
03	Invalid Merchant Number	Error	Fix	231	03
04	Pickup	Decline	Cust.	501	04
05	Do Not Honor	Decline	Cust.	530	05
06	Other Error	Decline	Cust.	594	06
07	Stop Deposit Order	Decline	Cust.	570	N/A
08	Approved Authorization, Honor with Identification	Approved	None	N/A	08
09	Revocation of Authorization	Decline	Cust.	571	N/A
10	Default Call	Decline	Voice	402	N/A
11	Approved Authorization, VIP Approval	Approved	None	N/A	11

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
12	Invalid Transaction Type	Decline	Cust.	606	12
13	Bad Amount	Decline	Fix	592	13
14	Invalid Credit Card Number	Decline	Fix	591	14
15	Default Call Low Fraud	Decline	Voice	442	N/A
16	Default Call Medium Fraud	Decline	Voice	443	N/A
17	Default Call High Fraud	Decline	Voice	444	N/A
18	Default Call Unavailable Fraud	Decline	Voice	445	N/A
19	Re-enter Transaction	Error	Resend	N/A	19
20	Floor Low Fraud	Decline	Cust.	332	N/A
21	Floor Medium Fraud	Decline	Cust.	333	N/A
22	Floor High fraud	Decline	Cust.	334	N/A
23	Floor Unavailable Fraud	Decline	Cust.	335	N/A
24	Validated	Approved	None	101	101
26	Pre-noted	Approved	None	103	103
27	No Reason to Decline	Approved	None	104	N/A
28	Received and Stored	Approved	None	105	N/A
29	Provided Authorization	Approved	None	106	N/A
30	Invalid Value in Message	Error	Fix	225	30
31	Request Received	Approved	None	107	N/A
32	BIN Alert	Approved	None	110	N/A
33	Card is Expired	Decline	Cust.	522	33
34	Approved for Partial	Approved	None	111	N/A
35	Zero Amount	Error	Fix	203	N/A
36	Bad Total Authorization Amount	Error	Fix	205	N/A
37	Invalid Secure Payment Data	Error	Fix	245	N/A
38	Merchant not MC SecureCode Enabled	Decline	Call	246	N/A
39	Previously Processed Transaction	Error	Fix	109	N/A
40	Requested Function not Supported	Error	Call or Fix	N/A	40
41	Lost/Stolen	Decline	Cust.	502	N/A
42	Account Not Active	Decline	Cust.	N/A	15

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
43	Lost/Stolen Card	Decline	Cust.	N/A	43
44	Account Not Active	Decline	Cust.	N/A	N/A
45	Duplicate Transaction	Decline	Cust.	551	N/A
46	Blanks not Passed in Reserved Field	Decline	Fix	248	N/A
50	Positive ID	Decline	Cust.	802	N/A
52	Processor Decline	Decline	Cust.	303	N/A
56	Restraint	Decline	Cust.	806	N/A
58	Transaction not Permitted to Terminal	Error	Call	N/A	58
59	Soft AVS	Decline	Cust.	260	N/A
60	Do Not Honor Low Fraud	Decline	Cust.	532	N/A
61	Do Not Honor Medium Fraud	Decline	Cust.	533	N/A
62	Do Not Honor High fraud	Decline	Cust.	534	N/A
63	Do Not Honor Unavailable Fraud	Decline	Cust.	535	N/A
64	CVV2/CVC2 Failure	Decline	Cust.	531	N/A
65	Invalid Amex CID	Decline	Cust.	811	N/A
66	Other Error	Error	Fix	204	N/A
68	Invalid CC Number	Error	Fix	201	N/A
69	Does not Match MOP	Error	Fix	233	N/A
71	No Account	Decline	Fix	825	N/A
72	Invalid Institution Code	Decline	Fix	602	N/A
73	Method of Payment is Invalid for Merchant	Error	Fix	834	834
74	Invalid Expiration Date	Decline	Cust.	605	54
75	Bad Amount	Error	Fix	202	N/A
77	Invalid Amount	Decline	Fix	607	N/A
78	Missing Companion Data	Error	Fix	227	N/A
79	Invalid Merchant	Error	Fix	833	N/A
80	Invalid MOP for Division	Error	Fix	239	N/A
81	Call Low Fraud	Decline	Voice	432	N/A
82	Call Medium Fraud	Decline	Voice	433	N/A
83	Call High Fraud	Decline	Voice	434	N/A

Table 13   Response code values

respCode	Definition	Status	Action[*]	Host Code Salem	Host Code Tampa
84	Call Unavailable Fraud	Decline	Voice	435	N/A
85	Duplicated Order #	Error	Fix	234	N/A
86	Auth Recycle Host down	Error	Wait	236	N/A
87	Invalid Currency	Error	Fix	238	N/A
88	Invalid Purch. Level 3	Error	Fix	243	N/A
89	Credit Floor	Decline	Cust.	302	N/A
91	Approved Low Fraud	Approved	None	112	N/A
92	Approved Medium Fraud	Approved	None	113	N/A
93	Approved High Fraud	Approved	None	114	N/A
94	Approved Fraud Service Unavailable	Approved	None	115	N/A
95	Invalid Data Type	Error	Fix	226	N/A
96	Invalid Record Sequence	Error	Fix	228	N/A
97	Percents Not Total 100	Error	Fix	229	N/A
98	Issuer Unavailable	Decline	Resend	301	N/A
99	No Answer/Unable to send	Error	Resend	000	99
A1	Payments Not Total Order	Error	Fix	230	N/A
A2	Bad Order Number	Error	Fix	232	N/A
A3	FPO Locked	Error	Wait	235	N/A
A4	FPO Not Allowed	Error	Call	237	N/A
A5	Auth Amount Wrong	Error	Fix	240	N/A
A6	Illegal Action	Error	Fix	241	N/A
A8	Invalid Start Date	Error	Fix	251	N/A
A9	Invalid Issue Number	Error	Fix	252	N/A
B1	Invalid Transaction Type	Error	Fix	253	N/A
B2	Account Previously Activated	Decline	Cust	580	16
B3	Unable to Void Transaction	Error	Fix	581	18
B5	Not on File	Decline	Fix	304	N/A
B7	Fraud	Decline	Cust.	503	N/A
B8	Bad Debt	Decline	Cust.	504	N/A
B9	On Negative File	Decline	Cust.	505	N/A

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
BA	Under 18 Years Old	Decline	Cust.	540	N/A
BB	Possible Compromise	Decline	Cust.	541	N/A
BC	Bill To Not Equal To Ship To	Decline	Cust.	542	N/A
BD	Invalid Pre-approval Number	Decline	Cust.	543	N/A
BE	Invalid Email Address	Decline	Cust.	544	N/A
BF	PA ITA Number Inactive	Decline	Cust.	545	N/A
BG	Blocked Account	Decline	Cust.	546	N/A
BH	Address Verification Failed	Decline	Cust.	547	N/A
BI	Not on Credit Bureau	Decline	Cust.	548	N/A
BJ	Previously Declined	Decline	Cust.	549	N/A
BK	Closed Account, New Account Closed	Decline	Cust.	550	N/A
BL	Re-Authorization	Decline	Cust.	560	N/A
BM	Re-Authorization – No Match	Decline	Cust.	561	N/A
BN	Re-Authorization – Timeframes Exceeded	Decline	Cust.	563	N/A
BO	Stand In Rules	Decline	Cust.	905	N/A
BP	Customer Service Phone Number required on Transaction Types 1 (MO/TO) and 2 (Recurring). MC Only	Error	Fix	257	N/A
BQ	Issuer has Flagged Account as Suspected Fraud. (Discover Only)	Decline	Cust.	596	N/A
BR	Invalid MCC Sent	Error	Fix	249	N/A
BS	New Card Issued	Decline	Cust.	595	N/A
BT	Not Authorized to send record	Decline	Fix	258	N/A
C1	Invalid Issuer	Decline	Cust.	506	N/A
C2	Invalid Response Code	Decline	Fix	507	N/A
C3	Excessive PIN Try	Decline	Cust.	508	N/A
C4	Over Limit	Decline	Cust.	509	N/A
C5	Over Freq Limit	Decline	Cust.	510	N/A
C6	Over Sav Limit	Decline	Cust.	511	N/A
C7	Over Sav Freq	Decline	Cust.	512	N/A
C9	Over Credit Freq	Decline	Cust.	514	N/A

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
D1	Invalid For Credit	Decline	Fix	515	N/A
D2	Invalid For Debit	Decline	Fix	516	N/A
D3	Rev Exceed Withdrawal	Decline	Cust.	517	N/A
D4	One Purchasing Limit	Decline	Cust.	518	N/A
D5	On Negative File	Decline	Cust.	519	519
D6	Changed Field	Decline	Fix	520	N/A
D7	Insufficient Funds	Decline	Cust.	521	N/A
D8	Encrypted Data Bad	Decline	Fix	523	96
D9	Altered Data	Decline	Fix	524	N/A
E3	Invalid Prefix	Decline	Fix	601	N/A
E4	Invalid Institution	Decline	Fix	603	N/A
E5	Invalid Cardholder	Decline	Fix	604	N/A
E6	BIN Block	Decline	Fix	610	N/A
E7	Stored	Approved	None	704	N/A
E8	Invalid Transit Routing Number	Error	Fix	750	750
E9	Unknown Transit Routing Number	Error	Fix	751	751
F1	Missing Name	Error	Fix	752	N/A
F2	Invalid Account Type	Error	Fix	753	N/A
F3	Account Closed	Error	Cust.	754	754
F4	No Account/Unable To Locate	Error	Fix	755	755
F5	Account Holder Deceased	Error	Cust.	756	756
F6	Beneficiary Deceased	Error	Cust.	757	757
F7	Account Frozen	Error	Cust.	758	758
F8	Customer Opt Out	Error	Cust.	759	759
F9	ACH Non-Participant	Error	Cust.	760	760
G1	No Pre-note	Error	Fix	761	N/A
G2	No Address	Error	Fix	762	N/A
G3	Invalid Account Number	Error	Fix	763	763
G4	Authorization Revoked by Consumer	Error	Cust.	764	764
G5	Customer Advises Not Authorized	Error	Cust.	765	765

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
G6	Invalid CECP Action Code	Error	Fix	766	N/A
G7	Invalid Account Format	Error	Fix	767	767
G8	Bad Account Number Data	Error	Fix	768	N/A
G9	No Capture	Decline	N/A	801	N/A
GA	Account Non-Convertible	Decline	N/A	769	769
H1	No Credit Function	Decline	N/A	803	N/A
H2	No Debit Function	Decline	N/A	804	N/A
H3	Rev Exceed Withdrawal	Decline	Cust.	805	N/A
H4	Changed Field	Decline	N/A	807	N/A
H5	Terminal Not Owned	Decline	N/A	808	N/A
H6	Invalid Time	Decline	Fix	809	N/A
H7	Invalid Date	Decline	Fix	810	N/A
H8	Invalid Terminal Number	Decline	Fix	812	N/A
H9	Invalid PIN	Decline	Cust.	813	38
I1	Block Activation Failed – Card Range Not Set Up for MOD 10	Error	Fix	582	N/A
I2	Block Activation Failed – E-mail or Fulfillment Flags were set to Y	Error	Fix	583	N/A
I3	Declined – Issuance Does Not Meet Minimum Amount	Declined	Cust	584	N/A
I4	Declined – No Original Auth Found	Decline	Cust	585	N/A
I5	Declined – Outstanding Auth, Funds On Hold	Decline	Cust	586	N/A
I6	Activation Amount Incorrect	Decline	Fix	587	N/A
I7	Block Activation Failed – Account Not Correct Or Block Size Not Correct	Decline	Fix	588	N/A
I8	Mag Stripe CVD Value Failed	Decline	Fix	589	N/A
I9	Max Redemption Limit Met	Decline	Fix	590	N/A
J1	No Manual Key	Decline	Fix	814	N/A
J2	Not Signed In	Decline	Fix	815	N/A
J3	Excessive PIN Try	Decline	Cust.	816	N/A
J4	No DDA	Decline	Fix	817	N/A
J5	No SAV	Decline	Fix	818	N/A

