



Website Payments Pro Payflow Edition - Fraud Protection Services User's Guide

For Professional Use Only
Currently only available in English.

A usage Professional Uniquement
Disponible en Anglais uniquement pour l'instant.

*Website Payments Pro Payflow Edition - Fraud Protection
Services User's Guide*

200019.en_US-200802

© 2008 PayPal, Inc. All rights reserved. PayPal is a registered trademark of PayPal, Inc. The PayPal logo is a trademark of PayPal, Inc. Other trademarks and brands are the property of their respective owners.

The information in this document belongs to PayPal, Inc. It may not be used, reproduced or disclosed without the written approval of PayPal, Inc. PayPal Europe S.à.r.l. & Cie, S.C.A. is authorized and regulated by the Commission de Surveillance du Secteur Financier in Luxembourg as a bank. PayPal RCS registration number: 118349

Notice of non-liability:

PayPal, Inc. is providing the information in this document to you "AS-IS" with all faults. PayPal, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. PayPal, Inc. assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. PayPal, Inc. reserves the right to make changes to any information herein without further notice.



Contents

Preface	7
Intended Audience	7
Document Conventions	7
Document Organization	7
For More Information.	8
Customer Service	8
Revision History	8
Chapter 1 Overview.	9
Growing Problem of Fraud	9
Reducing the Cost of Fraud	9
Chapter 2 How Fraud Protection Services Protect You	11
The Threats	11
Hacking	11
Credit Card Fraud	11
Protection Against the Threats—Fraud Filters	11
Example Filter	12
Configuring the Filters	12
Reviewing Suspicious Transactions	12
Special Considerations.	12
Merchants With an Instant Fulfillment Model	12
Merchants using the Recurring Billing Service	12
Chapter 3 Configuring the Fraud Protection Services Filters	13
Phase 1: Run Test Transactions Against Filter Settings on Test Transaction Security Servers	14
Phase 2: Run Live Transactions on Live Transaction Servers in Observe Mode	14
Phase 3: Run All Transactions Through the Live Transaction Security Servers Using Active Mode	15
Chapter 4 Assessing Transactions that Triggered Filters	17

Reviewing Suspicious Transactions	17
Acting on Transactions that Triggered Filters	20
Rejecting Transactions	20
Fine-tuning Filter Settings—Using the Filter Scorecard	20
Ensuring Meaningful Data on the Filter Scorecard	21
Re-running Transactions That Were Not Screened	22
Chapter 5 Screening Transactions Using the Payflow SDK	23
Downloading the Payflow SDK (Including APIs and API Documentation)	23
Transaction Data Required by Filters	23
Transaction Parameters Unique to the Filters	26
Existing Payflow Parameters Used by the Filters	26
Response Strings for Transactions that Trigger Filters	28
RESULT Values Specific to Fraud Protection Services	31
Changing the Verbosity Setting	32
Example Response for an Authentication Transaction With Verbosity=Low	32
Example Response for an Authentication Transaction With Verbosity=Medium	32
Accepting or Rejecting Transactions That Trigger Filters	36
Logging Transaction Information	36
Chapter 6 Responses to Credit Card Transaction Requests	39
An Example Response String	39
Contents of a Response to a Credit Card Transaction Request	39
PNREF Value	40
PNREF Format	41
RESULT Codes and RESPMSG Values	41
RESULT Values for Transaction Declines or Errors	41
RESULT Values for Communications Errors	47
Appendix A How Filters Work	49
How Filters Process a Transaction for Fraud	49
Pre-Processing Filters	51
Post-Processing Filters	52
Appendix B Fraud Filter Reference	53
Filters Included with the Fraud Protection Services	53

Filters Included with the Basic Fraud Protection Services Option	53
Filters Included with the Advanced Fraud Protection Services Option	54
About the Fraud Risk Lists	54
Filters Applied After Processing	54
Unusual Order Filters	55
Total Purchase Price Ceiling Filter	55
Total Item Ceiling Filter	55
Shipping/Billing Mismatch Filter	56
Product Watch List Filter	56
High-risk Payment Filters	57
AVS Failure Filter	57
Card Security Code Failure Filter	58
BIN Risk List Match Filter	60
Account Number Velocity Filter	60
High-risk Address Filters	60
ZIP Risk List Match Filter	61
Freight Forwarder Risk List Match Filter	61
USPS Address Validation Failure Filter	61
IP Address Match Filter	62
Email Service Provider Risk List Match Filter	62
Geo-location Failure Filter	63
IP Address Velocity Filter	64
High-risk Customer Filters	64
Bad Lists	64
International Order Filters	65
Country Risk List Match Filter	65
International Shipping/Billing Address Filter	65
International IP Address Filter	66
International AVS Filter	66
Accept Filters	67
Good Lists	67
Total Purchase Price Floor Filter	68
Custom Filters	68

Appendix C Testing the Transaction Security Filters 69

Good and Bad Lists	69
AVS Failure Filter	70
BIN Risk List Match Filter	70

Country Risk List Match Filter	71
Email Service Provider Risk List Match Filter	72
Freight Forwarder Risk List Match Filter	72
Geo-location Failure Filter	73
International AVS Filter	73
International IP Address Filter	74
International Shipping/Billing Address Filter	75
IP Address Match Filter	76
Shipping/Billing Mismatch Filter	76
Total Item Ceiling Filter.	77
Total Purchase Price Ceiling Filter	77
Total Purchase Price Floor Filter	78
USPS Address Validation Failure Filter	78
ZIP Risk List Match Filter	79
Appendix D Deactivating Fraud Protection Services81
Index.83



Preface

This document describes Fraud Protection Services and explains how you can use the Payflow SDK to perform transactions that will be screened by Fraud Protection Services filters.

For details on how to configure and use Fraud Protection Services through PayPal Manager, see PayPal Manager online help.

Intended Audience

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

Document Conventions

This document uses the term *fraudster* to represent an entity (typically a person) attempting fraudulent activity.

