



USER'S GUIDE

VeriSign Payment Services

User's Guide for Payflow Pro with Fraud Protection Services



Where it all comes together.™

Copyright © 2002 - 2005 VeriSign, Inc. All rights reserved.

The information in this document belongs to VeriSign. It may not be used, reproduced or disclosed without the written approval of VeriSign.

DISCLAIMER AND LIMITATION OF LIABILITY

VeriSign, Inc. has made efforts to ensure the accuracy and completeness of the information in this document. However, VeriSign, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. VeriSign, Inc. assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained in this document.

Further, VeriSign, Inc. assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner. VeriSign Inc. reserves the right to make changes to any information herein without further notice.

TRADEMARKS

VeriSign, the VeriSign logo, VeriSign Intelligence and Control Services, VeriSign Trust Network, Go Secure!, OnSite, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Other trademarks and service marks in this document are the property of their respective owners.

This document supports **VeriSign Payment Services 5.0** and all subsequent releases unless otherwise indicated in a new edition or release notes. This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your account representative to learn more about what is available with this VeriSign product. If you need help using this product, contact customer support.

vps-support@verisign.com

1-888-883-9770

Publication date: March 2005

Summary of Revisions

VeriSign Payment Services User's Guide for Payflow Pro with Fraud Protection Services

VeriSign, Inc. 00016778/Rev. 3

The following changes were made to this document since the last version:

Throughout document	Updated document cover and page layout.
Renamed document	Changed the title from <i>Fraud Protection Services Guide</i> to <i>User's Guide for Payflow with Fraud Protection Services</i> to more accurately describe its contents.
Added new RESULT codes	Added two new RESULT codes (150 and 151) to Table 9-2 on page 86.
Added Warn feature	Integrated the Warn feature for detecting fraud in host-based transactions. See Chapter 3, "Configuring the Fraud Protection Services," Chapter 4, "Assessing Transactions that Triggered Filters," and Appendix A, "How Filters Work."
Updated Filter descriptions	Identified all basic and advanced filters that can be used in host-based transactions. See Appendix B, "Fraud Filter Reference."
Parameter name correction	Changed the parameter name SHIPTOCOUNTRY to the correct name, COUNTRYCODE.
New processor support	Added the Amex APAC and the FDMS North processing platforms. See "Processors that Support AVS" on page 104 and "Processors and Credit Cards that Support CSC" on page 106.
PNREF format	Redefined the format of a PNREF value (Payflow Pro), also referred to as a Transaction ID value (Payflow Link), to more accurately reflect the flexibility of its design to support future expansion. See "PNREF Format" on page 85.

VeriSign, Inc. 00016778/Rev. 2

The following changes were made to this document since the last revision.

Buyer Authentication Service	Instructions for activating and configuring Payflow Buyer Authentication Service appears in Chapter 5, "Activating and Configuring the Buyer Authentication Service."
Using Payflow Pro to accept or reject transactions that triggered filters	Use the Payflow Pro API to accept or reject transactions that triggered filters. See "Accepting or Rejecting Transactions That Trigger Filters" on page 73.
Reference transactions	Previous revisions of this document incorrectly stated that merchants are not charged for Reference transactions that trigger filters. Merchants are charged for such transactions
SDK and APIs	Information on downloading the Payflow Pro software development kit (SDK) (including the APIs and API documentation) appears in Chapter 7, "Screening Transactions Using the Payflow Pro SDK."



Contents

+ Summary of Revisions	iii
+ Chapter 1 Introduction	1
Fraud Protection Services	2
Enrolling and Selecting Services	2
About this Document	3
Intended Audience	3
Document Organization	3
+ Chapter 2 How Fraud Protection Services Protect You	5
The Threats	5
Protection Against the Threats—The Account and Transaction Security Tools	6
Account Tools Protect Against Hacking	6
Filters Protect Against Credit Card Fraud	6
The VeriSign Buyer Authentication Service	7
Processing Platforms that Support the Buyer Authentication Service	8
Special Considerations	8
Merchants with an Instant Fulfillment Business Model	8
Merchants using the Recurring Billing Service	8



Where it all comes together.™

Protection From System-wide Threats—The Premium Services	9
Account Monitoring Service	9
Security Audit	9
+ Chapter 3 Configuring the Fraud Protection Services	11
Configuring Security Features: Part 1: Run the Account Wizard	12
Change your VeriSign Manager Password	14
Changing Settings	14
Transaction Settings	15
Configuring Security Features: Part 2: Run the Transaction Wizard	17
+ Chapter 4 Assessing Transactions that Triggered Filters	25
Reviewing Suspicious Transactions	26
Acting on Transactions that Triggered Filters	30
Rejecting Transactions	32
Fine-tuning Filter Settings—Using the Filter Scorecard	32
Ensuring Meaningful Data on the Filter Scorecard	33
Re-running Transactions That Were Not Screened	33
+ Chapter 5 Activating and Configuring the Buyer Authentication Service	35
Enrolling for the Buyer Authentication Service	35
Downloading the Payflow Pro SDK (Including APIs and API Documentation)	35
Configuring Buyer Authentication	35
Generate Transaction Request Software	36
Test and Activate the Service	38
+ Chapter 6 Performing Buyer Authentication Transactions Using the Payflow Pro SDK	41
Testing the Buyer Authentication Service	41
Buyer Authentication Transaction Overview	42
Buyer Authentication Terminology	42

Buyer Authentication Server URLs	43
Detailed Buyer Authentication Transaction Flow . . .	43
Example Buyer Authentication Transactions	48
Example Verify Enrollment Transaction	48
Example Validate Authentication Transaction . . .	49
Example Payflow Authorization or Sale Transaction	50
Buyer Authentication Transaction Parameters and Return Values	51
Transaction Parameters	51
Verify Enrollment Transaction Name/Value Pairs	51
Validate Authentication Transaction Name/Value Pairs	54
Standard Payflow Sale or Authorization Transaction	55
ECI Values	57
Logging Transaction Information	58
Audit Trail and Transaction Logging	58
 + Chapter 7 Screening Transactions Using the Payflow Pro SDK	 61
Response Values	61
Testing Filters	61
Downloading the Payflow Pro SDK (Including APIs and API Documentation)	62
Transaction Data Required by Filters	62
Transaction Parameters Unique to the Filters	64
Existing Payflow Pro parameters Used by the Filters	65
Response Strings for Transactions that Trigger Filters	67
RESULT Values Specific to Fraud Protection Services	70
Changing the Verbosity Setting	71
Example Response for an Authentication Transaction With Verbosity=Low	71
Example Response for an Authentication Transaction With Verbosity=Medium	71
Accepting or Rejecting Transactions That Trigger Filters	73

Logging Transaction Information	73
+ Chapter 8 Viewing Buyer Authentication Reports with VeriSign Manager	75
Generating a Buyer Authentication Audit Report ...	75
Example Buyer Authentication Audit Report	77
Generating a Buyer Authentication Transaction Report	78
Example Buyer Authentication Transaction Report	79
Transaction Detail Page	81
+ Chapter 9 Responses to Credit Card Transaction Requests	83
Contents of a Response to a Credit Card Transaction Request	83
PNREF Value	84
PNREF Format	85
RESULT Codes and RESPMSG Values	85
RESULT Values for Transaction Declines or Errors	86
RESULT Values for Communications Errors ...	91
+ Appendix A How Filters Work	93
+ Appendix B Fraud Filter Reference.	97
Filters Included with the Fraud Protection Services	97
Filters Included with the Basic Fraud Protection Services Option	98
Filters Included with the Advanced Fraud Protection Services Option	98
Special Case: Buyer Authentication Failure Filter	98
About VeriSign's Risk Lists	99
VeriSign's Guidance on Interpreting Filter Results	99
Filters Applied After Processing	99
Transaction Data Required by Filters	99
Unusual Order Filters	100
Total Purchase Price Ceiling Filter	100
Total Item Ceiling Filter	100
Shipping/Billing Mismatch Filter	101
Product Watch List Filter	101

High-risk Payment Filters	102
AVS Failure Filter	102
CSC Failure Filter	105
Buyer Authentication Failure Filter	107
BIN Risk List Match Filter	109
Account Number Velocity Filter	109
High-risk Address Filters	110
ZIP Risk List Match Filter	110
Freight Forwarder Risk List Match Filter	110
USPS Address Validation Failure Filter	111
IP Address Match Filter	112
E-mail Service Provider Risk List Match Filter	112
Geo-location Failure Filter	113
IP Address Velocity Filter	114
High-risk Customer Filters	115
Bad Lists	115
International Order Filters	116
Country Risk List Match Filter	116
International Shipping/Billing Address Filter	116
International IP Address Filter	117
International AVS Filter	117
Accept Filters	118
Good Lists	118
Total Purchase Price Floor Filter	119
Custom Filters	119
+ Appendix C Testing the Transaction	
Security Filters	121
Good and Bad Lists	121
AVS Failure Filter	121
BIN Risk List Match Filter	122
Country Risk List Match Filter	122
E-mail Service Provider Risk List Match Filter	123
Freight Forwarder Risk List Match Filter	124
Geo-location Failure Filter	124
International AVS Filter	125
International IP Address Filter	126
International Shipping/Billing Address Filter	126

IP Address Match Filter	127
Shipping/Billing Mismatch Filter	127
Total Item Ceiling Filter	128
Total Purchase Price Ceiling Filter	129
Total Purchase Price Floor Filter	129
USPS Address Validation Failure Filter	130
ZIP Risk List Match Filter	130
+ Appendix D Testing Buyer Authentication Transactions Using the Payflow Pro SDK	133
Testing Buyer Authentication Transactions	133
Buyer Authentication Test Server	133
Payflow Pro Test Server	133
Test Case Descriptions and Account Numbers . . .	134
Test Cases	134
Expected Result Codes for Buyer Authentication .	135
Buyer Authentication Testing Procedures	137
Verify Enrollment Transaction Test Cases	137
Example Return Values	137
Validate Authentication Transaction Test Cases	139
Procedure	139
Example Return Values	141
+ Appendix E Deactivating Fraud Protection Services	143
+ Index	145



Introduction

Online fraud is a serious and growing problem, one that cost merchants over \$2 *billion* in 2005.

While liability for fraudulent card-present or in-store transactions lies with the credit card issuer, liability for card-not-present transactions, including transactions conducted online, *falls to the merchant*. As you probably know, this means that a merchant that accepts a fraudulent online transaction (even if the transaction is approved by the issuer) does not receive payment for the transaction and additionally must often pay penalty fees and higher transaction rates. (One notable exception, Buyer Authentication, is described in this document.)

VeriSign's Fraud Protection Services, in conjunction with your Payflow service's standard security tools, can help you to significantly reduce these costs and the resulting damage to your business.

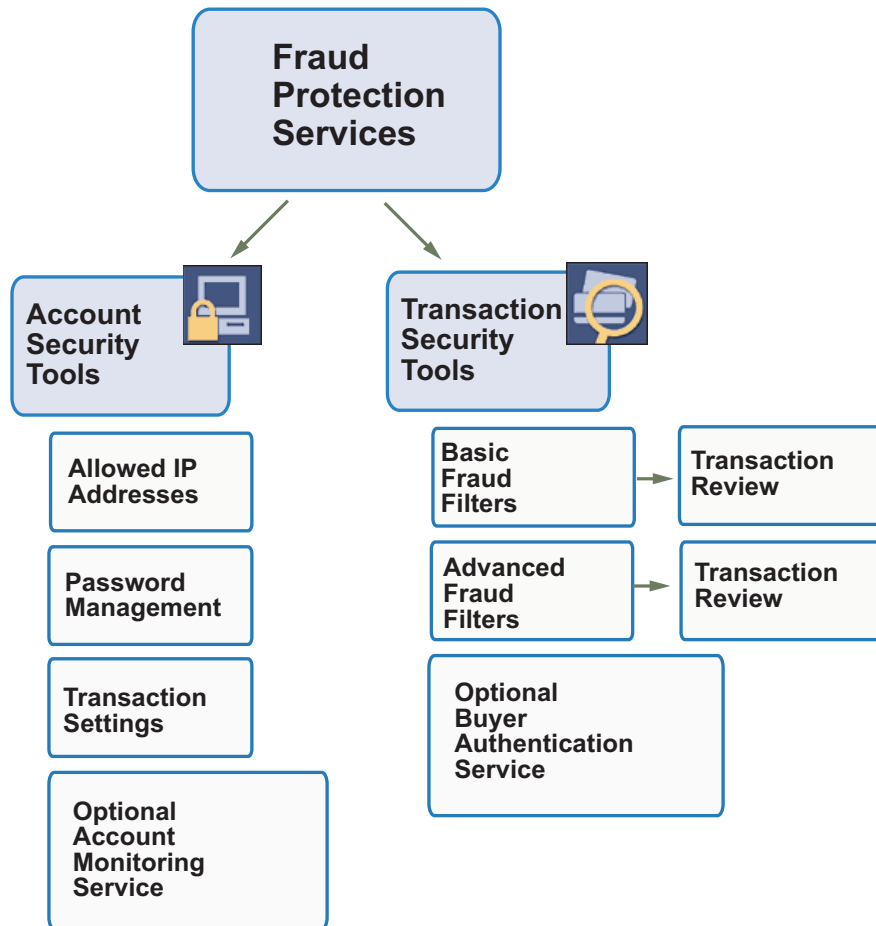
Note Merchants must meet the following eligibility requirements to enroll with and use the Fraud Protection Services products:

- Merchant must have a current, paid-up VeriSign Payflow Pro gateway service account.
- Merchant gateway service account must be activated (in Live mode).
- Merchant must have its business operations physically based in the United States of America.
- Merchant must use one of the following terminal-based processing platforms: American Express Phoenix, FDMS Nashville, FDMS South, Global Payments East, Nova, Paymentech New Hampshire, or Vital.

Fraud Protection Services

Enrolling and Selecting Services

To enroll for Fraud Protection Services, click the banner on VeriSign Manager's *Welcome* page and follow the on-screen instructions. The following services make up the Fraud Protection Services suite. To help you decide on the services that best meet your needs, the online enrollment pages describe each service.



About this Document

Intended Audience

This document is intended for Payflow Pro merchants who subscribe to any Fraud Protection Services options.

Note In this document, we use the term *fraudster* to represent an entity (typically a person) attempting fraudulent activity.

Document Organization

Chapter 2, “How Fraud Protection Services Protect You,” describes the security tools that make up the Fraud Protection Services.

Chapter 3, “Configuring the Fraud Protection Services,” describes the process of configuring all aspects of security management for your Payflow account.

Chapter 4, “Assessing Transactions that Triggered Filters,” describes how to review transactions that triggered filters, and provides guidance on deciding on risk.

Chapter 5, “Activating and Configuring the Buyer Authentication Service,” describes the process of activating and configuring Buyer Authentication transactions.

Chapter 6, “Performing Buyer Authentication Transactions Using the Payflow Pro SDK,” describes the process of performing Buyer Authentication transactions using the Payflow Pro SDK.

Chapter 7, “Screening Transactions Using the Payflow Pro SDK,” describes how to screen transactions for fraud using the Payflow Pro SDK.

Chapter 8, “Viewing Buyer Authentication Reports with VeriSign Manager,” describes how to generate and interpret Buyer Authentication reports.

Chapter 9, “Responses to Credit Card Transaction Requests,” describes the responses to a credit card transaction request.

Appendix A, “How Filters Work,” describes the order in which the various types of filter are applied.

Appendix B, “Fraud Filter Reference,” describes the Transaction filters that make up part of the VeriSign Fraud Protection Services.

Appendix C, “Testing the Transaction Security Filters,” provides Payflow Pro transactions that you can use to test the filters.

Appendix D, “Testing Buyer Authentication Transactions Using the Payflow Pro SDK,” provides Payflow Pro transactions that you can use to test the Buyer Authentication Service.

Appendix E, “Deactivating Fraud Protection Services,” describes the process of deactivating Fraud Protection Services.



How Fraud Protection Services Protect You

This chapter describes the security tools that make up the Fraud Protection Services.

In This Chapter

The Threats on page 5

Protection Against the Threats—The Account and Transaction Security Tools on page 6

The VeriSign Buyer Authentication Service on page 7

Special Considerations on page 8

Protection From System-wide Threats—The Premium Services on page 9

The Threats

There are two major types of fraud—hacking and credit card fraud.

Hacking. Fraudsters *hack* when they illegally access your customer database to steal card information or to take over your gateway account to run unauthorized transactions (purchases and credits). The Account Wizard features minimize the risk of hacking by enabling you to place powerful constraints on access to and use of your VeriSign Manager and Payflow accounts.

Credit Card Fraud. Fraudsters can use stolen or false credit card information to perform purchases at your Web site, masking their identity to make recovery of your goods or services impossible. To protect you against credit card fraud, Fraud Protection Services uses software *filters* that identify potentially fraudulent activity and let you decide whether to accept or reject the suspicious transactions.

Protection Against the Threats—The Account and Transaction Security Tools

Account Tools Protect Against Hacking

The Account Wizard takes you through configuration of the tools that shut down hackers:

- + On the **Allowed IP Addresses** page, you specify that all VeriSign Manager users must log in from computers that you identify by IP address. This security measure ensures that no one can log in from an unauthorized computer. In addition, Payflow Pro users can require that all transaction activity can originate only from authorized computers by specifying those IP Addresses.
- + On the **Transaction Settings** page, you specify rules governing administratively performed transactions. For example, you can require that credits can be issued only for existing transactions.
- + On the **Password Management** pages, you specify a password for access to VeriSign Manager and a separate password for Payflow Pro transactions. Use the password management pages to change the passwords frequently (VeriSign recommends once monthly).

Filters Protect Against Credit Card Fraud

The configurable filters screen each transaction for evidence of potentially fraudulent activity. When a filter identifies a suspicious transaction, the transaction is marked for review.

VeriSign Fraud Protection Services offers two levels of filters: Basic and Advanced. The filters are described in Appendix B, “Fraud Filter Reference.”

For detailed descriptions of the filter levels, the order and logic of the screening process, and for specific variations from the simple flow described here, see Appendix A, “How Filters Work.”

Example Filter

The Total Purchase Price Ceiling filter compares the total amount of the transaction to a maximum purchase amount (the ceiling) that you specify. Any transaction amount that exceeds the specified ceiling triggers the filter.

Configuring the Filters

You configure each filter by specifying the action to take whenever the filter identifies a suspicious transaction (either set the transaction aside for review or reject it). Typically, you specify setting the transaction aside for review. For transactions that

you deem extremely risky (for example, a known bad e-mail address), you might specify rejecting the transaction outright. You can turn off any filter so that it does not screen transactions.

For some filters, you also set the value that triggers the filter—for example the dollar amount of the ceiling price in the Total Purchase Price Ceiling filter.

Some filters are designed to automatically accept transactions that meet specific criteria, like a known good customer's account number that you specify.

The Transaction Wizard simplifies configuration by taking you through a step-by-step process. Chapter 3, “Configuring the Fraud Protection Services,” describes the process.

Reviewing Suspicious Transactions

As part of the task of minimizing the risk of fraud, you review each transaction that triggered a filter to determine whether to accept or reject the transaction. Chapter 4, “Assessing Transactions that Triggered Filters,” describes the process.

The VeriSign Buyer Authentication Service

VeriSign's Buyer Authentication Service integrates Visa's *Verified by Visa* and MasterCard's *SecureCode* into secure calls to the VeriSign-hosted Payflow service. These services prompt buyers to provide a password to their card issuer before being allowed to execute a credit card purchase.

Buyer Authentication is the only screening tool that promises to shift fraud liability from the merchant. The Buyer Authentication password is the digital equivalent to a shopper's handwritten signature. The use of the password protects merchants from some chargebacks when a customer claims not to have authorized the purchase.

The Buyer Authentication Service is a separately-purchased option and operates with the Buyer Authentication Failure filter. To enroll for the Buyer Authentication Service, click the Buyer Authentication banner on the VeriSign Manager *Security* welcome page. Follow the on-screen instructions. (In particular, both your processor and your acquiring bank must support buyer authentication. If they both support the service, then you can enroll for VeriSign's Buyer Authentication Service.)

Processing Platforms that Support the Buyer Authentication Service

The following processing platforms support the Buyer Authentication Service:

MasterCard Certified Processing Platforms

FDMS Nashville

Global Payments-East

Global Payments-Central

Paymentech New Hampshire

Vital

Visa Certified Processing Platforms

FDC South

FDMS Nashville

Paymentech New Hampshire

Vital

Special Considerations

Merchants with an Instant Fulfillment Business Model

For businesses with instant fulfillment business models (for example, software or digital goods businesses), the **Review** option does not apply to your business—you do not have a period of delay to review transactions before fulfillment to customers. Only the **Reject** and **Accept** options are applicable to your business model.

In the event of server outage, Fraud Protection Services is designed to queue transactions for online processing. This feature also complicates an instant fulfillment business model.

Merchants using the Recurring Billing Service

To avoid charging you to filter recurring transactions that you know are reliable, Fraud Protection Services filters do not screen recurring transactions.

To screen a prospective recurring billing customer, submit the transaction data using VeriSign Manager's *Manual Transactions* page. The filters screen the transaction in the normal manner. If the transaction triggers a filter, then you can follow the normal process to review the filter results.

Protection From System-wide Threats—The Premium Services

Account Monitoring Service

The Account Monitoring Service provides premium protection against unauthorized use of your Payflow account. VeriSign Account Monitoring Service includes:

- + Transaction monitoring by trained VeriSign security professionals who identify fraudulent account activity *prior to settlement*.
- + Proactive notification of suspicious account events
- + Call-in number to security representatives to discuss suspicious account activity
- + Complete investigation and research of suspicious account events. Includes:
 - Investigation of VeriSign internet log files and all audit trails relevant to your account
 - Packaging of all relevant data to be delivered to banks and law enforcement to assist in funds recovery and prosecution

Security Audit

Determine whether your e-commerce site is secure from hackers with a free one-time online security scan from Qualys, a VeriSign partner. Qualys's web-based security auditing service determines whether your e-commerce site can withstand hacker attacks. The audit requires just minutes as it non-intrusively tests for thousands of known vulnerabilities.

Scan results provide a complete view of your site's security in detailed browser-based reports that rank the severity of weak spots and link you to verified fixes. To request a free scan, see the Security section of VeriSign Manager.



CHAPTER 3

Configuring the Fraud Protection Services

This chapter describes the process of running the Account Wizard and the Transaction Wizard to configure all aspects of security management for your Payflow accounts.

Configuring Security Features: Part 1: Run the Account Wizard

Step 1 Configuring Allowed IP Addresses for VeriSign Manager

You can require that users access Payflow services only from computers that you have authorized—access from any other computer is denied. You designate the computers by specifying their IP addresses on the *Allowed IP Addresses* page.

- 1 Click **Security** → **Account Setup** → **Account Wizard**. The Welcome page opens. Read the instructions and click **Continue**. The *Allowed IP Addresses for VeriSign Manager* page opens.

The screenshot shows the 'Account Wizard' window with a title bar and a question mark icon. Below the title bar, there are three tabs: '1. Allowed IP Addresses' (selected), '2. Password Management', and '3. Transaction Settings'. The main content area has a dark blue header with the text 'Allowed IP Addresses for VeriSign Manager'. Below this, there is instructional text: 'You can limit access to your VeriSign Manager account to authorized computers only—access from any other computer is denied. Designate the authorized computers by specifying their IP addresses on this page.' and a note: 'Not all IP addresses identify a unique computer or user (to learn more, click [here](#)).' Below the text, it says 'Specify up to 16 authorized IP addresses:'. There are two columns of IP address input fields, labeled 'IP 1:' through 'IP 8:' on the left and 'IP 9:' through 'IP 16:' on the right. Each field is a small box with a dot separator. At the bottom, there are three buttons: '< Back', 'Cancel', and 'Save and Continue >'. A red 'WHAT DO I DO?' button is located in the top left corner of the window.

- 2 Read the instructions and enter the authorized IP addresses. Click the **What Do I Do** button for help in determining the appropriate IP addresses and in formatting the addresses properly. In particular, the help text describes what to do if you use a dial-up connection with possibly dynamic IP address.
- 3 Click **Save and Continue**.
- 4 A similar page appears that enables you to specify up to 16 IP addresses from which persons can submit Payflow Pro transactions. Enter the authorized IP addresses and click **Save and Continue**.

Step 2 Managing your Passwords

VeriSign strongly recommends that you create two separate passwords: a password that enables access to your VeriSign Manager account and a different password used to submit Payflow Pro transactions.

In the first of the Wizard's password management pages, you change the password that currently serves for both your VeriSign Manager account and for Payflow Pro transactions. In the next Wizard page, you optionally create a new VeriSign Manager account password. If you decide to take this option, your new Payflow Pro password remains as set in the first page, and you have a separate, new password to control access to your VeriSign Manager account.

CAUTION **Payflow Pro customers with a single password for both VeriSign Manager and Payflow Pro:** Changing your password affects both Manager and Payflow Pro processing. If you change the password, then the new password will work the next time you log into VeriSign Manager, and will work immediately for Payflow Pro transactions.

You must also change your Payflow Pro shopping cart or transaction script to use the new password. If not, then your Payflow Pro transactions will begin to fail within the next hour.

Follow this procedure:

Account Wizard

1. Allowed IP Addresses 2. Password Management 3. Transaction Settings

Password Management - Change Passwords

To ensure that Payflow Pro transactions (Payflow Pro API calls) can originate only from authorized computers, specify their IP addresses on this page.

Not all IP addresses identify a unique computer or user (to learn more, click [here](#)).

If you do not wish to change your password(s) at this time, click **Skip**.

Manager/Payflow Pro Password

Note: The password change takes effect immediately for all Payflow Pro transactions.

If you change your Payflow Pro password, then you must also update your Payflow Pro shopping cart or transaction script to use the new password. If you do not update the the shopping cart or transaction script, then Payflow Pro transactions will begin to fail within the next hour.

Old Password:

New Password:

Confirm Password:

< Back Cancel Save and Continue > Skip >

In the **Old Password** field, type your current password.

In the **New Password** field, type the new password.

In the **Confirm Password** field, retype the new password.

Click **Submit**.

