CHASE Paymentech

ORBITAL GATEWAY

ORBITAL GATEWAY 101

SUPPLEMENTAL REFERENCE

April 2009

Version 3.0

Preface

This edition of the Orbital Gateway 101 Supplemental Guide contains information available at the time of publication and supersedes, in its entirety, all previously published documents.

4200 West Cypress St.
Suite 350
Tampa, FL 33607
www.ChasePaymentech.com

Table of Contents

CHANGE LOG

Revision	Date	Description
1.0	3/17/03	Initial Release
2.0	3/17/2008	Overall Update of Document
3.0	4/21/2008	Revisions: Merchant Authentication, American Express CID

Chapter 1 OVERVIEW

Overview

The Chase Paymentech Orbital Gateway system is a proprietary XML Internet Processing System. The modular set of web-enabled tools permit merchants to securely accept and process card-not present payments over the Internet. These include but are not limited to credit card, electronic check, debit card, and gift card transactions. The Orbital Gateway works with both of Chase Paymentech's Host Processing Platforms - PNS and Salem. 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 processing and larger customers. Despite the name, both systems are co-located in Tampa, Florida and Salem, New Hampshire. Although Orbital supports the unique processing functionalities of each Platform, the features available to merchants are limited by the platform used.

This guide is intended to assist any party intending to use the Chase Paymentech Orbital Gateway system. Processing via any other Chase Paymentech system may require different processes. Please consult your technical consultant or relationship manager for any questions or concerns as to which processing system you are using.

Method of Payments

The Orbital Gateway supports the full range of payment methods offered by Chase Paymentech Solutions, including:

- American Express
- Bill Me Later *
- Discover Card
- JCB
- MasterCard
- Visa
- Gift Card (formerly FlexCache)
- PINless Debit *
- UK Maestro */Solo *
- Electronic Check transactions *
- European Direct Debit (EU DD) *

The Orbital Virtual Terminal also supports:

- Purchasing Card Level II and Level III data input (including American Express Level II data for Salem merchants) **
- All Chase Paymentech Solutions supported international currencies *
- Soft Descriptors *

* Not available to all merchants. Only supported on Salem host.
** Purchase Card Level III not available for Canadian processing.

Chapter 2 ORBITAL GATEWAY SYSTEM

API Interfaces

Chase Paymentech has adopted XML as its standard to process transactions over the Internet. Three types of XML APIs (Application Program Interface) may be used for XML processing on the Orbital Gateway. Each requires certification by an analyst. Please access http://download.chasepaymentech.com for detail integration information.

- Online XML API

  The Chase Paymentech API uses XML for card-not-present payment requests using HTTPS. This integration method requires the merchant to develop code that generates XML formatted message requests and receives XML formatted responses. The use of XML allows platform and programming language independence.

- Batch XML API

  The Orbital Gateway offers an XML based batch processing interface. This integration requires the merchant to develop code that generates XML formatted flat files with message requests. The files are sent via SFTP over the internet or FTP via Frame/Dial PPP. Response files with XML formatted response messages are retrieved later via the same method. This functionality allows for Multi-Merchant batch processing of up to 999,999 transactions per file.

- Web Service [SOAP] API

  The Orbital Gateway offers a Web Service [SOAP] processing interface. This integration requires the merchant to support the Orbital Gateway Web Service as defined by the following WSDL:

  - Web Service [SOAP] API
  - Orbital Gateway WSDL Only

Software Development Kits

In addition to XML Processing, Chase Paymentech offers Software Development Kits (SDKs) that can assist in programming, reducing development time and costs. These powerful and easy to use tools enable developers to quickly create and integrate real-time electronic payments. Although programming is required, the SDKs managed the creation of the communication protocol as well as the generation of the XML requests and the interpretation of the XML replies. SDKs are built in Java [1.4 and 1.5], COM, .NET [1.1 and 2.0 Framework], C++, and Perl. Certification of an implementation is required.

Virtual Terminal

The Orbital System consists of two components, the Orbital Gateway and the Orbital Virtual Terminal (VT). All merchants that have a Gateway account also have automatic access to a corresponding Virtual Terminal, which is a web-based application. The two key aspects of the Virtual Terminal are the informational features and processing functionalities. First, through the VT which is accessible via an Internet connected computer, all open, pending and processed orders are readily viewed [assuming the user has the appropriate rights and permissions]. Six months of historical data is available. Additionally, ad hoc reports are easily ordered, retrieved and reviewed.