Document Organization

- [Chapter 1, “Overview,”](#) presents the Fraud Protection Services suite.
- [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 Filters,”](#) describes how to configure Fraud Protection Services.
- [Chapter 4, “Assessing Transactions that Triggered Filters,”](#) makes recommendations on how to set up and fine-tune filters.
- [Chapter 5, “Activating and Configuring the Buyer Authentication Service,”](#) describes activating and configuring the Buyer Authentication service.
- [Chapter 6, “Performing Buyer Authentication Transactions Using the SDK,”](#) describes and provides an example of how to use Buyer Authentication.
- [Chapter 5, “Screening Transactions Using the Payflow SDK,”](#) describes how to screen transactions for fraud using the Payflow SDK.
- [Chapter 6, “Responses to Credit Card Transaction Requests,”](#) describes the responses to a credit card transaction request.

- [Appendix B, “Fraud Filter Reference,”](#) describes the Transaction filters that make up part of the Fraud Protection Services.
- [Appendix C, “Testing the Transaction Security Filters,”](#) provides Payflow SDK transactions that you can use to test the filters.
- [Appendix C, “Testing Buyer Authentication Transactions Using the Payflow SDK,”](#) provides examples of testing Buyer Authentication transactions.
- [Appendix D, “Deactivating Fraud Protection Services,”](#) describes the process of deactivating Fraud Protection Services.

For More Information

For answers to specific questions about PayPal products, search PayPal’s Knowledge Base at the following URL: <http://knowledge.paypal.com/>.

Customer Service

If you are having problems with Fraud Protection Services, contact Customer Service at:
Email: payflow-support@paypal.com.

Revision History

TABLE P.1 Revision History

Date	Description
February 2008	Updated test and live URLs. Minor edits for technical accuracy.
August 2007	AU Enhancements
April 2007	Updated guide to include PayPal Manager User Interface changes.
February 2007	Updated AVS responses rules. Added return codes: 51, 110, 119, 120, 121, 132, 133, 200, 201, 402, 403, 404, 600, and 601.
December 2006	Updated buyer auth test URL to pilot-buyerauth.verisign.com Minor corrections for technical accuracy

1

Overview

This chapter discusses how fraud can affect you the merchant and provides an overview of Fraud Protection Services.

In This Chapter

- “Growing Problem of Fraud” on page 9
- “Reducing the Cost of Fraud” on page 9

Growing Problem of Fraud

Online fraud is a serious and growing problem. 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.

Reducing the Cost of Fraud

Fraud Protection Services, in conjunction with your Website Payments Pro Payflow Edition 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 in and use the Fraud Protection Services products:

- Merchant must have a current, paid-in-full Website Payments Pro Payflow Edition service account.
- Merchant Website Payments Pro Payflow Edition 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 processors: American Express Phoenix, FDMS Nashville, FDMS North, FDMS South, Global Payments East, Nova, Paymentech New Hampshire, or Vital.

2

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 11
- “Protection Against the Threats—Fraud Filters” on page 11
- “Special Considerations” on page 12

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 Website Payments Pro Payflow Edition account to run unauthorized transactions (purchases and credits). Fraud Protection software *filters* minimize the risk of hacking by enabling you to place powerful constraints on access to and use of your PayPal Manager and Website Payments Pro Payflow Edition 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, the Fraud Protection filters identify potentially fraudulent activity and let you decide whether to accept or reject the suspicious transactions.

Protection Against the Threats—Fraud Filters

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

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

Through PayPal Manager, 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). See PayPal Manager online help for detailed filter configuration procedures.

Typically, you specify setting the transaction aside for review. For transactions that you deem extremely risky (for example, a known bad email 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.

Reviewing Suspicious Transactions

As part of the task of minimizing the risk of fraud, you review each transaction that triggered a filter through PayPal Manager to determine whether to accept or reject the transaction. See PayPal Manager online help for details.

Special Considerations

Merchants With an Instant Fulfillment 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 PayPal Manager's Virtual Terminal. 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.

3

Configuring the Fraud Protection Services Filters

This chapter describes how to configure the Fraud Filters for your Website Payments Pro Payflow Edition account. The chapter explains a phased approach to implementing the security of transactions. You are not required to use the approach described in this chapter. However it enables you to fine tune your use of filters before you actually deploy them in a live environment.

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 live **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 the phases described below, you must click the **Deploy** button to deploy the filter settings. Filter settings take effect only after you deploy them.*

Filter setting changes are updated hourly (roughly on the hour). This means that you might have to wait up to an hour for your changes to take effect. This waiting period only occurs when you move from one mode to the next.

- **Phase 1:** Run test transactions in **Test** mode using test transaction servers
In the test phase of implementation, you configure fraud 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 **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 **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.

NOTE: 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 live 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.

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

1. In the Service Summary section of the PayPal Manager home page, click the Basic or Advanced Fraud Protection link.

Click **Service Settings > Fraud Protection > Test Setup**.

2. **Basic or** Click **Edit Standard Filters**. The *Edit Standard Filters* page appears.
3. For each filter:
 - Click the filter check box to enable it and click-to-clear the check box to disable it.
 - Select the filter action that should take place when the filter is triggered.
For some filters, you set a trigger value. For example, the Total Purchase Price Ceiling filter trigger value is the transaction amount that causes the filter to set a transaction aside.

NOTE: To make decisions about how the filters work, see [Appendix B, “Fraud Filter Reference.”](#)

4. Once you complete editing the page, click **Deploy**.

IMPORTANT: *If you do not deploy the filters, then your settings are not saved.*

5. To run test transactions, you can use PayPal Manager’s Virtual Terminal. See PayPal Manager for online help instructions.
6. Review the filter results by following the instructions in [Chapter 4, “Assessing Transactions that Triggered Filters.”](#)
7. Based on your results, you may want to make changes to the filter settings. Simply return to the Edit Filters page, change settings, and redeploy them. Once you are happy with your filter settings, you can move to Phase 2.

Phase 2: Run Live Transactions on Live Transaction Servers in Observe Mode

In this phase, 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 between Observe and Active mode is that,

Phase 3: Run All Transactions Through the Live Transaction Security Servers Using Active Mode

regardless of the filter actions, all Observe mode 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 **Service Settings > Fraud Protection > Test Setup**. Click **Move Test Filter Settings to Live**. The **Move Test Filter Setting to Live** page appears. Remember that in this phase, you are configuring the live servers.
2. **Basic** or Click **Move Test Filter Settings to Live**. On the page that appears, click **Move Test Filter Settings to Live** again.
3. The *Move Test Filter Settings to Live* page prompts whether to deploy the filters in **Observe** mode or in **Active** mode. Click **Deploy to Observe Mode**.

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.