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
J6	Excess DDA	Decline	Cust.	819	N/A
J7	Excess DDA FREQ	Decline	Cust.	820	N/A
J8	Excess SAV	Decline	Cust.	821	N/A
J9	Excess SAV FREQ	Decline	Cust.	822	N/A
K1	Excess Card	Decline	Cust.	823	N/A
K2	Excess Card Freq	Decline	Cust.	824	N/A
K3	Reserved Future	Decline	N/A	826	N/A
K4	Reserved Closing	Decline	N/A	827	N/A
K5	Dormant	Decline	Cust.	828	N/A
K6	NSF	Decline	Cust.	829	N/A
K7	Future RD Six	Decline	N/A	830	N/A
K8	Future RD Seven	Decline	N/A	831	N/A
K9	Transaction Code Conflict	Decline	Fix	832	N/A
L1	In Progress	Decline	Wait	901	N/A
L2	Process Unavailable	Error	Resend	902	N/A
L3	Invalid Expiration	Error	Fix	903	N/A
L4	Invalid Effective	Error	Fix	904	N/A
L5	Invalid Issuer	Decline	Fix	N/A	15
L6	Transaction Not Allowed For Cardholder	Decline	Cust.	N/A	57
L7	Unable to Determine Network Routing	Error	Call	N/A	92
L8	System Error	Error	Call	N/A	97
L9	Database Error	Error	Call	N/A	98
M1	Merchant Override Decline	Decline	Cust.	Merchant Selectable Response	Merchant Selectable Response
M2	Partial Authorization Not Allowed	Decline	Cust	Partial Authorization Support	Partial Authorization Support
ND	Account number appears on European Direct Debit negative file	Decline	Cust	719	N/A
PA	Partial Approval	Approved	N/A	N/A	10
PB	Revocation of all Authorization	Decline	Cust.	572	17
PC	Country On Fraud Filter List	Decline	Cust	271	N/A

Table 13   Response code values

respCode	Definition	Status	Action*	Host Code Salem	Host Code Tampa
PD	Partial Authorization Override Not Allowed	Decline	Cust.	263	N/A
PP	No Match for Debit Authorization based on Trace, Account, and Division Number	Error	Fix	N/A	N/A
PQ	Unable to Validate Debit Auth Record Based on Amount, Action Code, and MOP	Error	Fix	N/A	N/A
PR	Refund Not Allowed – Refund Requested on a Star only BIN or BIN not Found	Error	Fix	599	N/A
R1	Blocked Card Number Prefix	Decline	Cust.	269	N/A
R2	Blocked Card Number	Decline	Cust.	270	N/A
R3	Blocked Issuing Country	Decline	Cust.	271	N/A
R4	Ceiling Limit	Decline	Cust.	275	N/A
R5	Not Authorized to Send Record	Decline	Cust	258	N/A
R6	Authorization Not Found	Decline	Cust.	307	N/A
R7	Amount Mismatch	Decline	Cust.	306	N/A
R8	Already Reversed or Nothing to Reverse	Decline	Cust.	305	N/A
R9	Authorization Code or Response Date Invalid	Decline	Cust.	262	N/A

A.3   AVS Response Codes

Table 14 describes the different values for the `<AVSRespCode>` field in a response message.

Table 14   AVS response code values

Code	AVS Message
1	No address supplied
2	Bill-to address did not pass Auth Host edit checks
3	AVS not performed
4 or R	Issuer does not participate in AVS
5	Edit-error - AVS data is invalid
6	System unavailable or time-out
7	Address information unavailable
8	Transaction Ineligible for AVS
9	Zip Match/Zip4 Match/Locale match

Table 14   AVS response code values

Code	AVS Message
A	Zip Match/Zip 4 Match/Locale no match
B	Zip Match/Zip 4 no Match/Locale match
C	Zip Match/Zip 4 no Match/Locale no match
D	Zip No Match/Zip 4 Match/Locale match
E	Zip No Match/Zip 4 Match/Locale no match
F	Zip No Match/Zip 4 No Match/Locale match
G	No match at all
H	Zip Match/Locale match
J	Issuer does not participate in Global AVS
JA	International street address and postal match
JB	International street address match. Postal code not verified.
JC	International street address and postal code not verified.
JD	International postal code match. Street address not verified.
M1	Cardholder name matches
M2	Cardholder name, billing address, and postal code matches
M3	Cardholder name and billing code matches
M4	Cardholder name and billing address match
M5	Cardholder name incorrect, billing address and postal code match
M6	Cardholder name incorrect, billing postal code matches
M7	Cardholder name incorrect, billing address matches
M8	Cardholder name, billing address and postal code are all incorrect
N3	Address matches, ZIP not verified
N4	Address and ZIP code not verified due to incompatible formats
N5	Address and ZIP code match (International only)
N6	Address not verified (International only)
N7	ZIP matches, address not verified
N8	Address and ZIP code match (International only)
N9	Address and ZIP code match (UK only)
R	Issuer does not participate in AVS
UK	Unknown
X	Zip Match/Zip 4 Match/Address Match

Table 14   AVS response code values

Code	AVS Message
Z	Zip Match/Locale no match
blank	Not applicable (non-Visa)

A.4   Process Status Codes and Messages

Table 15 describes the possible values for the `<ProcStatus>` element (Code column) and the associated `<ProcStatusMsg>` element (Description column) that indicate the success or failure of a request. The Action column indicates what action you should take in response to the message.

Table 15   Process Status and Process Status Message values

Code	Description	Action*
1	PWS_UNKNOWN_ERROR	Resend
2	PWS_NETWORK_ERROR	Resend
3	PWS_DB_ERROR Unknown Database Issues	Resend
5	DTD Error Either an element or the data inside an element does not match the Schema.	Fix
40	Cannot Get to Authorizer Service	Resend
54	Industry Type is Currently Not Supported for Merchant and BIN	Fix
205	PWS_DB_EXCEPTION_ERROR	Resend
208	PWS_ERROR_FAILED_TO_CONNECT	Resend
301	PWS_NW_OPEN_ERROR	Resend
303	PWS_NW_READ_ERROR	Resend
328	PWS_ERROR_BAD_REVERSAL_AMOUNT An invalid amount submitted on a Partial Void Request	Fix
329	PWS_ERROR_BAD_REQUEST_AMOUNT	Fix
330	PWS_ERROR_ALREADY_CAPTURED	Fix
331	PWS_ERROR_INVALID_ACTION	Fix
333	PWS_ERROR_MISSING_TRANSACTION_REFERENCE_INDEX	Fix
335	PWS_ERROR_SPLIT_AUTH_NOT_ALLOWED_ALREADY_MARKED	Fix
348	PWS_DID_NOT_ALLOW_A_CAPTURE_REQUEST_BECAUSE_THE_ORIGINAL_AUTH_WAS_NOT_SUCCESSFUL Cannot Void a Transaction in which the Mark for Capture Failed	Fix
350	The amount requested cannot be zero	Fix
351	This industry type does not allow a capture greater than the value of the auth	Fix

Code	Description	Action*
354	Re-Auth failed. This error is returned when a re-auth is attempted behind-the-scenes by the Gateway (usually in the case of a split transaction) and fails at the host.	Call
355	There is nothing to capture This error is returned when a Capture attempt is made on prior authorization, but there is no amount left to capture.	Fix
400	PWS_MANDATORY_FIELDS_ERROR	Fix
410	FE_NETWORK_ERROR (cannot connect to eHost)	Resend
411	FE_INTERRUPTED_SESSION (i/o problem while connecting to eHost)	Resend
516	The Merchant ID/Acquiring BIN ID is invalid or missing. Message rejected	Fix
518	This merchant is not active until … [This error is returned when a Merchant Account has been setup, but with an Activation date in the future of the present date].	Call Customer Service
519	This merchant is inactive	Call Customer Service
521	eHost has received a badly formatted message [This error is returned when required fields are missing]	Fix
523	An invalid TID was received [Terminal ID]	Fix
801	PWS_ERR_VALIDATION_AMOUNT	Fix
803	PWS_ERR_VALIDATION_AVSADDRESS	Fix
804	PWS_ERR_VALIDATION_AVSZIPCODE	Fix
806	PWS_ERR_VALIDATION_BIN	Fix
811	PWS_ERR_VALIDATION_CUSTOMERADDR	Fix
812	PWS_ERR_VALIDATION_CUSTOMEREMAIL	Fix
814	PWS_ERR_VALIDATION_CUSTOMERNAME	Fix
817	PWS_ERR_VALIDATION_CUSTOMERPHONE	Fix
818	PWS_ERR_VALIDATION_CVV2	Fix
822	PWS_ERR_VALIDATION_ISSUENUM	Fix
823	PWS_ERR_VALIDATION_LANGUAGE	Fix
825	PWS_ERR_VALIDATION_MERCHANTID	Fix
826	PWS_ERR_VALIDATION_ORDERDESCRIPTION	Fix
827	PWS_ERR_VALIDATION_ORDERID	Fix
831	PWS_ERR_VALIDATION_TAXAMT	Fix
832	PWS_ERR_VALIDATION_TAXINCLUDED	Fix
833	PWS_ERR_VALIDATION_TERMINALID	Fix
834	PWS_ERR_VALIDATION_TRANSDATE	Fix
835	PWS_ERR_VALIDATION_TRANSTIME	Fix

Code	Description	Action*
836	PWS_ERR_VALIDATION_ECOM	Fix
838	PWS_ERR_VALIDATION_ACNUMBER	Fix
839	PWS_ERR_VALIDATION_PAN_LUHN	Fix
840	PWS_ERR_VALIDATION_PAN_LENGTH	Fix
841	PWS_ERR_VALIDATION_PAN_RANGE	Fix
842	PWS_ERR_VALIDATION_EXP_DATE_FORMAT	Fix
844	PWS_ERR_VALIDATION_EXP_DATE_TOO_NEW	Fix
845	PWS_ERR_VALIDATION_START_DATE_FORMAT	Fix
846	PWS_ERR_VALIDATION_START_DATE_TOO_NEW	Fix
847	PWS_ERR_VALIDATION_PAN_FORMAT	Fix
848	PWS_ERR_VALIDATION_CURRENCY_FORMAT	Fix
849	PWS_ERR_VALIDATION_CURRENCY_UNSUPPORTED	Fix
850	PWS_ERR_VALIDATION_CURRENCY_BAD_EXPONENT	Fix
851	PWS_ERR_VALIDATION_MERCHANT_UNSUPPORTED	Fix
852	PWS_ERR_VALIDATION_BRAND_UNSUPPORTED	Fix
853	PWS_ERR_VALIDATION_BRAND_PAN_MISMATCH	Fix
881	The LIDM you supplied # does not match with any existing transaction (Cannot void or Mark a Transaction because the TxRefNum does match a transaction)	Fix
882	LOCKED_DOWN (Cannot mark or unmark transaction)	Fix
885	Error Validating Amount. Must be Numeric, Equal to Zero or Greater	Fix
886	Zero Dollar Auth: ZIP is Mandatory	Fix
887	Reversal: Invalid Reversal Indicator [%s]. Must be one of the following values: [YN]	Fix
888	Error validating ECP Routing Number	Fix
934	Expiry Date cannot be empty (Bin 000002 specific)	Fix
9591	Error matching Account Type in message with Account Type stored in profile.	Fix
9718	Invalid AVS Country Code [%s]. Supported values are [CA], [GB], [UK], or [US]	Fix
9719	Invalid Date Length: Format is YYYYMM	Fix
9720	Soft Desc: Merchant not activated for soft descriptors	Fix
9721	Soft Desc: Merchant Name is required if soft descriptor data is sent	Fix
9722	Soft Desc: Merchant Name exceeds max length of [%s] for %s transactions	Fix
9723	Soft Desc: [%s] cannot contain leading spaces	Fix
9724	Soft Desc: [%s] exceeds max length of [%s]	Fix
9725	Soft Desc: Product Description cannot be present if Merchant Name is > %s	Fix