VeriSign strongly recommends that you regularly change your passwords. Follow these guidelines when creating a password:

- The password must be 6 to 32 characters long.
- The password must contain a mix of letters, numbers, and/or special characters. Passwords containing only letters or only numbers are not accepted.
- The password is case-sensitive.
- Single quotes, double quotes, ampersands (" &), and spaces are not allowed.
- Successive passwords should not follow a pattern.
- The password cannot be the same as your Merchant Login name and should not contain any part of your company name or user name.
- Do not post or share your password or send your password to others by e-mail.

Change your VeriSign Manager Password

The next Wizard step enables you to change the password used to access your VeriSign Manager account. Follow the same process to create a new password for VeriSign Manager. As a result, you have one password for access to your VeriSign Manager account and a different password for Payflow Pro transactions.

Changing Settings

To change an IP address setting, click **Security → Account Setup → Allowed IPs**.

To change a password, click **Security → Account Setup → Password Management**.

Step 3 Configuring Transaction Settings

Use the *Transaction Settings* page to specify restrictions on transactions from either the Payflow Pro or VeriSign Manager service. These restrictions make hacking fraud extremely difficult.

Note The *Transaction Settings* differ from the filters in that they restrict operations performed by administrative account users (VeriSign Manager users) whereas the filters restrict incoming customer transactions.

The **Maximum amount per transaction** setting is the only exception. It places a limit on all transactions—both those initiated by a VeriSign Manager user and incoming customer transactions.

To enhance security for your account by preventing unauthorized changes to the settings on the *Transaction Settings* page, the page is handled in a special way:

- + The *Transaction Settings* page is freely available for accounts in Test mode. Use the instructions in this section to determine your preferred transaction settings.
- + When you move your account to Live mode, the transaction settings that you set in Test mode are applied to your account, and VeriSign removes the *Transaction Settings* page from the VeriSign Manager interface.

To make further changes to the settings, your authorized contact person must contact VeriSign Payment Services Customer Support at 1-888-883-9770 or **vps-support@verisign.com**. The Customer Support group then reactivates the *Transaction Settings* page in VeriSign Manager so that you can alter the settings.

Once you submit the settings, you will again no longer be able to view or edit them using VeriSign Manager. To alter the settings after you submit them, you must again contact Customer Support.

Transaction Settings

- + **Maximum amount per transaction:** Any **Authorization, Sale, Credit, Delayed Capture,** or **Voice Authorization** transaction greater than the amount that you specify is declined.

Leave the field blank to allow any transaction amount up to the limit established by the processor or acquirer.

IMPORTANT! The *Maximum amount per transaction* setting controls all transactions, even those with amounts less than specified for the *Total Purchase Price Ceiling* filter (page 100).

If the amount of a transaction is higher than the filter ceiling setting, but lower than the *Maximum amount per transaction* setting, then the transaction triggers the filter and is not affected by the *Maximum amount* setting.

If the amount of a transaction is greater than the *Maximum amount per transaction* setting, then the transaction is automatically rejected, regardless of the filter settings.

- + **Maximum amount for credits:** Any **Credit** transaction greater than the amount that you specify is declined.

A setting of **0** (zero) disables Credit transactions for the account.

- + **Allow non-referenced credits:** Specify **No** (the setting recommended by VeriSign) to permit Credits only against existing Sale, Delayed Capture, and Void transactions. With this setting, you can submit a Credit transaction by providing the Transaction ID (PNREF) of the original transaction that is to be credited against. You do not need to supply the credit card number.

Specify **Yes** to allow a Credit transaction to be submitted to any credit card account that you specify. With this setting, you must provide a credit card number to submit a Credit transaction. Take special care with this setting—non-referenced credits make it easier for employees to commit fraud.

Note If you specify **Yes** for this option, then you cannot specify **No** for the **Credits may exceed original transaction amount** option.

- + **Credits may exceed original transaction amount:** Specify **No** (recommended by VeriSign) to require that the accumulated credit amount against this transaction may not exceed the original transaction amount—the credit can be for any amount up to the original transaction amount. Specify **Yes** to allow any credit amount up to the limit established by the processor or acquirer. Take special care with this setting—unlimited credit amounts make it easier for employees to commit fraud.

Note If you specify **No** for this option, then you cannot specify **Yes** for the **Allow Non-referenced Credits** option.

- + **Allow Reference Transactions:** Specify whether to allow the use of an existing transaction as a starting point from which to generate a new Sale or Authorization transaction. By default, Reference transactions are not allowed.

For example, if you select **Yes**, then VeriSign Manager users can generate a new Sale or Authorization transaction from a specified original transaction. The user can modify any aspect of the transaction, including the amount, before submitting the new transaction. Reference transactions are fully described in *Payflow Pro Developer's Guide*.

Select **No** to disallow the use of Reference transactions.

Configuring Security Features: Part 2: Run the Transaction Wizard

VeriSign designed the Transaction tools to enable you to implement transaction security in phases. You first make and fine-tune filter settings in a **Test** environment. Then you move to a **Live** transaction environment to fine-tune operation in an **Observe**-only mode. Finally, when you are fully satisfied with your settings, you move to **Active** mode to begin screening all live transactions for fraud.

Filter operation is fully described in Appendix B, “Fraud Filter Reference.”

IMPORTANT! Upon completing the configuration procedures within each of these major phases described below, you must click the **Deploy** button to deploy the filter settings. Filter settings take effect only after you deploy them.

VeriSign updates filter setting changes hourly (roughly on the hour). This means that you might have to wait up to an hour for your changes to take effect.

Phase 1: Run test transactions using test Transaction servers

In the **Test** phase of implementation, you configure filter settings for test servers that do not affect the normal flow of transactions. You then run test transactions against the filters and review the results offline to determine whether the integration was successful. Once you are happy with the filter settings, you move to the next phase

and the settings that you decided upon in the Test phase are transferred to the live servers.

Phase 2: Run live transactions on live Transaction Security servers using the Observe mode

When you deploy to **Observe** mode, the settings that you decided upon in the Test phase are automatically transferred to the live servers.

In Observe mode, the filters examine each live transaction and mark the transaction with each triggered filter's action. You can then view the actions that would have been taken on the live transactions had the filters been active. Regardless of the filter actions, all transactions are submitted for processing in the normal fashion.

Phase 3: Run live transactions on live Transaction Security servers using the Active mode. Once you have set all filters to the optimum settings, you deploy the filters to **Active** mode. In Active mode, filters on the live servers examine each live transaction and take the specified action when triggered.

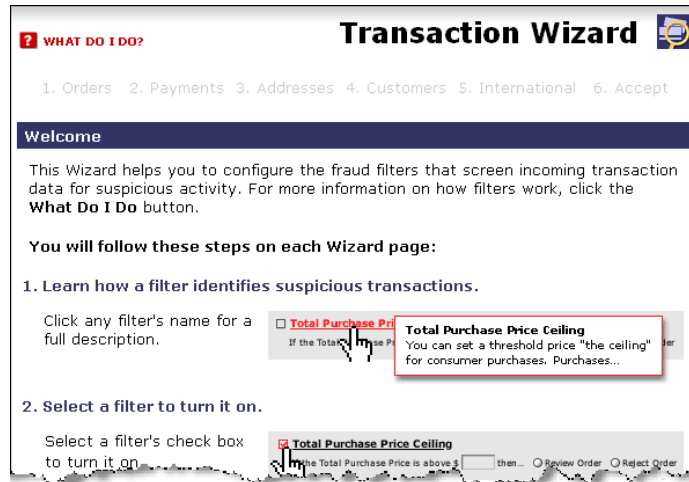
Tip Remember that you can test a new filter setting using the Test servers at any time (even if your account is in Active mode), and then, if desired, make an adjustment to the live filter settings.

Phase 1: Run test transactions against filter settings on test Transaction Security servers

In this phase of implementation, you configure filter settings for test servers that do not affect the normal flow of transactions. You then run test transactions against the filters and review the results offline to determine whether the integration was successful. Continue modifying and testing filters as required.

Tip There is no per-transaction fee when you use the test servers.

- 1 Click **Security** → **Test Setup** → **Transaction Wizard**. The *Transaction Wizard Welcome* page opens.



- 2 Move through each wizard page, following the on-screen instructions. At any time, click the **What Do I Do** button for instructions, or click a filter name to read a full description of the filter. Each filter is also described in Appendix B, “Fraud Filter Reference.”

For each filter, you:

- Turn the filter **ON** (enable it) or **OFF** (disable it).
- Specify the action that the filter should take when it is triggered.
- For some filters, you set the trigger value (for example, for the Price Ceiling filter, the trigger value is the transaction amount that causes the filter to set a transaction aside).

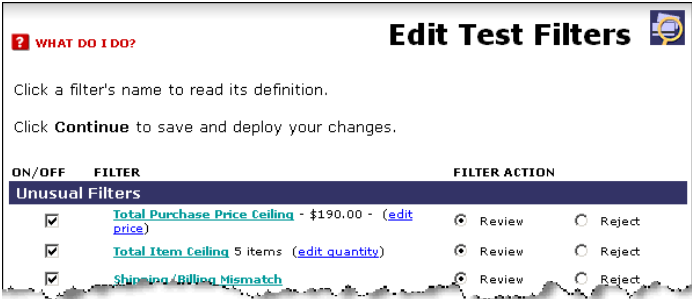
Note If you have not enrolled for the Buyer Authentication Service, then the Buyer Authentication Failure filter is grayed-out and you cannot configure it.

Items that you enter in the Test **Good**, **Bad**, or **Product Watch** lists are not carried over to your configuration for the Live servers, so do not spend time entering a complete list for the Test configuration.

- 3 Once you complete the wizard pages, click **Test** on the *Filter Deployment Test/Live* page.

IMPORTANT! If you do not deploy the filters by clicking **Test**, then your settings are not saved.

- 4 The *Required Data Fields* page displays the list of transaction data values that you must submit with each transaction. You may want to print this page. If a particular value is not submitted, then each filter that could not screen the transaction appears in the *Unused Filters* section of *Transaction Details* page (described in “Acting on Transactions that Triggered Filters” on page 30).
- 5 All filters are now configured, and you can begin testing the settings by running test transactions. Follow the procedures outlined in Appendix C, “Testing the Transaction Security Filters.” Review the filter results by following the instructions in “Reviewing Suspicious Transactions” on page 26.
- 6 Based on your results, you may want to make changes to the filter settings. Click **Security → Test Setup → Edit Filters** to open the *Edit Test Filters* page. You can change any filter setting on this page.



- 7 Once you are happy with your filter settings, you can move to Phase 2.

Phase 2: Run live transactions on live transaction servers using the Observe mode

In this phase of the implementation, you configure filters on live servers to the settings that you had fine-tuned on the test servers. In Observe mode, filters examine each live transaction and mark the transaction with the filter results. The important difference from Active mode is that, regardless of the filter actions, all transactions are submitted for processing in the normal fashion.

Observe mode enables you to view filter actions offline to assess their impact (given current settings) on your actual transaction stream.

Note You are charged the per-transaction fee to use the live servers in either Observe or Active mode.

- 1 Click **Security** → **Live Setup** → **Edit Filters**. The *Edit Filters* page opens. Remember that in this phase, you are configuring the live servers.
- 2 Make any needed changes from the Phase 1 settings.
- 3 Click **Continue** on the *Edit Live Filters* page and on the *Required Filter Data* page.

- 4 The *Filter Deployment* page prompts whether to deploy the filters in **Observe** mode or in **Active** mode. Click **Deploy Observe Mode**.

Filter Deployment

WHAT DO I DO?

You are currently in Observe Mode

Specify whether to deploy the filters in Observe Mode or in Active Mode. **Your Live Filter settings will not be saved until you specify Observe or Active.** In Active Mode, the service will begin Accepting, Rejecting and pending transactions for Review. Before continuing, we strongly recommend that you click the "What Do I Do" button to learn more about how Observe and Live Mode will impact your transactions.

Please note that your Observe/Active mode change can take up to 60 minutes to deploy.

Observe Mode	Active Mode
Observe mode gives you the opportunity to see how filters would impact your transactions without actually taking Accept, Reject or Review action. In Observe mode, every transaction is screened by the filters but no action is taken (transactions are not rejected, accepted, or set aside for review). Instead, transactions that trigger filters are marked as Observed .	Once Active mode is fully deployed, the filters that you have turned on immediately begin screening transactions and taking action when appropriate. Transactions will be rejected, accepted, or set aside for review as specified in the filter.
Deploy Observe Mode	Deploy Active Mode

Cancel

Once you deploy the filters, all transactions are sent to the live servers for screening by the live filters. In **Observe** mode, each transaction is marked with the filter action that would have occurred (Review, Reject, or Accept) had you set the filters to **Active** mode.

This enables you to monitor (without disturbing the flow of transactions) how actual customer transactions would have been affected by active filters. View the *Review Transactions* page to review filter performance.

IMPORTANT! VeriSign updates deployed filter setting changes hourly (roughly on the hour). This means that you might have to wait up to an hour for your changes to take effect.

- 5 The *Required Data Fields* page displays the list of transaction data elements that you must submit with each transaction. You may want to print this page. If a particular transaction data value is not submitted, then each filter that could not screen the transaction appears in the *Unprocessed Filters* section of *Transaction Details* page (described in “Acting on Transactions that Triggered Filters” on page 30).

- 6 Perform testing as in Step on page 18. The Filter Scorecard (described on page 32) will be particularly helpful in isolating filter performance that you should monitor closely and in ensuring that a filter setting is not set so strictly so as to disrupt normal business.
- 7 Once you are happy with your filter settings, you can move to Phase 3.

Phase 3: Run all transactions through the live Transaction Security servers using the Active mode

Once you have configured all filters to optimum settings, you convert to **Active** mode. Filters on the live servers examine each live transaction and take the specified action.

- 1 Click **Security** → **Live Setup** → **Edit Filters**. The *Edit Live Filters* page opens.
- 2 Click **Continue** on the *Edit Live Filters* page and on the *Required Filter Data* page.
- 3 On the *Filter Deployment* page, click **Deploy Active Mode**.

At the top of the next hour, all live transactions will be inspected by the filters.

- 4 Use the instructions in Chapter 4, “Assessing Transactions that Triggered Filters,” to detect and fight fraud.

IMPORTANT! Remember that you can make changes to fine-tune filter settings at any time. After changing a setting, you must re-deploy the filters so that the changes take effect.



Assessing Transactions that Triggered Filters

As part of the task of minimizing the risk of fraud, you review each transaction that triggered a filter. You decide, based on the transaction's risk profile, whether to accept or reject the transaction. This chapter describes how to review transactions that triggered filters, and provides guidance on deciding on risk.

Note The Fraud Protection Services package (Basic or Advanced) to which you subscribe determines the number of filters that screen your transactions. Basic subscribers have access to a subset of the filters discussed in this chapter. Advanced subscribers have full access. See “Filters Included with the Fraud Protection Services” on page 97 for complete lists of Basic and Advanced filters.

In This Chapter

Reviewing Suspicious Transactions on page 26

Fine-tuning Filter Settings—Using the Filter Scorecard on page 32

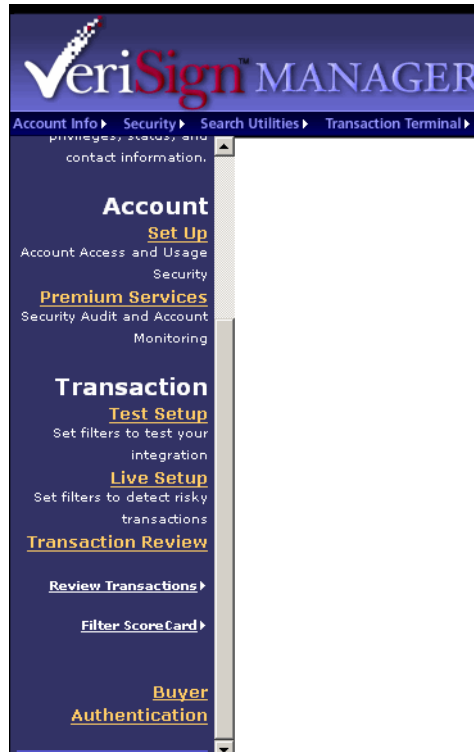
Re-running Transactions That Were Not Screened on page 33

Reviewing Suspicious Transactions

Transactions that trigger filters might or might not represent attempted fraud. It is your responsibility to analyze the transaction data and then to decide whether to accept or reject the transaction.

The first step in reviewing filtered transactions is to list the transactions:

- 1 Click **Security** → **Transaction Review** → **Review Transactions**.



The *Review Transactions* page opens.

WHAT DO I DO?

Review Transactions

Use this page to generate a list of transactions that occurred during the date range that you specify.

You can specify transactions that the filters rejected, accepted, or set aside for review. Alternatively, you can generate lists of transactions that either were or were not screened by filters.

Filtered Transactions

☐ Preset Time: Today (Wed Jul 21, 2004)
 ☒ Custom Time:
 From:
 March 21 2004
 Time: 00:00:00
 To:
 April 21 2003
 Time: 23:59:59
 Time Zone: Pacific Time (US, Canada); Tijuana

Transaction Type: Reject
 Mode: Review Test Transactions


Submit Reset

- 2 Specify the date range of the transactions to review.
- 3 Specify a **Transaction Type**:


Transaction Type	Description
Reject	Transactions that the filters rejected. These transactions cannot be settled. The type of filter that took this action is called a <i>Reject filter</i> .
Review	Transactions that the filters set aside for your review. The type of filter that took this action is called a <i>Review filter</i> .
Accept	Transactions that the filters allowed through the normal transaction submission process. The type of filter that took this action is called an <i>Accept filter</i> .
Not Screened by Filters	Transactions that were not screened by any filter. This condition (Result Code 127) indicates that an internal server error prevented the filters from examining transactions. You can re-screen any of these transactions through the filters as described in "Re-running Transactions That Were Not Screened" on page 33.
Screened by Filters	All transactions that were screened by filters, regardless of filter action or whether any filter was triggered.

- 4 Specify transactions screened by the **Live** or the **Test** servers, and click **Submit**.

The *Transaction Review* page displays all transactions that meet your search criteria (in this example, transactions that filters set aside for review).


WHAT DO I DO?

Transaction Summary



Click on a transaction ID below to see detailed information on which filters applied to this transaction.

Filtered Test Transactions

for

Fri Feb 07, 2003 00:00:00

to

Fri Mar 07, 2003 23:59:59

Transaction ID	Time	Type	Tender Type	Amount	Deployment Mode
1 VTHA55651739	March 07, 2003 15:12:59	Review	MasterCard	1.00	Test
2 V64A09482823	March 06, 2003 21:02:33	Review	Visa	2.00	Test
3 VTHA55651651	March 06, 2003 21:02:11	Review	Visa	2.00	Test

Note If filters are deployed in Observe mode, then all transactions have been submitted for processing and are ready to settle. Transactions are marked with the action that the filter would have taken had the filters been deployed in Active mode.

The following information appears in the report

Heading	Description
Transaction ID	Unique transaction identifier. Click this value to view the <i>Transaction Detail</i> page.
Time	Time and date that the transaction occurred.
Type	The transaction status that resulted from filter action, as described in Table 4-1 on page 29.
Tender Type	MasterCard or Visa
Amount	Amount of the transaction
Deployment Mode	Test, Observe, or Active

The following transaction status values can appear in the report:

Table 4-1 Transaction status values

Stage of Review	Transaction Status	Result Code	Result Message	Report in Which the Transaction Appears
Screened by filters	Pass	0	Approved	Approved report
Screened by filters	Review	126	Under Review by Fraud Service	Approved report
Screened by filters	Reject	125	Declined by Fraud Service	Declined report
Screened by filters	Accept	0	Approved	Approved report
Screened by filters	Service Outage	127	Unprocessed by Fraud Service	Approved report

Table 4-1 Transaction status values

After review by merchant	Accepted	0	Approved	Approved report
	Rejected	128	Declined by Merchant	Declined report

Click the **Transaction ID** of the transaction of interest.

The *Transaction Details* page opens, as discussed in the next section.

Acting on Transactions that Triggered Filters

The *Transaction Details* page displays the data submitted for a single transaction. The data is organized to help you to assess the risk types and to take action (accept, reject, or continue in the review state). As shown in the example on page 31, data that triggers a filter is marked by a link that displays the filter description.

Note The *Transaction Details* page associated with filters differs from the *Transaction Details* page associated with standard VeriSign Manager reports. The standard page shows the status of a transaction that has been submitted for processing. The *Transaction Details* page associated with filters shows the status of a transaction that triggered a filter.

Click the **What Do I Do** button to read VeriSign's recommendations for reviewing and acting on filtered transactions. You may wish to print these recommendations.

Transaction Details

Review the results, add notes, select Review, Reject or Accept and then click **Save Changes**.

LIVE Order: [VFHA28796745](#) **PLACED:** 03/10/04

Customer Contact	Triggered Filters		
Customer Name: Gian Paolo Torloni Email Address: gptorloni@buyer.com Phone Number: 201-555-1212			
Order Information	Triggered Filters		
Total Purchase Price: \$9,199.23 Total Items: 17 Product SKU: SKU58493802	Total Purchase Price Ceiling		
Payment Information	Triggered Filters		
Account Number: xxxxxxxxxxxx5100 AVS Street: Y AVS Zip: Y CSC: International AVS: N Buyer Authentication: Not submitted			
Address Information	Triggered Filters		
<table border="0"> <tr> <td>Bill To: Gian Paolo Torloni 12345 Maple Leaf Lane Bilright, MO 75432</td> <td>Ship To: Lucia Angela Messina 23456 Acorn Lane Putrite, MO 75432</td> </tr> </table>	Bill To: Gian Paolo Torloni 12345 Maple Leaf Lane Bilright, MO 75432	Ship To: Lucia Angela Messina 23456 Acorn Lane Putrite, MO 75432	Billing: Shipping/Billing Mismatch Filter Shipping: Shipping/Billing Mismatch Filter USPS Address Validation Failure
Bill To: Gian Paolo Torloni 12345 Maple Leaf Lane Bilright, MO 75432	Ship To: Lucia Angela Messina 23456 Acorn Lane Putrite, MO 75432		
IP Address: 255.255.255.255			
Skipped Filters - Data required for these filters was not provided			
CSC Failure International IP Address			

☒ REVIEW
 ☐ REJECT
 ☐ ACCEPT

Notes: Do not use the &, =, < or > characters.

Cancel Save Changes

This transaction was set aside because it triggered the **Total Purchase Price Ceiling** filter—(\$9,199.23 exceeds the ceiling that you configured for the filter). Other filters were also triggered. Click a link to view the filter description.

The transaction was not screened by any of the filters listed in the **Skipped Filters** section because data required by these filters did not appear in the transaction data or was badly formatted. In special cases, all filters appear here. See “Re-running Transactions That Were Not Screened” on page 33

Specify the action to take on the transaction:

- **Review:** Take no action. You can return to this page at any time to reject or accept the transaction. The transaction remains unsettled.
- **Reject:** Do not submit the transaction for processing. See “Rejecting Transactions” on page 32.
- **Accept:** Submit the transaction for normal processing.

You can enter notes here regarding the disposition of the transaction or the reasons for taking a particular action. Do not use the & < > or = characters.

Click **Save Changes** to save the notes, apply the action, and move to the next transaction.

Tip You can also view the *Transaction Details* page for transactions that were rejected or accepted. While you cannot change the status of such transactions, the page provides insight into filter performance.

Rejecting Transactions

If you decide to reject a transaction, you should notify the customer that you could not fulfill the order. Do not be explicit in describing the difficulty with the transaction because this provides clues for performing successful fraudulent transactions in the future. Rejected transactions are never settled.

Fine-tuning Filter Settings—Using the Filter Scorecard

The Filter Scorecard displays the number of times that each filter was triggered and the percentage of all transactions that triggered each filter during a specified time period.

This information is especially helpful in fine-tuning your risk assessment workflow. For example, if you find that you are reviewing too many transactions, then use the Filter Scorecard to determine which filters are most active. You can reduce your review burden by relaxing the settings on those filters (for example, by setting a higher amount for the Purchase Price Ceiling filter).

- 1 Click **Security** → **Transaction Review** → **Filter Scorecard**. The *Filter Scorecard* query page opens.

Filter Scorecard

Use this page to generate a Filter Scorecard that reports on overall filter performance during the date range that you specify. This information is especially helpful when fine-tuning your filter settings. For more information click [here](#)

Scorecard Date Selection

☒ **Preset Time:** Today (Wed Jul 21, 2004)

☐ **Custom Time:** From: July 21 2004 Time: 00:00:00 To: July 21 2004 Time: 23:59:59

Time Zone: Pacific Time (US, Canada): Tijuana


Mode: Query Live Transactions

- 2 Specify the date range of the transactions to review.
- 3 In the **Transaction Mode** field, specify transactions screened by the **Live** or the **Test** servers.

4 Click **Submit**.

The *Filter Scorecard* page displays the number of times that each filter was triggered and the percentage of all transactions that triggered each filter during the time span that you specified.

In this example, the **Total Item Ceiling** filter is triggered for 17% of all transactions—possibly indicating that you might consider whether the ceiling is set properly.

Filter Scorecard 		
<p>? WHAT DO I DO?</p> <p>The scorecard shows how often each filter was triggered and the percentage of all transactions that triggered the filter.</p>		
Test Scorecard		
for		
Fri Feb 07, 2003 00:00:00		
to		
Fri Mar 07, 2003 23:59:59		
Filter	Times Triggered	Trigger Percentage
Total Purchase Price Ceiling	9	0.77%
Total Item Ceiling	513	17.00%
Shipping/Billing Mismatch	51	4.69%
AVS Failure	23	0.74%
CSC Failure	9	0.77%
Freight Forwarder Match	0	0.00%

Ensuring Meaningful Data on the Filter Scorecard

The Scorecard shows the total number of triggered transactions for the time period that you specify, so if you had changed a filter setting during that period, the Scorecard result for the filter might reflect transactions that triggered the filter at several different settings.

For example, you changed the Total Purchase Price Ceiling on August 1 and again on August 7. You then run a Filter Scorecard for July 1 to August 31. Between July 1 to August 31, three different price ceiling settings caused the filter to trigger, yet the Scorecard would not indicate this fact.

To ensure meaningful results in the Filter Scorecard, specify a time period during which the filter settings did not change.

Re-running Transactions That Were Not Screened

If the Transaction Security service is unavailable, then transactions return Result Code 127. The transactions are not screened by any filters and are held for resubmission to the servers. Follow these steps to resubmit a transaction:

- 1 Request all unprocessed transactions using the *Review Transactions* page as described in “Reviewing Suspicious Transactions” on page 26.