Second, the Virtual Terminal serves as an Internet-based point of sale terminal for card-not-present transactions. Data may be manually entered or imported. A variety of user based permissions provides flexibility and control over the functional access granted employees. For example, one user can be granted rights for all processing capabilities the Virtual Terminal offers while another user is restricted to read only access. This is especially important for issuing credits or voiding transactions. For greater detail the Virtual Terminal User Guide may be downloaded from http://download.chasepaymentech.com. It may also be access by the Help icon in the VT.

Software Packages

Many software developers have created interfaces with the Orbital System. Merchants can purchase and install these software solutions. Certification is still required however the process is typically much shorter than a programmed interface using XML or a SDK.

Chapter 3 ORBITAL GATEWAY FUNCTIONALITIES

Merchant Authentication

Orbital Gateway System

The Orbital Gateway System authenticates merchants by one of the two following methods.

- Source IP Address

  During the certification process, the merchant is required to register the IP address of the system that communicates with the Gateway. Additionally the IP address must be affiliated with the merchant ID number. Any activity presented from an IP address that is not registered and associated with the correct merchant ID results in an error. If needed, the 24x7 customer support department is able to assist in changing or adding IP address configurations for the merchant.

- Connection Username/Password

  Similar to Source IP authentication, both the Connection Username and Password must be registered and associated with the merchant ID number. Once registered, both must be submitted along with each transaction.

Orbital Virtual Terminal

The Orbital Virtual Terminal authenticates users through a sign-on system requiring individual User IDs and passwords. Passwords must be changed every 90 days.

Cardholder Authentication (Card-Not-Present)

The Orbital Gateway supports the following three cardholder authentication systems. These were designed to mitigate fraud exposure in the Card-Not- Present (CNP) environment. Greater detail is provided in the CNP processing overview.

- Address Verification

  Address Verification, also known as AVS, is a cardholder authentication mechanism that validates the billing address provided by the cardholder against that which the card issuing institution has on record. In addition to providing merchants with an additional risk management tool, it is required by Visa to qualify for the lowest interchange rates and protects against certain chargeback conditions.

- Card Verification Numbers

  These numbers, either three or four digits long, are only found on the physical credit card. In order to provide the number to the merchant, the card most typically is in the physical possession of the person initiating the purchase. The merchant passes the verification number in the authorization request and the card issuer verifies if the card identification number is associated with the card account on record. Card verification numbers used in conjunction with address verification are effective tools for mitigating risk.

- Verified by Visa / MasterCard SecureCode

  For online purchases, Visa and MasterCard separately designed additional methods of authentication. For a cardholder who chooses this security option, the employed mechanism provides a unique transaction-specific token that verifies the cardholder originated the transaction. Merchants are required to request authorization for all Verified by Visa and MasterCard SecureCode ecommerce transactions.

Merchant Selectable Response (MSR)

Orbital's Merchant Selectable Response functionality helps protect your organization from fraud by providing the option to decline transactions based on predefined parameters. The merchant selects the Address Verification Service (AVS) or Card Verification Number response codes to auto-decline. For example you might choose to auto decline transactions receiving an AVS Code indicating there are no matches to the AVS fields. In such situations a decline messaged is returned.

Soft Descriptors

The Orbital Gateway supports soft descriptors. This functionality is related to how the merchant name appears on the consumer's statement. Optimally the name should be one that is readily recognizable by the consumer. However, due to business needs, the merchant name appearing on the CPS system may not be one that is easily recognized. Soft Descriptor Records allows greater flexibility in describing the company or trade name as well the ability to describe the product or service purchased.

Please note that it is at the card issuer's discretion as to whether or not the soft descriptors are displayed on the cardholder statement. Also, support for Soft Descriptors is not globally available to all customers using the Orbital Gateway. Please contact your Chase Paymentech representative for additional information.

Retry Logic (Duplicate Processing Protection)

Retry Logic is a function that checks reprocessed transactions when there is an unknown result from a XML transaction request. It is available to any merchant interfacing to the Orbital Gateway by simply including two new values to the MIME-Header: the Merchant ID and a transaction Trace Number. The Orbital Gateway uses the combination of the two values as an identifier to evaluate whether or not the transaction processed. It then takes one of two actions. If the resubmitted transaction was processed in the past 48 hours and received an approval code, the original approval response is sent to the merchant, eliminating a potential duplicate transaction. If the original transaction was declined or did not process, the re-submission is treated as a new request.