Code	Description	Action*
9726	Soft Desc: Product Description length cannot exceed [%s] if Merchant Name length is between %s and %s	Fix
9727	Soft Desc: Too many Merchant descriptors. Never send more than one of the following: City, phone, url OR email	Fix
9728	Soft Desc: [%s] is not allowed for ECP transactions	Fix
9729	Soft Desc: Invalid format for Merchant Phone. Must be nnn-nnn-aaaa or nnn-aaaaaaaa	Fix
9732	Pcard Level 2 data is invalid.	Fix
9735	Gift Card: Invalid Block Activation Count	Fix
9737	Gateway is Down	Resend
9738	Database Connection Problem: Cannot acquire Database Connection	Resend
9739	Invalid Approval Code	Fix
9740	Invalid CAVV value	
9743	Pcard 3 data was sent in parent split, but is missing in current request	Fix
9744	If Alt Tax is sent Alt Tax ID is required	Fix
9745	Three reasons could result in this error: Pcard 3 data can only be sent with MC and VI cards. Pcard 3 data cannot be sent on this request type. Pcard 3 data can only be sent with US or Canadian currency.	Fix
9746	Line item count must be between 1 and 98 inclusive	Fix
9747	Line item detail number [%s] is missing	Fix
9748	Cannot send Pcard 3 data without sending Pcard 2 field	Fix
9749	Minimal Pcard 3 base data missing or invalid	Fix
9750	Minimal Pcard 3 line item data missing or invalid on index	Fix
9751	Line Item Count does not match the number of line items sent	Fix
9752	Invalid debit indicator for Bin 000002 in index. Must be 'D' or 'C'	Fix
9753	Invalid Gross/Net for Bin 000002 in index. Must be 'Y' or 'N'	Fix
9754	Amount hash error, negative total on line item data index	Fix
9755	Amount hash error on line item data index. Total = [%s] Hash = [%s]	Fix
9756	Detail totals do not match requested amount	Fix
9757	Invalid Country Code	Fix
9758	Invalid Unit of Measure in index	Fix
9760	Invalid Discount Indicator in line item	Fix
9761	Invalid or out of sequence line item Index Number	Fix
9762	Invalid Discount Amount in line item.	

Code	Description	Action*
9763	Invalid [%s]:[%s]. The field is missing, invalid, or has exceeded the max length of: [%s].	Fix
9764	Invalid Currency: [%s]. Currency Must Be Euro [978] or GB Pound Sterling [826].	Fix
9765	The field is missing, invalid, or has exceeded the max length	Fix
9766	The Bill Me Later Card Type [BL] is Not Allowed with this transaction.	Fix
9767	Bill Me Later Generic Error Code	Fix
9768	Invalid [Values. Must be one of the following values: XXX or empty	Fix
9769	BML: Mandatory Field [Customer Birth Date] is missing for [New (N)] Customer Type	Fix
9781	Unknown SOAP version	Fix
9782	Pinless Debit: Biller Reference Number is required	Fix
9783	Pinless Debit: Expiration Date is required	Fix
9784	Pinless Debit: Profile is not Pinless Debit	Fix
9793	PINless Debit: Invalid. The field is missing, invalid, or has exceeded the max length.	Fix
9794	PINless Debit: The PINless Debit Card Type [DP] is Not Allowed with [%s] Transactions.	Fix
9795	PINless Debit: The PINless Debit Card Type [DP] is Only Allowed with [%s] Transactions	Fix
9796	PINless Debit: The PINless Debit Card Type [DP] must be sent with Industry Type of [%s].	Fix
9797	PINless Debit: Card Number Not Eligible for PINless Debit Processing	Fix
9806	Refund by TxRefNum only valid when original transaction was AUTH or AUTH CAPTURE	Fix
9807	Refund by TxRefNum must be less than or equal to original transaction amount	Fix
9810	Partial online reversals are not allowed.	Fix
9811	Online reversals are not allowed for cardtype [x].	Fix
9812	Age of auth is [x] minutes, max age for online reversal of this method of payment is [x] minutes.	Fix
9992	Internal Gateway Resource Unavailable	Call
10005	Error communicating with the host	Fix
10005	A specific element contains invalid data	Fix
10011	Response timed out waiting for Authorization Host	Resend
10096	Invalid Card Number	Fix
10204	Invalid AVS ZIP Code	Fix
10332	Invalid Message Format. Transaction was flagged as an eCommerce Industry Type but No ECOrderNum was sent	Fix
10333	The ECOrderNum or MailOrderNum was all Zero's or All Spaces. These are not valid	Fix

Code	Description	Action*
10334	Invalid Card Number	Fix
10336	Transaction Amount to Large	Fix
10337	Transaction Amount to Small	Fix
10349	Host eFalcon check requested from PNS [BIN 000002] – This functionality is not supported on this platform	Fix
11001	Locked Down: Unable to Perform a Partial Void on Industry Type: [RE].	Fix
All other 10000 - 11000	GATEWAY SYSTEM ERROR CONDITIONS This encompasses various processing errors.	Resend
19716	Invalid AVS Zip Code. Valid formats are []	Fix
19717	Invalid Recurring Indicator []. Supported values are [].	Fix
19718	A specific element is restricted to a specific method of payment.	Fix
19719	A specific element has an invalid value [], allowed values are [].	Fix
19720	Either mcSecureCodeAAV or useStoredAAVInd [but not both] must be present	Fix
19721	Static AAV is not on file for merchantID [%s]	Fix
19722	Industry type must be one of [%s] for Card Brand [%s]	Fix
19725	Invalid EUDD Country Code: [%s] for Currency: [%s], Valid values are: [%s]	Fix
19726	Invalid Transaction Type for ECP Action Code	Fix
19727	Invalid ECP Action code for Currency	Fix
19728	Invalid Transaction type for Industry	Fix
19729	Invalid ECP Auth Method for ECP Action Code	Fix
19730	Invalid ECP Auth Method for Currency	Fix
19731	Invalid ECP Auth Method for ECP Delivery Method	Fix
19732	Invalid ECP Auth Method: Other dependency	Fix
19733	Invalid currency when Check Serial Number is provided	Fix
19734	Check Serial Number cannot be longer than [] for BIN []	Fix
19735	Invalid ECP Delivery Method for ECP Back Acct Type	Fix
19736	Invalid ECP Delivery Method for Transaction Type	Fix
19737	Invalid ECP Delivery Method for Currency	Fix
19738	Invalid amount for ECP transaction	Fix
19739	Invalid amount for ECP transaction	Fix
19740	Missing Data for ECP Auth Method	Fix
19741	Element [] cannot be empty when [] is provided.	Fix
19742	Invalid [Element]:[Value]. Must be one of the following values:	Fix

Code	Description	Action*
19743	[Message Type]: [Element] is required	Fix
19744	[] is not supported for BIN []	Fix
19745	Fraud Analysis: Unable to perform Fraud Analysis. The associated transaction failed	Call
19746	Invalid Transaction Type for Fraud Analysis	Fix
19755	Error validating card/account number for signature debit eligibility	Fix
Profile Errors		
9549	Invalid Profile Status for request.	Fix
9550	Invalid Customer Reference Number From Order Indicator	Fix
9551	Invalid Customer Reference Number	Fix
9552	System Failure. Unable To Perform Customer Profile Request at This Time.	Call
9553	Invalid Action Indicator	Fix
9555	Invalid BIN	Fix
9556	Invalid Merchant ID	Fix
9557	Invalid Name	Fix
9558	Invalid Address	Fix
9559	Invalid Address 2	Fix
9560	Invalid City	Fix
9561	Invalid State	Fix
9562	Invalid ZIP	Fix
9563	Invalid Email	Fix
9564	Invalid Phone	Fix
9565	Invalid Order Description	Fix
9566	Invalid Amount	Fix
9567	Invalid Account Type Indicator	Fix
9568	Invalid Account Number	Fix
9569	Invalid Account Expire Date	Fix
9570	Invalid ECP Account DDA	Fix
9571	Invalid ECP Account Type Indicator	Fix
9572	Invalid ECP Account Route	Fix
9573	Invalid ECP Bank Payment Delivery Method	Fix
9574	Invalid Switch Solo Start Date	Fix
9575	Invalid Switch Solo Issue Number	Fix
9576	Unable to Perform Profile Transaction. The Associated Transaction Failed.	Call

Code	Description	Action*
9577	Invalid Order Override Indicator	Fix
9578	Merchant-Bin combination is not allowed to perform profile transactions.	Call
9579	Merchant-Bin is not active.	Call
9580	Cannot process profile for Cust Ref Num and MID combination. A database error has occurred	Call
9581	Cannot process profile. Profile does not exist for Cust Ref Num and MID.	Fix
9582	Cannot process profile. Profile already exists for Cust Ref Num and MID.	Fix
9583	Missing Switch Solo Account Information. Either start date or issue number is required.	Fix
9584	Missing Electronic Check Account Information.	Fix
9585	Missing Credit Card Account Information.	Fix
9587	Auto-Gen Cust Ref Num Error.	Call
9588	Unable to Determine Profile Action from Auth Request	Fix
9589	Cannot Create Profile: A Customer Profile Name is Required	Fix
9592	Invalid Profile Status Requested	Fix
9594	The Profile's status prohibits the type of transaction being attempted.	Fix
9595	Schedule Date – The Future Schedule Date Is Invalid	Fix
9596	Schedule Date – The Future Schedule Date Is In The Past	Fix
9597	Invalid Account Updater request	Fix
9598	Invalid Profile Fetch: Fetch by Cust Ref Num and Account Num in same request not supported.	Fix
9599	Invalid method of payment for profile ID generation	Call
9601	Merchant is not enabled for Account Updater.	Call
19723	Managed Billing type must be [%s] for Account Type [%s]	Fix
19724	Static AAV must be on file for merchantID [%s] when Managed Billing type is [%s] and Account Type is [%s]	Fix
Retry Errors		
9710	Message expired during retry	Resend
9711	Too many transactions to process	Wait & Resend
9712	Request timeout - Please try again	Resend
9713	Invalid MIME header - Merchant ID in MIME does not match XML message	Fix
9714	Invalid MIME header- Trace number must be between 1 and 9999999999999999	Fix
9715	The retry request did not match the original request for this trace number	Fix
9719	Invalid Date Length: Format is YYYYMM	Fix
IP Authentication Errors		