The summary page lists all unprocessed transactions

- 2 For each transaction that you wish to resubmit: Click the **Transaction ID** link to open the *Transaction Detail* page.
- 3 Click the **Rerun Transaction** button
 - If successful, a message notifies you *Transaction Successfully Processed by Filters*. Click **Done** to return to the unfiltered transaction list (notice that the transaction that you just resubmitted is no longer in the list). All transactions are ultimately recategorized to Status Code Accept, Reject, or Review.
 - If unsuccessful, you receive the following message: *Reprocessing by Filters Failed Please Try Again*. Click **Rerun Transaction** to retry.

Tip If multiple attempts at screening fail, then the transaction may have data formatting problems. Validate the data, and contact Customer Service.

If you encounter 50 or more transactions with Result Code 127, then contact Customer Service, who can resubmit them as a group.

Activating and Configuring the Buyer Authentication Service

Enrolling for the Buyer Authentication Service

To enroll for the Buyer Authentication Service, click the Buyer Authentication banner on the Security welcome page. Follow the on-screen instructions to determine whether both your processor and your acquiring bank support the Buyer Authentication service. If they both support the service, then you can follow the on-screen instructions to enroll.

Downloading the Payflow Pro SDK (Including APIs and API Documentation)

The Payflow Pro software development kit (SDK) is available either as a standalone client that you can integrate with your Web store using CGI scripts or as a set of APIs for direct integration with your application. *VeriSign Payflow Pro Developer's Guide* provides instructions for downloading the SDK appropriate to your platform.

IMPORTANT! Full API documentation is included with each SDK.

Configuring Buyer Authentication

To enable Buyer Authentication processing on your site, you will need to construct two transaction requests (messages) and construct a frameset. You can accomplish the tasks in a few hours.

In the standard PayFlow Pro implementation, when the customer submits a purchase request, your Web site sends a single Sale transaction request with all purchase details (message with transaction type S) to VeriSign. With Buyer Authentication, you must submit two additional transaction requests (types E—Verify Enrollment and Z—validate PARES response) before the Sale.

Follow these steps:

- 1 Log in to VeriSign Manager at <https://manager.verisign.com>.
- 2 Click **Security** → **Buyer Authentication** → **Buyer Authentication Set-Up**.
The *Buyer Authentication Set-Up* page opens.
- 3 Enter Registration information (complete all fields for both MasterCard and Visa).
 - Select your Acquirer (Acquirer Support) for MasterCard and Visa and select the activate acquirer check box.
 - Verify the Business Name (should be pre-populated).
 - Fully qualified URL (be sure to include <http://> or <https://>).
 - Country Code.
- 4 Click **Submit**.
- 5 On the main VeriSign Manager page click the **Download** link.
- 6 Download *User Guide for PayFlow Pro with Fraud Protection Services* (this document in PDF format). Read chapters 5 and 7 and Appendix D.
- 7 Download the PayFlow Pro SDK (Software Developer's Kit) appropriate for your software environment.
- 8 Download *PayFlow Pro Developer's Guide* (PDF format document). Read as much of *PayFlow Pro Developer's Guide* as you need.
- 9 Configure PayFlow Pro as described in the User Guide.

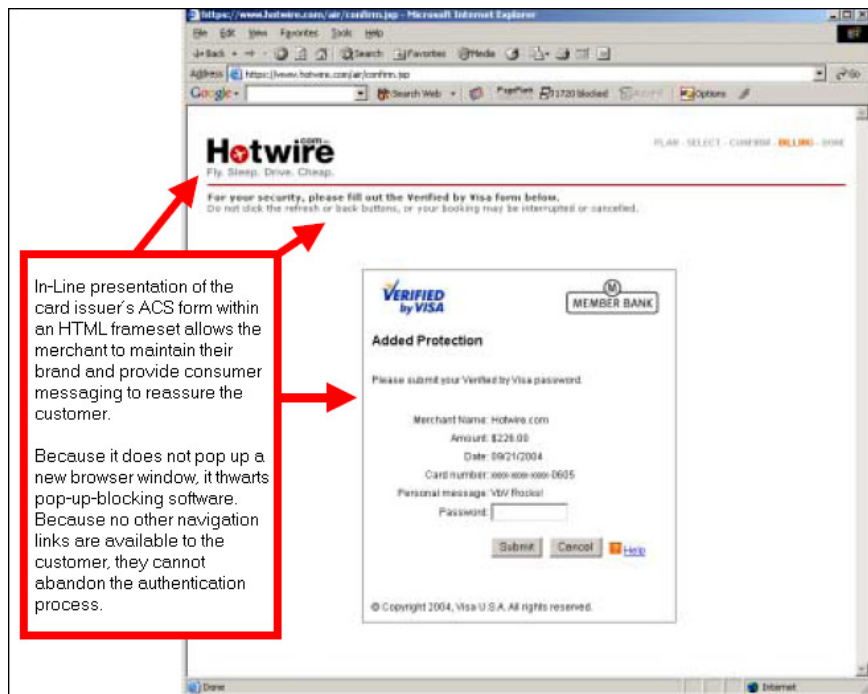
Generate Transaction Request Software

- 1 Submit a Verify Enrollment transaction request (type E) to determine whether the cardholder is enrolled in either the Verified by Visa or MasterCard SecureCode service. See the example on page 48.
- 2 The response is either Enrolled or Not Enrolled. See the example responses on page 49.
- 3 If the customer is enrolled, you populate the response data into a form page (hosted on your server) and post it to the URL of the card issuing bank (ACS) indicated in the response. Make sure the TermUrl field is properly specified, as this is where the ACS will post the response. See *Example ACS Redirect Code* on page -46.

- 4 The ACS responds to the post by presenting an Authentication window to the customer.

By Visa/MasterCard requirements, the HTML page for displaying the ACS form must be presented in-line (within the same browser session as the e-commerce transaction), preferably as framed-inline.

The ACS form should be displayed in a frame set, as shown in the following example. The message across the top of the frame is required.



- 5 When the customer enters their password and clicks **Submit**, the ACS verifies the password and posts a response to the TermURL (the page on your site that is configured to receive ACS responses).
- 6 Submit a Validate Authentication Response transaction request (type Z) to validate (ensure that the message has not been falsified or tampered with) and decompose the Authentication Response from the card-issuing bank (ACS). See *Example Validate Authentication Response* on page -49.
- 7 The response contains the following three data elements:
 - XID

- ECI. E-commerce Indicator
- Visa: CAVV. Cardholder Authentication Verification Value
- or —

MasterCard: AAV. Accountholder Authentication Value

Submit these values, along with the standard transaction data, in a standard Sale or Authorization transaction request, as described in “Call 4: Submit the intended transaction request to the Payflow Pro server” on page 47.

Test and Activate the Service

- 1 Make these other required UI modifications:

Payment page pre-messaging. The example text in the red boxes must appear on your payment page to advise the customer that authentication may take place.

The screenshot shows the Hotwire website interface for a car rental booking. The browser is Microsoft Internet Explorer. The URL is <http://www.hotwire.com/car/buying.asp>. The page title is "Hotwire: Airline Tickets, Hotel Reservations, Car Rentals - Discount Travel Deals, Last Minute - Microsoft Internet Explorer".

The main navigation bar includes links for Home, Flights, Hotels, Car Rentals, Packages, Weekender, Cruises, and Deals & Destinations. The "Car Rentals" link is highlighted.

The page content includes a "Select your payment option." section with a "PLEASE NOTE: The name of the car rental company will be shown only after you buy." warning. Below this is a "Car Rental in Tampa, FL" section showing a "Full-size car" for \$211.54. The "Driver Contact Details" section shows the primary driver as Richard S. Lynch with contact information.

Annotations with red arrows point to specific links and sections:

- A red box highlights the "Consumer Questions" section, which includes links for "Why am I being asked for a password to use my credit card?", "Can I purchase a car rental for someone else using my credit or debit card?", and "Can I add drivers to my reservation?". A red arrow points from the text "Consumer Messaging 'Learn More' links & 'reminder'" to this section.
- A red box highlights the "MasterCard VERIFIED by VISA" logo, with a red arrow pointing from the same text.
- A red box highlights the "PURCHASE" button and the "VERIFIED by VISA" logo, with a red arrow pointing from the same text.

On the left side of the page, there is a sidebar with a "VERIFIED by VISA" logo and a "Learn More" link. A red arrow points from the text "Consumer Messaging 'Learn More' links & 'reminder'" to this link.

Failure messaging. The example text in the red box handles cases where customers cannot successfully authenticate themselves. The text requests another form of payment.



Consumer Messaging for Failed Authentication: Please submit new form of payment.

- 2 Perform a last round of test transactions as described in Appendix D, “Testing Buyer Authentication Transactions Using the Payflow Pro SDK,” to ensure the flow and screen presentation is correct.
- 3 Once all message flows and customer messaging and required logos are in place, you can activate Buyer Authentication to accept live transactions.

Performing Buyer Authentication Transactions Using the Payflow Pro SDK

This chapter describes the process of performing Buyer Authentication transactions using the Payflow Pro SDK. For information on using the SDK and on transaction syntax see *VeriSign Payflow Pro Developer's Guide*.

The content and format of responses to transaction requests are described in “Buyer Authentication Transaction Parameters and Return Values” on page 51. Standard Payflow Pro response values are described in *VeriSign Payflow Pro Developer's Guide*.

VeriSign XMLPay client support for Buyer Authentication is described in *VeriSign XMLPay 4.2 Core Specification*.

Testing the Buyer Authentication Service

Information on testing Buyer Authentication Service transactions appears in Appendix D, “Testing Buyer Authentication Transactions Using the Payflow Pro SDK.”

In This Chapter

Buyer Authentication Transaction Overview on page 42.

Buyer Authentication Terminology on page 42.

Buyer Authentication Server URLs on page 43.

Detailed Buyer Authentication Transaction Flow on page 43.

Example Buyer Authentication Transactions on page 48.

Buyer Authentication Transaction Parameters and Return Values on page 51.

ECI Values on page 57.

Logging Transaction Information on page 58.

Buyer Authentication Transaction Overview

To implement Buyer Authentication, you use VeriSign's Payflow Pro SDK to write software that:

- 1 Receives the customer's account number and determines whether it is enrolled in the Verified by Visa or MasterCard SecureCode buyer authentication program.
- 2 If the cardholder is enrolled, then your program redirects the customer to the issuing bank's buyer authentication page. The customer submits their username and password. The issuing bank authenticates the customer's identity by returning a payer authentication response value to your program.
- 3 Your program then validates the authentication response.
- 4 If the authentication data is valid, then your program submits a standard Payflow Pro authorization or sale transaction that includes the buyer authentication data.

Note The Buyer Authentication Service supports only Sale and Authorization transaction types.

Buyer Authentication Terminology

The following terms are used in this chapter:

Term	Definition
Merchant Plug-in	The software component that implements merchant's client functionalities in 3-D Secure protocol. VeriSign's 3-D Secure server at https://buyerauth.verisign.com/DDDSecure/MerchantPlug-In implements MPI's specification as a payment gateway.
PAREQ	The Payer Authentication Request message that you send to the issuing bank's buyer authentication page.
PARES	Payer Authentication Response, digitally signed by the issuing bank.
CAVV	Cardholder Authentication Verification Value. The value generated by card issuing bank to prove that the cardholder has been authenticated with a particular transaction.
XID	Buyer authentication Transaction ID. Used only by Verified by Visa to identify a unique buyer authentication transaction.

Term	Definition
ECI	E-Commerce Indicator. The ECI value indicates the level of security supported by the merchant when the cardholder provided the payment card data for an Internet purchase. When returned in a buyer authentication response, it is determined by the issuing bank.
Authentication Status	Key component in the 3-D Secure protocol. A server run by card issuer performing functionalities of enrolling a card for 3-D Secure, verifying card enrollment, and authenticating cardholder and issuing a digitally signed payment authentication response (PARES).

Buyer Authentication Server URLs

IMPORTANT! URLs listed here are used only for buyer authentication transactions: Verify Enrollment (TRXNTYPE=E) and Validate Authentication (TRXNTYPE=Z).

- + VeriSign's production Buyer Authentication server URL is **buyerauth.verisign.com**
- + VeriSign's Test Buyer Authentication server URL is **test-buyerauth.verisign.com**

Detailed Buyer Authentication Transaction Flow

A buyer authentication transaction involves the following four program calls. Examples of exact syntax appear in "Example Buyer Authentication Transactions" on page 48.

Note XMLPay uses the VerifyEnrollment transaction for Call 1 on page 44.

XMLPay uses the ValidateAuthentication transaction for Call 2 on page 45.

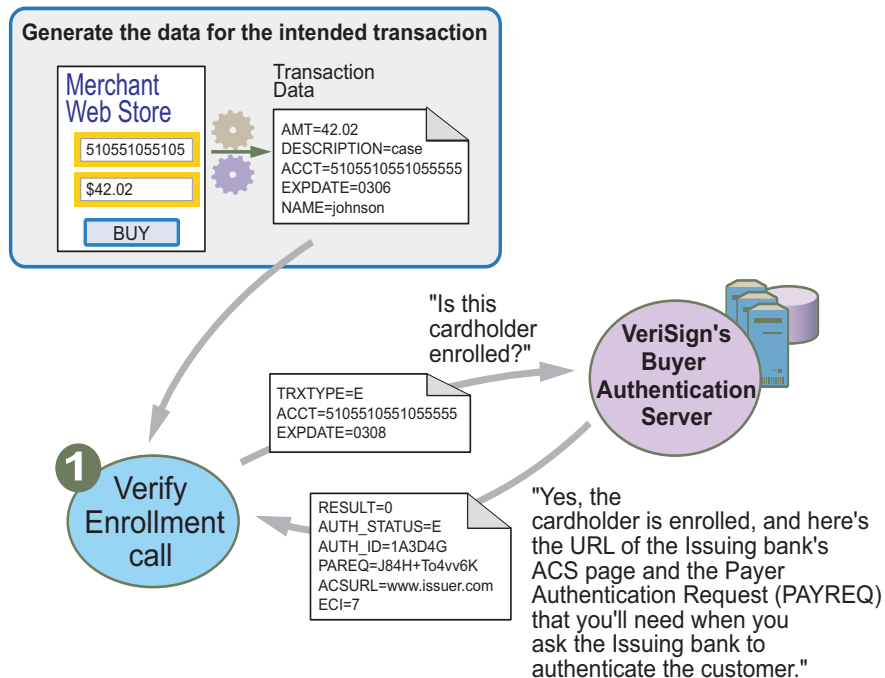
For Call 4 on page 47, pass AUTHENTICATION_STATUS=<status>, AUTHENTICATION_ID=<id>, CAVV=<cavv value>, and XID=<xid value>, ECI=<eci value> in the ExtData for Authorization and Sale transactions.

Call 1: Verify that the cardholder is enrolled in the 3-D Secure program

For the Verify Enrollment call (VerifyEnrollment transaction in XMLPay), you determine whether the cardholder is enrolled in the 3-D Secure program. Send a transaction (TRXTYPE=E) to the VeriSign Buyer Authentication server (buyerauth.verisign.com or test-buyerauth.verisign.com).

VeriSign returns the AUTHENTICATION_STATUS of enrollment (E means enrolled), an AUTHENTICATION_ID value, and an ECI value (electronic commerce indicator, defaulted to 7 [Authentication Unsuccessful] because authentication has not yet occurred). If the cardholder is enrolled, then the message also includes a PAREQ (payer authentication request) value and the ACSURL—the URL of the Issuer's ACS (access control server) page at which buyers provide their password to authenticate themselves. The PAREQ is used in the next call to ask the Issuing bank to authenticate the customer.

If the cardholder is not enrolled (AUTHENTICATION_STATUS=O), cannot be verified (X), or an error occurred (I), skip to Call 4, "Call 4: Submit the intended transaction request to the Payflow Pro server" and submit a standard Payflow Pro authorization or sale transaction that includes the AUTHENTICATION_STATUS, AUTHENTICATION_ID, and ECI values.



Call 2: POST the authentication request to and redirect the customer's browser to the ACS URL

If the card is enrolled, you place the following values in an HTTP form and then HTTP POST the values to the ACS URL (the issuer's ACS site):

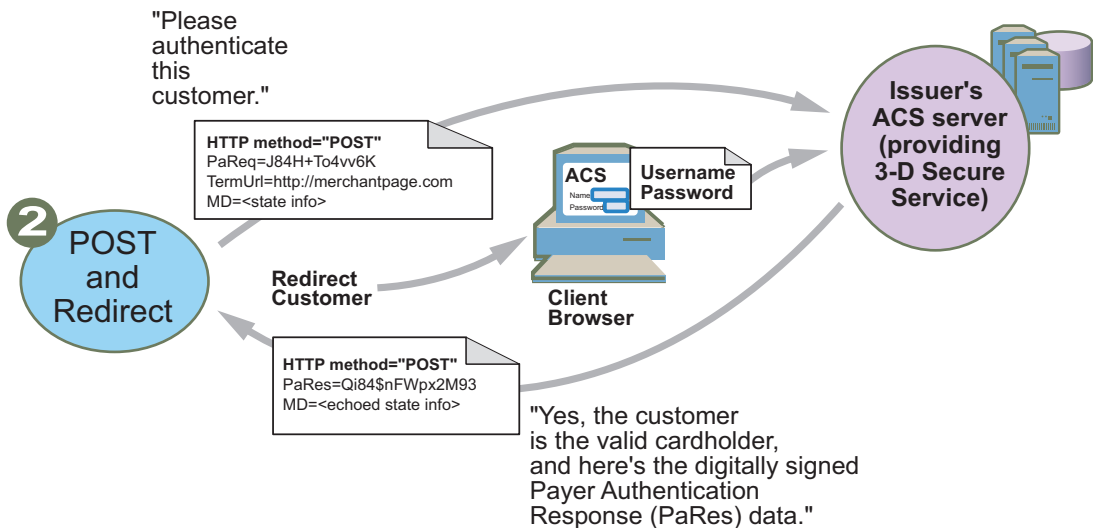
- + PaReq: The value of the PaReq returned in the Verify Enrollment call.
- + TermUrl: Your server—the one that should accept the authentication response.
- + MD: (Required) Any data that you want returned (echoed) to the TermUrl by the ACS server. Typically, this is state information.

(XMLPay uses the ValidateAuthentication transaction for this purpose.)

Your server then redirects the customer's browser to the ACS URL.

The customer views the ACS form, enters their 3-D Secure password, and submits the form to the Issuing bank.

The issuer's ACS server validates the password, authenticates the customer's identity, and then generates and digitally signs a PaRes value (payer authentication response). The ACS server then HTTP POSTs the signed PaRes and the unchanged value of the MD to the TermUrl that you specified.



Example ACS Redirect Code

The following example HTML page redirects a customer to an ACS URL with a PAREq and returns the URL for receiving the PARES. Customize tags marked with \$ with your information.

```
<head>
<title>Authentication Body</title>
<SCRIPT LANGUAGE="Javascript">
function OnLoadEvent()
{
document.downloadForm.submit();
}
</SCRIPT>
</head>

<body bgcolor="{ $BACKCOLOR}" background="{ $BACKGROUND}"
onload="OnLoadEvent()">
<form name="downloadForm" action="{ $acsUrl}" method="POST">
<noscript>
<br/>
<br/>
<center>
<h1>Processing your 3-D Secure Transaction</h1>
<h2>JavaScript is currently disabled or is not supported by your browser.<br/></h2>
<h3>Click <b>Submit</b> to continue processing your 3-D Secure transaction.</h3>
<input type="submit" value="Submit"/>
</center>
</noscript>

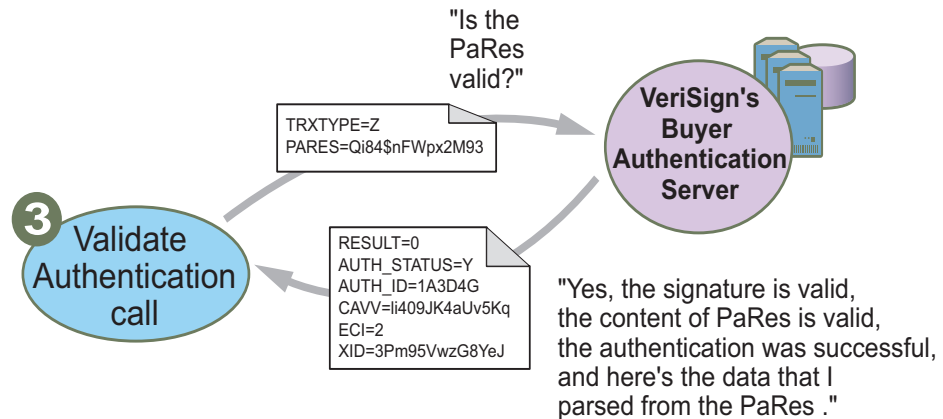
<input type="hidden" name="TermUrl" value="{ $redirectUrl}"/>
<input type="hidden" name="MD" value="{ $messageId}"/>
<input type="hidden" name="PaReq" value="{ $paReq}"/>
</form>
</body>
</HTML>
```

Call 3: Validate the PARES authentication data returned by the ACS server

Your application at TermUrl performs the Validate Authentication call for security reasons. You validate that the PARES is the proper data from the Issuer by sending a request for validation of the digital signature on the PARES to the VeriSign Buyer Authentication server. Use TRXTYPE=Z.

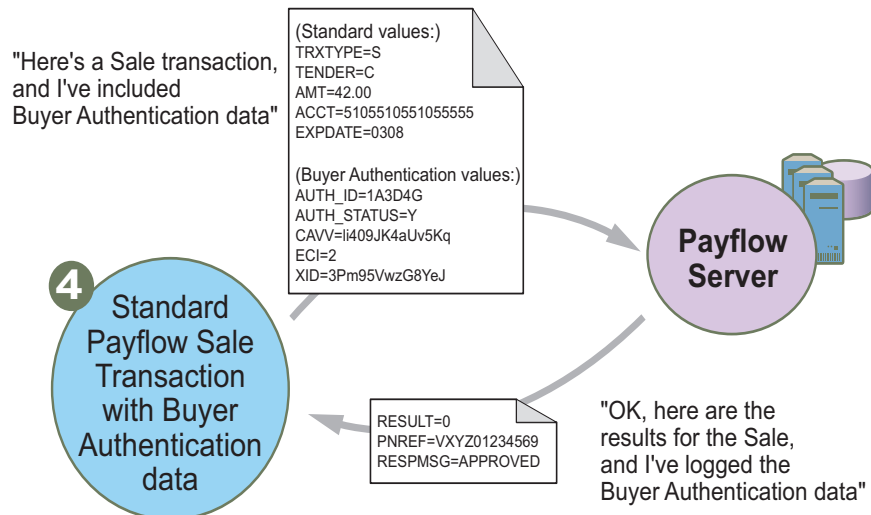
VeriSign uses the Issuer's digital certificate to validate the signature and then returns the parsed authentication information from the PARES:
AUTHENTICATION_STATUS (Y means valid signature),

AUTHENTICATION_ID, CAVV (cardholder authentication verification value), XID, and ECI.



Call 4: Submit the intended transaction request to the Payflow Pro server

Now that the buyer authentication process is complete, you submit the intended sale or authorization payment transaction (TRXNTYPE=S or A) to the Payflow Pro server. In addition to the standard sale or authorization transaction data, you include additional buyer authentication data, as follows:



- ♦ **Cardholder is Enrolled in the 3-D Secure Program**

You perform the intended Payflow authorization or sale payment transaction using the standard name/value pairs plus the values returned to the Validate Authentication transaction: AUTHENTICATION_ID, AUTHENTICATION_STATUS, CAVV, XID and final ECI.

- ♦ **Cardholder is Not Enrolled**

If there is no PAREQ returned in the response to the Verify Enrollment call, then the cardholder is not enrolled and you do not perform any additional buyer authentication transactions. You perform the intended Payflow authorization or sale payment transaction using the standard name/value pairs plus the AUTHENTICATION_ID, AUTHENTICATION_STATUS, and ECI values returned by the Verify Enrollment call.

XMLPay Users: Pass AUTHENTICATION_STATUS=<status>, AUTHENTICATION_ID=<id>, CAVV=<cavv value>, and XID=<xid value>, ECI=<eci value> in the ExtData for Authorization and Sale transactions.

Example Buyer Authentication Transactions

The values returned in the transaction responses shown in these examples are described in “Buyer Authentication Transaction Parameters and Return Values” on page 51. Standard Payflow return values are described in *VeriSign Payflow Pro Developer's Guide*.

All return parameter names for transactions with VeriSign's Buyer Authentication Server include length tags. Length tags specify the exact number of characters and spaces that appear in the value. For example, RESPMSG[2]=OK.

Note The examples in this chapter use the syntax of the pfpro executable client. Other Payflow Pro clients differ in where and how the parameter values are set, but the meaning and uses are the same.

Example Verify Enrollment Transaction

Use TRXTYPE=E to submit a Verify Enrollment transaction.

```
pfpro test-buyerauth.verisign.com 443
"TRXTYPE=E&ACCT=5105105105100&AMT=19.25&CURRENCY=840&EXPDAT
E=1206&PARTNER=VeriSign&PWD=p12345&VENDOR=SuperMerchant&USER=Sup
erMerchant" 30
```

Example Verify Enrollment Response

The PARES returned by the Issuer is a very large, digitally signed string containing the information required to direct the consumer to the issuer.

Cardholder is enrolled in 3-D Secure program

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=f43669e4921cf8b504c
4&AUTHENTICATION_STATUS[1]=E&PAREQ[428]=eJxVku1ugjAUhm+FeAH0A3Boz
pr48WP+2GK23UA9HJVECpYy9e7XCkzXkPS8fcvD6Vvg+2iJ1I+EnSUF79S2+kBRWb
xO9mkync4onUmB+3yX8RTTiYLT4pPOCn7ltmVtlh5LIGN0hMsHrVxCjSel5sPJcMANii
oyG7WSGwDWK/B6lrUkloXrfTpVJqDn20Rreqq0eYG7O4D1p1x9qbylAMbBXT2pl7ON
XPGLpdLvPMU7CHoGTHWFbCwB9ijuW0XqtYzr2Whpi+5FEWOIGOWU06U7f0HggO
FdqQk5wmXlokEn3M5T1Jg93XQVWhCiVksM3/GXkET4lvRCs7zCvioLRkcjzEqoGtTG
/17fFz/NRTUom99mB59r95CxOh8epngzw8Pad+NgLSKJ6lnWg8lr7HhDtlw3b769xv8A
hQarWM=&ACSURL[66]=http://test-buyerauth-post.verisign.com/DDDSecure/Acs3DS
ecureSim/start
```

Cardholder is not enrolled

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=48c92770755039d6bb
3d&AUTHENTICATION_STATUS[1]=O&ECI[1]=1
```

Example Validate Authentication Transaction

Use TRXTYPE=Z to submit a Validate Authentication transaction to validate the Issuer's digital signature on the PaRes, validate the content of the PaRes, and to parse the PaRes.