Customer Profile Management and Managed Billing

The Orbital Gateway includes functionality called Customer Profile Management, which allows Cardholder data to be stored by the Orbital Gateway. A merchant can process transaction by simply passing a unique token value, such as a customer profile number, that represents the cardholder.

Once a Profile is created, transactions can be processed, using either the on-line interface or the Orbital Virtual Terminal (VT), simply by referencing the Customer Profile and filling in any additional information not stored in the profile.

Managed Billing extends the capabilities of Profiles to included Recurring, Installment, and Deferred billing. With this feature, merchants can establish and assign predefined billing schedules to Profiles. The Orbital Gateway then initiates an authorization and capture transaction on behalf of the merchant in accordance with the schedule.

Both the Customer Profile Management and Managed Billing functionalities are only available to merchants using the Chase Paymentech Orbital Gateway.

Authorization Recycling

The optional service re-authorizes transactions that receive soft declines from the issuing bank. A soft decline is a decline that has the potential to be approved at a later date such as an Over-Limit Decline. The merchant chooses which soft declines to be recycled, the number of re-authorization attempts, and the interval between authorization attempts. The maximum limit is four attempts within 16 days. The Authorization Recycling process continues for each transaction until an approval is obtained, a hard decline is received, or the number of designated attempts is exhausted.

Chapter 4 CARD-NOT-PRESENT PROCESSING OVERVIEW

Card processing normally has two classifications. Card Present transactions occur when the cardholder and card are both present at the point of sale. The classification of Card-Not-Present (CNP) applies to those situations in which the card and/or cardholder are not physically present at the time of purchase (e.g. Internet, phone or mail orders, recurring billings).

Although the Orbital Gateway supports a variety of payment methods, listed in Chapter 1, the following CNP overview focuses on traditional credit card processing. For information regarding the additional methods of payments, you may reference the interface documentations found on http://download.chasepaymentech.com.

As a reminder, this guide is only applicable to Orbital Gateway Merchants and for the CNP environment. There are functionalities and logic that the Orbital System has incorporated to assist in the merchant's CNP processing. These may not be available on other Chase Paymentech platforms.

Basic CNP Processing Flow (Credit Cards)

The two basic aspects to credit card processing are the authorization of the transaction and its capture, which is also known as settlement. In the Card-Not-Present arena merchants must first authorize a transaction and capture or settle it only when the product is provided or shipped.

An authorization is a request by a merchant to verify that the cardholder is in good standing. It is required in the Card-Not-Present environment. A response is returned from the financial institution that issued the card. The responses fall in to an approval, decline, or referral category. An approval reserves the specified dollar amount for future settlement. The specified amount is removed from the cardholder's available credit limit or funds (also referred to as "open-to-buy"). An authorization is valid for 7 days for Visa. For the other card types, it is valid for 30 days. In the case of Debit or Check cards, the account funds are impacted for 3 days. If an authorization code is used after the valid time frame it is considered "stale." (Please see Interchange Qualifications for more information.)

Approved transactions are subsequently submitted for payment, i.e., capture. Whether the authorization and capture is a two step or one step process typically depends on the type of product involved. There are basically two types of products, hard goods or soft goods.

Hard Goods (or Future Fulfillment)

Hard Goods are physical products that are sold and shipped. Examples are numerous: books, clothing, auto parts, etc. Since the shipment could be delayed due to inventory or packaging problems, the standard transaction normally involves a two step process. An authorization is submitted at the time the order is placed. It is followed by a capture transaction once the product is shipped.

Soft Goods (or Immediate Fulfillment)

Soft goods are non-physical goods. Services, instantly downloadable products, and recurring charges are examples of soft goods. In this model, due to the immediate delivery of the product, there is no shipping. Merchants may use the convenient single step Auth/ Capture transaction. There are many variations to the processing models. Please contact your technical analyst for further assistance.

Transaction Request Types

The types of products sold influences the type of transactions a merchant submits. Each credit card transaction request type has a specific purpose. For greater detail please see the section titled Definition of Request Types. Orbital supports the following transaction request types:

- Auth Only
- Auth/Capture
- Mark for Capture
- Force or Capture of Prior Auth
- Credit/Refund
- Void
- Split Shipments or Ship Partial
- End of Day – Settlement Transaction

Interchange Qualifications

In order to obtain get the best Interchange Rate (rates charged by the Card Associations such as MasterCard and Visa) merchants must comply with the association guidelines. The merchant should refer to these guidelines to ensure cost efficient processing. To assist merchants in their efforts the Gateway employs Aged Authorization Logic. The Orbital Gateway system automatically attempts to reauthorize any transaction when the authorization is considered “stale” or past time frame for deposit.