IMPORTANT: *Deployed filter setting changes are updated hourly (roughly on the hour). This means that you might have to wait up to an hour for your changes to take effect. This waiting period only occurs when you move from one mode to the next.*

4. Review the filter results by following the instructions in [Chapter 4, “Assessing Transactions that Triggered Filters.”](#) The Filter Scorecard (described on [page 20](#)) 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.
5. 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 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.

6. **Basic** or Click **Move Test Filter Settings to Live**. On the page that appears, click **Move Test Filter Settings to Live** again.
7. On the *Move Test Filter Settings to Live* page, click **Deploy to Active Mode**.

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

8. 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.*

4

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 83](#) for complete lists of Basic and Advanced filters.

In This Chapter

- [“Reviewing Suspicious Transactions” on page 17](#)
- [“Fine-tuning Filter Settings—Using the Filter Scorecard” on page 20](#)
- [“Re-running Transactions That Were Not Screened” on page 22](#)

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. Accepting a transaction requires no further action. To reject a transaction, a separate void of the transaction is required.

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

1. Click **Reports > Fraud Protection > Fraud Transactions**

The *Fraud Transactions Report* page appears.

FIGURE 4.1 Fraud Transactions Report page

Fraud Transactions Report

Fraud Protection report enables you 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.

Report Options

Save Template As:

(Required only when saving a template. Only alphanumeric characters are allowed)

Date Range: Custom

From: 06 / 26 / 2006 Time: 00 : 00 : 00

To: 06 / 26 / 2006 Time: 23 : 59 : 59

Time Zone: U.S. Pacific

Transaction Type: Review

Transaction Mode: Live

Download Report: Format: ASCII Text

2. Specify the date range of the transactions to review.

3. Specify a **Transaction Type**:

TABLE 4.1 Transaction types

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. This conditional occurs only in Test mode or Live mode. In Observe mode all results codes are always 0. You can re-screen any of these transactions through the filters as described in “Re-running Transactions That Were Not Screened” on page 22.
Screened by Filters	All transactions that were screened by filters, regardless of filter action or whether any filter was triggered.

4. Specify the Transaction Mode, and click **Run Report**.

The *Fraud Transactions Report* page displays all transactions that meet your search criteria.

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:

TABLE 4.2 Transactions Report field descriptions

Heading	Description
Report Type	The type of report created.
Date	Date and time range within which the transactions in this report were run.
Time Zone	Time zone represented in this report.
Transaction Mode	Test, Observe, or Active
Transaction ID	Unique transaction identifier. Click this value to view the <i>Transaction Detail</i> page.
Transaction Time	Time and date that the transaction occurred.
Transaction Type	The transaction status that resulted from filter action, as described in Table 4.1 .
Card Type	MasterCard or Visa.
Amount	Amount of the transaction.

The following transaction status values can appear in the report:

TABLE 4.3 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
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 *Fraud Details* page appears, as discussed in the next section.

Acting on Transactions that Triggered Filters

The *Fraud 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).

The following notes describe data in the *Fraud Details* page shown in the figure.

1. This transaction was set aside because it triggered the AVS Failure filter.
2. The transaction was not screened by any of the filters in the Skipped Filters section because the 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 22](#)
3. Specify the action to take on the transaction:
 - Review: Take no action. You can return to this page at any time or reject or accept the transaction. The transaction remains unsettled.
 - Reject: Do not submit the transaction for processing. See [“Rejecting Transactions” on page 20](#).
 - Accept: Submit the transaction for normal processing.
4. You can enter notes regarding the disposition of the transaction or the reasons for taking a particular action. Do not use the & < > or = characters.
5. Click **Submit** to save the notes, apply the action, and move to the next transaction.

NOTE: You can also view the *Fraud 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 **Reports > Filter Scorecard**. The *Filter Scorecard Report* page appears.

FIGURE 4.2 Filter Scorecard Report page

Filter Scorecard Report

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.

Report Options

Save Template As:
(Required only when saving a template. Only alphanumeric characters are allowed)

Date Range: Custom
 From: 06 / 26 / 2006 Time: 00 : 00 : 00
 To: 06 / 26 / 2006 Time: 23 : 59 : 59

Time Zone: U.S. Pacific

Transaction Mode: Live

Download Report: Format: ASCII Text

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 **Run Report**.

The *Filter Scorecard Report* 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.

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.

Say, 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

Perform the following steps if you wish to re-run a transaction that was not screened by filters (transactions with Result Code 127):

1. Navigate to **Reports > Fraud Protection > Fraud Transaction Report**. The *Fraud Transaction Report* page appears.
2. Select the appropriate time period for the search, and select the “Not Screened by Filters” option for **Transaction Type**.
3. Click **RunView Report**. The *Fraud Transaction Report Results* page appears. It contains all the transactions that were not screened by filters.
4. Click on the Transaction ID of the transaction you would like to re-run. The *Confirm Rerun* page appears.
5. Click **Yes** to re-run that transaction. The *Success* page appears if your transaction was successful.

NOTE: 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.

5

Screening Transactions Using the Payflow SDK

This chapter describes the process of using the Payflow 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 *Website Payments Pro Payflow Edition Developer's Guide*.

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

Response Values. Payflow response values are described in “RESULT Codes and RESPMSG Values” on page 45.

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

In This Chapter

- “Downloading the Payflow SDK (Including APIs and API Documentation)” on page 29
- “Transaction Parameters Unique to the Filters” on page 32
- “Existing Payflow parameters Used by the Filters” on page 32
- “Response Strings for Transactions that Trigger Filters” on page 34
- “Accepting or Rejecting Transactions That Trigger Filters” on page 40
- “Logging Transaction Information” on page 41

Downloading the Payflow SDK (Including APIs and API Documentation)

The Payflow 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. *Website Payments Pro Payflow Edition Developer's Guide* The *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 parameter values that are required by the filters.

TABLE 5.1 Parameters required by filter

Filter	Required Transaction Data	Payflow Parameters
Account Number Velocity	Credit card number	ACCT
AVS Failure	Billing address - street address	STREET
	Billing address - ZIP (postal) code	ZIP
Bad Lists	Customer email address	EMAIL
	Credit card number	ACCT
BIN Risk List Match	Credit card number	ACCT
Country Risk List Match	Billing address - country	COUNTRY
	Shipping address - country	COUNTRYCODE
Card Security Code Failure	Card security code information from credit card	CSC
Email Service Provider Risk List	Customer email 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 email address	EMAIL
	Credit card number	ACCT

TABLE 5.1 Parameters required by filter

Filter	Required Transaction Data	Payflow Parameters
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

The Payflow server accepts the parameters listed in this section.