Code	Description	Action*
9716	Security Information is Missing	Call Customer Service
9717	Security Information - agent/chain/merchant is missing	Call Customer Service
Managed Billing Errors		
9850	Managed Billing features are not supported for Bill Me Later or Pinless Debit transaction types	Fix
9851	Merchant account is not configured to use Managed Billing features	Call
9852	Profile level for merchant account is set to 'chain-level.' In order to use Managed Billing, the profile level must be set to 'merchant-level'	Call
9853	Invalid Order ID Generation Method. Use a valid value.	Fix
9854	Invalid Managed Billing Type for merchant	Call
9861	Deferred Billing Date must be a valid date (at least 1 day in the future – and at most 365 days in the future)	Fix
9862	Recurring Start Date must be a valid date at least 1 day in the future	Fix
9863	Only one Recurring End Date Trigger can be selected	Fix
9864	Invalid Recurring No End Date flag. Must be 'Y' or 'N'.	Fix
9865	Invalid Max Number of Recurring Billings.	Fix
9866	Recurring End Date must be a valid date at least 1 day greater than Recurring Start Date	Fix
9867	One of the 3 available Recurring Triggers must be set	Fix
9868	Invalid Recurring Format	Fix
9869	Industry Type of 'IN' can only be used when merchant is configured for a Managed Billing type of Recurring	Fix
9871	Missing Default Managed Billing values. All values must be set in transaction payload	Fix
9873	Cancel Date must be a valid date	Fix
9874	Daily Frequency Patterns are not accepted	Fix
9875	Scheduling is not complete. Contact Gateway Support.	Call
9876	Profile is locked for update in progress	Call
9877	Cancel or Restore Payment requests must be made separately from other Managed Billing Profile updates	Fix
9878	Future payment date could not be found to cancel	Fix
9879	Cancelled payment date could not be found to restore	Fix
9880	Start Date and End Date range is too small for selected recurring frequency (there are no possible future billings)	Fix
9881	Existing deferred payment is already in progress	Fix
9882	User does not have proper privileges to set-up a Managed Billing profile	Call

Code	Description	Action*
9883	Industry type of Recurring is not allowed to be set-up as Deferred Managed Billing type	Fix
9884	Error occurred while searching for transaction related to retry trace ID	Call
9885	Failed to find transaction associated with retry trace ID	Fix

A.5   Profile Process Status Response Codes

Table 16 describes the possible values for the <ProfileProcStatus> element (Code column) and the associated <ProfileProcStatusMsg> element (Description column) that indicate the success or failure of a Profile Management request. As you can see in the Status column, all codes other than 0 indicate an error. The Action column indicates what action you should take in response to the message.

Table 16   Profile Process Status code and message response values

Code	Message/Description	Status	Action*
0	Profile Action Successful	Success	None
9550	Invalid Customer Reference Number From Order Indicator	Error	Fix
9551	Invalid Customer Reference Number	Error	Fix
9552	System Failure. Unable To Perform Customer Profile Request at This Time.	Error	Call
9553	Invalid Action Indicator	Error	Fix
9555	Invalid BIN	Error	Fix
9556	Invalid Merchant ID	Error	Fix
9557	Invalid Name	Error	Fix
9558	Invalid Address	Error	Fix
9559	Invalid Address 2	Error	Fix
9560	Invalid City	Error	Fix
9561	Invalid State	Error	Fix
9562	Invalid ZIP	Error	Fix
9563	Invalid Email	Error	Fix
9564	Invalid Phone	Error	Fix
9565	Invalid Order Description	Error	Fix
9566	Invalid Amount	Error	Fix
9567	Invalid Account Type Indicator	Error	Fix
9568	Invalid Account Number	Error	Fix
9569	Invalid Account Expire Date	Error	Fix
9570	Invalid ECP Account DDA	Error	Fix

Table 16   Profile Process Status code and message response values

Code	Message/Description	Status	Action*
9571	Invalid ECP Account Type Indicator	Error	Fix
9572	Invalid ECP Account Route	Error	Fix
9573	Invalid ECP Bank Payment Delivery Method	Error	Fix
9574	Invalid Switch Solo Start Date	Error	Fix
9575	Invalid Switch Solo Issue Number	Error	Fix
9576	Unable to Perform Profile Transaction. The Associated Transaction Failed.	Error	Call
9577	Invalid Order Override Indicator	Error	Fix
9578	Merchant-Bin combination is not allowed to perform profile transactions.	Error	Call
9579	Merchant-Bin is not active.	Error	Call
9580	Cannot process profile for Cust Ref Num and MID combination. A database error has occurred	Error	Call
9581	Cannot process profile. Profile does not exist for Cust Ref Num and MID.	Error	Fix
9582	Cannot process profile. Profile already exists for Cust Ref Num and MID.	Error	Fix
9583	Missing Switch Solo Account Information. Either start date or issue number is required.	Error	Fix
9584	Missing Electronic Check Account Information.	Error	Fix
9585	Missing Credit Card Account Information.	Error	Fix
9587	Auto-Gen Cust Ref Num Error.	Error	Call
9588	Unable to Determine Profile Action from Auth Request	Error	Fix
9589	Cannot Create Profile: A Customer Profile Name is Required	Error	Fix
9592	Invalid Profile Status Requested	Error	Fix
9595	Schedule Date – The Future Schedule Date Is Invalid	Error	Fix
9596	Schedule Date – The Future Schedule Date Is In The Past	Error	Fix
19725	Invalid EUDD Country Code: [] for Currency: [], Valid values are: []	Error	Fix

A.6   CVV Request Response Codes

Table 17 describes the possible values for the `<CVV2RespCode>` element, which will be included in a response to a Card Verification Value Request.

Table 17   CVV request response code values

Code	Description
M	CVV Match
N	CVV No match

Table 17   CVV request response code values

Code	Description
P	Not processed
S	Should have been present
U	Unsupported by issuer/Issuer unable to process request
I	Invalid
Y	Invalid
blank	Not applicable (non-Visa)

A.7   Level 3 Data Codes

This section contains tables describing the *ISO country codes* and *unit of measure codes* that can be used in Level 3 data elements.

Table 18   ISO country codes

ISO Code	Country	ISO Code	Country
AFG	AFGANISTAN	LBY	LIBYAN ARAM JAMAHIRAYA
ALB	ALBANIA	LIE	LIECHTENSTEIN
DZA	ALGERIA	LTU	LITHUANIA
ASM	AMERICAN SAMOA	LUX	LUXEMBOURG
AND	ANDORRA	MAC	MACAU
AGO	ANGOLA	MDG	MADAGASCAR
AIA	AIGUILLA	MWI	MALAWI
ATA	ANTARCTICA	MYR	MALAYSIA
ATG	ANTIGUA & BARBUDA	MDV	MALDIVES
ARG	ARGENTINA	MLI	MALI
ABW	ARUBA	MLT	MALTA
AUD	AUSTRALIA	MHL	MARSHALL ISLANDS
AUT	AUSTRIA	MTQ	MARTINQUE
AZE	AZERBAIJAN	MRT	MAURITANIA
BHS	BAHAMAS	MUS	MAURITIUS
BHR	BAHRAIN	MEX	MEXICO
BGD	BANGLADESH	FSM	MICRONESIA, FEDERATED STATES OF
BRB	BARBADOS	MDA	MOLDOVA, REPUBLIC OF
BLR	BELARUS	MCO	MONACO
BEL	BELGIUM	MNG	MONGOLIA

ISO Code	Country
BLZ	BELIZE
BEN	BENIN
BMU	BERMUDA
BTN	BHUTAN
BOL	BOLIVIA
BIH	BOSNIA & HERZEGOWINA
BWA	BOTSWANA
BVT	BOUVET ISLAND
BRA	BRAZIL
IOT	BRITISH INDIAN OCEAN TERRITORY
BRN	BRUNEI DARUSSALAM
BGR	BULGARIA
BFA	BURKINA FASO
BDI	BURUNDI
KHM	CAMBODIA
CMR	CAMEROON
CAN	CANADA
CPV	CAPE VERDE
CYM	CAYMAN ISLAND
CAF	CENTRAL AFRICAN REPUBLIC
TCD	CHAD
CHL	CHILE
CHN	CHINA
CXR	CHRISTMAS ISLAND
CCK	COCOS KEELING ISLANDS
COL	COLOMBIA
COM	COMOROS
COD	CONGO, THE DEMOCRATIC REPUBLIC OF
COK	COOK ISLANDS
CRI	COSTA RICA
CIV	COTE D'IVORE
HRV	CROATIA (local name: Hrvatska)
CYP	CYPRUS
CZE	CZECH REPUBLIC

ISO Code	Country
MNE	MONTENEGRO
MSR	MONTSERRAT
MAR	MOROCCO
MOZ	MOZAMBIQUE
NRU	NAURU
NPL	NEPAL
NLD	NETHERLANDS
ANT	NETHERLANDS ANTILLES
NCL	NEW CALEDONIA
NZD	NEW ZEALAND
NIC	NICARAGUA
NER	NIGER
NGA	NIGERIA
NIU	NIUE
NFK	NORFOLK ISLAND
MNP	NORTHERN MARIANA ISLAND
NOR	NORWAY
OMN	OMAN
PAK	PAKISTAN
PLW	PALAU
PSE	PALASTINIAN TERRITORY, OCCUPIED
PAN	PANAMA
PNG	PAPUA NEW GUINEA
PRY	PARAGUAY
PER	PERU
PHL	PHILIPPINES
PCN	PITCAIRN
POL	POLAND
PRT	PORTUGAL
PRI	PUERTO RICO
QAT	QATAR
REU	REUNION
ROU	ROMANIA
RUS	RUSSIAN FEDERATION

ISO Code	Country
DNK	DENMARK
DJI	DJIBOUTI
DMA	DOMINICA
DOM	DOMINICAN REPUBLIC
ECU	ECUADOR
EGY	EGYPT
SLV	EL SALVADOR
GNQ	EQUATORIAL GUINEA
EST	ESTONIA
ETH	ETHIOPIA
FLK	FALKLAND ISLANDS (MALVINAS)
FRO	FAROE ISLANDS
FJI	FIJI
FIN	FINLAND
FRA	FRANCE
GUF	FRENCH GUIANA
PYF	FRENCH POLYNESIA
ATF	FRENCH SOUTHERN TERRIRORIES
GAB	GABON
GMB	GAMBIA
GEO	GEORGIA
DEU	GERMANY
GHA	GHANA
GIB	GIBRALTAR
GRC	GREECE
GRL	GREENLAND
GRD	GRENADA
GLP	GUADELOUPE
GUM	GUAM
GTM	GUATEMALA
GIN	GUINEA
GNB	GUINEA-BISSAU
GUY	GUYANA
HTI	HAITI

ISO Code	Country
RWA	RWANDA
SHN	SAINT HELENA
KNA	SAINT KITTS AND NEVIS
LCA	SAINT LUCIA
SPM	SAINT PIERRE & MIQUELON
VCT	SAINT VINCENT & THE GRENADINES
WSM	SAMOA
SMR	SAN MARINO
STP	SAO TOME & PRINCIPE
SAU	SAUDI ARABIA
SEN	SENEGAL
SRB	SERBIA
SYC	SEYCHELLES
SLE	SIERRA LEONE
SGD	SINGAPORE
SVK	SLOVAKIA
SVN	SLOVENIA
SLB	SOLOMON ISLANDS
SOM	SOMALIA
ZAD	SOUTH AFRICA
ESP	SPAIN
LKA	SRI LANKA
SUR	SURINAME
SJM	SVALBARD & JAN MAYEN ISLANDS
SWZ	SWAZILAND
SWE	SWEDEN
CHE	SWITZERLAND
SYR	SYRIAN ARAB REPUBLIC
TWN	TAIWAN, PROVINCE OF CHINA
TJK	TAJIKISTAN
TZA	TANZANIA, UNITED REPUBLIC OF
THA	THAILAND
TLS	TIMOR-LESTE
TGO	TOGO