Address Verification

AVS (Address Verification Service) or AAV (Automated Address Verification by American Express) were designed to reduce the fraudulent use of credit cards for mail, telephone, and Internet transactions.

Each verification process is executed by comparing the consumer entered billing address with the billing address data that is kept on file for the cardholder in the Card Issuer’s database. The AVS/AAV request is routed along with the authorization request from the merchant through the Chase Paymentech system and card association to the issuing card institution. The numeric portion of the address information is then compared to the cardholder billing address on file. The result of the AVS/AAV comparison is included in the authorization response message returned to the Merchant. The AVS response is reflected as an AVS Code.

It is important to note that if AVS is not a valid match; a transaction can still be approved even though the AVS response is negative. Card issuers practices vary as to whether a transaction with an invalid AVS match is approved (assuming all other approval criteria is met) or declined. As an additional note, for Visa transactions, the merchant will not qualify for the best interchange rate unless a minimal Zip Code AVS check is performed.

Card Verification Numbers

An important security and fraud mitigation feature for CNP processing is the "Card Verification Number" (CVN). The purpose of the number is to verify that the consumer has possession of the card. Therefore it is against card association regulations to store the CVN value. It is temporally captured for use in the transaction but it should not be stored or retained. Each card association program has its own acronym for the number.

- American Express CID (Card Holder ID) – 4 digits
- Discover CID (Card Holder ID) – 3 digits
- MasterCard CVC2 (Card Verification Code) – 3 digits
- Visa CVV2 (Card Verification Value) – 3 digits

The values for MasterCard, Visa and Discover are located on the back of the card in the signature panel. For American Express it is located on the front of the card above the card number.

Although there is not an Interchange benefit for using this tool, Chase Paymentech considers it a best business practice to perform this check with each transaction. Just like AVS, merchants receive a positive or negative response. Card issuers practices vary as to whether a transaction with an invalid CVN match is approved (assuming all other approval criteria is met) or declined.

American Express CID: Two important notes regarding American Express CID.

- American Express CID only works if your American Express account is activated for the program by American Express. Contact American Express directly for more information.
- When American Express CID is used, it behaves differently than MasterCard and Visa CVC2/CVV2.
  - For proprietary American Express cards, the transaction is declined if there is not a matching CID value. If the CID does match, the transaction is approved assuming all other criteria are met. There are no specific CID response values.
  - For American Express cards issued by other banks, a CID response value may be returned.

Verified by Visa / MasterCard SecureCode

For additional security surrounding online purchases, Visa and MasterCard designed separate but somewhat similar systems. Each communicates authentication information among the cardholder, card issuer, merchant and acquirer (in this case Chase Paymentech Solutions.) Both use 3-D Secure Protocol and require a compliant Merchant Server Plug-in (MPI) software application. Both use Base 64 encoding of the unique transaction-specific token [known as by Visa as CAVV and by MasterCard as AAV] before sending the value to Chase Paymentech. In both systems the cardholder registers the card to participate in the program. Merchants are required to request authorization for all Verified by Visa and MasterCard SecureCode ecommerce transactions.

Although a brief description is found below, behind the scenes there is a significant amount of matching and verification of registered data occurring under secure protocols. For additional detail, please review one of the various specifications such as Orbital Gateway Interface Specification [V 4.3] found the download page http://download.chasepaymentech.com. Please note that although Verified by Visa and MasterCard SecureCode are supported by the Orbital Gateway through the various interfaces, they are not supported on the Virtual Terminal.

Verified by Visa

In the online environment, the cardholder selects the merchandise to be purchased and proceeds to the checkout page. After providing payment information, the "buy" button is selected which activates the Merchant Server Plug-In (MPI) software application. The application checks to determine if the cardholder's Visa number participates in the program and if a current authentication is available for the card account. If it is, the cardholder is subsequently redirected to a screen to enter a password. Afterwards a Cardholder Authentication Verification Value (CAVV) is generated and returned to the merchant. This is submitted [in Base 64 coding] along with the appropriate ECI indicator in the authorization request. The fields are used during authorization processing to verify that authentication, or attempted authentication, was performed and to qualify for the ecommerce Customer Payment Services. If the CAVV does not match, the transaction is declined.