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

TABLE 5.2 Parameters accepted by the Payflow server

Name	Description	Type	Max. Length	Example
BILLTOSTREET2	Extended billing address	Alpha-numeric 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 email address	40	abc@xyz.com
COUNTRYCODE	Optional. Country code of the shipping country. The country code depends on the processor.	Alpha-numeric String	3	US, USA, 840

Existing Payflow Parameters Used by the Filters

The following existing Payflow parameters (described in) 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
BROWERTIME
BROWERCOUNTRYCODE
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 Website Payments Pro Payflow Edition accounts. The following values (described in *Website Payments Pro Payflow Edition Developer's Guide*) are returned: {RESULT, PNREF, RESPMSG, AUTHCODE, AVSADDR, AVSZIP, CVV2MATCH, IAVS, CARDSECURE}

The following values are specific to Fraud Protection Services:

TABLE 5.3 Low VERBOSITY parameters

Parameter	Description
RESULT	See “RESULT Values Specific to Fraud Protection Services” on page 37 .
PREFPSMSG	Preprocessing Fraud Protection Services messages. These apply to all filters except: AVS Failure, Card Security Code Failure, and Custom Filters.
POSTFPSMSG	Postprocessing Fraud Protection Services messages. These apply to the following filters only: AVS Failure, Card Security Code Failure, and Custom Filters.

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

TABLE 5.4 Medium VERBOSITY parameters

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.
RESPTEXT	char	17	Text corresponding to the response code returned by the processor. This text is not normalized.
PROCAVS	char	2	AVS (Address Verification Service) response from the processor
PROCCVV2	char	1	CVV2 (buyer authentication) response from the processor
PROCCARDSECURE	char	1	VPAS/SPA response from the processor
ADDLMSG	char	Up to 1048 characters. Typically 50 characters.	Additional error message that indicates that the merchant used a feature that is disabled

TABLE 5.4 Medium VERBOSITY parameters

Parameter	Type	Length	Description
TRANSSTATE	Integer	10	<p>State of the transaction. The values are:</p> <p>0 = General succeed state</p> <p>1 = General error state</p> <p>3 = Authorization approved</p> <p>6 = Settlement pending (transaction is scheduled to be settled)</p> <p>7 = Settlement in progress (transaction involved in a currently ongoing settlement)</p> <p>8 = Settled successfully</p> <p>9 = Authorization captured (once an authorization type transaction is captured, its TRANSSTATE becomes 9)</p> <p>10 = Capture failed (an error occurred while trying to capture an authorization because the transaction was already captured)</p> <p>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)</p> <p>12 - Unsettled transaction because of incorrect account information</p> <p>14 = For various reasons, the batch containing this transaction failed settlement</p> <p>16 = Merchant ACH settlement failed; (need to manually collect it). For information on TRANSSTATE incremental values, see the table below.</p>
DATE_TO_SETTLE	Date format YYYY-MM-DD HH:MM:SS	19	Value available only before settlement has started.

TABLE 5.4 Medium VERBOSITY parameters

Parameter	Type	Length	Description
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.

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

TABLE 5.5 TRANSSTATE value increments

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 PayPal Manager, or 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 5.6 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

TABLE 5.6 Transaction RESULTS/RESPMSGs(Continued)

RESULT	RESPMSG and Explanation
128	Fraud Protection Services Filter — Declined by merchant after being flagged for review by filters
131	Version 1 Payflow client no longer supported. Upgrade to the most recent version of the Payflow client.

Changing the Verbosity Setting

Setting the default verbosity level for all transactions

Contact 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&PREFFPSMSG=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(0)&PNREF=VFHA28926593&RESPMSG=Under review by Fraud
Service (Approved) &AUTHCODE=041PNI&AVSADDR=Y&AVSZIP=N&CVV2MATCH=X&HOSTCODE=A
&PROCAVS=A&PROCCVV2=X&IAVS=N&PREFFPSMSG=Review: More than one rule was
triggered for Review&FPS_PREXMLDATA[2898]=<triggeredRules><rule
num="1"><ruleId>2</ruleId><ruleAlias>CeilingAmount</ruleAlias><ruleDescript
ion>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><ruleDescri
```



```

ption>Total
ItemCeiling</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><valuetype="Integer">15</value></ruleParameter></
rulevendorparms></rule>(Remove text
completely<rulenum="3"><ruleId>7</ruleId><ruleAlias>BillShipMismatch</ruleA
lias><ruleDescription>Shipping/BillingMismatch</ruleDescription><action>R</
action><triggeredMessage>The billing and shipping addresses did not
match</triggeredMessage></rule><rulenum="4"><ruleId>13</ruleId><ruleAlias>H
ighRiskBinCheck</ruleAlias><ruleDescription>BIN Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The card number
is in a high risk bin
list</triggeredMessage></rule><rulenum="5"><ruleId>37</ruleId><ruleAlias>Hi
ghRiskZIPCheck</ruleAlias><ruleDescription>Zip Risk List
Match</ruleDescription><action>R</action><triggeredMessage>High risk
shipping
zip</triggeredMessage></rule><rulenum="6"><ruleId>16</ruleId><ruleAlias>Bil
lUSPostalAddressCheck</ruleAlias><
ruleDescription>USPS Address Validation
Failure</ruleDescription><action>R</action><triggeredMessage>The billing
address is not a valid US
Address</triggeredMessage><rulevendorparms><ruleParameter num="1"><name>Addr
essToVerify</name><valuetype="String">bill</value></ruleParameter></ruleven
dorpams></rule>(Remove text
completely) <rulenum="7"><ruleId>10</ruleId><ruleAlias>HighRiskEmailCheck</r
uleAlias><ruleDescription>Email Service Provider Risk List
Match</ruleDescription><action>R</action><triggeredMessage>The email
address fraud@asiamail.com in bill Email was found in a high risk email
providerlist</triggeredMessage></rule><rulenum="8"><ruleId>38</ruleId><rule
Alias>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><rulenum="9"><ruleId>8</ruleId><ruleAlias>NonUS
IPAddress</ruleAlias><ruleDescription>International IP
Address</ruleDescription><action>R</action><triggeredMessage>The IP address

```