ISO Code	Country
HMD	HEARD & MCDONALD ISLANDS
VAT	HOLY SEE (VATICAN CITY STATE(
HND	HONDURAS
HKD	HONGKONG
HUN	HUNGARY
ISL	ICELAND
IND	INDIA
IDN	INDONESIA
IRQ	IRAQ
IRL	IRELAND
ISR	ISRAEL
ITA	ITALY
JAM	JAMAICA
JPY	JAPAN
JOR	JORDAN
KEN	KENYA
KIR	KIRBATI
PRK	KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF
KOR	KOREA, REPUBLIC OF
QZZ	KOSOVO, UNITED NATIONS INTERIM ADMINISTRATION IN
KWT	KUWAIT
KGZ	KYRGYZSTAN
LAO	LAO PEOPLE'S DEMOCRATIC REPUBLIC
LVA	LATVIA
LBN	LEBANON
LSO	LESOTHO
LBR	LIBERIA

ISO Code	Country
TKL	TOKELAU
TON	TONGA
TTO	TRINIDAD & TOBAGO
TUN	TUNISIA
TUR	TURKEY
TKM	TURKMENISTAN
TCA	TURKS & CAICOS ISLANDS
TUV	TUVALU
UGA	UGANDA
UKR	UKRAINE
ARE	UNITED ARAB EMIRATES
GBR	UNITED KINGDOM
USA	UNITED STATES
UMI	UNITED STATES MINOR OUTLYING ISLANDS
QZZ	UNMIK
URY	URUGUAY
UZB	UZBEKISTAN
VUT	VANUATU
VEN	VENEZUELA
VNM	VIETNAM
VGB	VIRGIN ISLANDS (BRITISH)
VIR	VIRGIN ISLANDS (U.S.)
WLF	WALLIS & FUTUNA ISLANDS
ESH	WESTERN SAHARA
YEM	YEMEN
ZMB	ZAMBIA

Table 19   Unit of measure codes

UoM Code	Unit Name

UoM Code	Unit Name

Table 19   Unit of measure codes

UoM Code	Unit Name
ACR	Acre
ASM	Alcoholic strength by mass
ASV	Alcoholic strength by volume
AMP	Ampere
AMH	Ampere-hour (3,6 kC)
ARE	Are (100 m2)
BAR	Bar
BLL	Barrel (petroleum) (158,987 dm3)
BQL	Becquerel
BIL	Billion EUR
MLD	Billion US
BFT	Board foot
BHP	Brake horse power (245,7 watts)
BTU	British thermal unit (1,055 kilojoules)
BUA	Bushel (35,2391 dm3)
BUI	Bushel (36,36874 dm3)
CDL	Candela
CCT	Carrying capacity in metric tonnes
CNT	Cental GB (45,359237 kg)
CGM	Centigram
CLT	Centilitre
CMT	Centimetre
DTN	Centner, metric (100 kg)
WCD	Cord (3,63 m3)
COU	Coulomb
CKG	Coulomb per kilogram
CMQ	Cubic centimeter
DMQ	Cubic decimeter
INQ	Cubic inch
MTQ	Cubic metre
MQH	Cubic metre per hour
MQS	Cubic metre per second
MMQ	Cubic millimetre

UoM Code	Unit Name
KTN	Kilotonne
KVR	Kilovar
KVT	Kilovolt
KVA	Kilovolt-ampere
KWT	Kilowatt
KWH	Kilowatt-hour
KNT	Knot (1 nautical mile per hour)
LEF	Leaf
GLL	Liquid gallon (3,78541 dm3)
PTL	Liquid pint (0,473176 dm3)
QTL	Liquid quart (0,946353 dm3)
LTR	Litre (1dm3)
LPA	Litre of pure alcohol
CWI	(Long) hundredweight GB (50,802345 kg)
LTN	Long ton GB, US (1,0160469 t)
LUM	Lumen
LUX	Lux
MHZ	Megahertz
MAL	Megalitre
MAM	Megametre
MPA	Megapascal
MVA	Megavolt-ampere (1000 KVA)
MAW	Megawatt
MWH	Megawatt-hour (100 kW/h)
MTR	Metre
MTS	Metre per second
MSK	Metre per second squared
CTM	Metric carat (200 mg = 2.10-4 kg)
TNE	Metric ton (1000 kg)
MLD	Milliard
MBR	Millibar
MCU	Millicurie
MGM	Milligram

Table 19   Unit of measure codes

UoM Code	Unit Name	UoM Code	Unit Name
YDQ	Cubic yard	MLT	Millilitre
FTQ	Cubit foot	MMT	Millimetre
CUR	Curie	MIO	Million
DAY	Day	HMQ	Million cubic metres
DAA	Decare	MIU	Million international units
DLT	Decilitre	MIN	Minute
DMT	Decimetre	MON	Month
DTN	Decitonne	NMI	Nautical mile (1852 m)
CEL	Degree Celsius	NTT	Net (register) ton
FAH	Degree Fahrenheit	NEW	Newton
	Degree Kelvin: see *Kelvin*	NMB	Number
DPT	Displacement tonnage	NAR	Number of articles
DZN	Dozen	NBB	Number of bobbins
DZP	Dozen packs	NCL	Number of cells
DZR	Dozen pairs	NIU	Number of international units
DCP	Dozen pieces	NMP	Number of packs
DRL	Dozen rolls	NMR	Number of pairs
DRM	Drachm GB (3,887935 g)	NPL	Number of parcels
DRI	Dram GB (1,771745 g)	NPT	Number of parts
DRA	Dram US (3,887935 g)	NRL	Number of rolls
BLD	Dry barrel (115,627 dm3)	OHM	Ohm
GLD	Dry gallon (4,404884 dm3)	ONZ	Ounce GB, US (28,349523 g)
PTD	Dry pint (0,55061 dm3)	APZ	Ounce GB, US (31,10348 g)
QTD	Dry quart (1,101221 dm3)	PAL	Pascal
FAR	Farad	DWT	Pennyweight GB, US (1,555174 g)
OZI	Fluid ounce (28,413 cm3)	PCE	Piece
OZA	Fluid ounce (29,5735 cm3)	PTI	Pint (0,568262 dm3)
FOT	Foot (0,3048 m)	LBR	Pound GB, US (0,45359237 kg)
GLI	Gallon (4,546092 dm3)	PGL	Proof gallon
GBQ	Gigabecquerel	QTI	Quart
GWH	Gigawatt-hour (1 million kW/h)	QAN	Quarter (of a year)
GII	Gill (0,142065 dm3)	QTR	Quarter, GB (12,700586 kg)
GIA	Gill (11,8294 cm3)	DTN	Quintal, metric (100 kg)

Table 19   Unit of measure codes

UoM Code	Unit Name	UoM Code	Unit Name
GRN	Grain GB, US (64,798910 mg)	RPM	Revolution per minute
GRM	Gram	RPS	Revolution per second
GFI	Gram of fissile isotopes	SCO	Score
GGR	Great gross (12 gross)	SCR	Scruple GB, US (1,295982 g)
GRO	Gross	SEC	Second
GRT	Gross (register) ton	SET	Set
SAN	Half year (six months)	SHT	Shipping ton
HAR	Hectare	SST	Short standard
HBA	Hectobar	STN	Short ton GB, US (0,90718474 t)
HGM	Hectogram	SIE	Siemans
DTH	Hectokilogram	CMK	Square centimeter
HLT	Hectolitre	DMK	Square decimeter
HPA	Hectolitre of pure alcohol	FTK	Square foot
HMT	Hectometre	INK	Square inch
HTZ	Hertz	KMK	Square kilometer
HUR	Hour	MTK	Square metre
CEN	Hundred	MIK	Square mile
BHX	Hundred boxes	MMK	Square millimeter
HIU	Hundred international units	TDK	Square yard
CLF	Hundred leaves	WSD	Standard
CNP	Hundred packs	ATM	Standard atmosphere (101325 Pa)
CWA	Hundredweight US (45,3592 kg)	SMI	(Statute) mile (1609,344 m)
INH	Inch (25,4 mm)	STI	Stone GB (6,350293 kg)
JOU	Joule	ATT	Technical atmosphere (98066,5 Pa)
KEL	Kelvin	DAD	Ten days
KBA	Kilobar	TPR	Ten pairs
KGM	Kilogram	MIL	Thousand
KPH	Kilogram of caustic potash	TAH	Thousand ampere-hour
KSH	Kilogram of caustic soda	MBF	Thousand board feet (2,36 m3)
KNS	Kilogram of named substance	TQD	Thousand cubic metres per day
KNI	Kilogram of nitrogen	MBE	Thousand standard brick equivalent
KPP	Kilogram of phosphonic anhydride	TSH	Ton of steam per hour
KPP	Kilogram of phosphorus pentoxide	TNE	Tonne (1000 kg)

Table 19   Unit of measure codes

UoM Code	Unit Name	UoM Code	Unit Name
KPH	Kilogram of potassium hydroxide	TSD	Tonne of substance 90% dry
KPO	Kilogram of potassium oxide	TRL	Trillion EUR
KSH	Kilogram of sodium hydroxide	BIL	Trillion US
KSD	Kilogram of substance 90% dry	APZ	Troy Ounce
KUR	Kilogram of uranium	LBT	Troy pound, US (373,242 g)
KMQ	Kilogram per cubic meter	VLT	Volt
KGS	Kilogram per second	WTT	Watt
KHZ	Kilohertz	WHR	Watt-hour
KJO	Kilojoule	WEB	Weber
KMT	Kilometre	WEE	Week
KMH	Kilometre per hour	YRD	Yard
KPA	Kilopascal	ANN	Year

A.8   Verified by Visa CAVV Response Codes

Table 20 describes the possible values for the `<CAVVRespCode>` element, which will be included in a response to a Verified by Visa Card Authentication Verification Value (CAVV) request.

Table 20   Verified by Visa CAVV response code values

Code	Description
blank	CAVV Not Present
0	CAVV Not Validated due to erroneous data submitted.
1	CAVV Failed Validation – Authentication Transaction
2	CAVV Passed Validation – Authentication Transaction
3	CAVV Attempt: A 3-D Secure authentication value of 7 from the **Issuer ACS** indicates authentication was attempted. (Determined that the Issuer ACS generated this value from the use of Visa CAVV keys).
4	CAVV Failed Validation – Attempt: A 3-D Secure authentication value of 7 from **Visa's ACS** indicates that an authentication attempt was performed. (Determined that Visa generated this value from the use of CAVV keys).
5	Reserved for Future Use – NOT USED
6	CAVV Not Validated – Issuer not participating in CAVV validation.
7	CAVV Failed Validation – Attempt (CAVV generated with Visa Key)
8	CAVV Passed Validation – Attempt (CAVV generated with Visa Key)
9	CAVV Failed Validation – Attempt (CAVV generated with Visa Key – Issuer ACS unavailable)
A	CAVV Passed Validation – Attempt (CAVV generated with Visa Key – Issuer ACS unavailable)

Table 20   Verified by Visa CAVV response code values

Code	Description
B	CAVV Passed Validation – Information only, no liability shift (CAVV with ECI = 7)
C	CAVV Not Validated – Attempt – Issuer did not return a CAVV results code in the Authorization response.
D	CAVV Not Validated – Authentication – Issuer did not return a CAVV results code in the authorization response.
I	Invalid Security Data
U	Issuer does not participate or 3-D Secure data not utilized.