Tip Ensure that you include no stray carriage returns with the **PaRes** value, especially at the end of the string.

```
pfpro test-buyerauth.verisign.com 443
TRXTYPE=Z&PARTNER=VeriSign&PWD=p12345&VENDOR=SuperMerchant&USER
=SuperMerchant&PARES[3648]=eJzdWFmTokoW/isdPW9T0c3iUnLDNiKTXQURWYU
3NIIEUUBAfv0kWi1I91TPXebhTowRBpmHkyfPfr5gbiRIFHF6FFzKaDFXoqry4uhTGn7
7PAvH4SQKp1MvmEbTnYcf4efF/AVoUXVj2HD7XjWCzskU0slkGrG33TzqTsUxwhz0n
Hhbz4l35U7ecfHPh9/dnIE6N7aLeZ0ePITqRp9XtVdfqo
```

...

```
oZbuHePyp/FUqxyFTXlgV5l/+jMqjde/12HNLjbqW/Qqgfe7Qw9GjcKgt2OdvTspJPI2ey
uRw0nbn9JKdp6eVP1u3xUyaKN1qYzVksB9vKCe6kqRIV4qfUJP1jvSWI9OKuSbn5zpK
0ouzXI9mNfoARhDv30qlt+8n719Wbh9fb5+EH++Fj5+K/wWCuWQ
```

Example Validate Authentication Response

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=8d4d5ed66ac6e6faac6
d&AUTHENTICATION_STATUS[1]=Y&CAVV[28]=OTJIMzViODhiOTIIMjBhYmVmKMGU
=&ECI[1]=5&XID[28]=YjM0YTkwNGFkZTI5YmZmZWWE1ZmY
```

Displaying the ACS Form

The Issuer ACS page presents transaction information to the cardholder. Visa/MasterCard require that the HTML page for displaying the ACS form must be presented in an in-line frame set. This window must occur within the same browser session as your e-commerce transaction.

The window should have the following browser-independent attributes:

width=390 (minimum), height=400 (minimum), resizable=no, scrollbars=yes, toolbar=no, location=no, directories=no, status=yes, menubar=no

Example Payflow Authorization or Sale Transaction

The Buyer Authentication Service supports only Authorization and Sale transaction types.

The name/value pairs that you submit with the intended Payflow Pro transaction depend upon whether the cardholder is enrolled in the 3-D Secure program, as follows:

- ◆ **Cardholder Enrolled in 3-D Secure Program**

You perform the intended transaction using the standard name/value pairs plus the values returned to the Validate Authentication transaction:

AUTHENTICATION_ID, AUTHENTICATION_STATUS, CAVV, XID, and ECI.

```
pfpro test-payflow.verisign.com 443
"TRXTYPE=S&TENDER=C&PARTNER=VeriSign&VENDOR=SuperMerchant&USER
=SuperMerchant&PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308&AMT
=123.00&AUTHENTICATION_ID[20]=8d4d5ed66ac6e6faac6d&CAVV[28]=OTJIMzVi
ODhiOTIIMjBhYmVkMGU=&AUTHENTICATION_STATUS[1]=1&ECI[1]=5&XID[28]=Yj
M0YTkWNGFkZTI5YmZmZWE1ZmY" 30
```

- ◆ **Cardholder Not Enrolled**

If there is no PAREQ returned in the response to the Verify Enrollment call, then the cardholder is not enrolled. You perform the intended transaction using the standard name/value pairs plus the AUTHENTICATION_ID, AUTHENTICATION_STATUS, and ECI returned by the Verify Enrollment transaction.

```
pfpro test-payflow.verisign.com 443
"TRXTYPE=S&TENDER=C&PARTNER=VeriSign&VENDOR=SuperMerchant&USER
=SuperMerchant&PWD=x1y2z3&ACCT=5555555555554444&EXPDATE=0308&AMT
=123.00&AUTHENTICATION_ID[20]=8d4d5ed66ac6e6faac6d&AUTHENTICATION_S
TATUS[1]=O&ECI[1]=7&"30
```

Example Payflow Authorization or Sale Transaction Response

For Visa transactions, the response includes a CARDSECURE value of Y (CAVV is valid), N (CAVV is not valid), or X (cannot determine CAVV).

- ♦ **Cardholder Enrolled in 3-D Secure Program**

```
RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&AVSZIP=N&IAVS=Y&CVV2MATCH=Y&CARDSECURE=Y
```

- ♦ **Cardholder Not Enrolled**

```
RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&AVSZIP=N&IAVS=Y&CVV2MATCH=Y&CARDSECURE=N
```

Buyer Authentication Transaction Parameters and Return Values

VeriSign's Buyer Authentication server accepts the parameters listed in this section. This section also describes expected return values for buyer authentication transactions.

Note Be sure to follow the guidelines for specifying the parameters. Standard Payflow Pro parameters, parameters that you can pass for reporting purposes, as well as return values are described in *VeriSign Payflow Pro Developer's Guide*.

Transaction Parameters

In the following tables, **ANS** indicates alphanumeric-special characters—the set of alphanumeric characters plus characters like / = + : %.

Verify Enrollment Transaction Name/Value Pairs

Name	Description	Type	Max. Length
TRXTYPE	E		1
VENDOR	Vendor name		
USER	User name		
PARTNER	Partner name		
PWD	Vendor's password		

ACCT	PAN, card number		
EXPDATE	Expiration mmyy		
AMT	Decimal Amount		
CURRENCY	Required. ISO 3-number Currency Code (The code for US dollars is 840)		
PUR_DESC	Optional. Purchase description.		

Verify Enrollment Return Values

Name	Description	Type	Max. Length
RESULT	0: successful transaction, otherwise error. See "RESULT Values for Transaction Declines or Errors" on page 52.	integer	1
RESPMSG	Error description if result is not 0. See "RESULT Values for Transaction Declines or Errors" on page 52.	ANS	256
AUTHENTICATION_ID	Unique identifier for this VE event. Value returned only for valid requests.	ANS	64
AUTHENTICATION_STATUS	Value returned only for valid requests. E: Card Enrolled O: Card Not Enrolled X: Unable to determine I: Verify Enrollment request failed	alpha	1
PAREQ	PAREQ. Value returned only if AUTHENTICATION_STATUS=E.	ANS	1024
ACSURL	ACS URL. Value returned only if AUTHENTICATION_STATUS=E.	ANS	256
ECI	Initial ECI value returned. Value returned only for valid requests.	integer	1

RESULT Values for Transaction Declines or Errors

A RESULT value greater than zero indicates a decline or error. For this type of error, a RESPMSG name/value pair is included. The exact wording of the RESPMSG may vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

Table 6-1 VeriSign Transaction RESULTS/RESPMSGs

RES ULT	RESPMSG/Explanation
1001	Buyer Authentication Service unavailable
1002	Buyer Authentication Service — Transaction timeout
1003	Buyer Authentication Service — Invalid client version
1004	Buyer Authentication Service — Invalid timeout value
1011	Buyer Authentication Service unavailable
1012	Buyer Authentication Service unavailable
1013	Buyer Authentication Service unavailable
1014	Buyer Authentication Service — Merchant is not enrolled for Buyer Authentication Service (3-D Secure). To enroll, log in to VeriSign Manager, click Security, and then click the Buyer Authentication Service banner on the page.
1021	Buyer Authentication Service — Invalid card type
1022	Buyer Authentication Service — Invalid or missing currency code
1023	Buyer Authentication Service — Merchant status for 3D secure is invalid
1041	Validate Authentication failed: missing or invalid PARES
1042	Validate Authentication failed: PARES format invalid
1043	Validate Authentication failed: Cannot find successful Verify Enrollment
1044	Validate Authentication failed: Signature validation failed for PARES
1045	Validate Authentication failed: Mismatched or invalid amount in PARES
1046	Validate Authentication failed: Mismatched or invalid acquirer in PARES
1047	Validate Authentication failed: Mismatched or invalid Merchant ID in PARES
1048	Validate Authentication failed: Mismatched or invalid card number in PARES

Table 6-1 VeriSign Transaction RESULTS/RESPMSGs (Continued)

RES ULT	RESPMSG/Explanation
1049	Validate Authentication failed: Mismatched or invalid currency code in PARES
1050	Validate Authentication failed: Mismatched or invalid XID in PARES
1051	Validate Authentication failed: Mismatched or invalid order date in PARES
1052	Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction

Validate Authentication Transaction Name/Value Pairs

Name	Description	Type	Max. Length
TRXTYPE	Z	alpha	1
VENDOR	Vendor name		
USER	User name		
PARTNER	Partner name		
PWD	Merchant's password		
PARES	The complete XML PARES message generated by the ACS.		

Validate Authentication Return Values

Name	Value	Type	Max Length
RESULT	0: successfully verified	integer	1
RESPMSG	Error description if result is not 0	ANS	256
AUTHENTICATION_ID	Message ID of the response, passed with authorization transaction	ANS	64

AUTHENTICATION_STATUS	The status of the PARES: Y: Authentication Successful — the password was correct. A: Authentication Attempted — the issuing bank does not support buyer authentication N: Authentication Failed (bad password) U: Unable to Authenticate (network error) F: Validate Authentication transaction error	alpha	1
CAVV	CAVV value. Returned if AUTHENTICATION_Status is Y or A	ANS	64
XID	Transaction ID. Returned if AUTHENTICATION_Status is Y or A	ANS	64
ECI	ECI if the ECI value is returned in the PARES. 1 - Cardholder not Authenticated (MasterCard) 2 - Cardholder Authenticated (MasterCard) 5 - Authentication Successful (Visa) 6 - Authentication Attempted (Visa) 7 - Authentication Unsuccessful (Visa)	integer	1

Standard Payflow Sale or Authorization Transaction

In addition to the parameters described in *VeriSign Payflow Pro Developer's Guide*, you submit the following parameters that are specific to the buyer authentication functionality:

Name	Value
AUTHENTICATION_ID	If the Verify Enrollment call returned AUTHENTICATION_STATUS=E, then submit the AUTHENTICATION_ID value returned by the Validate Authentication call. Otherwise, submit the AUTHENTICATION_ID value returned by the Verify Enrollment call.

AUTHENTICATION_STATUS	If the Verify Enrollment call returned AUTHENTICATION_STATUS=E, then submit the AUTHENTICATION_STATUS value returned by the Validate Authentication call. Otherwise, submit the AUTHENTICATION_STATUS value returned by the Verify Enrollment call.
XID	XID value returned by the Validate Authentication call (if applicable).
ECI	If the Verify Enrollment call returned AUTHENTICATION_STATUS=E, then submit the ECI value returned by the Validate Authentication call. Otherwise, submit the ECI value returned by the Verify Enrollment call.

Sale or Authorization Response Value

Visa only: In addition to the return values described in *VeriSign Payflow Pro Developer's Guide*, the following value is returned:

Name	Value
CARDSECURE	Visa only. CAVV validity. Y =valid, N =Not valid, X =cannot determine

ECI Values

Description of Scenario	Merchant Region	Response to TRXNTYPE=E	Response to TRXNTYPE=X	ECI	Merchant calculates ECI because cannot authenticate?
Visa - Not Enrolled	USA	O	N/A	6	Y
Visa - Unable to determine enrollment	USA	X	N/A	7	Y
Visa - Verify Enrollment transaction error	USA	I	N/A	7	Y
Visa - Card Enrolled - Successful Authentication	USA	E	Y	5	N
Visa - Card Enrolled - Authentication Attempted	USA	E	A (Contact Visa to verify that this value is returned.)	6	N
Visa - Card Enrolled - Authentication Failed	USA	E	N	7	Y
Visa - Card Enrolled - Unable to Authenticate	USA	E	U	7	Y
Visa - Card Enrolled - Error in transaction	USA	E	F	7	Y
MasterCard - Not Enrolled	WORLD	O	N/A	1	Y
MasterCard - Unable to determine enrollment	WORLD	X	N/A	1	Y
MasterCard - Verify enrollment transaction error	WORLD	I	N/A	1	Y
MasterCard - Card Enrolled - Successful Authentication	WORLD	E	Y	2	Y

Description of Scenario	Merchant Region	Response to TRXNTYPE=E	Response to TRXNTYPE=X	ECI	Merchant calculates ECI because cannot authenticate?
MasterCard - Card Enrolled - Authentication Attempted	WORLD	E	A (should never occur)	1	Y
MasterCard - Card Enrolled - Authentication Failed	WORLD	E	N	1	Y
MasterCard - Card Enrolled - Unable to Authenticate	WORLD	E	U	1	Y
MasterCard - Card Enrolled - Validation Failed	WORLD	E	F	1	Y

Logging Transaction Information

VeriSign maintains a record of all transactions executed on your account. Use VeriSign Manager to view the record and use the information to help reconcile your accounting records.

Note This record is not the official bank statement. The activity on your account is the official record.

In addition, VeriSign strongly recommends that you log all transaction results (except for check information) on your own system. At a minimum, log the following data:

- + PNREF (called the Transaction ID in VeriSign Manager reports)
- + Transaction Date
- + Transaction Amount

If you have any questions regarding a transaction, use the PNREF to identify the transaction.

Audit Trail and Transaction Logging

The Buyer Authentication server logs Verify-Enrollment transactions, PAREQ values, and PARES values.

Verify Enrollment Transactions

Verify Enrollment transactions are logged when all of the following items occur:

- The merchant passes authentication data
- The server connects to Visa or MasterCard and gets a meaningful response (card enrollment AUTHENTICATION_STATUS=E, U or X). If status is Y, then the PAREQ value is logged along with the Verify Enrollment transaction data.

Otherwise, the transaction is not logged.

Validate Authentication Transactions

The Buyer Authentication server will log the PARES value only when all of the following items occur:

- There is a matching PAREQ (by Message ID, not by content) in the database.
- There is no other PARESeS with the same Message ID in the database. This means that if a duplicate PARES is submitted, it is logged only once.

Screening Transactions Using the Payflow Pro SDK

This chapter describes the process of using the Payflow Pro SDK to perform transactions that will be screened by the Fraud Protection Services filters. For information on using the SDK, and on transaction syntax, see *VeriSign Payflow Pro Developer's Guide*.

IMPORTANT! Recurring Billing transactions are not screened by Fraud Protection Services filters.

Response Values

Payflow Pro response values are described in “RESULT Codes and RESPMSG Values” on page 85.

Testing Filters

Information on testing filters appears in Appendix C, “Testing the Transaction Security Filters.”

In This Chapter

Downloading the Payflow Pro SDK (Including APIs and API Documentation) on page 62.

Transaction Parameters Unique to the Filters on page 64.

Existing Payflow Pro parameters Used by the Filters on page 65.

Response Strings for Transactions that Trigger Filters on page 67.

Accepting or Rejecting Transactions That Trigger Filters on page 73.

Logging Transaction Information on page 73.

Downloading the Payflow Pro SDK (Including APIs and API Documentation)

The Payflow Pro software development kit (SDK) is available either as a standalone client that you can integrate with your Web store using CGI scripts or as a set of APIs for direct integration with your application. *VeriSign Payflow Pro Developer's Guide* provides instructions for downloading the SDK appropriate to your platform.

IMPORTANT! Full API documentation is included with each SDK.

Transaction Data Required by Filters

This table lists each filter and the Payflow Pro parameter values that are required by the filters.

Filter	Required Transaction Data	Payflow Pro Parameters
Account Number Velocity	Credit card number	ACCT
AVS Failure	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
Bad Lists	Customer e-mail address	EMAIL
	Credit card number	ACCT
Buyer Auth Failure	You must be enrolled in the Buyer Authentication Services	See Chapter 6, "Performing Buyer Authentication Transactions Using the Payflow Pro SDK."
BIN Risk List Match	Credit card number	ACCT
Country Risk List Match	Billing address - country	COUNTRY
	Shipping address - country	COUNTRYCODE
CSC Failure	CSC information from credit card	CSC
E-mail Service Provider Risk List	Customer e-mail address	EMAIL

Freight Forwarder Match	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
	Shipping address - city	SHIPTOCITY
	Shipping address - state/province	SHIPTOSTATE
	Shipping address - country	COUNTRYCODE
Geo-location Failure	Customer IP address	CUSTIP
	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
	Billing address - state/province	STATE
	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
	Shipping address - city	SHIPTOCITY
	Shipping address - state/province	SHIPTOSTATE
Good Lists	Customer e-mail address	EMAIL
	Credit card number	ACCT
International AVS	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
International Shipping/Billing Address	Billing address - country	COUNTRY
	Shipping address - country	COUNTRYCODE
International IP Address	Customer IP address	CUSTIP
IP Address Risk List Match	Customer IP address	CUSTIP
IP Address Velocity	Customer IP address	CUSTIP
Product Watch List	Product SKU or other identifying information	L_SKUn

Shipping/Billing Mismatch*	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
	Billing address - state/province	STATE
	Shipping address - street address	SHIPTOSTREET
	Shipping address - ZIP (postal) code	SHIPTOZIP
	Shipping address - city	SHIPTOCITY
	Shipping address - state/province	SHIPTOSTATE
Total Item Ceiling	Total quantity	Total of QTY for all line items within the transaction
Total Purchase Price Ceiling	Total amount	Total of AMT for all line items within the transaction
Total Purchase Price Floor	Total amount	Total of AMT for all line items within the transaction
USPS Address Validation Failure	Billing address - street address	STREET
	Shipping address - street address	SHIPTOSTREET
ZIP Risk List Match	Billing address - ZIP (postal) code	ZIP
	Shipping address - ZIP (postal) code	SHIPTOZIP

Transaction Parameters Unique to the Filters

VeriSign's Payflow server accepts the parameters listed in this section.

Standard Payflow Pro parameters, parameters that you can pass for reporting purposes, and return values are described in *VeriSign Payflow Pro Developer's Guide*.

Name	Description	Type	Max. Length	Example
BILLTOSTREET2	Extended billing address	Alphanumeric String	30	Apt. 107
BILLTOPHONE2	Alternative Phone Number for the billing contact.	Numeric String	20	0119120513621, 6104463591
SHIPTOSTREET2	Extended shipping address	String	30	Bldg. 6, Mail Stop 3

SHIPTOPHONE	Primary Phone Number for the shipping contact	String	20	0119120513621, 6104463591
SHIPTOPHONE2	Primary Phone Number for the shipping contact	String	20	0119120513621, 6104463591
SHIPTOEMAIL	Optional. E-mail Address for the shipping contact	String formatted as an e-mail address	40	abc@xyz.com
COUNTRYCODE	Optional. Country code of the shipping country. The country code depends on the processor.	Alphanumeric String	3	US, USA, 840

Existing Payflow Pro parameters Used by the Filters

The following existing Payflow Pro parameters (described in *VeriSign Payflow Pro Developer's Guide*) are also used by the filters (if they are provided in the transaction request or response):

User Authentication

PARTNER
VENDOR
USER
PWD

Transaction Information

TRXTYPE
TENDER
ACCT
EXPDATE
AMT

Billing Information

FIRSTNAME
MIDDLENAME
LASTNAME
STREET
BILLTOSTREET2
CITY

STATE
ZIP
COUNTRY
PHONENUM
BILLTOPHONE2
EMAIL

Shipping Information

SHIPTOFIRSTNAME
SHIPTOLASTNAME
SHIPTOMIDDLENAME
SHIPTOSTREET
SHIPTOSTREET2
SHIPTOCITY
SHIPTOSTATE
SHIPTOZIP
COUNTRYCODE
SHIPTOPHONE
SHIPTOPHONE2
SHIPTOEMAIL

Order Information

DOB
DL
SS
CUSTIP
BROWSERUSERAGENT
BROWSETIME
BROWSECOUNTRYCODE
FREIGHTAMT
TAXAMT
COMMENT1
DESC
CUSTREF
PONUM

Line Item (each item is appended with the line item number)

L_COST0
L_UPC0
L_QTY0

L_DESC0
L_SKU0
L_TYPE0

Response Strings for Transactions that Trigger Filters

In the response string to a transaction that triggered filters, you have the option to view either a summary statement or a detailed list of each triggered filter's response. The response depends on your setting for the **VERBOSITY** parameter in the transaction request.

- + **VERBOSITY=LOW:** This is the default setting for VeriSign accounts. The following values (described in *VeriSign Payflow Pro Developer's Guide*) are returned: {RESULT, PNREF, RESPMSG, AUTHCODE, AVSADDR, AVSZIP, CVV2MATCH, IAVS, CARDSECURE}

The following values are specific to Fraud Protection Services:

Parameter	Description
RESULT	See "RESULT Values Specific to Fraud Protection Services" on page 70.
PREFPSMSG	Preprocessing Fraud Protection Services messages. These apply to all filters except: AVS Failure, CSC Failure, and Custom Filters.
POSTFPSMSG	Postprocessing Fraud Protection Services messages. These apply to the following filters only: AVS Failure, CSC Failure, and Custom Filters.

- + **VERBOSITY=MEDIUM:** Returns all of the values returned for a LOW setting, plus the following values:

Parameter	Type	Length	Description
FPS_PREXMLDATA	char		Itemized list of responses for triggered filters.
HOSTCODE	char	7	Response code returned by the processor. This value is not normalized by VeriSign.
RESPTEXT	char	17	Text corresponding to the response code returned by the processor. This text is not normalized by VeriSign.
PROCAVS	char	2	AVS (Address Verification Service) response from the processor

Parameter	Type	Length	Description
PROCCVV2	char	1	CVV2 (buyer authentication) response from the processor
PROCCARDSECURE	char	1	VPAS/SPA response from the processor
ADDLMSGs	char	Up to 1048 characters. Typically 50 characters.	Additional error message that indicates that the merchant used a feature that is disabled
TRANSSTATE	Integer	10	State of the transaction. The values are: 0 = General succeed state 1 = General error state 3 = Authorization approved 6 = Settlement pending (transaction is scheduled to be settled) 7 =Settlement in progress (transaction involved in a currently ongoing settlement) 8 = Settled successfully 9 = Authorization captured (once an authorization type transaction is captured, its TRANSSTATE becomes 9) 10 =Capture failed (an error occurred while trying to capture an authorization because the transaction was already captured) 11 = Failed to settle (transactions fail settlement usually because of problems with the merchant's processor or because the card type is not set up with the merchant's processor) 12 - Unsettled transaction because of incorrect account information 14 = For various reasons, the batch containing this transaction failed settlement 16 = Merchant ACH settlement failed; (need to manually collect it). For information on TRANSSTATE incremental values, see the table below.

Parameter	Type	Length	Description
DATE_TO_SETTLE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only before settlement has started.
BATCHID	Integer	10	Value available only after settlement has assigned a Batch ID.
SETTLE_DATE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only after settlement has completed.

Note If you use Nashville, TeleCheck, or Paymentech, then you must use a client version newer than 2.09 to take advantage of the MEDIUM verbosity setting. For information on interpreting the responses returned by the processor for the **MEDIUM** Verbosity setting, contact your processor directly. Processor contact information appears in the “Introduction” chapter of *VeriSign Payflow Pro Developer’s Guide*.

The table below shows the increments that are possible on basic TRANSSTATE values.

Increment	Meaning
+100	No client acknowledgment (ACK) is received (=status 0 in V2), for example, 106 is TRANSSTATE 6.
+200	The host process never receives ACK from the transaction broker (or backend payment server). A transaction with a TRANSSTATE of +200 is basically in limbo and will not be settled.
+1000	Voided transactions. Any TRANSSTATE of +1000 (for example, 1006) means the transaction was settle pending. However, it was voided either through the API, VeriSign Manager, or VeriSign Customer Service.

RESULT Values Specific to Fraud Protection Services

A RESULT value greater than zero indicates a decline or error. For this type of error, a RESPMSG name/value pair is included. The exact wording of the RESPMSG may

vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

Table 7-1 VeriSign Transaction RESULTS/RESPMSGs

RESULT	RESPMSG and Explanation
125	Fraud Protection Services Filter — Declined by filters
126	Fraud Protection Services Filter — Flagged for review by filters
127	Fraud Protection Services Filter — Not screened by filters
128	Fraud Protection Services Filter — Declined by merchant after being flagged for review by filters
131	Version 1 Payflow Pro SDK client no longer supported. Upgrade to the most recent version of the Payflow Pro client.

Changing the Verbosity Setting

- ◆ **Setting the default verbosity level for all transactions**

Contact VeriSign Customer Service to set your account's verbosity setting to **LOW** or **MEDIUM** for all transaction requests.

- ◆ **Setting the verbosity level on a per-transaction basis**

To specify a setting for verbosity that differs from your account's current setting, include the **VERBOSITY=<value>** name/value pair in the transaction request, where **<value>** is **LOW** or **MEDIUM**.

Note In the examples below, the <action> tag value is the state to which the transaction has been set. Values are: R = Review, J = Reject, A = Accept.

Example Response for an Authentication Transaction With Verbosity=Low

RESULT=126&PNREF=VFHA28926593&RESPMSG=Under review by Fraud Service&AUTHCODE=041PNI&AVSADDR=Y&AVSZIP=N&CVV2MATCH=X&HOSTCODE=A&PROCAVS=A&PROCCVV2=X&IAVS=N&PREFPSMSG=Review: More than one rule was triggered for Review&POSTFPSMSG=Review: More than one rule was triggered for Review

Example Response for an Authentication Transaction With Verbosity=Medium