```

is from:
CZ</triggeredMessage></rule><rulenum="10"><ruleId>41</ruleId><ruleAlias>HighRiskFreightCheck</ruleAlias><ruleDescription>Freight Forwarder Match</ruleDescription><action>R</action><triggeredMessage>High risk freight forwarder</triggeredMessage></rule> (Remove text completely</triggeredRules>&POSTFPSMSG=Review:More than one rule was triggered for Review&FPS_POSTXMLDATA[682]=<triggeredRules><rulenum="1"><ruleId>1</ruleId><ruleAlias>AVS</ruleAlias><ruleDescription>AVS Failure</ruleDescription><action>R</action><triggeredMessage>AVS check failed: Full Security</triggeredMessage><rulevendorparms><ruleParametername="1"><name>Value</name><valuetype="String">Full</value></ruleParameter></rulevendorparms></rule> (Remove text completely) <rulenum="2"><ruleId>23</ruleId><ruleAlias>CSCFailure</ruleAlias><ruleDescription>CSC Failure</ruleDescription><action>R</action><triggeredMessage>CSC check failed, returned X</triggeredMessage><rulevendorparms><ruleParametername="1"><name>Value</name><valuetype="String">Full</value></ruleParameter></rulevendorparms></rule></triggeredRules>

```

```

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&PREFPMSG=Review: More than one rule was triggered for
Review&FPS_PREXMLDATA[2898]=<triggeredRules><rule
num="1"><ruleId>2</ruleId><ruleAlias>CeilingAmount</ruleAlias><ruleDescript
ion>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><ruleDescri
ption>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><ruleDescr
iption>Shipping/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><ruleDescr
iption>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><ruleDescr
iption>Zip Risk List
Match</ruleDescription><action>R</action><triggeredMessage>High risk
shipping zip</triggeredMessage></rule><rule
num="6"><ruleId>16</ruleId><ruleAlias>BillUSPostalAddressCheck</ruleAlias><
ruleDescription>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><ruleDe
scription>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><ruleDescr
iption>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><ruleDescrip
tion>International IP
Address</ruleDescription><action>R</action><triggeredMessage>The IP address
is from: CZ</triggeredMessage></rule><rule

```

```

num="10"><ruleId>41</ruleId><ruleAlias>HighRiskFreightCheck</ruleAlias><ruleDescription>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></trigge
redRules>

```

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 21.

- **Accept:** Submit the transaction for normal processing.
- **Reject:** Do not submit the transaction for processing. See [“Rejecting Transactions”](#) on page 23.

NOTE: You must contact Customer Service to enable this feature. Telephone: 1-888-883-9770.
E-mail: payflow-support@paypal.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

A record is maintained of all transactions executed on your account. Use PayPal 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, it is 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 PayPal Manager reports)
- Transaction Date
- Transaction Amount

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

6

Responses to Credit Card Transaction Requests

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

In This Chapter

- “An Example Response String” on page 39
- “Contents of a Response to a Credit Card Transaction Request” on page 39
- “PNREF Value” on page 40
- “RESULT Codes and RESPMSG Values” on page 41

An Example Response String

When a transaction finishes, the server 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&AVSADDR=Y&AVSZIP=N&IAVS=Y&CVV2MATCH=Y&CORRELATIONID=2e52df7ddf292
```

Contents of a Response to a Credit Card Transaction Request

All transaction responses include values for RESULT, PNREF, and RESPMSG. A value for AUTHCODE is included for Voice Authorization transactions. Values for AVSADDR and AVSZIP are included if you use address verification system (AVS). [Table 6.1](#) describes the values returned in a response string.

TABLE 6.1 Transaction response values

Field	Description	Type	Length
PNREF	Reference ID, a unique number that identifies the transaction. PNREF is described in “ PNREF Format ” on page 41.	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 41.	Numeric	Variable

TABLE 6.1 Transaction response values (Continued)

Field	Description	Type	Length
CVV2MATCH	Result of the card security code (CVV2) check. The issuing bank may decline the transaction if there is a mismatch. In other cases, the transaction may be approved despite a mismatch.	Alpha Y, N, X, or no response	1
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 41.	Alpha- numeric	Variable
PPREF	Unique transaction ID of the payment. If the TRXTYPE of the request is A, then you will need the value of PPREF for use with Authorization and Delayed Capture transactions.	string	17
AVSADDR	AVS address responses are for advice only. This process does not affect the outcome of the authorization.	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.	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.	Alpha Y, N, X, or no response	1
PAYMENTTYPE	Response indicating whether the payment is instant or delayed.	String	7
CORRELATIONID	Value used for tracking this Direct Payment transaction.	Alphanumer ic	13

PNREF Value

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

- The PNREF value is used as the ORIGID 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 ORIGID 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:

- EFHP0D426838
- 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.

The PNREF in a transaction response tells you that your transaction is connecting to the server.

Historically, the contents of a PNREF indicated a test or a live transaction. 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 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 6.2 Payflow transaction RESULT values and RESPMSG text

RESULT	RESPMSG and Explanation
0	Approved
1	<p>User authentication failed. Error is caused by one or more of the following:</p> <ul style="list-style-type: none"> • Login information is incorrect. Verify that USER, VENDOR, PARTNER, and PASSWORD have been entered correctly. VENDOR is your merchant ID and USER is the same as VENDOR unless you created a Payflow Pro user. All fields are case sensitive. • Invalid Processor information entered. Contact merchant bank to verify. • "Allowed IP Address" security feature implemented. The transaction is coming from an unknown IP address. See PayPal Manager online help for details on how to use Manager to update the allowed IP addresses. • You are using a test (not active) account to submit a transaction to the live PayPal servers. Change the host address from the test server URL to the live server URL.
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. Use the format: “#####.##” Do not include currency symbols or commas.
5	Invalid merchant information. Processor does not recognize your merchant account information. Contact your bank account acquirer to resolve this problem.
6	Invalid or unsupported currency code
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
12	Declined. Check the credit card number, expiration date, and transaction information to make sure they were entered correctly. If this does not resolve the problem, have the customer call their card issuing bank to resolve.
13	Referral. Transaction cannot be approved electronically but can be approved with a verbal authorization. Contact your merchant bank to obtain an authorization and submit a manual Voice Authorization transaction.
14	Invalid Client Certification ID. Check the HTTP header. If the tag, X-VPS-VIT-CLIENT-CERTIFICATION-ID, is missing, RESULT code 14 is returned.