A.9   HTTP Responses

Table 21 lists some of the more common responses and what they mean in the context of the Orbital Gateway. You can find a listing of the possible generic HTTP responses and their descriptions at http://www.w3.org/Protocols/rfc2616/rfc2616.html.

Table 21   Gateway-specific and common HTTP responses

Code	Definition	Status
200	Approved	An HTTP Session was established with the Orbital Gateway. Error conditions can still be returned.
400	Invalid Request	The server, due to malformed syntax, could not understand the request.
403	Forbidden: SSL Connection Required	A Clear Text (or unencrypted) request was made to the Orbital Gateway. All transactions must be SSL Encrypted to interface to Orbital.
408	Request Timed Out	The Response could not be processed within the maximum time allowed.
412	IP Security Failure	A non-registered IP Address attempted to connect to the Orbital Gateway. The HTTP connection was refused as a result.
500	Internal Server Error	The server encountered an unexpected condition, which prevented it from fulfilling the request.
502	Connection Error	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.

A.10   Currency Codes and Exponents

Table 22 describes the different values for the `<CurrencyCode>` and `<CurrencyExponent>` elements in a New Order request message.

Table 22   Currency codes and exponents

Currency	Code	Exponent	Currency	Code	Exponent
Algerian Dinar	012	2	Lebanese Pound	422	2
Argentine Peso	032	2	Lithuanian Litas	440	2
Armenian Dram	051	2	Macau Pataca	446	2
Aruban Guilder	533	2	Malagasy Franc	450	0

Table 22   Currency codes and exponents

Currency	Code	Exponent	Currency	Code	Exponent
Australian Dollar	036	2	Malawi Kwacha	454	2
Azerbaijanian Manat	031	2	Malaysian Ringgit	458	2
Bahamian Dollar	044	2	Maldive Rufiyaa	462	2
Bangladeshi Taka	050	2	Mauritania Ouguiya	478	2
Barbados Dollar	052	2	Mauritius Rupee	480	2
Belarussian Ruble	974	0	Mexican Peso	484	2
Belize Dollar	084	2	Moldovan Leu	498	2
Bermudian Dollar	060	2	Mongolia Tugrik	496	2
Bolivian Boliviano	068	2	Moroccan Dirham	504	2
Botswana Pula	072	2	Mozambique Metical	508	2
Brazilian Real	986	2	Namibia Dollar	516	2
British Pound	826	2	Nepalese Rupee	524	2
Brunei Dollar	096	2	Netherlands Antillean Guilder	532	2
Bulgarian Lev	975	2	New Guinea Kina	598	2
Burundi Franc	108	0	New Zealand Dollar	554	2
CFA Franc BCEAO	952	0	Nicaraguan Cordoba Oro	558	2
CFA Franc BEAC	950	0	Nigerian Naira	566	2
CFP Franc	953	0	Norwegian Krone	578	2
Canadian Dollar	124	2	Pakistan Rupee	586	2
Cambodian Riel	116	2	Panamanian Balboa	590	2
Cape Verdi Escudo	132	2	Paraguay Guarani	600	0
Cayman Islands Dollar	136	2	Peruvian Nuevo Sol	604	2
Chilean Peso	152	2	Philippines Peso	608	2
Chinese Yuan Renminbi	156	2	Polish Zloty	985	2
Colombian Peso	170	2	Qatari Rial	634	2
Comoro Franc	174	0	Romania Leu	642	2
Costa Rican Colon	188	2	Russian Ruble	643	2
Czech Koruna	203	2	Rwanda Franc	646	0
Danish Krone	208	2	Saint Helena Pound	654	2
Djibouti Franc	262	0	Samoan Tala	882	2
Dominican Peso	214	2	Sao Tome & Principe Dobra	678	2
East Caribbean Dollar	951	2	Saudi Riyal	682	2
Egyptian Pound	818	2	Seychelles Rupee	690	2

Table 22   Currency codes and exponents

Currency	Code	Exponent	Currency	Code	Exponent
El Salvador Colon	222	2	Sierra Leonean Leone	694	2
Estonian Kroon	233	2	Singapore Dollar	702	2
Ethiopian Birr	230	2	Solomon Islands Dollar	090	2
Euro	978	2	Somali Shilling	706	2
Falkland Islands Pound	238	2	South African Rand	710	2
Fiji Dollar	242	2	South Korean Won	410	0
Gambian Dalasi	270	2	Sri Lanka Rupee	144	2
Georgian Lari	981	2	Swaziland Lilangeni	748	2
Ghanaian Cedi	288	2	Swedish Krona	752	2
Gibraltar Pound	292	2	Swiss Franc	756	2
Guatemala Quetzal	320	2	Taiwan Dollar (New)	901	2
Guinea Franc	324	2	Tanzanian Shilling	834	2
Guinea-Bissau Peso	624	2	Thai Baht	764	2
Guyanese Dollar	328	2	Tonga Pa'anga	776	2
Haitian Gourde	332	2	Trinidad & Tobago Dollar	780	2
Honduras Limpera	340	2	Turkish Lira (New)	949	2
Hong Kong Dollar	344	2	Uganda Shilling	800	0
Hungarian Forint	348	2	Ukrainian Hryvnia	980	2
Iceland Krona	352	2	United Arab Emirates Dirham	784	2
Indian Rupee	356	2	Uruguayan Peso	858	2
Indonesian Rupiah	360	2	US Dollar	840	2
Israeli New Shekel	376	2	Uzbekistan Sum	860	2
Jamaican Dollar	388	2	Vanuatu Vatu	548	0
Japanese Yen	392	0	Venezuelan Bolivar	862	2
Kazakhstan Tenge	398	2	Vietnamese Dong	704	2
Kenyan Shilling	404	2	Yemeni Rial	886	2
Kyrgyzstan Som	417	2	Zambian Kwacha	894	2
Laos Kip	418	0	Zimbabwe Dollar	716	2
Latvian Lats	428	2			

A.11 Fraud Filter Country Codes

Table 23 describes the possible values for <ISOCountryCode>, which is a New Order response element. This element is returned by the Salem Host when a merchant is enabled for country based fraud filtering.

For Country codes used in Level 3 data, please refer to *Level 3 Data Codes.*

Table 23   Gateway-specific and common HTTP responses

Code	Country	Code	Country
AF	AFGHANISTAN	LY	LIBYAN ARAB JAMAHIRIYA
AL	ALBANIA	LT	LITHUANIA
DZ	ALGERIA	MO	MACAU
AS	AMERICAN SAMOA	MG	MADAGASCAR
AD	ANDORRA	MW	MALAWI
AO	ANGOLA	MV	MALDIVES
AI	ANGUILLA	ML	MALI
AQ	ANTARCTICA	MT	MALTA
AG	ANTIGUA AND BARBUDA	MH	MARSHALL ISLANDS
AR	ARGENTINA	MQ	MARTINIQUE
AW	ARUBA	MR	MAURITANIA
AZ	AZERBAIJAN	MU	MAURITIUS
BS	BAHAMAS	FM	MICRONESIA, FEDERATED STATES OF
BH	BAHRAIN	MD	MOLDOVA, REPUBLIC OF
BD	BANGLADESH	MC	MONACO
BB	BARBADOS	MN	MONGOLIA
BY	BELARUS	ME	MONTENEGRO
BZ	BELIZE	MS	MONTSERRAT
BJ	BENIN	MA	MOROCCO
BM	BERMUDA	MZ	MOZAMBIQUE
BT	BHUTAN	NR	NAURU
BO	BOLIVIA	NP	NEPAL
BA	BOSNIA AND HERZEGOWINA	AN	NETHERLANDS ANTILLES
BW	BOTSWANA	NC	NEW CALEDONIA
BV	BOUVET ISLAND	NI	NICARAGUA
BR	BRAZIL	NE	NIGER
IO	BRITISH INDIAN OCEAN TERRITORY	NG	NIGERIA
BN	BRUNEI DARUSSALAM	NU	NIUE

Code	Country
BG	BULGARIA
BF	BURKINA FASO
BI	BURUNDI
KH	CAMBODIA
CM	CAMEROON
CV	CAPE VERDE
KY	CAYMAN ISLANDS
CF	CENTRAL AFRICAN REPUBLIC
TD	CHAD
CL	CHILE
CN	CHINA
CX	CHRISTMAS ISLAND
CC	COCOS (KEELING) ISLANDS
CO	COLOMBIA
KM	COMOROS
CD	CONGO, THE DEMOCRATIC REPUBLIC OF THE
CK	COOK ISLANDS
CR	COSTA RICA
CI	COTE D'IVOIRE
HR	CROATIA (local name: Hrvatska)
CY	CYPRUS
DJ	DJIBOUTI
DM	DOMINICA
DO	DOMINICAN REPUBLIC
EC	ECUADOR
EG	EGYPT
SV	EL SALVADOR
GQ	EQUATORIAL GUINEA
EE	ESTONIA
ET	ETHIOPIA
FK	FALKLAND ISLANDS (MALVINAS)
FO	FAROE ISLANDS
FJ	FIJI

Code	Country
NF	NORFOLK ISLAND
MP	NORTHERN MARIANA ISLANDS
OM	OMAN
PK	PAKISTAN
PW	PALAU
PS	PALESTINIAN TERRITORY, OCCUPIED
PA	PANAMA
PG	PAPUA NEW GUINEA
PY	PARAGUAY
PE	PERU
PH	PHILIPPINES
PN	PITCAIRN
PT	PORTUGAL
PR	PUERTO RICO
QA	QATAR
RE	REUNION
RO	ROMANIA
RU	RUSSIAN FEDERATION
RW	RWANDA
SH	SAINT HELENA
KN	SAINT KITTS AND NEVIS
LC	SAINT LUCIA
PM	SAINT PIERRE AND MIQUELON
VC	SAINT VINCENT AND THE GRENADINES
WS	SAMOA
SM	SAN MARINO
ST	SAO TOME AND PRINCIPE
SA	SAUDI ARABIA
SN	SENEGAL
RS	SERBIA
SC	SEYCHELLES
SL	SIERRA LEONE
SI	SLOVENIA

Code	Country
GF	FRENCH GUIANA
PF	FRENCH POLYNESIA
TF	FRENCH SOUTHERN TERRITORIES
GA	GABON
GM	GAMBIA
GE	GEORGIA
GH	GHANA
GI	GIBRALTAR
GL	GREENLAND
GD	GRENADA
GP	GUADELOUPE
GU	GUAM
GT	GUATEMALA
GN	GUINEA
GW	GUINEA-BISSAU
GY	GUYANA
HT	HAITI
HM	HEARD AND MCDONALD ISLANDS
VA	HOLY SEE (VATICAN CITY STATE)
HN	HONDURAS
IN	INDIA
ID	INDONESIA
IQ	IRAQ
IE	IRELAND
JM	JAMAICA
JO	JORDAN
KE	KENYA
KI	KIRIBATI
KP	KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF
KR	KOREA, REPUBLIC OF
QZ	KOSOVO, UNITED NATIONS INTERIM ADMINISTRATION MISSION IN
KW	KUWAIT

Code	Country
SB	SOLOMON ISLANDS
SO	SOMALIA
ES	SPAIN
LK	SRI LANKA
SR	SURINAME
SJ	SVALBARD AND JAN MAYEN ISLANDS
SZ	SWAZILAND
SY	SYRIAN ARAB REPUBLIC
TW	TAIWAN, PROVINCE OF CHINA
TJ	TAJIKISTAN
TZ	TANZANIA, UNITED REPUBLIC OF
TH	THAILAND
TL	TIMOR-LESTE
TG	TOGO
TK	TOKELAU
TO	TONGA
TT	TRINIDAD AND TOBAGO
TN	TUNISIA
TR	TURKEY
TM	TURKMENISTAN
TC	TURKS AND CAICOS ISLANDS
TV	TUVALU
UG	UGANDA
UA	UKRAINE
UM	UNITED STATES MINOR OUTLYING ISLANDS
QZ	UNMIK
UY	URUGUAY
UZ	UZBEKISTAN
VU	VANUATU
VE	VENEZUELA
VN	VIET NAM
VG	VIRGIN ISLANDS (BRITISH)

Code	Country
KG	KYRGYZSTAN
LA	LAO PEOPLE'S DEMOCRATIC REPUBLIC
LV	LATVIA
LB	LEBANON
LS	LESOTHO
LR	LIBERIA

Code	Country
VI	VIRGIN ISLANDS (U.S.)
WF	WALLIS AND FUTUNA ISLANDS
EH	WESTERN SAHARA
YE	YEMEN
ZM	ZAMBIA

Appendix B   General Card Validation

There are three common edits that catch the greatest majority of bad card numbers:

- MOD 10 check digit
- Credit card prefix check
- Credit card length validation

B.1   MOD 10 Check Digit

The MOD 10 check digit calculation validates the credit card by calculating the last digit of the card number based on a calculation performed upon all the digits preceding it. This operation, called a MOD 10 check-digit routine, is illustrated in Example 6.