```

RESULT=126&PNREF=VFHA28926593&RESPMSG=Under review by Fraud
Service&AUTHCODE=041PNI&AVSADDR=Y&AVSZIP=N&CVV2MATCH=X&HOSTCO
DE=A&PROCAVS=A&PROCCVV2=X&IAVS=N&PREFPSMSG=Review: More than one
rule was triggered for Review&FPS_PREXMLDATA[2898]=<triggeredRules><rule
num="1"><ruleId>2</ruleId><ruleAlias>CeilingAmount</ruleAlias><ruleDescription>Total
Purchase Price Ceiling</ruleDescription><action>R</action><triggeredMessage>The
purchase amount of 7501 is greater than the ceiling value set of
7500</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>CeilingValue</name><value
type="USD">75.00</value></ruleParameter></rulevendorparms></rule><rule
num="2"><ruleId>6</ruleId><ruleAlias>HighOrderNumber</ruleAlias><ruleDescription>
Total Item Ceiling</ruleDescription><action>R</action><triggeredMessage>16 items
were ordered, which is over the maximum allowed quantity of
15</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><value
type="Integer">15</value></ruleParameter></rulevendorparms></rule><rule
num="3"><ruleId>7</ruleId><ruleAlias>BillShipMismatch</ruleAlias><ruleDescription>S
hipping/Billing Mismatch</ruleDescription><action>R</action><triggeredMessage>The
billing and shipping addresses did not match</triggeredMessage></rule><rule
num="4"><ruleId>13</ruleId><ruleAlias>HighRiskBinCheck</ruleAlias><ruleDescription
>BIN Risk List Match</ruleDescription><action>R</action><triggeredMessage>The card
number is in a high risk bin list</triggeredMessage></rule><rule
num="5"><ruleId>37</ruleId><ruleAlias>HighRiskZIPCheck</ruleAlias><ruleDescription
>Zip Risk List Match</ruleDescription><action>R</action><triggeredMessage>High risk
shipping zip</triggeredMessage></rule><rule
num="6"><ruleId>16</ruleId><ruleAlias>BillUSPostalAddressCheck</ruleAlias><ruleDe
scription>USPS Address Validation
Failure</ruleDescription><action>R</action><triggeredMessage>The billing address is
not a valid US Address</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>AddressToVerify</name><value
type="String">bill</value></ruleParameter></rulevendorparms></rule><rule
num="7"><ruleId>10</ruleId><ruleAlias>HighRiskEmailCheck</ruleAlias><ruleDescripti
on>Email Service Provider Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The email address
fraud@asiamail.com in billEmail was found in a high risk email provider
list</triggeredMessage></rule><rule
num="8"><ruleId>38</ruleId><ruleAlias>GeoLocationCheck</ruleAlias><ruleDescription
>Geo-Location
Failure</ruleDescription><action>R</action><triggeredMessage>GeoLocation
difference: Bill Address and IP, GeoLocation difference: Ship Address and
IP</triggeredMessage></rule><rule
num="9"><ruleId>8</ruleId><ruleAlias>NonUSIPAddress</ruleAlias><ruleDescription>I
nternational IP Address</ruleDescription><action>R</action><triggeredMessage>The IP
address is from: CZ</triggeredMessage></rule><rule
num="10"><ruleId>41</ruleId><ruleAlias>HighRiskFreightCheck</ruleAlias><ruleDescri

```

```
ption>Freight Forwarder
Match</ruleDescription><action>R</action><triggeredMessage>High risk freight
forwarder</triggeredMessage></rule></triggeredRules>&POSTFPSMSG=Review: More
than one rule was triggered for
Review&FPS_POSTXMLDATA[682]=<triggeredRules><rule
num="1"><ruleId>1</ruleId><ruleAlias>AVS</ruleAlias><ruleDescription>AVS
Failure</ruleDescription><action>R</action><triggeredMessage>AVS check failed: Full
Security</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><value
type="String">Full</value></ruleParameter></rulevendorparms></rule><rule
num="2"><ruleId>23</ruleId><ruleAlias>CSCFailure</ruleAlias><ruleDescription>CSC
Failure</ruleDescription><action>R</action><triggeredMessage>CSC check failed,
returned X</triggeredMessage><rulevendorparms><ruleParameter
num="1"><name>Value</name><value
type="String">Full</value></ruleParameter></rulevendorparms></rule></triggeredRules
>
```

Accepting or Rejecting Transactions That Trigger Filters

You can submit a transaction request that either accepts or rejects a transaction that triggered a filter (Result code 126). This is the functional equivalent of the operations discussed in “Acting on Transactions that Triggered Filters” on page 30.

- + **Accept:** Submit the transaction for normal processing.
- + **Reject:** Do not submit the transaction for processing. See “Rejecting Transactions” on page 32.

Note You must contact VeriSign Customer Support to enable this feature.
Telephone: 888-883-9770 or 650-426-3150. E-mail: vps-support@verisign.com

To accept or reject a transaction, include the following values in the transaction request:

- + TRXTYPE=U
 - + ORIGID=<PNREF returned for the original transaction>
 - + UPDATEACTION=APPROVE (to accept)
- or —
- UPDATEACTION=FPS_MERCHANT_DECLINE (to reject)

Logging Transaction Information

VeriSign maintains a record of all transactions executed on your account. Use VeriSign Manager to view the record and use the information to help reconcile your accounting records.

Note This record is not the official bank statement. The activity on your account is the official record.

In addition, VeriSign strongly recommends that you log all transaction results (except for check information) on your own system. At a minimum, log the following data:

- + PNREF (called the **Transaction ID** in VeriSign Manager reports)
- + Transaction Date
- + Transaction Amount

If you have any questions regarding a transaction, use the **PNREF** to identify the transaction.

Viewing Buyer Authentication Reports with VeriSign Manager

If you subscribe to VeriSign's Buyer Authentication Service, the you can use the *Buyer Authentication* section on the VeriSign Manager *Reports* page to generate the following types of reports:

- + Use the *Buyer Authentication Audit* report to view authentication results. Because you are charged only for buyer authentication transactions for which the cardholder is enrolled, this report can help you to understand your VeriSign Buyer Authentication bill. In addition, you can use this report to troubleshoot the Buyer Authentication service. See page 75.
- + Use the *Buyer Authentication Transaction* report to view both authentication results and the associated payment authorizations. The report provides an end-to-end view of authentication through authorization. You can view any or all authentication result types: successful, unsuccessful, and attempted. See page 78.

Tip You can generate reports as far back as one year and for a time range (span) of three months.

To view the details of a transaction, click the **Transaction ID** link in any transaction report, as described in *VeriSign Manager User's Guide*.

Generating a Buyer Authentication Audit Report

Use the *Buyer Authentication Audit* report to view authentication results. Because you are charged only for buyer authentication transactions for which the cardholder is enrolled, this report can help you to understand your VeriSign Buyer Authentication bill. In addition, you can use the report to troubleshoot the Buyer Authentication service.

Note The *Buyer Authentication Audit* report is available only for Payflow Pro accounts.

- 1 Click **Reports** → **Buyer Authentication Audit Report**. The *Buyer Authentication Audit Report* page opens.

Buyer Authentication Audit Report

Use this form to generate a list of all Verify Enrollment and Validate Authentication transactions.

Buyer Authentication Audit Report

☒ **Preset Time:** Today (Fri Mar 14, 2003)

☐ **Custom Time:** From: March 14, 2003 Time: 00 : 00 : 00
To: March 14, 2003 Time: 23 : 59 : 59

View: Transactions I Am Billed For

Tender Type: ☒ MasterCard ☒ Visa

Display as: HTML (Not recommended for large reports)

Sort by: Transaction Time Ascending

Mode: View Live Transactions

- 2 Specify the date range of transactions to include in the report.
- 3 Specify the type of transactions to view:
 - Transactions for which you are billed. You are billed for any Verify Enrollment transaction that indicates that the cardholder is enrolled. That is, Payflow Pro TRXNTYPE=E with RESULT=E.
 - Verify Enrollment transactions. (Payflow Pro TRXNTYPE=E) In Verify Enrollment transactions, the Issuer provides a “yes/no/could-not-determine” response to the question of whether the cardholder is enrolled in the buyer authentication program.
 - Validate Authentication transactions. (Payflow Pro TRXNTYPE=Z) In Validate Authentication transactions, the VeriSign buyer authentication servers validate the digital signature on the Issuer’s statement of whether the customer submitted the correct password on the buyer authentication page.
 - All Verify Enrollment and Validate Authentication transactions
- 4 Specify the **Tender Type** to include in the report: **MasterCard** and/or **Visa**.
- 5 In the **Display as** field, specify either **HTML** or **ASCII** output.

- 6 In the **Sort by** field, specify that the results should be ordered by **Authentication ID** or by **Transaction Time**. Then specify either an **Ascending** or a **Descending** sort.
- 7 In the **Mode** field, specify either **Live** or **Test** transactions.
- 8 Click **Submit**.

Example Buyer Authentication Audit Report

Buyer Authentication Audit Report for Fri Feb 14, 2003 to Fri Mar 14, 2003 Sorted By: Transaction Time					
Page 1 of 1					
#	Authentication ID	Timestamp	Transaction Type	Tender Type	Result
1.	f75cca3a6bac1694a2f8	Mar 12, 2003 12:14:52 PM	Verify Enrollment	MasterCard	E - Card Enrolled
2.	de75a5c57827c9f2c84f	Mar 12, 2003 12:15:34 PM	Verify Enrollment	MasterCard	E - Card Enrolled
3.	6652abcc18421e301d96	Mar 12, 2003 12:15:43 PM	Verify Enrollment	MasterCard	E - Card Enrolled

The following information appears in the *Buyer Authentication Audit* report:

Table 8-1 Pre-Authorization report

Field	Description
#	Temporary number assigned to the transaction. This number is used for reference purposes only while viewing the report, and is not associated with the transaction.
Authentication ID	<p>Unique identifier associated with the authentication of the customer for this transaction. Click this value to view the <i>Transaction Detail</i> page, as described on page 81.</p> <p>Note: The <i>Transaction Detail</i> page describes the transactions required to authenticate the customer, and is not the same as the standard payment <i>Transaction Detail</i> page.</p> <p>You cannot perform a search on the Authentication ID using VeriSign Manager.</p>
Timestamp	Time and date that the transaction occurred.
Transaction Type	Verify Enrollment transaction (Payflow Pro TRXNTYPE=E) or Validate Authentication transaction (Payflow Pro TRXNTYPE=Z).
Tender Type	MasterCard or Visa

Table 8-1 Pre-Authorization report (Continued)

Field	Description
Result	<p>Result of the buyer authentication process — the AUTHENTICATION_STATUS value.</p> <p>E - Cardholder enrolled O - Cardholder not enrolled Y - Authentication Successful X - Unable to verify I - Error While Verifying Enrollment</p>

Generating a Buyer Authentication Transaction Report

The *Buyer Authentication Transaction* report lists transactions that involved buyer authentication transactions (that is, the database holds ECI or Authentication ID data for these transactions). You have the option of viewing successful, unsuccessful, and attempted transactions to authenticate the cardholder.

- 1 Click **Reports → Buyer Authentication Transaction Report**. The *Buyer Authentication Transaction* page opens.

Buyer Authentication Transaction Report

Use this form to search for transaction types specific to the buyer authentication service.

Buyer Authentication Report

☒ **Preset Time:** Today (Fri Mar 14, 2003)

☐ **Custom Time:** From: March 14, 2003 Time: 00 : 00 : 00
 To: March 14, 2003 Time: 23 : 59 : 59

Tender Type: ☒ MasterCard ☒ Visa

ECI Indicators: ☒ Buyer Authentication Successful ☐ Buyer Authentication Unsuccessful ☐ Buyer Authentication Attempted

Display as: HTML (Not recommended for large reports)

Sort by: Transaction Time Ascending

Mode: View Live Transactions

- 2 Specify the date range of transactions to include in the report.
- 3 Specify the **Tender Type** to include in the report: **MasterCard** and/or **Visa**.
- 4 Specify any or all of the **ECI Indicators** to use to extract the data:
 - **Buyer Authentication Successful:** Show all transactions for which the customer provided the correct buyer authentication password. (ECI= 2 or 5 and CAVV_RESPONSE is not N)

- **Buyer Authentication Unsuccessful:** Show all transactions for which the attempt at buyer authentication failed for any reason. (ECI= 1 or 7 and CAVV_RESPONSE=N)
 - **Buyer Authentication Attempted:** Show all transactions for which an attempt at buyer authentication was made, regardless of the result. (ECI=6 and CAVV_RESPONSE is not N)
- 5 In the **Display as** field, specify either **HTML** or **ASCII** output.
 - 6 In the **Sort by** field, specify that the results should be ordered by **Transaction ID**, by **Transaction Time**, or by **ECI Indicator**. Then specify either an **Ascending** or a **Descending** sort.
 - 7 In the **Mode** field, specify either **Live** or **Test** transactions.
 - 8 Click **Submit**.

Example Buyer Authentication Transaction Report

Buyer Authentication Transaction Report								
for								
Fri Feb 14, 2003 to Fri Mar 14, 2003								
Sorted By: Transaction Time								
Page 1 of 1								
#	Transaction ID	Time	Transaction Type	Tender Type	Amount	Result	Response Message	ECI
1.	VGIA57894393	Feb 27, 2003 02:44:47 PM	Sale	Visa	\$3.10	0	Approved	05
2.	VGIA57894478	Feb 27, 2003 02:46:08 PM	Sale	Visa	\$3.10	0	Approved	05
3.	VGIA58696081	Mar 01, 2003 06:03:54 PM	Sale	M/C	\$1.10	0	Approved	2

The following information appears in the *Buyer Authentication Transaction* report:

Table 8-2 Buyer Authentication report

Field	Description
#	Temporary number assigned to the transaction. This number is used for reference purposes only while viewing the report, and is not associated with the transaction.
Transaction ID	Unique Transaction Identification number generated by VeriSign. This is the same as the Payflow Pro PNREF value. Click this value to view the <i>Transaction Detail</i> page, as described in <i>VeriSign Manager User's Guide</i> . Note: The Transaction ID link leads to the standard payment <i>Transaction Detail</i> page, not to the <i>Transaction Detail</i> page associated with Buyer Authentication transactions.
Time	Time and date that the transaction occurred.
Transaction Type	Sale or Authorization transaction.
Tender Type	MasterCard or Visa
Amount	The amount of the transaction.
Result	Result of the payment transaction. Result codes are described in "RESULT Codes and RESPMSG Values" on page 85.
Response Message	Plain-language description associated with the Result Code.
ECI	Electronic Commerce Indicator. This value describes the status of the attempt to authenticate the buyer. Described in the table below.

ECI Values

State	Visa	MasterCard
Successful	5	2
Attempted	6	—
Unsuccessful	7	1

Transaction Detail Page

The *Transaction Detail* page displays the results associated with the buyer authentication transaction.

Transaction Detail			
This report provides information on a specific transaction.			
Buyer Authentication - Verify Enrollment			
Authentication ID:	834949962ed17a07cffe	Event Timestamp:	2003-02-10 17:52:10
Transaction Type:	E	Authentication Result:	E - Card Enrolled
Card Number Last 4 Digits:	0002	Tender Type:	Visa
ECI:		Error Code:	0 - Successful
Client IP Address:	192.168.101.19	Client Version:	300

Note Contact VeriSign Customer Support if you need to request PARES information needed to resolve a dispute with your issuer.

Responses to Credit Card Transaction Requests

This chapter describes the contents of a response to a credit card transaction request.

When a transaction finishes, VeriSign returns a response string made up of name/value pairs. For example, this is a response to a credit card **Sale** transaction request:

```
RESULT=0&PNREF=VXYZ01234567&RESPMSG=APPROVED&AUTHCODE=123456&AVSADDR=Y&AVSZIP=N&IAVS=Y&CVV2MATCH=Y
```

Contents of a Response to a Credit Card Transaction Request

All transaction responses include values for RESULT, PNREF, RESPMSG. A value for AUTHCODE is included for Voice Authorization transactions. Values for AVSADDR and AVSZIP are included if you use AVS. Table 9-1 describes the values returned in a response string.

Table 9-1 Transaction response values

Field	Description	Type	Length
PNREF	VeriSign Reference ID, a unique number that identifies the transaction. PNREF is described in “PNREF Format” on page 85.	Alpha-numeric	12
RESULT	The outcome of the attempted transaction. A result of 0 (zero) indicates the transaction was approved. Any other number indicates a decline or error. RESULT codes are described in “RESULT Codes and RESPMSG Values” on page 85.	Numeric	Variable
CVV2MATCH	Result of the card security code (CVV2) check. This value does not affect the outcome of the transaction.	Alpha Y, N, X, or no response	1

Table 9-1 Transaction response values (Continued)

Field	Description	Type	Length
RESPMSG	The response message returned with the transaction result. Exact wording varies. Sometimes a colon appears after the initial RESPMSG followed by more detailed information. Response messages are described in "RESULT Codes and RESPMSG Values" on page 85.	Alpha-numeric	Variable
AUTHCODE	Returned for Sale, Authorization, and Voice Authorization transactions. AUTHCODE is the approval code obtained over the phone from the processing network. AUTHCODE is required when submitting a Force (F) transaction.	Alpha-numeric	6
AVSADDR	AVS address responses are for advice only. This process does not affect the outcome of the authorization. See "Using Address Verification Service (AVS)" on page 40.	Alpha Y, N, X, or no response	1
AVSZIP	AVS ZIP code responses are for advice only. This process does not affect the outcome of the authorization. See "Using Address Verification Service (AVS)" on page 40.	Alpha Y, N, X, or no response	1
IAVS	International AVS address responses are for advice only. This value does not affect the outcome of the transaction. Indicates whether AVS response is international (Y), US (N), or cannot be determined (X). Client version 3.06 or later is required. See "Using Address Verification Service (AVS)" on page 40.	Alpha Y, N, X, or no response	1

PNREF Value

The PNREF is a unique transaction identification number issued by VeriSign that identifies the transaction for billing, reporting, and transaction data purposes. The PNREF value appears in the Transaction ID column in VeriSign Manager reports.

- The PNREF value is used as the TRANSID value (original transaction ID) in delayed capture transactions (TRXTYPE=D), credits (TRXTYPE=C), inquiries (TRXTYPE=I), and voids (TRXTYPE=V).
- The PNREF value is used as the TRANSID value (original transaction ID) value in reference transactions for authorization (TRXTYPE=A) and Sale (TRXTYPE=S).

Note The PNREF is also referred to as the Transaction ID in Payflow Link documentation.

PNREF Format

The PNREF is a 12-character string of printable characters, for example:

- VADE0B248932
- ACRAF23DB3C4

Note Printable characters also include symbols other than letters and numbers such as the question mark (?). A PNREF typically contains letters and numbers only.

Historically, the contents of a PNREF indicated a test or a live transaction:

- For Test servers, the first and fourth characters were alpha characters (letters), and the second and third characters were numeric, for example: V53A17230645.
- For Live servers, the first four characters were alpha characters (letters), for example: VPNE12564395.

However, this is not always the case, and as a rule, you should not place any meaning on the contents of a PNREF.

RESULT Codes and RESPMSG Values

RESULT is the first value returned in the VeriSign server response string. The value of the RESULT parameter indicates the overall status of the transaction attempt.

- A value of 0 (zero) indicates that no errors occurred and the transaction was approved.

- A value less than zero indicates that a communication error occurred. In this case, no transaction is attempted.
- A value greater than zero indicates a decline or error.

The response message (RESPMSG) provides a brief description for decline or error results.

RESULT Values for Transaction Declines or Errors

For non-zero Results, the response string includes a RESPMSG name/value pair. The exact wording of the RESPMSG (shown in **bold**) may vary. Sometimes a colon appears after the initial RESPMSG followed by more detailed information.

Table 9-2 VeriSign transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
0	Approved
1	User authentication failed. Error is caused by one or more of the following: <ul style="list-style-type: none"> ■ Invalid User ID, Merchant Login ID, Partner ID, or Password entered in your parameter string. Login information is case-sensitive. ■ Invalid Processor information entered. Contact merchant bank to verify. ■ "Allowed IP Address" security feature implemented. ■ Test account submitting transactions to live VeriSign servers.
2	Invalid tender type. Your merchant bank account does not support the following credit card type that was submitted.
3	Invalid transaction type. Transaction type is not appropriate for this transaction. For example, you cannot credit an authorization-only transaction.
4	Invalid amount format
5	Invalid merchant information. Processor does not recognize your merchant account information. Contact your bank account acquirer to resolve this problem.
7	Field format error. Invalid information entered. See RESPMSG.
8	Not a transaction server
9	Too many parameters or invalid stream
10	Too many line items
11	Client time-out waiting for response

Table 9-2 VeriSign transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
12	Declined. Check the credit card number and transaction information to make sure they were entered correctly. If this does not resolve the problem, have the customer call the credit card issuer to resolve.
13	Referral. Transaction was declined but could be approved with a verbal authorization from the bank that issued the card. Submit a manual Voice Authorization transaction and enter the verbal auth code.
19	Original transaction ID not found. The transaction ID you entered for this transaction is not valid. See RESPMSG.
20	Cannot find the customer reference number
22	Invalid ABA number
23	Invalid account number. Check credit card number and re-submit.
24	Invalid expiration date. Check and re-submit.
25	Invalid Host Mapping. Not signed up for this tender type.
26	Invalid vendor account
27	Insufficient partner permissions
28	Insufficient user permissions
29	Invalid XML document. This could be caused by an unrecognized XML tag or a bad XML format that cannot be parsed by the system.
30	Duplicate transaction
31	Error in adding the recurring profile
32	Error in modifying the recurring profile
33	Error in canceling the recurring profile
34	Error in forcing the recurring profile
35	Error in reactivating the recurring profile
36	OLTP Transaction failed
37	Invalid recurring profile ID
50	Insufficient funds available in account
99	General error. See RESPMSG.

Table 9-2 VeriSign transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
100	Transaction type not supported by host
101	Time-out value too small
102	Processor not available
103	Error reading response from host
104	Timeout waiting for processor response. Try your transaction again.
105	Credit error. Make sure you have not already credited this transaction, or that this transaction ID is for a creditable transaction. (For example, you cannot credit an authorization.)
106	Host not available
107	Duplicate suppression time-out
108	Void error. See RESPMSG. Make sure the transaction ID entered has not already been voided. If not, then look at the Transaction Detail screen for this transaction to see if it has settled. (The Batch field is set to a number greater than zero if the transaction has been settled). If the transaction has already settled, your only recourse is a reversal (credit a payment or submit a payment for a credit).
109	Time-out waiting for host response
111	Capture error. Either an attempt to capture a transaction that is not an authorization transaction type, or an attempt to capture an authorization transaction that has already been captured.
112	Failed AVS check. Address and ZIP code do not match. An authorization may still exist on the cardholder's account.
113	Merchant sale total will exceed the sales cap with current transaction. ACH transactions only.
114	Card Security Code (CSC) Mismatch. An authorization may still exist on the cardholder's account.
115	System busy, try again later
116	VPS Internal error. Failed to lock terminal number

Table 9-2 VeriSign transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
117	<p>Failed merchant rule check. One or more of the following three failures occurred:</p> <ul style="list-style-type: none"> ■ An attempt was made to submit a transaction that failed to meet the security settings specified on the VeriSign Manager <i>Security Settings</i> page. If the transaction exceeded the Maximum Amount security setting, then no values are returned for AVS or CSC. See <i>VeriSign Manager User's Guide</i> for information on the <i>Security Settings</i> page. ■ AVS validation failed. The AVS return value should appear in the RESPMSG. ■ CSC validation failed. The CSC return value should appear in the RESPMSG.
118	Invalid keywords found in string fields
122	Merchant sale total will exceed the credit cap with current transaction. ACH transactions only.
125	Fraud Protection Services Filter — Declined by filters
126	<p>Fraud Protection Services Filter — Flagged for review by filters</p> <p>Important Note: Result code 126 indicates that a transaction triggered a fraud filter. This is not an error, but a notice that the transaction is in a review status. The transaction has been authorized but requires you to review and to manually accept the transaction before it will be allowed to settle.</p> <p>This result occurred due to that fact that all new Payflow accounts include a “test drive” of the Fraud Protection Services at no charge. The filters are on by default, and a suspicious transaction triggered Result code 126. You can modify these settings based on your business needs.</p> <p>Result code 126 is intended to give you an idea of the kind of transaction that is considered suspicious to enable you to evaluate whether you can benefit from using the Fraud Protection Services.</p> <p>To eliminate result 126, turn the filters off.</p> <p>For more information, see the chapter entitled “Assessing Transactions that Triggered Filters” in <i>Fraud Protection Services Guide</i> or <i>User's Guide for Payflow Link Guide With Fraud Protection Services</i>.</p>
127	Fraud Protection Services Filter — Not processed by filters
128	Fraud Protection Services Filter — Declined by merchant after being flagged for review by filters
131	Version 1 Payflow Pro SDK client no longer supported. Upgrade to the most recent version of the Payflow Pro client.
150	Issuing bank timed out

Table 9-2 VeriSign transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
151	Issuing bank unavailable
1000	Generic host error. This is a generic message returned by your credit card processor. The RESPMSG will contain more information describing the error.
1001	Buyer Authentication Service unavailable
1002	Buyer Authentication Service — Transaction timeout
1003	Buyer Authentication Service — Invalid client version
1004	Buyer Authentication Service — Invalid timeout value
1011	Buyer Authentication Service unavailable
1012	Buyer Authentication Service unavailable
1013	Buyer Authentication Service unavailable
1014	Buyer Authentication Service — Merchant is not enrolled for Buyer Authentication Service (3-D Secure). To enroll, log in to VeriSign Manager, click Security, and then click the Buyer Authentication Service banner on the page.
1016	Buyer Authentication Service — 3-D Secure error response received. Instead of receiving a PARES response to a Validate Authentication transaction, an error response was received.
1017	Buyer Authentication Service — 3-D Secure error response is invalid. An error response is received and the response is not well formed for a Validate Authentication transaction.
1021	Buyer Authentication Service — Invalid card type
1022	Buyer Authentication Service — Invalid or missing currency code
1023	Buyer Authentication Service — merchant status for 3D secure is invalid
1041	Buyer Authentication Service — Validate Authentication failed: missing or invalid PARES
1042	Buyer Authentication Service — Validate Authentication failed: PARES format is invalid
1043	Buyer Authentication Service — Validate Authentication failed: Cannot find successful Verify Enrollment
1044	Buyer Authentication Service — Validate Authentication failed: Signature validation failed for PARES

Table 9-2 VeriSign transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
1045	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid amount in PARES
1046	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid acquirer in PARES
1047	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid Merchant ID in PARES
1048	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid card number in PARES
1049	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid currency code in PARES
1050	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid XID in PARES
1051	Buyer Authentication Service — Validate Authentication failed: Mismatched or invalid order date in PARES
1052	Buyer Authentication Service — Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction

RESULT Values for Communications Errors

A value for RESULT less than zero indicates that a communication error occurred. In this case, no transaction is attempted.

A value of -1 or -2 usually indicates a configuration error. Either the VeriSign server is unavailable, or incorrect server/socket pairs have been specified. A value of -1 can also result when there are Internet connectivity errors. Refer other errors to VeriSign at vps-support@verisign.com.

Table 9-3 RESULT values for communications errors

RESULT	Description
-1	Failed to connect to host
-2	Failed to resolve hostname
-5	Failed to initialize SSL context
-6	Parameter list format error: & in name

Table 9-3 RESULT values for communications errors (Continued)

RESULT	Description
-7	Parameter list format error: invalid [] name length clause
-8	SSL failed to connect to host
-9	SSL read failed
-10	SSL write failed
-11	Proxy authorization failed
-12	Timeout waiting for response
-13	Select failure
-14	Too many connections
-15	Failed to set socket options
-20	Proxy read failed
-21	Proxy write failed
-22	Failed to initialize SSL certificate
-23	Host address not specified
-24	Invalid transaction type
-25	Failed to create a socket
-26	Failed to initialize socket layer
-27	Parameter list format error: invalid [] name length clause
-28	Parameter list format error: name
-29	Failed to initialize SSL connection
-30	Invalid timeout value
-31	The certificate chain did not validate, no local certificate found
-32	The certificate chain did not validate, common name did not match URL
-99	Out of memory



APPENDIX A

How Filters Work

The filters screen transactions using the following order and logic (see the illustration on the next page):

- 1 The merchant generates a transaction. The transaction must include the data values required by the filters. For example if you have turned on the Shipping/Billing Address Mismatch filter, then the data must include all shipping and billing address information. Remember that recurring transactions are not screened by filters.

- 2 The group of filters that are set to reject transactions that meet particular criteria screens the transaction. These filters are known as *Reject filters*.

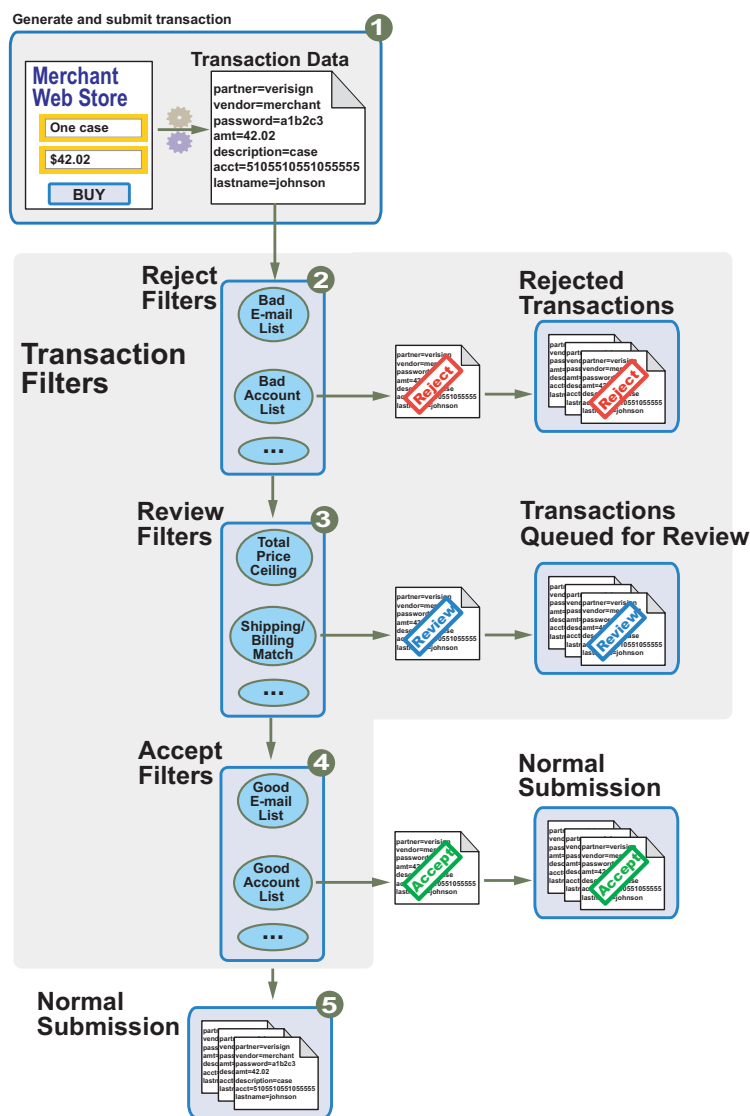
If the transaction includes data that meets the criteria of one of the filters (for example, the e-mail address appears in the Bad List), then the transaction is rejected, all other filters are skipped, and the filters move on to screen the next transaction.

If none of the Reject filters is triggered, then the transaction passes to the next set of filters.

- 3 If the transaction triggers no Reject filter, then the group of filters that are set to review transactions that meet particular criteria screens the transaction. These filters are known as *Review filters*.

If the transaction includes data that meets the criteria of one of the Review filters (for example, the shipping address differs from the billing address), then the filter

marks the transaction for review. Next, the remaining Review filters also screen the transaction.



Once all Review filters have screened the transaction, the transaction is sent to a queue for your review. No further steps are taken by the filters. You later review the reasons that the transaction triggered the filters to determine which action to take (accept or reject).

- 4 If the transaction triggers no Reject filter and no Review filter, then the group of filters that are set to accept transactions that meet particular criteria screens the transaction. These filters are known as *Accept filters*.

If the transaction includes data that meets the criteria of one of the filters (for example, the account number appears in the Good List), then the transaction is sent to the normal transaction submission process, and all other filters are skipped.

- 5 If the transaction triggers no filter of any type, then the server sends the transaction to the normal transaction submission process.



Fraud Filter Reference

This appendix describes the filters that make up part of the VeriSign Fraud Protection Services. Filters analyze transactions and act on those that show evidence of potential fraudulent activity. Filters can set such transactions aside for your review or reject them outright, depending on settings that you specify.

Filters are grouped to help you to assess the risk types and to take action (accept, reject, or continue in the review state).

In This Chapter

Filters Included with the Fraud Protection Services, described on page 97

About VeriSign's Risk Lists, described on page 99

VeriSign's Guidance on Interpreting Filter Results, described on page 99

"Transaction Data Required by Filters" on page 99

Unusual Order Filters, described on page 100

High-risk Payment Filters, described on page 102

High-risk Address Filters, described on page 110

High-risk Customer Filters, described on page 115

International Order Filters, described on page 116

Accept Filters, described on page 118

Custom Filters, described on page 119

Filters Included with the Fraud Protection Services

VeriSign's Fraud Protection Services offers Basic and Advanced options. The filters included with each option are listed here. In addition, the optional **Buyer Authentication Failure** filter is described on page 98.

Filters Included with the Basic Fraud Protection Services Option

Total Purchase Price Ceiling Filter, described on page 100

Total Item Ceiling Filter, described on page 100

Shipping/Billing Mismatch Filter, described on page 101

AVS Failure Filter, described on page 102

CSC Failure Filter, described on page 105

ZIP Risk List Match Filter, described on page 110

Freight Forwarder Risk List Match Filter, described on page 110

IP Address Velocity Filter, described on page 114

Filters Included with the Advanced Fraud Protection Services Option

All Basic filters plus:

USPS Address Validation Failure Filter, described on page 111

BIN Risk List Match Filter, described on page 109

E-mail Service Provider Risk List Match Filter, described on page 112

IP Address Match Filter, described on page 112

Account Number Velocity Filter, described on page 109

Geo-location Failure Filter, described on page 113

Bad Lists, described on page 115

International Shipping/Billing Address Filter, described on page 116

International AVS Filter, described on page 117

International IP Address Filter, described on page 117

Country Risk List Match Filter, described on page 116

Good Lists, described on page 118

Total Purchase Price Floor Filter, described on page 119

Custom Filters, described on page 119

Product Watch List Filter, described on page 101

Account Number Velocity Filter, described on page 109

Special Case: Buyer Authentication Failure Filter

The optional Buyer Authentication service is described in “The VeriSign Buyer Authentication Service” on page 7. The **Buyer Authentication Failure** filter, which

screens the customer authentication data returned by the service, is described on page 107.

About VeriSign's Risk Lists

Filters whose name includes “Risk List” make use of lists that VeriSign manages. VeriSign performs extensive statistical analysis of millions of e-commerce transactions to determine transaction data elements (for example BIN numbers or ZIP codes) that are statistically more likely than average to be correlated with fraudulent transactions.

Inclusion in a Risk List is not an absolute indication of fraud, only a statistical correlation that indicates that you should evaluate the transaction more closely (and in conjunction with other filter results for the transaction).

VeriSign's Guidance on Interpreting Filter Results

VeriSign provides detailed guidance on interpreting filter responses in a *Transaction Review Primer*. To view the primer, click the **What Do I Do** button on the *Transaction Details* page.

Filters Applied After Processing

Most filters are applied to the transaction request before forwarding the request to the processor. The following filters are applied to the transaction results that the processor returns:

- + AVS Failure filter (described on page 102)
- + CSC Failure filter (described on page 105)
- + International AVS filter (described on page 117)
- + Compound filters (described on page 119)

Transaction Data Required by Filters

“Downloading the Payflow Pro SDK (Including APIs and API Documentation)” on page 62 provides the full list, for each filter, of each transaction value that you must send to Payflow Pro. For example, to ensure that the Total Item Ceiling filter can screen an order, you must provide the total number of items that make up the order.

Unusual Order Filters

Unusual Order Filters identify transactions that exceed the normal size for your business. Because fraudsters might not feel limited in their purchasing power, they sometimes place orders that are much larger than the norm.

Total Purchase Price Ceiling Filter

What does the filter do?

This filter compares the total amount of the transaction (including tax, shipping and handling fees) to the maximum purchase amount (the ceiling) that you specify.

The specified action is taken whenever a transaction amount exceeds the specified ceiling.

IMPORTANT! The *Maximum amount per transaction* setting in the Account menu controls all transactions, even those that are less than or exceed the *Total Purchase Price Ceiling* filter. See “Configuring Transaction Settings” on page 14.

How does the filter protect me?

An unusually high purchase amount (compared to the average for your business) can indicate potential fraudulent activity. Because fraudsters are not paying with their own money, they are not price-sensitive.

Total Item Ceiling Filter

What does the filter do?

This filter compares the total number of items (or volume for bulk commodities) to the maximum count (the ceiling) that you specify.

The specified action is taken whenever the item count in a transaction exceeds the specified ceiling.

How does the filter protect me?

An unusually high item count (compared to the average for your business) can indicate potential fraudulent activity. Fraudsters frequently attempt to order large numbers of attractive items that can easily be resold.

Tip In addition, some items are more susceptible to fraud than others. For example, a computer can be resold for much more money than can a pair of sport shoes. The likelihood of selling the item quickly is also a factor.

Shipping/Billing Mismatch Filter

What does the filter do?

This filter screens for differences between the shipping information and the billing information (street, state, ZIP code, and country).

The specified action is taken whenever the shipping information differs from the billing information.

Data Normalization

The Shipping/Billing Mismatch filter is tolerant of minor address inaccuracies that result from typographical or spelling errors. The filter checks relationships among the street address, city, state, and ZIP code and determines if a minor change is needed before screening the transaction.

Note This normalization is performed purely on the billing and shipping data, and does not authenticate the customer.

Because this normalization happens during data validation by the Payflow server, the data as entered by the customer will still appear in its original form on all transaction data review pages. This means that you might see the following entries not flagged as mismatches on the *Transaction Details* page:

Billing	Shipping
Steve Morrison	Steve Morrison
4390 Ramirez	4390 Ramires
San Fran <i>ic</i> sco, CA	San Fran <i>ci</i> sco, CA
94114	94113

How does the filter protect me?

There are legitimate reasons for a shipping/billing mismatch with a customer purchase—for example, gift purchases might fit this profile. But a mismatch could also indicate that someone is using a stolen identity to complete a purchase (and having the items sent to another address from which they can retrieve the stolen items).

To help to distinguish between legitimate and fraudulent orders, review all mismatches by cross-checking other purchase information such as **AVS** and **CSC**.

Product Watch List Filter

What does the filter do?

The Product Watch List filter compares the SKUs (or other product identifier) of the products in a transaction against a Product Watch List that you create. Any transaction

containing an SKU in the list triggers the filter. If you enable this filter, then you must set up the list of products that should be monitored.

Tip Items that you enter in the Test Product Watch List are not carried over to the configuration for the Live servers, so do not spend time entering a complete list for the Test configuration.

How does the filter protect me?

Some products are attractive to fraudsters (especially popular products with high resale value like computers or televisions). The Product Watch List filter gives you the opportunity to review transactions involving such products to ensure that the order is legitimate.

High-risk Payment Filters

High-risk Payment Filters identify transactions that show billing/shipping discrepancies or an indication that someone other than the legitimate account holder is initiating the transaction.

AVS Failure Filter

What does the filter do?

Address Verification Service (AVS), compares the street number and the ZIP code submitted by the customer against the data on file with the issuer.

The AVS response is composed of a **Y**, **N**, or **X** value for the customer's street address and a **Y**, **N**, or **X** value for the ZIP code. For example, the response for a correct street number and an incorrect ZIP code is **YN**.

If AVS information is not submitted with the transaction, then the response is **NN**.

Result	Meaning
Y	The submitted information matches information on file with the account holder's bank.
N	The submitted information does not match information on file with the account holder's bank.
X	The account holder's bank does not support AVS checking for this information.
(Null)	In some cases banks return no value at all.

Note AVS checks only for a street number match, not a street name match, so **123 Main Street** returns the same response as **123 Elm Street**. The **USPS Address Validation Failure Filter** (page 111) validates the address information.

The specified action is taken whenever the AVS response does not meet the criterion that you specified.

CAUTION The AVS Failure filter performs the action after the transaction is processed. This means that, if set to reject, the filter rejects the transaction after the transaction is authorized by the processor. To charge the customer for such a transaction, you must resubmit the transaction data.

Processors that Support AVS

VeriSign supports the AVS services as listed in the table below.

Processing Platform	American Express	Discover	MasterCard	Visa
American Express Phoenix	✓	—	—	—
American Express APAC	✓	—	—	—
FDMS Nashville	✓	✓	✓	✓
FDMS North	✓	✓	✓	✓
FDMS South	✓	✓	✓	✓
Global Payments Central	✓	✓	✓	✓
Global Payments East	✓	✓	✓	✓
Norwest	—	—	—	—
Nova	✓	✓	✓	✓
Paymentech New Hampshire	✓	✓	✓	✓
Vital	✓	✓	✓	✓
Wells Fargo Bank	✓	✓	✓	✓

♦ To specify the level of AVS checking

Specify one of the AVS settings:

- + **Full:** Take action if any value other than **YY** is returned (**Y** for street address and **Y** for ZIP code).
- + **Medium:** Take action if a transaction returns values other than these: (**YY**, **Y N**, **YX**, **NY**, or **XY**).
- + **Light:** Take action only if **NN** is returned.

This table summarizes AVS levels:

AVS Setting	Allowed Responses
Full	(Y, Y)
Medium	(Y, Y), (Y, N), (Y, X), (N, Y), (X, Y)

AVS Setting	Allowed Responses
Light	(Y, Y), (Y, N), (Y, X), (N, Y), (X, Y), (N, X), (X, N)

How does the filter protect me?

Buyers who can provide the street number and ZIP code on file with the issuing bank are more likely to be the actual account holder.

AVS matches, however, are not a guarantee. Use **Card Security Code (CSC)** and **Buyer Authentication** in addition to **AVS** to increase your certainty.

CSC Failure Filter

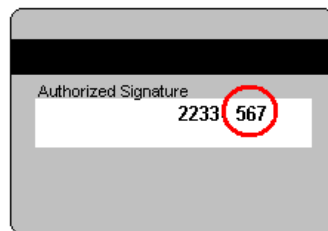
What does the filter do?

The card security code (CSC) is a 3- or 4-digit number (not part of the credit card number) that appears on credit card. Because the CSC appears only on the card and not on receipts or statements, the CSC provides some assurance that the physical card is in the possession of the buyer.

CAUTION The CSC Failure filter performs the action after the transaction is processed. This means that, if set to reject, the filter rejects the transaction after the transaction is authorized by the processor. To charge the customer for such a transaction, you must resubmit the transaction data.

About the CSC

The CSC is printed on the back of most cards (usually in the signature field). All or part of the card number appears before the CSC (**567** in the example). For American Express, the 4-digit number (**1122** in the example) is printed on the front of the card, above and to the right of the embossed account number. Be sure to explain this to your customers.



The CSC check compares the number provided by the customer with the number on file with the issuer and returns one of the following responses:

Result	Meaning
Y	The submitted information matches information on file with account holder's bank.
N	The submitted information does not match information on file with the account holder's bank.
X	Account holder's bank does not support this service.
(Null)	In some cases banks return no value at all.

CSC Failure Filter Action

The specified action is taken whenever the CSC response is the value that you specified.

The Best Practices action is to review all transactions with responses other than **Y**. You set the “strength” of the filter as follows:

- + **Full:** Take action if a value of **N** or **X** is returned.
- + **Medium:** Take action only if a value of **N** is returned.

Processors and Credit Cards that Support CSC

VeriSign supports CSC validation as listed in the table below. **CSC** appears on the *Edit Configuration* page only if VeriSign is certified with your processor

Processing Platform	American Express	Discover	MasterCard	Visa
American Express Phoenix	✓	—	—	—
American Express APAC	✓	—	—	—
FDMS Nashville	✓	—	✓	✓
FDMS North	✓	✓	✓	✓
FDMS South	✓	—	✓	✓
Global Payments Central	—	✓	✓	✓
Global Payments East	✓	✓	✓	✓
Norwest	—	—	—	—

Processing Platform	American Express	Discover	MasterCard	Visa
Nova	—	✓	✓	✓
Paymentech New Hampshire	✓	—	✓	✓
Vital	✓	✓	✓	✓

Even though your processor may be certified for CSC, they may not be certified for all card types (for example, American Express (CID), or Discover). The list will change as VeriSign continues to enhance its service offering. See

<http://www.verisign.com/support/payflow/cardSecurityCode.html> for the latest information.

Special Case: American Express

To enable the account to accept the CSC code, you must send an e-mail request to ES.Fraud.Prevention@aexp.com. Once American Express has approved the request and has activated CSC for the you, you can begin using CSC. If you attempt to send CSC data without having requested setup, American Express does not send a response.

This fraud prevention tool has various names, depending on the processor. Visa calls it CVV2, MasterCard calls it CVC2, and American Express calls it CID. To ensure that your customers see a consistent name, VeriSign recommends use of the term Card Security Code (CSC) on all end-user materials.

How does the filter protect me?

Because the CSC appears only on the card and not on receipts or statements, the CSC provides some assurance that the physical card is in the possession of the buyer.

CSC does not, however, provide a guarantee that the actual account holder is making the purchase. Use the **AVS Failure** and **Buyer Authentication** filters in addition to **CSC** to increase your certainty. The **Buyer Authentication Failure** filter is designed to provide greater assurance that the actual account holder is initiating the transaction.

Buyer Authentication Failure Filter

You must enroll for the Buyer Authentication Service in the Fraud Protection Services suite to make use of the **Buyer Authentication Failure** filter. The filter is grayed out on configuration pages if you are not enrolled.

Buyer Authentication refers to the card-sponsored authentication services such as **Verified by Visa** and **MasterCard Secure Code** that make use of the 3-D Secure protocol. These authentication methods prompt buyers to provide a password to their

card issuer before being allowed to execute a credit card purchase. The Buyer Authentication Service is described in “The VeriSign Buyer Authentication Service” on page 7

What does the filter do?

The filter is triggered when the customer's identity is not adequately authenticated, according to criteria that you specify.

Buyer Authentication Results

Although MasterCard and Visa both use the underlying 3-D Secure protocol to implement the Buyer Authentication service, they have different liability rules regarding buyer authentication results. Those rules appear in Table B-1.

MasterCard converts 3-D Secure results into UCAF fields. To simplify for the merchant, VeriSign normalizes all responses into the values listed in Table B-1.

Buyer Authentication returns one of the following responses in the AUTHENTICATION_STATUS name/value pair (values are for Visa USA region):

Table B-1 Responses in the AUTHENTICATION_STATUS name/value pair

Result	Description	Liability Impact (Subject to Change)
Y	Successful authentication—the password was correct.	Both Visa and MasterCard shift liability for fraud from the merchant.
A	The merchant attempted to authenticate the buyer, but the issuer does not support buyer authentication.	Visa shifts liability for fraud from the merchant. MasterCard does not shift liability for fraud from the merchant.
N	Unsuccessful authentication—the password was not correct.	Neither Visa nor MasterCard shift liability for fraud from the merchant.
U	Authentication could not be completed due to network error.	Neither Visa nor MasterCard shift liability for fraud from the merchant.
F	Card issuers authentication credentials could not be validated.	Neither Visa nor MasterCard shift liability for fraud from the merchant

Actions

You set the “strength” of the filter as follows:

- + **Full:** Trigger if a value of **N**, **U**, or **F** is returned.
- + **Medium:** Trigger only if a value of **N** is returned.

Tip To enforce the minimum Visa regulations, set the filter to **Medium** strength with an action of **Reject**. This setting rejects **N** responses, however, so there is no liability benefit.

How does the filter protect me?

Buyer Authentication is the only screening tool that promises to shift fraud liability from the merchant. The password used with **Verified by Visa** and **MasterCard Secure Code** is the digital equivalent to a shopper's handwritten signature.

Tip Make use of **Buyer Authentication** if your processor and acquirer support it. The use of the password protects merchants from some chargebacks when a customer claims not to have authorized the purchase.

Widespread account holder enrollment in Buyer Authentication programs may take some time and depends on the card issuers supporting and marketing the option.

BIN Risk List Match Filter

What does the filter do?

The Bank Identification Number (BIN) makes up the first six digits of a credit card number. The BIN identifies the bank that issued the card. This filter screens every credit card number for BINs on VeriSign's high-risk list.

The specified action is taken whenever a BIN matches one on the list.

How does the filter protect me?

Certain BINs might be associated with a greater degree of fraud because the issuer uses less stringent authentication policies when issuing cards. In other cases, because some issuers have a large number of cards in circulation, the cards are more likely to fall into the hands of fraudsters.

Account Number Velocity Filter

What does the filter do?

The Account Number Velocity filter triggers when any credit card account number is used five times within a three-day (72-hour) period.

CAUTION The specified action is performed on only the transaction that triggered the filter and not on the previous four transactions. You must manually review and act upon those transactions. Generate a Transaction Details report and click the Account Velocity link to view the transactions.

What is *Velocity*?

In the risk management industry, an event's *velocity* is a measure of its frequency of occurrence during a defined time period. Unusually high velocity is can be associated with a fraudster making repeated attacks on a system. Legitimate customers do not typically perform multiple transactions in quick succession.

How does the filter protect me?

Fraudsters often submit multiple purchases with a single account number to try to discover the card's valid billing address or Card Security Code (CSC). Alternatively, the fraudster may attempt to bypass ceiling filters by making multiple small purchases with a know good account number.

High-risk Address Filters

High Risk Address Filters identify transactions associated with high-risk geographical locations or poorly-matched transaction data.

ZIP Risk List Match Filter

What does the filter do?

This filter compares the **Ship To** and **Bill To** ZIP codes (US only) against a high-risk list managed by VeriSign. VeriSign determines high-risk ZIP codes based on analysis of millions of e-commerce transactions.

The specified action is taken whenever a submitted ZIP code appears in the VeriSign risk list.

Note Fraud tends to correlate to densely populated areas like major cities. For this reason, ZIP codes on the risk list will likely correlate to major cities.

How does the filter protect me?

Matching a ZIP code on the risk list does not necessarily indicate a fraudulent purchase, but that you should evaluate these transactions more closely than other transactions.

Freight Forwarder Risk List Match Filter

What does the filter do?

This filter screens the full **Ship To** address against a list of addresses of freight forwarders managed by VeriSign.

Note Unlike the other Risk Lists, the Freight Forwarder Risk List was not developed through statistical evaluation of e-commerce transactions. Rather, this is a list of known addresses associated with freight forwarders.

The specified action is taken whenever a shipping address matches the address of a known freight forwarding service.

Note The **Freight Forwarder** filter requires a valid US shipping address. If the **USPS Address Validation** filter determines that the address does not exist, then the **Freight Forwarder** filter is skipped and placed in the **Unused Filters** list on the *Transaction Details* page.

How does the filter protect me?

Freight forwarding services enable a customer to open an account using the forwarder's corporate address, and to have the service forward all packages to another end destination. While there are legitimate uses for a freight forwarding service, forwarders also enable fraudsters to hide their true location.

Whenever a customer orders delivery to a freight forwarder, you should research the transaction more closely.

USPS Address Validation Failure Filter

What does the filter do?

This filter screens the **Ship To** and **Bill To** addresses (street number, street name, state, and ZIP code) against the United States Postal Service database of existing addresses. The USPS updates the database continually.

The specified action is taken whenever the address cannot be validated (it does not exist or is incorrect in some way).

Note The filter does not validate that the person named in the transaction data lives at that address or even that the address is currently occupied—only that the address exists in the database.

How does the filter protect me?

To trick a merchant's filters, fraudsters sometimes deliberately misspell or make up street names. This enables the fraudster to spoof AVS, geo-location, and high-risk address filters. You can identify this basic form of spoofing by using the USPS Address Validation filter to determine whether an address really exists.

Note One useful side effect of the filter is that mis-keyed addresses of legitimate customers can be identified before shipping.

IP Address Match Filter

What does the filter do?

This filter screens the IP address from which a transaction originates against a list of high-risk IP addresses managed by VeriSign. An IP (Internet protocol) address is a unique identifier for a computer on a TCP/IP network that can identify a particular network and a particular computer on that network.

Note IP Addresses are not always fixed like the addresses to physical buildings. Some computers get a new IP address each time they connect to a network. The most general level of the IP address indicates the region or country from which the computer is connecting, and is thus relatively fixed. Therefore the IP Address risk list is most effective as a screen for overseas fraud.

The specified action is taken whenever a submitted IP address appears in the VeriSign risk list.

How does the filter protect me?

A customer's IP address identifies a country, region, state, or city. As with ZIP codes, these addresses can be associated with higher or lower likelihood of fraud. This is especially true with high-risk countries that are known to be associated with especially high rates of fraud.

Required Transaction Data

You must send the customer's IP address to use this filter.

E-mail Service Provider Risk List Match Filter

What does the filter do?

This filter compares the e-mail service provider used by the customer against a list of high-risk e-mail service providers managed by VeriSign.

Tip Fraudsters most often use free services at which they do not need to provide traceable billing information. (Free services are also popular among legitimate shoppers—because they are free.)

It is therefore a good practice to check whether the billing name appears in some form in the e-mail address. For example, Tina Johnson should have an e-mail address of TinaJohnson@hotmail.com or Johnson42@hotmail.com, or some similar variant. Such an e-mail address is less suspicious than xy12@hotmail.com.

The specified action is taken whenever the e-mail service provider is found in the VeriSign risk list.

How does the filter protect me?

Online merchants rarely talk to their customers. The customer's e-mail address is a critical communications channel between the merchant and customer. For example, e-mail is often used to confirm a purchase and to notify the customer that shipment has been made.

It is therefore important for merchants to determine how reliably the e-mail address is tied to the identity of the customer. Some e-mail service providers make it especially easy to open and close e-mail accounts without ever providing personal information, enabling fraudsters to use false identities to cover their tracks.

You should examine any transaction in which a high-risk e-mail service provider is involved.

Geo-location Failure Filter

What does the filter do?

This filter compares the IP address of the customer's computer (captured in real-time when the transaction is submitted) and compares its geographical location to the billing and shipping addresses. IP (Internet protocol) addresses are unique identifiers for computers that can often be mapped to a specific city or area code.

The specified action is taken whenever the IP address, shipping address, and billing address do not fall within a 100 mile radius. If you provide only one physical address (billing or shipping address), then the filter triggers when the distance between the IP address and the address that you provided is greater than 100 miles.

Note Gift purchases shipped far from the billing address will trigger the filter.

VeriSign has made every effort to ensure that IP address mapping is accurate and up-to-date. Given the nature of the Internet's architecture, however, some Internet Service Providers use data centers far from the customers being serviced. In addition, as described in the **IP Address Risk List Match** filter, IP addresses can change dynamically. For these reasons, treat this filter as an indicator of suspicious activity, not as a definitive result.

How does the filter protect me?

Comparing the geographical location associated with the IP address to the submitted shipping and billing information can be an effective method for identifying identity spoofing. Fraudsters often pretend to live in a location, but live and shop from another.

All three elements should match one realistic customer profile. For example, a customer with a billing address in New York would typically shop from a computer in New York, and request delivery to a New York address. While there may be some minor inconsistencies in the overall profile, it should generally fit together.

Remember, however, that gift purchases sent to another part of the country will not fit this profile.

Note You should be especially wary when a customer has an international IP address but uses U.S. billing and shipping information.

IP Address Velocity Filter

What does the filter do?

The IP Address Velocity filter triggers when five or more transactions within three days (72 hours) originate from any individual IP address.

CAUTION The specified action is performed on only the transaction that triggered the filter and not on the previous four transactions. You must manually review and act upon those transactions. Generate a Transaction Details report and click the IP Address Velocity link to view the transactions.

IP addresses do not always identify a unique computer or user. For example, an Internet Service Provider (ISP) may use a limited number of IP addresses for all of its users. To protect against triggering the filter in this case, set up an IP Address Velocity Ignore List (described in the online help).

What is *Velocity*?

In the risk management industry, an event's *velocity* is a measure of its frequency of occurrence during a defined time period. Unusually high velocity is can be associated with a fraudster making repeated attacks on a system. Legitimate customers do not typically perform multiple transactions in quick succession.

How does the filter protect me?

Fraudsters often submit multiple purchases using an automated script that tests unknown card numbers. Alternatively, the fraudster may attempt to bypass other filters by making multiple small purchases with multiple stolen account numbers.

High-risk Customer Filters

Bad Lists

What does the filter do?

This filter compares the customer's e-mail address and credit card number against lists (that *you* create) of addresses and numbers for known bad customers.

Note Unlike the Risk lists that VeriSign manages, you, solely, manage and update the Bad Lists.

Any transaction that is an exact match with an entry in one of your bad lists triggers the filter.

If you enable this filter, then your next step will be to set up lists of bad e-mail addresses and bad card numbers. Be sure to type the e-mail addresses and credit card numbers accurately. Enter only numerals in the credit card number list—no spaces or dashes.

Tip Items that you enter in the Test **Bad** lists are not carried over to your configuration for the Live servers, so do not spend time entering a complete list for the Test configuration.

How does the filter protect me?

This filter enables you to block repeat fraud.

In the e-commerce world, once someone successfully performs a fraudulent transaction, they are very likely to try again. For this reason, you should set up lists of cards and e-mail addresses and configure this filter to take action on transactions with data elements appearing in the bad lists.

International Order Filters

International Order Filters identify transactions associated with risky international locations.

Country Risk List Match Filter

What does the filter do?

This filter screens the customer's shipping and billing address information for matches with countries on VeriSign's list of high-risk countries.

The specified action is taken whenever any of the information matches a country on the risk list.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens and the difficulty of cross-border legal enforcement against fraudulent activities.

Certain countries, however, are much riskier than others. These countries have high likelihood of fraud and you should evaluate transactions from these countries closely.

International Shipping/Billing Address Filter

What does the filter do?

This filter screens the customer's shipping and billing information for non-U.S. addresses. The filter checks for country code 840, or any derivation of "United States" (U.S., USA, United States of America, America, and so on) in the country fields. Any other country name triggers the filter.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens and the difficulty of cross-border legal enforcement against fraudulent activities.

The **International Shipping/Billing Address** filter sets aside transactions from customers in foreign countries so that you can evaluate them more fully.

International IP Address Filter

What does the filter do?

This filter screens for international IP addresses. An IP (Internet protocol) address is a unique identifier for a computer that can identify a particular network and a particular computer on that network.

The specified action is taken whenever the IP address indicates an international computer or network.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens as well as the difficulty of cross-border legal enforcement against fraudulent activities.

The **International IP Address** filter sets aside transactions from customers in foreign countries so that you can evaluate them more fully.

International AVS Filter

What does the filter do?

International Address Verification Service (IAVS), determines whether the issuer is domestic (US) or international.

Result	Meaning
Y	The card number is associated with an international issuer.
N	The card number is associated with a US issuer.
X	Account holder's bank does not support IAVS.
(Null)	In some cases banks return no value at all.

The specified action is taken whenever AVS returns **Y**.

Special Requirements

- + You must use Payflow Pro client version 3.06 or newer to use the IAVS filter.
- + International AVS is not currently widely supported by processors. Check to see if your processor supports international AVS.
 - FDMS Nashville and NOVA return IAVS responses for all card types.
 - EDS Aurora and FDMS South return IAVS responses for VISA cards only.

- All other processors always return **N** or **X**.

How does the filter protect me?

Orders from customers in foreign countries are more likely to be fraudulent than orders from domestic customers. This is due to the difficulty of authenticating foreign citizens as well as the difficulty of cross-border legal enforcement against fraudulent activities.

The **International AVS** filter sets aside transactions from customers with cards issued in foreign countries so that you can evaluate them more fully.

Accept Filters

Accept Filters immediately approve transactions that meet characteristics that you specify. If a filter in this group is triggered, then the transaction is accepted regardless of Review filter results.

IMPORTANT! The Accept filters are designed to reduce the load on your staff by reducing the number of transactions set aside for review. The Accept filters do not reduce risk.

Good Lists

What does the filter do?

This filter compares the customer's e-mail address and credit card number against lists (that *you* create) of addresses and numbers for known good customers. *You* create the lists.

Any transaction for which the e-mail address or credit card number is an exact match with an entry in one of your good lists is accepted and no other filters are applied. Enter only numerals in the credit card number list—no spaces or dashes.

Note Unlike the Risk lists that VeriSign manages, you, solely, manage and update the Good Lists.

Items that you enter in the Test Good lists are not carried over to your configuration for the Live servers, so do not spend time entering a complete list for the Test configuration.

If you activate this filter, then you must set up lists of good e-mail addresses and good card numbers. Be sure to type the e-mail addresses and credit card numbers accurately.

CAUTION The Good Lists do not authenticate individuals. If a fraudster were to steal e-mail addresses or credit card account numbers from this list, then they would be able to bypass the filter.

How does the filter protect me?

To ensure that loyal repeat customers are not held up by your fraud review process, you may wish to create lists of e-mail addresses and card numbers that should be accepted. This ensures that an abnormal shopping pattern on the part of a loyal customer (for example making a purchase while on vacation overseas) does not trigger a filter and delay the transaction.

Total Purchase Price Floor Filter

What does the filter do?

This filter screens the total amount of a transaction (including tax, shipping and handling fees).

If a transaction amount is below the price set for this filter, then the transaction is accepted and no other filters are applied.

How does the filter protect me?

Merchants with an especially high transaction volume can use this filter to reduce the number of transactions that their staff must review—transactions below the specified price level are accepted *without further analysis*.

Custom Filters

You create Custom filters by combining up to five existing filters. A well-designed Custom filter can more accurately identify suspicious transactions because it is fine-tuned to the unique needs of your business (for example, you can specify a particular combination of amount, buyer location, and shipping location). For this reason, fewer legitimate transactions are unnecessarily held for review.

For example, a Custom filter that triggers only when both the CSC Failure and AVS Failure filters trigger will set aside transactions that are quite suspicious.

Note You can create a combined maximum (Test plus Live) of 15 Custom Filters. For example, if you currently have 5 Test Custom Filters and 10 Live Custom Filters, you cannot create any more Custom Filters until you delete one of the existing Custom Filters.

See the online help for details on creating a custom filter.



Testing the Transaction Security Filters

Each example transaction shown in this chapter is designed to test the operation of a single filter. To test a filter, disable all other filters and submit the transaction. The filter should be triggered and display its results in the *Transaction Details* page.

In the examples, the critical transaction data is shown in **bold red** type.

Good and Bad Lists

To test the Good and Bad List filters, add good and bad entries to the list and then submit a transaction using a value in the list.

AVS Failure Filter

pfpro 443

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[4]=1.02&BILLTOPHONE2=650-555-0123&BROWSERCOUNTRYCODE=203&BROWSERTIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Campbell&COMMENT1=Automated testing from AdminTester&COUNTRY=US&CUSTIP=194.213.32.220&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[17]=Admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=Mountain View&COUNTRYCODE=US&SHIPTOEMAIL[17]=Admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=487 East Middlefield Road&SHIPTOSTREET2=487 East Middlefield Road&SHIPTOZIP=94043&SS=565796510&STATE=CA&STREET=667 W. Rincon Ave&BILLTOSTREET2=Unit C&TAXAMT=1.02&TENDER=C&USER=TESTAVSRejectFull&VENDOR=TESTAVSRejectFull&ZIP=99999" 30
```