If the card account is not a participant in the program, an "authentication not available" message generated and returned to the merchant. The process proceeds with the standard authorization steps and authorization request.

MasterCard SecureCode

The process for MasterCard Secure Code is very similar to that described above. A key difference is the successful authentication message returned to the merchant for a participating card number. Evidence of cardholder authentication is provided by a 28-byte AAV cryptographically generated value. Like the CAVV, this value is subsequently included in the authorization request in Base 64 coding. It is passed to the issuer for validation. An approval or declined is returned by the issuer.

If the card account is not a participant in the program, an "authentication not available" message generated and returned to the merchant. The process proceeds with the standard authorization steps and authorization request.

Chapter 5 DEFINITION OF REQUEST TYPES

Various types of requests are used in credit card processing. Brief explanations of those supported by the Orbital Gateway follow.

Auth Only

A request used for the purpose of verifying cardholder funds. It is typically employed when merchants do not fulfill orders immediately. The transaction is not settled. (Future Fulfillment Model)

Auth/Capture

A request used to verify cardholder funds and to submit the transaction for settlement funding. The transaction is included in the next batch processed for the merchant. Typically a merchant uses this combined request when the order can be fulfilled immediately. (Immediate Fulfillment Model)

Mark for Capture

A request used to settle a previous Auth Only transaction. Basically the previous transaction is 'marked' for capture. It typically occurs at a later date than the original authorization. (Future Fulfillment Model)

Force

A request used to submit a transaction for settlement when a manual (also known as a voice) authorization is obtained. The transaction is "forced" into the next batch for capture. The voice authorization code is entered as the approval code.

Credit/Refunds

A credit does not involve real-time processing to the Host systems or the issuing bank. It is automatically placed in a status of Marked for Capture. It is processed in the next batch that is settled. Should the need arise a credit can be voided prior to settlement. This effectively cancels the credit.

Void

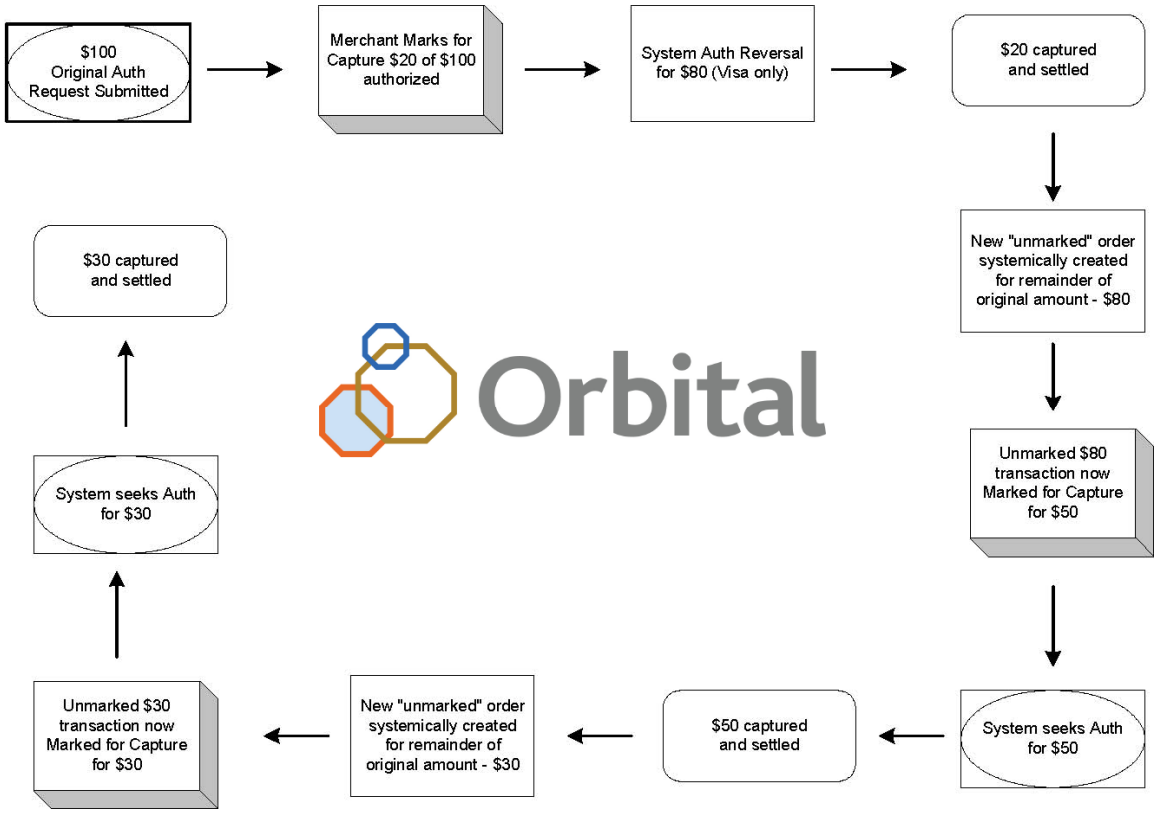
This request removes a transaction from the settlement batch. The settlement transaction is not passed forward, is not funded, and does not appear on the cardholder's account. However, since the transaction was authorized, the impact to the cardholder's "open-to-buy" line of credit remians. Once a transaction is voided, it cannot be settled or "unvoided".