TABLE 6.2 Payflow transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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. You are trying to process a tender type such as Discover Card, but you are not set up with your merchant bank to accept this card type.
26	Invalid vendor account. Login information is incorrect. Verify that USER, VENDOR, PARTNER, and PASSWORD have been entered correctly. VENDOR is your merchant ID and USER is the same as VENDOR unless you created a Payflow Pro user. All fields are case sensitive.
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
51	Exceeds per transaction limit
99	General error. See RESPMSG.
100	Transaction type not supported by host
101	Time-out value too small
102	Processor not available
103	Error reading response from host

TABLE 6.2 Payflow transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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
110	Referenced auth (against order) Error
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
117	Failed merchant rule check. One or more of the following three failures occurred: An attempt was made to submit a transaction that failed to meet the security settings specified on the PayPal Manager <i>Security Settings</i> page. If the transaction exceeded the Maximum Amount <i>security setting</i> , then no values are returned for AVS or CSC. 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
119	General failure within PIM Adapter
120	Attempt to reference a failed transaction
121	Not enabled for feature

TABLE 6.2 Payflow transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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>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 Fraud Protection Services documentation for your payments solution. It is available on the PayPal Manager Documentation page.</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.
132	Card has not been submitted for update
133	Data mismatch in HTTP retry request
150	Issuing bank timed out
151	Issuing bank unavailable
200	Reauth error
201	Order error
402	PIM Adapter Unavailable
403	PIM Adapter stream error
404	PIM Adapter Timeout
600	Cybercash Batch Error
601	Cybercash Query Error
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

TABLE 6.2 Payflow transaction **RESULT** values and **RESPMSG** text (Continued)

RESULT	RESPMSG and Explanation
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).
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
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

TABLE 6.2 Payflow transaction RESULT values and RESPMSG text (Continued)

RESULT	RESPMSG and Explanation
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 caused by an incorrect URL or by configuration issues with your firewall.

A value of -1 or -2 can also be possible if the PayPal servers are unavailable, or an incorrect server/socket pair has been specified. A value of -1 can also result when there are internet connectivity errors. Contact customer support regarding any other errors.

TABLE 6.3 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
-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

TABLE 6.3 RESULT values for communications errors(Continued)

RESULT	Description
-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
-40	Unexpected Request ID found in request.
-41	Required Request ID not found in request
-99	Out of memory
-100	Parameter list cannot be empty
-103	Context initialization failed
-104	Unexpected transaction state
-105	Invalid name value pair request
-106	Invalid response format
-107	This XMLPay version is not supported
-108	The server certificate chain did not validate
-109	Unable to do logging
-111	The following error occurred while initializing from message file: <Details of the error message>
-113	Unable to round and truncate the currency value simultaneously

A

How Filters Work

This appendix describes how filters screen transactions.

Filters are of two major types:

- Pre-processing filters are a set of rules that are applied to a transaction before it is sent to the processor for authorization. See [“Pre-Processing Filters” on page 51](#) for a list of these filters.
- Post-processing filters are a set of rules that are applied after the processor authorizes the transaction and are run based on the results returned from the processor. See [“Post-Processing Filters” on page 52](#) for a list of these filters.

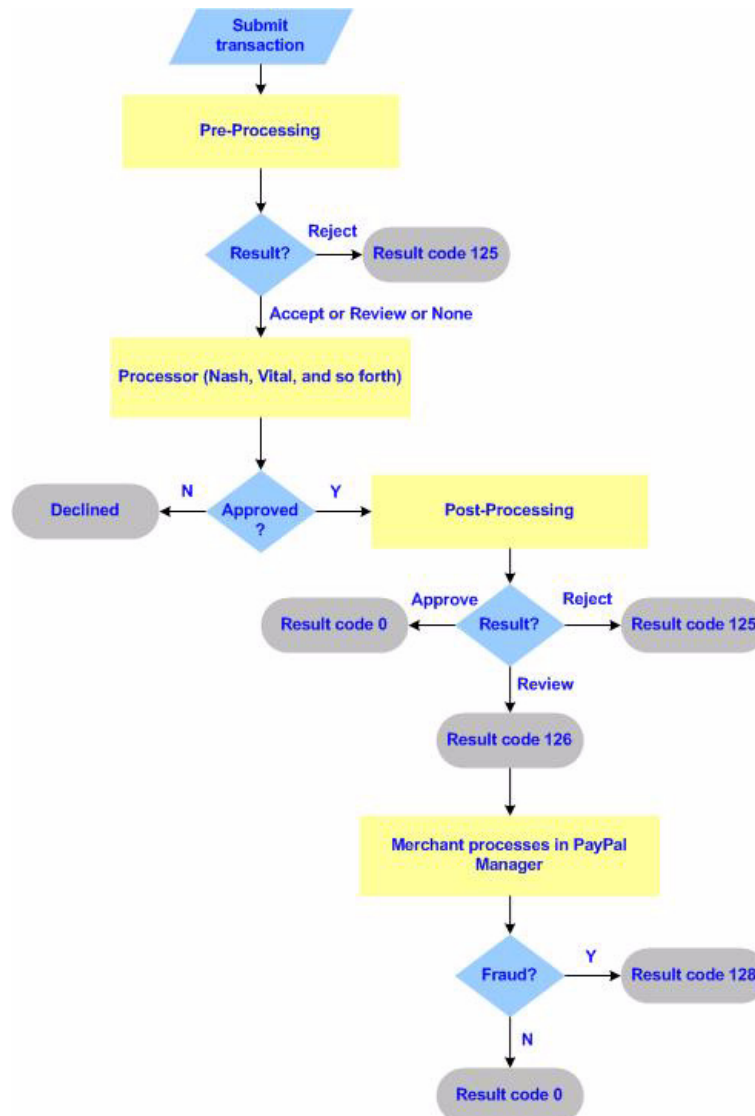
How Filters Process a Transaction for Fraud

The filter workflow is as follows and is illustrated in [Figure A.1](#):

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.

NOTE: Recurring transactions are not screened by filters.

2. The transaction is sent to the re-processing filters. Pre-processing filters can mark the transaction for Accept, Reject, or Review.