Expected Response Message

resp msg=RESULT=125&PNREF=VBCA25034255&RESPMSG=Declined by Fraud Service&AUTHCODE=421PNI&AVSADDR=X&AVSZIP=X&IAVS=X&PREFPSMSG=No Rules Triggered&POSTFPSMSG=Reject AVS
!!ERROR 16:55:6 result=125 TRXTYPE=A!!

BIN Risk List Match Filter

Pass in the appropriate credit card number for the card brand:

- American Express: 378282246310005
- MasterCard: 5555555555554444
- Visa: 4610251000010168

pfp443

"TRXTYPE=A&**ACCT=4610251000010168**&AMT[8]=\$1000.00&BILLTOPHONE2=650-555-0123&BILLTOSTREET2=123
BILLTOSTREET&BROWSECOUNTRYCODE=203&BROWSETIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No City&COMMENT1=Automated testing from AdminTester&COUNTRY=203&CUSTIP=66.218.71.93&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=1.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No City&COUNTRYCODE=203&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main St.&BILLTOSTREET2=123 SHIPTOSTREET 2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskBinCheckReject&VENDOR=TESTHighRiskBinCheckReject&ZIP=11111" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25033363&RESPMSG=Declined by Fraud Service&PREFPSMSG=Reject HighRiskBinCheck
!!ERROR 15:52:54 result=125 TRXTYPE=A!!

Country Risk List Match Filter

Pass in the specified country or country code.

pfpro 443

"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=\$1000.00&BROWSECOUNTRYC
ODE=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=AD&COUNTRYCODE=AD&CUSTIP=172.131.193.25&CUST
REF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@
merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAM
E=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_
TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PART
NER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPC
ARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRST
NAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMI
DDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPT
OSTATE=CA&SHIPTOSTREET=123 Main St.&SHIPTOSTREET2=123 SHIPTOSTREET
2&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123 Main
St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskCountryCheckReject&VENDOR=
TESTHighRiskCountryCheckReject&ZIP=60649" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25031715&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskCountryCheck
!!ERROR 14:7:57 result=125 TRXTYPE=A!!

E-mail Service Provider Risk List Match Filter

Pass in the specified e-mail address.

pfpro 443

"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=\$1000.00&BROWSECOUNTRYC
ODE=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=AD&COUNTRYCODE=AD&CUSTIP=172.131.193.25&CUST
REF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@
asiamail.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME
=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_T
YPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTN
ER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCA
RRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No
City&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNA
ME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDD
LENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOS
TATE=CA&SHIPTOSTREET=123 Main St.&SHIPTOSTREET2=123 SHIPTOSTREET
2&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123 Main
St.&BILLTOSTREET2=123 SHIPTOSTREET

2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskEmailCheckReject&VENDOR=TESTHighRiskEmailCheckReject&ZIP=60649" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25031907&RESPMSG=Declined by Fraud Service&PREFPSMSG=Reject HighRiskEmailCheck
!!ERROR 14:20:5 result=125 TRXTYPE=A!!

Freight Forwarder Risk List Match Filter

Pass in the specified shipping address.

pfpro 443

"TRXTYPE=A&ACCT=3528000000000015&AMT[5]=\$1000&BILLTOPHONE2=650-555-0123&BROWSERCOUNTRYCODE=203&BROWSETIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Indianapolis&COMMENT1=Automated testing from AdminTester&COUNTRY=US&CUSTIP=255.255.255.255&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&**SHIPTOCITY=Indianapolis**&COUNTRYCODE=US&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&**SHIPTO STATE=IN**&**SHIPTOSTREET=973 N Shadeland Ave**&SHIPTOSTREET2=UNIT #C&**SHIPTOZIP=46219**&SS=565796510&STATE=IN&STREET=973 N Shadeland&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskFreightCheckReject&VENDOR=TESTHighRiskFreightCheckReject&ZIP=46219" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25087954&RESPMSG=Declined by Fraud Service&PREFPSMSG=Reject HighRiskFreightCheck
!!ERROR 15:43:53 result=125 TRXTYPE=A!!

Geo-location Failure Filter

Pass in the specified Shipping address, billing address, and IP address.

pfpro 443

"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=\$1000.00&BILLTOPHONE2=650-555-0123&BROWSERCOUNTRYCODE=203&BROWSETIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&**CITY=Campbell**&COMMENT1=Automated testing from AdminTester&**COUNTRY=US**&**CUSTIP=192.6.165.40**&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=

1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&**SHIPTOCITY=Mountain View**&**COUNTRYCODE=US**&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&**SHIPTOSTREET=487 East Middlefield Road**&SHIPTOSTREET2=487 East Middlefield Road&**SHIPTOZIP=94043**&SS=565796510&STATE=CA&**STREET=236 W. Rincon Ave**&BILLTOSTREET2=Unit C&TAXAMT=1.01&TENDER=C&USER=TESTGeoLocationCheckReject&VENDOR=TESTGeoLocationCheckReject&**ZIP=95008**" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25088015&RESPMSG=Declined by Fraud Service&PREFPSMSG=Reject GeoLocationCheck
!!ERROR 15:44:28 result=125 TRXTYPE=A!!

International AVS Filter

Pass in the specified ZIP codes and billing address.

pfpro 443

"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=\$1000.00&BROWSERCOUNTRYCODE=203&BROWSETIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&**CITY=No City**&COMMENT1=Automated testing from AdminTester&**COUNTRY=US&COUNTRYCODE=USA**&CUSTIP=66.218.71.93&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTO**STATE=CA**&SHIPTOSTREET=123 Main St.&SHIPTOSTREET2=123 SHIPTOSTREET 2&**SHIPTOZIP=00101**&SS=565796510&STATE=CA&**STREET=123 Main St.**&BILLTOSTREET2=123 SHIPTOSTREET 2&TAXAMT=1.01&TENDER=C&USER=TESTInternationalAVSReject&VENDOR=TESTInternationalAVSReject&**ZIP=00101**" 30

Expected Response Message

```
resp msg=RESULT=125&PNREF=VBCA25032988&RESPMSG=Declined by Fraud  
Service&AUTHCODE=890PNI&AVSADDR=Y&AVSZIP=Y&IAVS=Y&PREFPSMSG=No  
Rules Triggered&POSTFPSMSG=Reject InternationalAVS  
!!ERROR 15:30:41 result=125 TRXTYPE=A!!
```

International IP Address Filter

Pass in the specified IP address.

```
pfpro 443  
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYC  
ODE=203&BROWSETIME[22]=July 11, 2002  
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Campbell&COM  
MENT1=Automated testing from  
AdminTester&COUNTRY=US&COUNTRYCODE=US&CUSTIP=194.213.32.220&CUST  
REF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@a  
siamail.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=  
Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_T  
YPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTN  
ER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCA  
RRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=Mountain  
View&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTN  
AME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMID  
DLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTO  
STATE=CA&SHIPTOSTREET=487 East Middlefield Road&SHIPTOSTREET2=487 East  
Middlefield Road&SHIPTOZIP=94043&SS=565796510&STATE=CA&STREET=236 W.  
Rincon Ave&BILLTOSTREET2=Unit  
C&TAXAMT=1.01&TENDER=C&USER=TESTNonUSIPAddressReject&VENDOR=TEST  
NonUSIPAddressReject&ZIP=95008" 30
```

Expected Response Message

```
resp msg=RESULT=125&PNREF=VB0A25032282&RESPMSG=Declined by Fraud  
Service&PREFPSMSG=Reject NonUSIPAddress  
!!ERROR 14:49:23 result=125 TRXTYPE=A!!
```

International Shipping/Billing Address Filter

Pass in a non-US Country code to either the billing or shipping address.

```
pfpro 443  
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYC  
ODE=203&BROWSETIME[22]=July 11, 2002  
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No  
City&COMMENT1=Automated testing from  
AdminTester&COUNTRY=CZ&COUNTRYCODE=USA&CUSTIP=66.218.71.93&CUSTR  
EF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@m  
erchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=
```

Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=123 Main St.&SHIPTOSTREET2=123 SHIPTOSTREET2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main St.&BILLTOSTREET2=123 SHIPTOSTREET2&TAXAMT=1.01&TENDER=C&USER=TESTInternationalOrderReject&VENDOR=TESTInternationalOrderReject&ZIP=11111" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25032493&RESPMSG=Declined by Fraud Service&PREFPSMSG=Reject InternationalOrder
!!ERROR 15:0:24 result=125 TRXTYPE=A!!

IP Address Match Filter

pfpro test-payflow.verisign.com 443
"TRXTYPE=A&ACCT=5105105105105100&AMT[6]=\$75.00&BILLTOPHONE2=650-555-1234&BILLTOSTREET2=&BROWSECOUNTRYCODE=203&BROWSETIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No City&COMMENT1=Test to trigger
rules&COUNTRY=US&CUSTIP=207.208.119.12&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[21]=lastName@verisign.com&EXPDATE=1209&FIRSTNAME=FirstName&FREIGHTAMT=1.11&LASTNAME=LastName&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=VeriSign&PHONENUM=650-555-1234&PONUM=PONUM&PWD=password1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No City&COUNTRYCODE=US&SHIPTOEMAIL[17]=test@verisign.com&SHIPTOFIRSTNAME=&SHIPTOLASTNAME=&SHIPTOMIDDLENAME=&SHIPTOPHONE=650-555-1235&SHIPTOPHONE2=650-555-1236&SHIPTOSTATE=CA&SHIPTOSTREET=487 East Middlefield Road&SHIPTOSTREET2=&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=487 East northfield Road&BILLTOSTREET2=&TAXAMT=1.01&TENDER=C&USER=testFilters&VENDOR=testFilters&ZIP=15071" 50

Shipping/Billing Mismatch Filter

Pass in the specified shipping and billing addresses.

pfpro 443
"TRXTYPE=A&ACCT=3528000000000015&AMT[4]=1000&BROWSECOUNTRYCOD

E=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&**CITY=No**
City&COMMENT1=Automated testing from
AdminTester&**COUNTRY=203**&**COUNTRYCODE=203**&CUSTIP=255.255.255.255&CU
STREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admi
n@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTN
AME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0
&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&P
ARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&S
HIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&**SHIPTOCITY=SHIPTO**
CITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRST
NAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMI
DDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&**SHIPT**
OSTATE=CA&**SHIPTOSTREET=SHIPTOSTREET**&SHIPTOSTREET2=123
SHIPTOSTREET 2&**SHIPTOZIP=11111**&SS=565796510&**STATE=CA**&**STREET=123**
Main
St.&TAXAMT=1.01&TENDER=C&USER=TESTBillShipMismatchReject&VENDOR=TES
TBillShipMismatchReject&**ZIP=11111**" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25031150&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject BillShipMismatch
!!ERROR 13:34:27 result=125 TRXTYPE=A!!

Total Item Ceiling Filter

First, set the filter to trigger on 5 or fewer items. For testing, pass in more than 5 items, as shown here.

pffpro 443
"TRXTYPE=A&ACCT=3528000000000015&AMT[4]=1000&BROWSECOUNTRYCOD
E=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=255.255.255.255&CU
STREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admi
n@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTN
AME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&**L_QTY0=6**&L_SKU0=L_SKU0
&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&P
ARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&S
HIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=SHIPTO
CITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRST
NAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMI
DDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPT
OSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123
SHIPTOSTREET 2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123
Main

St.&TAXAMT=1.01&TENDER=C&USER=TESTHighOrderNumberReject&VENDOR=TE
STHighOrderNumberReject&ZIP=11111" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25030952&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighOrderNumber
!!ERROR 13:19:25 result=125 TRXTYPE=A!!

Total Purchase Price Ceiling Filter

First, set the filter to trigger at 1000.00. For testing, pass in an amount higher than 1000, as shown here.

pfpro 443

"TRXTYPE=A&ACCT=3528000000000015&AMT[7]=1000.01&BROWSERCOUNTRYC
ODE=203&BROWsertime[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=255.255.255.255&CU
STREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0
&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&P
ARTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&S
HIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=SHIPTO
CITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRST
NAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMI
DDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPT
OSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123
SHIPTOSTREET 2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123
Main
St.&TAXAMT=1.01&TENDER=C&USER=TESTCeilingAmountReject&VENDOR=TESTC
eilingAmountReject&ZIP=11111" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25030756&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject CeilingAmount
!!ERROR 13:11:4 result=125 TRXTYPE=A!!

Total Purchase Price Floor Filter

To test the Total Purchase Price Floor filter, submit a transaction with an amount lower than the trigger amount.

USPS Address Validation Failure Filter

pfpro 443

"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=\$1000.00&BROWSECOUNTRYC
ODE=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&**CITY=No**
City&COMMENT1=Automated testing from
AdminTester&**COUNTRY=US&COUNTRYCODE=US**&CUSTIP=203.81.64.19&CUSTRE
F=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@asia
mail.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNAME=Joh
nson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&L_TYPE
0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=
VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRI
ER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&**SHIPTOCITY=No**
City&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTN
AME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMID
DLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&**SHIPTO**
STATE=CA&COUNTRYCODE=US&SHIPTOSTREET=123 Main St.
blah&SHIPTOSTREET2=&**SHIPTOZIP=60649**&SS=565796510&STATE=CA&**STREET**
=123 Main St. blah&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTBillUSPostalAddressCheckReject&VEND
OR=TESTBillUSPostalAddressCheckReject&**ZIP=60649**" 30

Expected Response Message

resp msg=RESULT=125&PNREF=VB0A25032101&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject BillUSPostalAddressCheck
!!ERROR 14:39:3 result=125 TRXTYPE=A!!

ZIP Risk List Match Filter

Pass in the specified ZIP codes.

pfpro 443

"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=\$1000.00&BROWSECOUNTRYC
ODE=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No
City&COMMENT1=Automated testing from
AdminTester&COUNTRY=203&COUNTRYCODE=203&CUSTIP=172.131.193.25&CUS
TREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[20]=admin
@merchant.com&EXPDATE=1209&FIRSTNAME=John&FREIGHTAMT=1.11&LASTNA
ME=Johnson&L_COST0=11.11&L_DESC0=L_DESC0&L_QTY0=1&L_SKU0=L_SKU0&
L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PA
RTNER=VeriSign&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHI
PCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRST
NAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMI
DDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPT
OSTATE=CA&SHIPTOSTREET=123 Main St.&SHIPTOSTREET2=123 SHIPTOSTREET

2&**SHIPTOZIP=60649**&SS=565796510&STATE=CA&STREET=123 Main
St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskZIPCheckReject&VENDOR=TES
THighRiskZIPCheckReject&**ZIP=60649**" 30

Expected Response Message

resp mesg=RESULT=125&PNREF=VB0A25031523&RESPMSG=Declined by Fraud
Service&PREFPSMSG=Reject HighRiskZIPCheck
!!ERROR 13:55:6 result=125 TRXTYPE=A!!



Testing Buyer Authentication Transactions Using the Payflow Pro SDK

This chapter describes the process of testing Buyer Authentication transactions using the Payflow Pro SDK. For complete information on using the SDK, see *VeriSign Payflow Pro Developer's Guide*.

The content and format of responses to transaction requests are described in “Buyer Authentication Transaction Parameters and Return Values” on page 51.

In This Chapter

Testing Buyer Authentication Transactions on page 133.

Test Case Descriptions and Account Numbers on page 134.

Expected Result Codes for Buyer Authentication on page 135.

Buyer Authentication Testing Procedures on page 137.