Split Shipments

Split Shipments or Ship Partial allow a future fulfillment merchant to partial ship an order and settle the portion shipped. Bankcard regulations prohibit charging a consumer for goods prior to shipment. If a consumer purchases several items and multiple shipments occur on different days (back orders, etc.), then the order must be charged to the consumer in multiple increments. The ship partial transaction accommodates this situation. The original transaction can be split into multiple transactions.

Sample Split Shipment Process Flow

A shipment can be split into two or more transactions. The Orbital Virtual Terminal automatically obtains an authorization for each portion of the transaction that is Marked for Capture. The flow chart below explains the steps that occur for a split transaction.



Special Rules:

- Once a transaction is split, the first portion of the split cannot be split again; the remaining portion can be split as many times as necessary.
- The first portion of the split can be voided to cancel or postpone settlement.
- XML processing: A split transaction is initiated by performing a Mark for Capture (MFC) with an amount less then the original or remaining amount on the order.

Settlement

Settlement processing involves settlement of all transactions that are "Marked for Capture" for funding. Once settled, no additional actions can be taken on the transactions. There are three possible ways to initiate End of Day settlement.

- Auto Settle – A merchant requests and designates a time for the End of Day processing to kick off automatically.
- XML – An End of Day request is sent.
- Virtual Terminal – Click on the "Settle" command button.

Important Note: In order to meet the Host System funding windows please perform an End of Day prior to the following times:

- Salem – 8:30 PM EST
- Tampa – 4:30 AM EST

Appendix A PROCESSING SCENARIOS

Many merchants have similar processing models and similar questions regarding processing. Below are three common situations.

Authorization Exceeds Capture Amount

Merchant authorizes for $100.00 but needs to settle for $75.00.

This scenario may occur in a backorder situation or if a cardholder cancels a part of the order. The settlement transaction of $75 is submitted using the original authorization code and date. In the case of a Visa transaction, Chase Paymentech will perform a partial authorization reversal for $25.00. The value of the authorization is reduced to $75.

Capture Exceeds Authorization Amount

Merchant authorizes for $100.00 but needs to settle for $150.00.

This scenario can occur if the cardholder calls and adds an item to the order or if the shipping cost was not included in the original authorization. The merchant submits an authorization for $100 and receives an authorization code and authorization date. The value of this authorization is $100. If the cardholder subsequently adds $50 to the order the merchant should treat this as a separate order and perform a new authorization. Two capture transactions should be submitted, one for $100 and one for $50.

If the merchant treats the $150.00 as a completely new order and re-authorizes for $150, the cardholder's "open to buy" is negatively impacted. The cardholder's open line of credit is reduced by $250 ($100 + $150) rather than the correct amount of $150 ($100 + $50). Therefore this second approach is not recommended.

Please note the Orbital System rejects any attempt to settle a dollar amount higher than the authorized amount.

Authentication of Cardholder

Merchant needs to authenticate cardholder.

In some instances a merchant may want to authenticate the cardholder and credit card, but does not want to charge the card. In order to perform an authentication and not impact the cardholder's "open to buy" Currently Chase Paymentech recommends performing a $1.00 Authorization with AVS and CVN. This minimizes the impact to the cardholder's line of credit while authenticating the card. However, please note that due to new associated processing guidelines, this approach should be changed as of July 2009. Please see your account representative for details.