FIGURE A.1 Fraud transaction processing

3. If the result of pre-processing is Reject, the server sends a response to the merchant with Result code 125. If the result is Accept or Review, the server submits the transaction to the processor where more statistics are collected.
4. If the processor approves the transaction, then the transaction is post-processed. Post-processing determines the final result.
 - If the result of post-processing is Reject, the server sends the failed transaction response to the merchant with Result code 125.
 - If the result is Accept, the server sends the approved transaction response to the merchant with a Result code 0.

- If the result is Review, the server sends the transaction response to the merchant with Result code 126. The filters take no further steps. Later in PayPal Manager, the merchant reviews the reasons that the transaction triggered the filters to determine which action to take (Accept or Reject).

Pre-Processing Filters

Pre-processing filters are filters that can be applied to evaluate a fraud transaction readily based on the transaction details already embedded in the transaction at the time that the merchant submits it. The pre-processing filters are listed below:

Total Purchase Price Ceiling

Total Item Ceiling

Shipping/Billing Mismatch

Product Watch List

Good Lists

Bad Lists

Total Purchase Price Floor

IP Address Velocity

Account Number Velocity

International Shipping/Billing Address

BIN Risk List Match

ZIP Risk List Match

IP Address Match

Email Service Provider Risk List Match

Geo-location Failure

Freight Forwarder Risk List Match

USPS Address Validation Failure

Post-Processing Filters

Post-processing filters are applied to a fraud transaction after pre-processing is completed and subsequent processor approval for a transaction. The post-processing filters are listed below:

AVS Failure

Card Security Code Failure

International AVS

Custom Filters

B

Fraud Filter Reference

This appendix describes the filters that make up part of the 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 Appendix

- [“Filters Included with the Fraud Protection Services” on page 53](#)
- [“About the Fraud Risk Lists” on page 54](#)
- [“Filters Applied After Processing” on page 54](#)
- [“Unusual Order Filters” on page 55](#)
- [“High-risk Payment Filters” on page 57](#)
- [“High-risk Address Filters” on page 60](#)
- [“High-risk Customer Filters” on page 64](#)
- [“International Order Filters” on page 65](#)
- [“Accept Filters” on page 67](#)
- [“Custom Filters” on page 68](#)

Filters Included with the Fraud Protection Services

Fraud Protection Services offers Basic and Advanced options. The filters included with each option are listed here.

Filters Included with the Basic Fraud Protection Services Option

- [“Total Purchase Price Ceiling Filter” on page 55](#)
- [“Total Item Ceiling Filter” on page 55](#)
- [“Shipping/Billing Mismatch Filter” on page 56](#)
- [“AVS Failure Filter” on page 57](#)
- [“Card Security Code Failure Filter” on page 58](#)
- [“ZIP Risk List Match Filter” on page 61](#)
- [“Freight Forwarder Risk List Match Filter” on page 61](#)

- “IP Address Velocity Filter” on page 64

Filters Included with the Advanced Fraud Protection Services Option

All Basic filters plus:

- “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.” on page 59
- “USPS Address Validation Failure Filter” on page 61
- “Email Service Provider Risk List Match Filter” on page 62
- “IP Address Match Filter” on page 62
- “Account Number Velocity Filter” on page 60
- “Geo-location Failure Filter” on page 63
- “Bad Lists” on page 64
- “International Shipping/Billing Address Filter” on page 65
- “International AVS Filter” on page 66
- “International IP Address Filter” on page 66
- “Country Risk List Match Filter” on page 65
- “Good Lists” on page 67
- “Total Purchase Price Floor Filter” on page 68
- “Custom Filters” on page 68
- “Product Watch List Filter” on page 56

About the Fraud Risk Lists

Filters whose name includes “Risk List” make use of lists that the Fraud Protections Services manage. Extensive statistical analysis of millions of e-commerce transactions is performed 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).

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 57](#))
- Card Security Code Failure filter (described on [page 58](#))
- International AVS filter (described on [page 66](#))
- Custom filters (described on [page 68](#))

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.*

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.

NOTE: 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 *Fraud Details* page:

Billing	Shipping
Steve Morrison	Steve Morrison
4390 Ramirez	4390 Ramires
San Francisco, CA	San Franc c isco, 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 **card security code**.

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.

NOTE: 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?

This filter 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**.

TABLE B.1 AVS responses

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.

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” on page 61](#) validates the address information

NOTE: .

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

IMPORTANT: *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.*

Specifying the Level of AVS Checking

Specify one of the AVS settings:

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

This table summarizes AVS levels:

TABLE B.2 AVS responses

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

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** and **Buyer Authentication** in addition to **AVS** to increase your certainty.

Card Security Code Failure Filter

What does the filter do?

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

IMPORTANT: *The Card Security Code 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 Card Security Code

The card security code is printed on the back of most cards (usually in the signature field). All or part of the card number appears before the card security code (**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 card security code check compares the number provided by the customer with the number on file with the issuer and returns one of the following responses:

TABLE B.3 Card security code 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.

Card Security Code Failure Filter Action

The specified action is taken whenever the card security code 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.

NOTE: 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.

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 the 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.

IMPORTANT: *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. 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 the high-risk list. High-risk ZIP codes are determined based on analysis of millions of e-commerce transactions. The specified action is taken whenever a submitted ZIP code appears in the 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.

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 *Fraud 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. 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 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.

Email 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.

NOTE: 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 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.

Every effort has been made 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.

IMPORTANT: *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 managed by PayPal, 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 email 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.

NOTE: 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 email 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 the 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.

TABLE B.4 AVS filter results

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 PayPal 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 email addresses and good card numbers. Be sure to type the e-mail addresses and credit card numbers accurately.

IMPORTANT: *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 want 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 Card Security Code 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 PayPal Manager online help for details on creating a custom filter.

C

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.