Testing Buyer Authentication Transactions

Test cases are described in “Test Case Descriptions and Account Numbers” on page 134. Use the card number associated with a test case and the appropriate password to generate the results appropriate to the case.

Buyer Authentication Test Server

Direct **Verify Enrollment** transactions (**TRXTYPE=E**) and **Validate Authentication** transactions (**TRXTYPE=Z**) to VeriSign's test Buyer Authentication Server:

test-buyerauth.verisign.com

Payflow Pro Test Server

Direct the standard Payflow Pro sale or authentication test transaction to:

test-payflow.verisign.com

Test Case Descriptions and Account Numbers

To generate particular results, use the test account numbers listed in Table D-1. Test transaction results are determined solely by the test account number submitted, so you can enter any password on the test ACS page.

Account numbers starting with 5 are MasterCard. Numbers starting with 4 are Visa. In the table, VE stands for the Verify Enrollment transaction and VA stands for the Validate Authentication transaction.

Test Cases

Table D-1 Generating buyer authentication result

Case	Test Scenario	Test Account Number
1	Card enrolled (VE AUTH_STATUS=E) Successful authentication (AUTH_STATUS=Y for VA) Successful signature verification	5100000000000008
		5200000000000007
		4000000000000002
		4000000000000101
2	Card enrolled (VE AUTH_STATUS=E) Failed authentication (AUTH_STATUS=N for VA) Successful signature verification	5100000000000008
		5200000000000007
		4000000000000002
		4000000000000101
3	Card enrolled (VE AUTH_STATUS=E) Attempt authentication (VA AUTH_STATUS=A) Successful signature verification	4111111111111111
4	Card not enrolled (VE AUTH_STATUS=O)	5105105105105100
		4000000000000507
5	Can not verify card enrollment (VE AUTH_STATUS=X)	5555555555554444
		4012888888881881
6	Card eligible for authentication (VE AUTH_STATUS=E) User cancelled authentication by clicking the Cancel button on the ACS page.	5100000000000008
		5200000000000007
		4000000000000002
		4000000000000101

Table D-1 Generating buyer authentication result

7	Card enrolled for authentication (VE AUTH_STATUS=E) Unable to authenticate (VA AUTH_STATUS=U) Successful signature verification	5300000000000006 4000000000000309
8	Card enrolled (VE AUTH_STATUS=E) VA transaction error (VA AUTH_STATUS=F)	5500000000000004
12	Merchant not registered for this feature or is deactivated. (merchant authentication failure)	Any valid MasterCard or Visa account number

Expected Result Codes for Buyer Authentication

IMPORTANT! All returned name/value pairs for transactions with VeriSign's Buyer Authentication Server include length tags. Length tags specify the exact number of characters and spaces that appear in the value. For example, **RESPMSG[2]=OK**.

The following Result Codes (**RESULT** return values) are associated with the Buyer Authentication Service. The full list of Result Codes appears in "RESULT Codes and RESPMSG Values" on page 85.

Result Code	Description
0	Successful
3	Invalid transaction type
4	Invalid amount
7	Field format error
23	Invalid or missing account number
24	Invalid or missing expiration date
1001	Service unavailable
1002	Transaction timeout
1003	Invalid client version

Result Code	Description
1004	Invalid timeout value
101	Service unavailable
1012	Service unavailable
1013	Service unavailable
1014	Merchant has not activated buyer authentication for this card type
1021	Invalid card type
1022	Invalid or missing currency code
1023	Merchant has not activated buyer authentication for this card type
1041	Validate Authentication failed: missing or invalid PARES
1042	Validate Authentication failed: PARES format is invalid
1043	Validate Authentication failed: Cannot find successful Verify Enrollment
1044	Validate Authentication failed: Signature validation failed for PARES
1045	Validate Authentication failed: Mismatched or invalid amount in PARES
1046	Validate Authentication failed: Mismatched or invalid acquirer in PARES
1047	Validate Authentication failed: Mismatched or invalid Merchant ID in PARES
1048	Validate Authentication failed: Mismatched or invalid card number in PARES
1049	Validate Authentication failed: Mismatched or invalid currency code in PARES
1050	Validate Authentication failed: Mismatched or invalid XID in PARES
1051	Validate Authentication failed: Mismatched or invalid order date in PARES
1052	Validate Authentication failed: This PARES was already validated for a previous Validate Authentication transaction

Buyer Authentication Testing Procedures

Follow these steps to test your Buyer Authentication integration:

Step 1 Perform the Verify Enrollment Transaction

Direct the **Verify Enrollment** transaction (**TRXTYPE=E**) to VeriSign's test buyer authentication server: **test-buyerauth.verisign.com**

Pfpro test-buyerauth.verisign.com

"TRXTYPE=E&ACCT=5105105105105100&AMT=19.25&EXPDATE=1203&PARTNER=VeriSign&PWD=p12345&VENDOR=SuperMerchant&USER=SuperMerchant" 30

Verify Enrollment Transaction Test Cases

AUTH_STATUS of Verify Enrollment Transaction	Test Case
E (Card Eligible for authentication)	1, 2, 3, 6, 7, 8
O (Attempt not available)	4
X (Unable to fulfill request)	5

Example Return Values

Note **AUTHENTICATION_ID**, **AUTHENTICATION_STATUS**, and **ECI** should be returned in all cases. For buyer authentication transaction types, the **AUTHENTICATION_ID** value performs the same function as the **PNREF** value that is returned to standard Payflow Pro transactions.

♦ Account is enrolled in the 3-D Secure program

If the cardholder is enrolled (test cases 1, 2, 3, 6, 7, 8, and 11), then the **AUTHENTICATION_STATUS** should be **E**, and **PAREQ** and **ACSURL** should return non-null values.

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=f43669e4921cf8b504c4
&AUTHENTICATION_STATUS[1]=E&PAREQ[428]=eJxVku1ugjAUhm+FeAH0A3Bozpr4
8WP+2GK23UA9HJVECpYy9e7XCkzXkPS8fcvD6Vvg+2iJ1l+EnSUF79S2+kBRWbxO9
mkync4onUmB+3yX8RTTiYLT4pPOCn7ltmVtlh5LIGN0hMsHrVxCjSel5sPJcMANiiyG7
WSgwDWK/B6lrUkloXrfTpVJqDn20Rreqq0eYG7O4D1p1x9qbylAMbBXT2pl7ONXPGLp
dLvPMU7CHoGTHWFbCwB9ijuW0XqtYzr2Whpi+5FEWOIGOWU06U7f0HggOFdqQk5w
mXlokEn3M5T1Jg93XQVWhCiVksM3/GXkET4lvRCs7zCvioLRkcjzEgoGtTG/I7fFx/NRT
Uom99mB59r95CxOh8epngzw8Pad+NgLSKJ6lnWg8lr7HhDtlw3b769xv8AhQarWM=&A
CSURL[66]=http://test-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/start
```

♦ All other cases

If the cardholder is not enrolled or other conditions (test cases 4, 5, 9, and 10), then the following is returned:

```
RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=48c92770755039d6b  
b3d&AUTHENTICATION_STATUS[1]=O&ECI[1]=1
```

PAREQ and **ACSURL** should not be returned, but **AUTHENTICATION_ID** and **ECI** must be returned. (for example, Test Case 4 with a test MasterCard account):

Step 2 POST the PAREQ to the ACS URL

PAREQ and **ACSURL** values are returned for test cases 1,2,3,6,7,8, and 11. For other cases, skip to Step 4 on page 141.

- 1 Construct an HTML page with a form that performs a POST to VeriSign's ACS Simulator

(<http://test-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/start>)

The form must contain the following fields (fieldnames are case-sensitive):

PaReq — Copy and paste the PAREQ value from the previous step.

TermUrl — The merchant URL to which the reply must be posted. For testing, use:

<https://test-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/pares>

MD — The Merchant Data field: Merchant state data that must be returned to the merchant. This field is used to accommodate the different ways merchant systems handle session state. If the merchant system can associate the final post with the original shopping session without any further assistance, the MD field may be empty. If the merchant system does not maintain state for a given shopping session, the MD can carry whatever data the merchant needs to continue the session. Since the content of this field varies by merchant implementation, the ACS must preserve it unchanged and without assumptions about its content.

The MD field must contain only ASCII characters in the range 0x20 to 0x7E. If other data is needed, then the field must be Base64-encoded. The size of the field (after Base64 encoding, if applicable) is limited to 1024 bytes.

If MD includes confidential data (such as the PAN), then it must be encrypted.

- 2 POST to VeriSign's ACS Simulator.

(<http://test-buyerauth-post.verisign.com/DDDSecure/Acs3DSecureSim/start>)

- 3 The results depend upon the test account number that you used:

- + For test cases 1, 2, 6, and 8, the ACS page opens and prompts for a password. The correct password (**password**) results in an authenticated user. Enter any other string to test case 2.
- + For test case 3 (attempted authentication of a card that is not enrolled—Visa only), ACS does not display a page asking for cardholder’s password but directly generates a **PAREQ** and POSTs it back to the specified **TermUrl**.

Step 3 Validate Authentication Transaction

Validate Authentication Transaction Test Cases

AUTHENTICATION_STATUS of Validate Authentication Transaction	Test Case
Y	1
N	2
A (Visa only)	3
U	7
F	8

Procedure

Direct the **Validate Authentication** transaction (**TRXTYPE=Z**) to VeriSign’s test buyer authentication server: **test-buyerauth.verisign.com**. Use the **PARES** value from the ACS return POST or use the example value that appears on page 140.

CAUTION To avoid format errors, the submitted **PaRes** value should be a single line with no carriage returns (check especially at the end of the message).

For this call, you must use the **pfpro_file.exe** script—do not use the **pfpro.exe** client. Save the **Validate Authentication** transaction in a file and then use the **pfpro_file** script to send the request to the test Buyer Authentication server:

Example Validate Authentication transaction

```
pfpro test-buyerauth.verisign.com
"TRXTYPE=Z&PARTNER=VeriSign&PWD=p12345&VENDOR=SuperMerchant&USER=
SuperMerchant&PARES[3648]=eJzdWFmTokoW/isdPW9T0c3iUnLDNiKTXQURWYU3NI
IEUUBAfv0kW1191TPXebhTowRBpmHkyfPfr5gbiRIFHF6FFzKaDFXoqry4uhTGn77PAv
H4SQKp1MvmEbTnYcf4efF/AVoUXVj2HD7XjWCzskU0slkGr9sorJKi+OC+kp+pebE9y2
RF3F6xNLLIPGO9WLuBWcoqwtq+M2J1938EJUydyfe6Pf9nHg/93IZVhXWtEvDxe1iY9+
```

qorB3DXniHNyDa/OUe3C+zYmBYx56dbSgSXJE

...

kKpX27a3+0P6ATMpQGwInl2WoZbuHePyp/FUqxyFTXlgV5l/+jMqjde/12HNLjbqW/Qqgf
e7Qw9GjcKgt2OdvTspJPI2eyuRw0nBr9JKdp6eVP1u3xUyaKN1qYzVksB9vKCe6kqRIV
4qfUJP1jvSWI9OKuSbn5zpK0ouzXl9mNfoARhDv30qlt+8n719Wbh9fb5+EH++Fj5+K/wW
CuWQX" 30

Example PaRes Value

PARES[3648]=eJzdWFmTokoW/isdPW9T0c3iUnLDNiKTXQURWYU3NIIEUUBafv0kW1I
91TPXebhTowRBpmHkyfPfr5gbiRIFHF6FzKaDFXoqry4uhTGn77PAvH4SQQp1MvmEb
TnYcf4efF/AVoUXVj2HD7XjWCzskU0slkGr9sorJKi+OC+kp+pebE9y2RF3F6xNLLIPGO9
WLuBWcoqwtq+M2J1938EJUydyfe6Pf9nHg/93IZVhXWtEvDxe1iY9+qorB3DXniHNyDa/
OUe3C+zYmBYx56dbSgSXJE0tT4EzX+bTT6jSTnxl0+Pw3iwKG4YNkUQ0/mxCNlJn1SR
sfgupiN8ZG33TzqTsUxwhz0nHhbz4l35U7ecfHPh9/dnIE6N7aLeZ0ePITqRp9XtVdfqoUz
J15X88BrmsXGWOZKb6UbLkk3Rp4rGUycg7VXRBmbe2OZR0G6ILEVw/N2CuRxUaZ1
clhQd553wpwYyVCFu4VzM9TQ+4svK6FN3yl/Vt89JXZ9+I4i2bb+2069FGRNYYZlgGQlzh
FUa/+Pz/VQUysdd8aeOsd6xOKaBl6e9V+P8UKl6KcJPb7p9JMbQBkkUofHsFyzqS0CNj
18GCjmiJlgm8bHQB8v+yC0/K1tW3pcq8ajhgp8ELeZatlUGjlg+mZr87fM/PqgHLo2jqv4rN
3+/9VHCd3mWl1+ixXnnMLvLKlXrgXx85qoZEVlv5Vbsbtn/yDkn3lR9teMetAfn3BkTbIP2h
Ste6ujJXl3GRiaJhCpimMZvc/YnMYsW9ZpOtFhxant685Lbj3r6JrLqDzbZ/KU5PVsz9vec
t34eig5l70qyYSZkfR24qSyj6AHLitLDaoqTnXnFFdnaa/LPZlFUBNTe4b2400VixUSiL4pSrK
tJBfumpbnNOCz6MCIW7iFVLbfHglYauUqut6t2k5lHvNq777SL34WBbXq4eJi1W8gPKTH
tKpLry7KOfEzX+0IG5V1usPJhJuElsviNmNZGKcxaGUIYnmIA93XweuvByqM9+dkn4pM
S0KATAFwLDwa/FFhTzHVz6lu+yMO8UugOU4wUiskqlw0E7+Qagcmql927o6tHkZ1gq
qWhY5nlWQyLdLy+z5tQL2lqBMnoUKA5Bxx93uVC0lAgPuqdw/ak2Q8Z4C4ztfomilFq6u
mF8cu43R+x0dZ4D1/WxIQF7LfxvWSRzw7jTF4MI33eTbewY6tJoHl6WVvkBVOKXFFf
8pFQOXe0bDf1lY4CjaE4rgJsdHN9S0BUPLDPvQ2mZhCJzVWRxpWdy0T+D7wAYi+rgv
xStYlw45SU7TtSrxOKXq1e552p8ZPqC0jPLpxXy22nUBP1VT3ib3YdgYnmzjCaHuQzK
b+eugCFZW/3Zs1qdhPU0hFEmp7rrZbK+UjPK1nL0UHrik3YTEQROYbMJjsimfDbtc+W9
DRRPMoYWyPft8HSpCEQ2llgCEmYnVICUKVTT5fKZIsbbjNtZQ4gAluxzHsczhcRtdlQR
43cQOjwAugT3ZO2S1JCblskZ1zs7Nk8lLizKbK0Hfwv6QofB7M2Dq5AkHZhmV20zRjtNh
S1NHekbc/K3elJmxaOeDzJ4h77MFH0oF0iZ7kqXDlpAhWgPRSSPa/oDjhwOdBIPk3V7n
aZufoEr8m07cHyHnPHALIIPosdJPpURef4lyE+Qz7BThEN27rc4qYVrXiP64rvBM7ZLvee
PUIGHJvdxyCud90Hf5Hmjf847dv+cdwmnBxo2lBDHAPgUABm0C9zNM9qMj2N+iusS
qhkL6TMLqSn+y4k7W7vbMF0fZ01BwzD/cO85J3bapBtpq5W7Vf8+rmZasmvmj1rihXN
35SQze6BSnn0J2cq3IV+DqPdPwUcA0c3ZNDW/ez1k97U238g3tyR9i2LbaDHlcarzDYN
yT2yaDDbf9xTDoe9dQQFwLLu4ZifvBsFdeJpbtt8FnSM9mLoal64djUmer5i80k3oHKwt
FtcL7/sVWdYpXTsFlu3r2kslyGj+HzXC/lkSx5UEjyYUilR2k86agBYq7le9k05OuH/kwW
GI4SR7i6el7bEpTFfz9QGvdYbDupKaPbn6dFetH/rE0pBbTbRqnXSywR/BdZlFh3al2R7G
cQlJXoAowPWts8ByBrqOc3758K4FhQcb8U/GzxSWSMctLaNq4r1YGvrW73Q9PA+t
LYz/mwfXG8/Me5+sE+zmkgSPdv2te417sHOe5dR3suu8/7NWvsWTqF1qF6leYmYRzEH
rXYBrncMqdkZb5otAHOL6D/zx7yJn7fWhrkR6uKW+rTXAtcz/6wx15kkYGXNGsR295enn
lp8t/qO/mpHnVXYIDU/ks02OePKC1dH14sO/w6zm0/b34HlHLgVt/MwCSCAJkFnD32SKh
GW7mCouHfhu698AcsnIrA2e1ah0lgciqbcbHh3iPf9siUQltw0VfiMD9hq7AKDPBsGPYlXllg
ghitDgGfOl9EE0QZNC/9wOetzioFwWmj7yb2lUdwDZWo19dqSLXJdNslD/LN9x3/k3+j0
fGt4YOZjEpCmQd+pMnXjMU/qTNeISnn5lFen5X86dnGsOp22XWt0u1FdnqdzRZJQJix
/nB4uNnExikXxETiZhJ5g+jCqhd3YHTPJ+Nsdpyikg9hitDjsROIbZCFZczuipvngFKEX8C
U4n8UpogYQnyHKbz5CEnew6FoSsuJ7xDj9D6KeBUqclZfUKdXOL5TMvzMULexioFGv
dlwXDFJxSra2CW7JcYmJ/5hEW+Lktr7PPx1ihjvNsNEYS1LeRirsQH2jKyGwcvddZT41lV
dXL7+SH6wr/i1fYhs2fZ2ds232q39KVrbivGrzZ36OH5/al+K0A73PsACHpcZ4PQWtDpW
ESgo5TzRivJzJ6zEeEzEmdpNbWly2U3S8+WMyKk+eVKtK9rEL8fWZ2YixWqbs0M+e3
QN1JGHnHxygpcd8WFL6E29FdcBC1oe182GBUyF2/zLVhlq/b2MLfzkNM9DBd6gRcjFYl

ZQG4288fPeuPBSX4e6JTFC3qxG090+yoCL4zK0RR53i5EAZJ6D4xUQFBAimAJeAcj4s
e0A02m59rE1mdhqHhI9C0f3dpRBWbLwCNJjaFSjHqL1dUWI6pY02VO+1qbXddDo6VS
Ep6kOT//HdRln4NTvEqXPn9WcJBhRvI7ywFgP8Eq5+2oH8XqFIS3QURuHYhwHU/y/iH
GQVK4o3OAEhgMDBHqAcPwdu0FTqcspPET4xUm8Sb7t49sDN20k3vIcW1ruXmwaJ
8eRjeGTPsOjwr0yxFu7jve26pkcMjT8AbzJsin8f0c3BT8NdZxvb2NbXqZOHRNBaJ2wSPz
v4ZZ2KcXZ7SshthYj6MT8RgSC+JARxgSN/H7OwXg4vaF34+TmcO/HfqSAvcIkbD/fwV1
H+M3xADIWBT+aHkKpX27a3+0P6ATMpQGWIInl2WoZbuHePyp/FUqxyFTXlgV5l/+jMqj
de/12HNLjBqW/Qqgfe7Qw9GjcKgt2OdvTspJPI2eyuRw0nBr9JKdp6eVP1u3xUyaKN1qY
zVksB9vKCe6kqRIV4qfUJP1jvSWI9OKuSbn5zpK0ouzXI9mNfoARhDv30qIt+8n719Wbh
9fb5+Eh++Fj5+K/wWCuWQX

Example Return Values

The result should look like the following:

RESULT[1]=0&RESPMSG[2]=OK&AUTHENTICATION_ID[20]=8d4d5ed66ac6e6faac6d
&AUTHENTICATION_STATUS[1]=Y&CAVV[28]=OTJIMzViODhiOTIIMjBhYmVkMGU=&
ECI[2]=05&XID[28]=YjM0YTkwNGFkZTI5YmZmZWE1ZmY=

Note The = character at the end of the XID value is correct (it is the 28th character).

Step 4 Submit the Payflow Sale or Authorization transaction with buyer authentication data

Direct the sale or authorization transaction (**TRXTYPE=S** or **A**) to VeriSign's test Payflow Pro server: **test-payflow.verisign.com**.

The response should include a value for **CARDSECURE**.

To Generate a Particular CARDSECURE value (Visa only)

- Any dollar amount with 11 cents (xx.11) causes **CARDSECURE=N**
- Any dollar amount with 22 cents (xx.22) causes **CARDSECURE=X**
- All other amounts cause **CARDSECURE=Y**

♦ If the Cardholder is Enrolled:

If the **Validate Authentication** transaction returns a verified enrollment, include the following additional buyer authentication name/value pairs from the **Validate Authentication** response:

- AUTHENTICATION_ID
- AUTHENTICATION_STATUS
- CAVV (The test servers use the following CAVV values for all accounts:
ZDQzMTMzMjhMTc1MzgwZTAwNTA= returns a response of 1,
814UqW4Wg0aBA5w0wR8wuQQFBQA= returns a response of 6,
all others return 2.)

- XID (Visa only)
- ECI

♦ **Otherwise:**

Include the following additional buyer authentication name/value pairs from the **Verify Enrollment** response:

- AUTHENTICATION_ID
- AUTHENTICATION_STATUS
- ECI



APPENDIX E

Deactivating Fraud Protection Services

This appendix describes the process of deactivating Fraud Protection Services.

Deactivating Fraud Protection Services removes the Security menu and Transaction Review functions (making it impossible to settle transactions). Therefore, before deactivating the service, you must first perform the following steps:

- 1 Turn off filters so that no new transactions are sent to the Fraud review queue.
- 2 Clear the queue of transactions awaiting review by deciding to accept or reject them.
- 3 Print hard copies of your audit trails as a permanent record.
- 4 Once you have completed steps 1 through 3, call VeriSign Customer Support to request deactivation.

VeriSign deactivates the service. Any remaining transactions settle normally.

Index

A

- Accepted transactions 28
- Account Monitoring Service 9
- Account Number Velocity Filter 109
- account security
 - specifying 12, 19, 23
- Active mode 18
- Allow non-referenced credits 16
- allowed IP addresses 6
 - specifying 12, 19, 23
- APIs
 - documentation 35, 62
 - downloading 35, 62
- AUTHCODE 84
- authentication status 43
- AVS Failure Filter 102
- AVSADDR 84
- AVSZIP 84

B

- BIN Risk List Match Filter 109
- Buyer Authentication
 - examples 48
 - logging results 58
 - parameters 51
 - testing transactions 133
- Buyer Authentication Audit report 75
- Buyer Authentication Failure Filter 98, 107
- Buyer Authentication server 43
- Buyer Authentication Service 7, 42
 - XMLPay 43

- Buyer Authentication Transaction report 78

C

- card security code 105
- CAVV 42
- changing
 - your password 13
- communications errors 91
- configuring filters 6
- credit card fraud 5
- CSC Failure Filter 105
- CSC, *see* card security code

D

- deactivation 143
- deploying filters 22
- documentation
 - API 35, 62
- downloading APIs 35, 62

E

- ECI 43
- ECI values 57
- Edit Test Filters page 20
- E-mail Service Provider Risk List Match Filter 112
- enrolling for Fraud Protection Services 2
- enrollment requirements 1

F

- Filter Scorecard 32

filter types

High-risk Address 110

High-risk Payment 102

Unusual Order 100

filters

Account Number Velocity 109

AVS Failure 102

BIN Risk List Match 109

Buyer Authentication Failure 98, 107

configuring 6

CSC Failure 105

defined 6

E-mail Service Provider Risk List Match 112

examples 6

Freight Forwarder Risk List Match 110

Geo-location Failure 113

interpreting results 99

IP Address Match 112

IP Address Velocity 114

parameters 64

Product Watch List 101

required transaction data 62

response string 67

Shipping/Billing Mismatch Filter 101

testing 121

Total Item Ceiling 100

Total Purchase Price Ceiling 100

USPS Address Validation Failure 111

ZIP Risk List Match 110

fraud liability

reducing 7

Fraud Protection Services

enrolling 2

Freight Forwarder Risk List Match Filter 110

G

Geo-location Failure Filter 113

H

hacking 5

High-risk Address Filters 110

High-risk Payment Filters 102

I

instant fulfillment 8

interpreting filter responses 99

IP Address Match Filter 112

IP Address Velocity Filter 114

L

liability

reducing 7

logging transaction information 58, 73

logging transaction results 58

M

Maximum amount per transaction 15

Merchant Plug-in 42

O

Observe mode 18, 21

P

PAREQ 42

PARES 42

passwords

guidelines 14

managing 6, 13

PNREF 83

format of value 85

PNREF value 84

processors supporting Buyer Authentication Service 8

Product Watch List Filter 101

Q

Qualys 9

R

recurring transactions 8

rejected transactions 28

rejecting transactions 32

reports

- Buyer Authentication Audit 75
- Buyer Authentication Transaction 78 described 75

RESPMSG 84

RESPMSG value 86

responses 67

- credit card transaction 83

resubmitting transactions 33

RESULT 83

RESULT value 85

RESULT values

- communication errors 91

Reviewed transactions 28

reviewing transactions 28, 30

risk lists 99

S

SecureCode 7

security

- access control 23
- account control 12, 19
- CSC 105

security scan 9

security settings

- Credits may exceed original transaction amount 16
- Maximum amount for credits 16
- Maximum amount per transaction 15

Shipping/Billing Mismatch Filter 101

Skipped Filters section 31

T

Test phase 17

testing 18

- Buyer Authentication transactions 133
- filters 121

Total Item Ceiling Filter 100

Total Purchase Price Ceiling Filter 100

Transaction Detail page 81

Transaction Details page 30

transaction ID 75

transaction response

- PNREF parameter 84
- RESPMSG parameter 86
- RESULT parameter 85

Transaction Settings 6

transaction status values 29

Transaction Wizard 17

transactions

- logging 73
- rejecting 32
- resubmitting 33
- reviewing 30

U

Unusual Order Filters 100

USPS Address Validation Failure Filter 111

V

Validate Authentication call 46

VERBOSITY parameter 67

Verified by Visa 7

Verify Enrollment call 35, 44

X

XID 42

XMLPay

- Buyer Authentication Service 43

Z

ZIP Risk List Match Filter 110