Example 6   Calculating the MOD 10 check digit for card number 5240159910151573


```
5  2  4  0  1  5  9  9  1  0  1  5  1  5  7    Remove the check digit from the card number—in this example 3.
                                               Then start from the right and proceed to the left until all digits
                                               are multiplied by weight (2 and 1 alternately ).

                                   7 * 2 = 14      sum = 1 +4                    = 5
                                   5 * 1 = 5       sum = sum(5)       + 5        = 10
                                   1 * 2 = 2       sum = sum(10)      + 2        = 12
                                   5 * 1 = 5       sum = sum(12)      + 5        = 17
                                   1 * 2 = 2       sum = sum(17)      + 2        = 19
                                   0 * 1 = 0       sum = sum(19)      + 0        = 19
                                   1 * 2 = 2       sum = sum(19)      + 2        = 21
                                   9 * 1 = 9       sum = sum(21)      + 9        = 30
                                   9 * 2 = 18      sum = sum(30)      + 1 + 8    = 39
                                   5 * 1 = 5       sum = sum(39)      + 5        = 44
                                   1 * 2 = 2       sum = sum(44)      + 2        = 46
                                   0 * 1 = 0       sum = sum(46)      + 0        = 46
                                   4 * 2 = 8       sum = sum(46)      + 8        = 54
                                   2 * 1 = 2       sum = sum(54)      + 2        = 56
                                   5 * 2 = 10      sum = sum(56)      + 1 + 0    = 57

                                   sum = 57
                                   sum MOD 10 ➔ 57 MOD 10 = 7
                                   10 - 7 = 3
                                   check digit of 5240159910151573 is 3
```

Example 7   Sample check digit routine, written in C

```
/* The operator for module arithmetic in C is % */
long mod10(card,card_len_1);    /* module 10 check digit function */
char * card;                    /* credit card number */
short card_len;                 /* card length */
{
    register  int count;        /* a counter */
    register  int weight;       /* weight to apply to digit being checked */
    register  int sum;          /* sum of weights */
    register  int digit;        /* digit being checked */
    long      mod;

    weight = 2;
    sum    = 0;

    /* compute the sum */
    for (count = card_len -1; count>=0; count=count-1)
       {
       digit = weight * (card[count]-'0');
       /* add both the tens digit and the ones digit to the sum */
       sum = sum + (digit / 10) + (digit % 10);
       if (weight == 2)
          weight =1;
       else
          weight = 2;
       }

    /* subtract the ones digit of the sum from 10 and return the ones digit of that result */
    mod = (10 – sum%10) % 10;
    return (mod);
}
```

B.2   Card Prefix Check

The prefix check is the comparison of the first few digits of each card number to a list of known prefixes.

Table 24   Credit card prefixes

Card Type	Prefix
American Express/Optima	37, 34
Bill Me Later	504990, 621993
Carte Blanche	389
Diners Club	30, 36, 381–388
Discover (Novus)	60110, 60112, 60113, 60114, 60119
International Maestro	See *3.2.8 International Maestro*
JCB	3528–3589
MasterCard	51–55
PINless Debit	See *3.2.4 PINless Debit*
Visa/Delta	4

B.3   Card Length Check

The number of digits for each card is constant, allowing a validation to be performed by verifying the number of digits for each card number.

Table 25   Credit card number lengths

Card Type	Length
American Express/Optima	15
Bill Me Later	16
Carte Blanche	14
Diners Club	14
Discover (Novus)	16
International Maestro	13-19
JCB	16
MasterCard	16
PINless Debit	12–19
Visa/Delta	13 or 16

Appendix C   Level 2 & 3 Data Reference

This appendix contains tables highlighting the requirements for processing Purchase Cards or Commercial cards. Please see section *3.2.1.2 Level 2 and Level 3 Data* for more information.

C.1   Level 2 Data Summary

Each card type that supports Level 2 processing maintains its own standards for the data elements therein. Below is a summary of each potential field; listed as Mandatory, Conditional, Optional, on Non Applicable. Fields left as N/A should be null filled unless otherwise stated in *4.1 New Order Request Elements* or *4.3 Mark for Capture Request Elements*.

Legend: M – Mandatory
C – Conditional (See accompanying notes)
O – Optional
N/A – Not Applicable: Corresponding Tag should be null filled or left out of message

Table 26   Salem (BIN 000001) Level 2 information

Data Type	Visa	MasterCard	Discover	Amex	Notes
Purchase Order #	M	M	M	O	17 characters, Alphanumeric only
Destination Zip	M	M	M	M	Allows for 5 digit, 9 digit, or Canadian zip
Tax Indicator	O	O	O	O	Visa does not allow level 2 transactions to be tax exempt. Tax exempt merchants should attempt level 3 processing.
Tax Amount	M	M	M	O	• This may not be zero. • Acceptable thresholds vary by card type.
Requestor Name	N/A	N/A	N/A	M	30 alphanumeric characters
Destination Address (1 & 2)	N/A	N/A	N/A	M	30 alphanumeric characters per line
Destination City	N/A	N/A	N/A	M	20 alphanumeric characters
Destination State	N/A	N/A	N/A	C	• 2 alphabetic characters • Optional for Canada, Mandatory for U.S.
TAA Records	N/A	N/A	N/A	M	• TAA records are extended P Card information. • Up to four free-form records are allowed. • Contact Amex or your Account Exec for info on what data is expected in these fields

Table 27   PNS (Tampa - BIN 000002) Level 2 information

Data Type	Visa	MasterCard	Notes
Purchase Order #	M	M	17 characters, Alphanumeric only
Destination Zip	M	M	Allows for 5 digit, 9 digit, or Canadian zip
Tax Indicator	M	M	Visa does not allow level 2 transactions to be tax exempt
Tax Amount	M	M	This may not be zero to qualify as level 2. Acceptable thresholds vary by card type.

C.2   Level 3 Data Summary

Level 3 data can be thought of in two sections – Order Data, and Line Item data. Order Data is submitted once per transaction, and Line Item data is submitted recursively for as many line items are needed in the transaction (maximum of 98). The below tables describe both sections of Level 3 processing.

Legend: M – Mandatory
            C – Conditional (See accompanying notes)
            O – Optional
            N/A – Not Applicable: Tag should be null filled or left out of the message

Table 28   Salem (BIN 000001) Level 3 information

Data Type	Visa	MasterCard	Discover	Notes
Level 2 Data	C	M	C	• Both card types require the Destination Zip Code be sent. • All Level 2 fields are required to process level 3 on MasterCard transactions.
Freight Amount	M	M	N/A	Highlights the amount of the purchase which is for shipping.
Duty Amount	M	M	N/A	Highlights the amount of the purchase which is for duty.
Ship From ZIP	M	M	N/A	Allows for 5 digit, 9 digit, or Canadian zip
Destination Country Code	C	C	N/A	This defaults to USA if not submitted. See *Table 18 ISO country codes* for further reference
Discount Amount	M	N/A	N/A	Visa only: A listing of any discount given to the order as a whole, as opposed to a discount on a particular line item.
VAT Tax Amount	O	N/A	N/A	Value Add Tax or other Tax Amount included in total sale
VAT Tax Rate	O	N/A	N/A	Value Add Tax or other Tax Rate included in total sale
Alternate Tax Amount	N/A	O	N/A	Equivalent to VAT Tax Amount for MasterCard
Alternate Tax Rate	N/A	O	N/A	Equivalent to VAT Tax Rate for MasterCard
Line Item Data	M	M	M	A transaction must include 1-98 line items to qualify. Each data element below is submitted once per line item for all line items.
Detail Index	M	M	M	The line item number. "This is line item ___ of [Total # of Line items"
Detail Description	M	M	M	An alphanumeric description of the Line Item. • 26 characters for Visa, 35 for MasterCard
Detail Product Code	M	M	M	These values are defined by the Card Issuer.
Detail Quantity	M	M	M	The quantity of said items submitted • 13 digits, with 4 implied decimals • Visa and MC: Minimum value is 1 • Mastercard: This value is truncated to a 5 digit integer.

Data Type	Visa	MasterCard	Discover	Notes
Detail Unit of Measure	M	M	M	See *Table 19 Unit of measure codes* for accepted values.
Detail Tax Amount	M	M	M	Lists the amount of the line item which is Tax
Detail Tax Rate	M	M	M	Lists the tax rate applied to this transaction. • 5 digits, with 3 implied decimal places - Example: Submit 14287, which means 14.287% • The hundredths place is truncated off for Visa • 12345 is truncated to mean 12.34%
Detail Line Total	M	M	M	Generally this is Price * Quantity.
Detail Discount	O	O	N/A	The discount applied, if any, to this specific line item.
Detail Commodity Code	M	N/A	M	Accepted values of this field are defined by Visa.
Detail Unit Cost	M	C	M	• 4 implied decimals • Mastercard: Required for the UK if transaction exceeds a minimum threshold
Detail Gross Net	M	M	N/A	Indicates if Tax is included in this line item. Must be Y or N.
Detail Tax Type	N/A	O	N/A	Four alphabetic characters.
Detail Discount Indicator	N/A	M	N/A	Indicates if a discount was applied. Defaults to N if Discount Amount is empty.
Detail Debit Indicator	O	O	N/A	This field is only used by PNS only.
Detail Discount Rate	N/A	N/a	M	Discover only. 4 implied decimals.

Table 29   PNS (Tampa - BIN 000002) Level 3 information

Data Type	Visa	MasterCard	Notes
Level 2 Data	C	M	• Both card types require the Destination Zip Code be sent. • All Level 2 fields are required to process level 3 on MasterCard transactions.
Freight Amount	M	M	Highlights the amount of the purchase which is for shipping.
Duty Amount	M	M	Highlights the amount of the purchase which is for duty.
Ship From ZIP	M	M	Allows for 5 digit, 9 digit, or Canadian zip
Destination Country Code	C	C	This defaults to USA if not submitted. See *Table 18 ISO country codes* for further reference
Discount Amount	M	N/A	Visa only: A listing of any discount given to the order as a whole, as opposed to a discount on a particular line item.

Data Type	Visa	MasterCard	Notes
VAT Tax Amount	O	N/A	Value Add Tax or other Tax Amount included in total sale
VAT Tax Rate	O	N/A	Value Add Tax or other Tax Rate included in total sale
Alternate Tax Amount	N/A	O	Equivalent to VAT Tax Amount for MasterCard
Alternate Tax Rate	N/A	O	Equivalent to VAT Tax Rate for MasterCard
Line Item Data	M	M	A transaction must include 1-98 line items to qualify. Each applicable data element below is submitted once per line item for all line items.
Detail Index	M	M	The line item number. "This is line item ___ of [Total # of Line items"
Detail Description	M	M	An alphanumeric description of the Line Item. • 35 characters for both Visa and MasterCard • All letters must be in CAPS
Detail Product Code	M	M	These values are defined by the Card Issuer.
Detail Quantity	M	M	The quantity of said items submitted • 13 digits, with 4 implied decimals
Detail Unit of Measure	M	M	See *Table 19 Unit of measure codes* for accepted values.
Detail Tax Amount	M	M	Lists the amount of the line item which is Tax
Detail Tax Rate	M	M	
Detail Line Total	M	M	Generally this is Price * Quantity.
Detail Discount	O	O	The discount applied, if any, to this specific line item.
Detail Commodity Code	M	N/A	Accepted values of this field are defined by Visa.
Detail Unit Cost	M	M	4 implied decimals
Detail Gross Net	M	M	Indicates if Tax is included in this line item. Must be Y or N.
Detail Tax Type	N/A	N/A	Four alphabetic characters.
Detail Discount Indicator	N/A	N/A	Indicates if a discount was applied. Defaults to N if Discount Amount is empty.
Detail Debit Indicator	M	M	Implies that the line item total amount is being added (a Debit) or subtracted (a Credit) to the total of the purchase. • Must be a D or a C.
Detail Discount Rate	N/A	N/A	Discover Only. Only supported on Salem (Bin 000001).

Appendix D   Safetech Fraud Analysis Reference

This appendix contains tables highlighting the requirements for including the Safetech service with transaction processing. Please see section *3.3.6 Safetech Fraud Tools* for more information.

D.1   Request Element Reference

The Safetech service is supported in the `NewOrder`, `FlexCache`, and `SafetechFraudAnalysis` request types. All elements directly related to the Safetech service are contained in the `FraudAnalysis` parent element and listed below.

The short form request is listed below as FS1. The long form request is listed as FS2.

Legend: M – Mandatory
             C – Conditional (See accompanying notes)
             O – Optional
             N/A – Not Applicable: Tag should be null filled or left out of the message

Table 30   Safetech Request Element Information

Data Type	FS1	FS2	Notes
FraudAnalysis	M	M	Parent element of Fraud Analysis elements. Must be present to submit a request to the Safetech Service
FraudScoreIndicator	M	M	Used to indicate if the request falls under the short (FS1) or long (FS2) forms
RulesTrigger	O	O	Used to prompt the Safetech service to return all of the rules enabled in the Safetech Web Console which the transaction triggered
SafetechMerchantID	M	M	A static value issued to a merchant as part of the setup process. Can be defaulted through the Virtual Terminal
KaptchaSessionID	O	O	A unique session ID for the Safetech service.
WebsiteShortName	O	O	This can be defaulted as part of the setup process.
CashValueOfFencibleItems	N/A	O	This element has two implied decimal points.
CustomerDOB	N/A	O	Format: YYYY-MM-DD, including dashes.
CustomerGender	N/A	O	Indicates the customer is Male or Female.
CustomerDriverLicense	N/A	O	This element is recommended for ECP transactions.
CustomerID	N/A	O	This value is merchant-generated and does not have to imply a tokenized customer profile.
CustomerIDCreationTime	N/A	O	A unix timestamp for the previous element.
KTTVersionNumber	C	C	A hardcoded version number. All fields beginning with ktt are optional fields tied to shopping cart data and/or custom rule triggers. Unless all three KTT elements are included in the request, no KTT data is forwarded to the Safetech Service.

Data Type	FS1	FS2	Notes
KTTDataLength	C	C	This is the numeric length of the following element.
			All fields beginning with ktt are optional fields tied to shopping cart data and/or custom rule triggers.
			Unless all three KTT elements are included in the request, no KTT data is forwarded to the Safetech Service.
KTTDataString	C	C	A distinctly formatted string of shopping cart and/or custom rule trigger data.
			All fields beginning with ktt are optional fields tied to shopping cart data and/or custom rule triggers.
			Unless all three KTT elements are included in the request, no KTT data is forwarded to the Safetech Service.

D.2   Safetech Response Element Reference

The Safetech service may return data to a merchant through the `newOrderResponse`, `flexCacheResponse`, or `safetechFraudAnalysisResponse` elements. In addition to the corresponding `fraudAnalysisProcStatus` and `fraudAnalysisProcMsg` elements, additional response data is included in the `fraudAnalysisResponse` parent element within the response message.

The short form response is listed below as FS1. The long form response is listed as FS2

Legend: M – Mandatory
               C – Conditional (See accompanying notes)
               O – Optional
               N/A – Not Applicable: Tag will be null filled or left out of the message

Table 31   Safetech Response Element Information

Data Type	FS1	FS2	Notes
FraudAnalysisResponse	M	M	Parent Element for Safetech data elements
FraudScoreIndicator	M	M	This echoes the request element, indicating a short or long form response.
FraudStatusCode	C	C	This is the Safetech service's equivalent to a host response code. The format is unique to the service.
			Please refer to the Safetech Web Console for additional notes.
RiskInquiryTransactionID	C	C	The Safetech service's equivalent to an Order ID.
AutoDecisionResponse	O	O	A recommendation of action from the Safetech service, determined by settings in the Safetech Web Console
RiskScore	C	C	A numeric rating of the risk involved in the transaction.
			Fraud scoring must be successful to receive a value.
KaptchaMatchFlag	O	O	Kaptcha is a process within the Safetech service. This element is the result of that validation.
WorstCountry	N/A	O	The riskiest country associated with the persona of the customer.

Data Type	FS1	FS2	Notes
CustomerRegion	N/A	O	An estimation of the region of the customer Lower case is a state/province. Upper case is a country.
PaymentBrand	N/A	O	The method of payment, as identified by the Safetech service.
FourteenDayVelocity	N/A	O	A count of prior transactions by the customer in the last 14 days.
SixHourVelocity	N/A	O	Similar to the previous element, but under a more focused window
CustomerNetwork	N/A	O	An indicator to add detail to the location of the customer
NumberOfDevices	N/A	O	This element and the two following elements are additional customer information collected by the Safetech service as part of scoring the transaction
NumberOfCards	N/A	O	
NumberOfEmails	N/A	O	
DeviceLayers	N/A	O	A period-delimited collection of five layers of device information collected by the Safetech service. When progressing from layers one through five, data becomes less precise. The layers are defined as 1 Network/OS/SSL layer 2 Flash layer 3 Javascript layer 4 HTTP layer 5 Browser layer
DeviceFingerprint	N/A	O	A hash of device constants.
CustomerTimeZone	N/A	O	This element and the following element are used to identify the local time of the customer.
CustomerLocalDateTime	N/A	O	
DeviceRegion	N/A	O	This element and the twelve following elements are all technology information about the customer, as identified by the Safetech fraud tools.
DeviceCountry	N/A	O	
ProxyStatus	N/A	O	
JavascriptStatus	N/A	O	
FlashStatus	N/A	O	
CookiesStatus	N/A	O	

Data Type	FS1	FS2	Notes
BrowserCountry	N/A	O	
BrowserLanguage	N/A	O	
MobileDeviceIndicator	N/A	O	
MobileDeviceType	N/A	O	
MobileWirelessIndicator	N/A	O	
VoiceDevice	N/A	O	
PCRemoteIndicator	N/A	O	
RulesDataLength	C	C	The numeric length of the data in the next element.
RulesData	C	C	This is a delimited list of all rules the transaction invoked in the Safetech service. This response element is conditional on use of the `rulesTrigger` response element.

D.3   Safetech Response Codes

The Safetech service returns a response code for any approved or declined request. This is returned in the Fraud Status Code element of the response message.

The first character of the fraud status code can be used to identify the type of response returned from the Safetech service. Possible values for this field include:

- A – Successful fraud score
- K – Fraud system error
- T – No fraud score – internal error
- X – Pre authorization check
- Y – Post authorization check

The following chart lists possible fraud status codes.

Table 32   Fraud Status Codes

Fraud Status Code	Description
Y001	Authorization timed out. Fraud scoring inquiry not attempted.
X001	Merchant not enabled for Safetech fraud scoring
X002	MOP not supported for Safetech fraud scoring
X003	Action Code not supported for Safetech fraud scoring
X004	Transaction Type not supported for Safetech fraud scoring
X005	Safetech Merchant ID not sent on transaction

X006	Safetech Merchant ID supplied does not match the division setup on file
X008	Invalid Shopping Cart Data. Fraud scoring inquiry not attempted.
X009	Invalid User-Defined Field Data. Fraud scoring inquiry not attempted.
A000	Fraud score successful
A001	Fraud score replayed from historical database.
T998	Internal server error where the fraud system is unreachable
T999	Fraud system unreachable
K201	The version number is missing. Internal to Chase Paymentech.
K202	The mode is missing.
K203	The Merchant ID is missing.
K204	The Session ID is missing
K205	The Fraud Score Transaction ID is missing.
K211	The Currency Code is missing.
K212	The Total Authorization Amount is missing.
K221	The Email Address is missing.
K222	The Phone Number is missing.
K223	The Website ID is missing.
K231	The Payment Type is missing.
K232	A Payment Type of Card is missing.
K233	The Payment Type of MICR is missing. MICR is the Magnetic Ink Character Recognition (MICR) line on a check.
K235	The Payment Token (Amount) is missing
K241	The customer IP Address is missing.
K251	The merchant acknowledgement flag is missing.
K261	The POST is missing
K271	The Product Type code is missing.
K272	The Product Item code is missing.
K273	The Product Description is missing.
K274	The Product Quantity is missing.
K275	The Product Price is missing.
K301	The Version Number is invalid.
K302	The Mode is invalid.
K303	The merchant ID is invalid.
K304	The Session ID is invalid.
K305	The Fraud Score Transaction ID is invalid.
K311	The currency code is invalid.

K312	The total authorization amount is invalid.
K321	The customer's email address is invalid.
K322	The customer's phone number is invalid.
K323	The Website ID is invalid.
K324	The format of the Fraud Score response is invalid.
K331	The payment type of the transaction is invalid.
K332	The card used as payment is invalid.
K333	The Payment Type of MICR is invalid. MICR is the Magnetic Ink Character Recognition (MICR) line on a check.
K336	The Bill Me Later account number is invalid.
K341	The customer IP address is invalid.
K351	The merchant acknowledgement flag is invalid.
K362	The shopping cart data is invalid.
K371	The Product Type code is invalid.
K372	The Product Item code is invalid.
K373	The Product Description is invalid.
K374	The Product Quantity is invalid.
K375	The Product Price is invalid.
K399	The label either doesn't exist or was associated with the wrong data type.
K401	Extra data was included in the transaction.
K402	The payment types were mis-matched.
K403	A customer phone number was sent in, but was unnecessary.
K404	A Payment Token was sent in that was unnecessary.
K501	A Scoring request was sent in that was not authorized.
K502	A merchant ID was sent in that was not authorized.
K503	An IP address was sent in that was not authorized.
K504	A password was used that was not authorized.
K601	A system error occurred.
K701	A header is missing from the transaction.