In This Appendix

- “Good and Bad Lists” on page 69
- “AVS Failure Filter” on page 70
- “BIN Risk List Match Filter” on page 70
- “Country Risk List Match Filter” on page 65
- “Email Service Provider Risk List Match Filter” on page 72
- “Freight Forwarder Risk List Match Filter” on page 72
- “Geo-location Failure Filter” on page 73
- “International AVS Filter” on page 73
- “International IP Address Filter” on page 74
- “International Shipping/Billing Address Filter” on page 75
- “IP Address Match Filter” on page 76
- “Shipping/Billing Mismatch Filter” on page 76
- “Total Item Ceiling Filter” on page 77
- “Total Purchase Price Ceiling Filter” on page 77
- “Total Purchase Price Floor Filter” on page 78
- “USPS Address Validation Failure Filter” on page 78
- “ZIP Risk List Match Filter” on page 79

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

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[4]=1.02&BILLTOPHONE2=650-555-0123&BROWSECOUNTRYCODE=203&BROWSETIME[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=PayPal&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"
```

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

```
"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=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=PayPal&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"
```

Expected Response Message

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

Country Risk List Match Filter

Pass in the specified country or country code.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=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&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=PayPal&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 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"
```

Expected Response Message

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

Email Service Provider Risk List Match Filter

Pass in the specified e-mail address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=203&BROWSERTIME[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&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=PayPal&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No City&SHIPTOEMAIL[18]=fraud@asiamail.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=60649&SS=565796510&STATE=CA&STREET=123 Main St.&BILLTOSTREET2=123 SHIPTOSTREET 2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskEmailCheckReject&VENDOR=TESTHighRiskEmailCheckReject&ZIP=60649"
```

Expected Response Message

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

Freight Forwarder Risk List Match Filter

Pass in the specified shipping address.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[5]=$1000&BILLTOPHONE2=650-555-0123&BROWSECOUNTRYCODE=203&BROWSERTIME[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=PayPal&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&SHIPTOSTATE=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"
```


Expected Response Message

```
resp msg=RESULT=125&PNREF=VB0A25087954&RESPMSG=Declined by Fraud
Service&PREFPMSG=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.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BILLTOPHONE2=650-555-
0123&BROWSECOUNTRYCODE=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&LAS
TNAME=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=PayPal&PHONENUM=650-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=Mountain
View&COUNTRYCODE=US&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAM
E&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=TESTGeoLocationCheckRej
ect&ZIP=95008"
```

Expected Response Message

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

International AVS Filter

Pass in the specified ZIP codes and billing address.

Testing the Transaction Security Filters

International IP Address Filter

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=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&FRE
IGHTAMT=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=PayPal&PHONENUM=650-
555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=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=TESTInternationalAVSRej
ect&ZIP=00101"
```

Expected Response Message

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

International IP Address Filter

Pass in the specified IP address.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=203&BROWSETIME[22]=July 11, 2002
12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=Campbell&COMMENT1=Automated testing
from
AdminTester&COUNTRY=US&COUNTRYCODE=US&CUSTIP=194.213.32.220&CUSTREF=CUSTREF&DESC=DESC
&DL=CA111111&DOB=CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=1209&FIRSTNAME=John&FR
EIGHTAMT=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=PayPal&PHONENUM=650
-555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=Mountain
View&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=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=TESTNonUSIPAddressReject&VENDOR=TESTNonUSIPAddressReject&
ZIP=95008"
```

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.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=203&BROWSETIME[2]  
2]=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&CUSTREF=CUSTREF&DESC=DESC&  
DL=CA111111&DOB=CA123456&EMAIL[20]=admin@merchant.com&EXPDATE=1209&FIRSTNAME=John&FRE  
IGHTAMT=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=PayPal&PHONENUM=650-  
555-  
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT  
Y=No  
City&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM  
E=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=TESTInternationalOrderReject&VENDOR=TESTInternationalOrde  
rReject&ZIP=11111"
```

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

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[6]=$75.00&BILLTOPHONE2=650-555-1234&BILLTOSTREET2=&BROWSECOUNTRYCODE=203&BROWSERTIME[22]=July 11, 2002 12:12:12&BROWSERUSERAGENT=BROWSERUSERAGENT&CITY=No City&COMMENT1=Test to trigger rules&COUNTRY=US&CUSTIP=172.131.193.25&CUSTREF=CUSTREF&DESC=DESC&DL=CA111111&DOB=CA123456&EMAIL[21]=lastName@paypal.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=PayPal&PHONENUM=650-555-1234&PONUM=PONUM&PWD=password1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=No City&COUNTRYCODE=US&SHIPTOEMAIL[17]=test@paypal.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"
```

Shipping/Billing Mismatch Filter

Pass in the specified shipping and billing addresses.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[4]=1000&BROWSECOUNTRYCODE=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&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=PayPal&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=SHIPTOCITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=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=TESTBillShipMismatchReject&ZIP=11111"
```

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.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[4]=1000&BROWSECOUNTRYCODE=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&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=6&L_SKU0=L_SKU0&L_TYPE0=L_TYPE0&L_UPC0=L_UPC0&MIDDLENAME=Z&ORDERTIMEZONE=1&PARTNER=PayPal&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=SHIPTOCITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123 SHIPTOSTREET2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main St.&TAXAMT=1.01&TENDER=C&USER=TESTHighOrderNumberReject&VENDOR=TESTHighOrderNumberReject&ZIP=11111"
```

Expected Response Message

```
resp msg=RESULT=125&PNREF=VB0A25030952&RESPMSG=Declined by Fraud
Service&PREFPMSG=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.

```
"TRXTYPE=A&ACCT=3528000000000015&AMT[7]=1000.01&BROWSECOUNTRYCODE=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&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=PayPal&PHONENUM=650-555-0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCITY=SHIPTOCITY&SHIPTOEMAIL[20]=admin@merchant.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAME=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=CA&SHIPTOSTREET=SHIPTOSTREET&SHIPTOSTREET2=123 SHIPTOSTREET2&SHIPTOZIP=11111&SS=565796510&STATE=CA&STREET=123 Main St.&TAXAMT=1.01&TENDER=C&USER=TESTCeilingAmountReject&VENDOR=TESTCeilingAmountReject&ZIP=11111"
```

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

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=203&BROWSETIME[2
2]=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&CUSTREF=CUSTREF&DESC=DESC&D
L=CA111111&DOB=CA123456&EMAIL[18]=fraud@asiamail.com&EXPDATE=1209&FIRSTNAME=John&FREI
GHTAMT=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&PARTNER=PayPal&PHONENUM=650-
555-
0123&PONUM=PONUM&PWD=testing1&SHIPCARRIER=SHIPCARRIER&SHIPMETHOD=SHIPMETHOD&SHIPTOCIT
Y=No
City&SHIPTOEMAIL[18]=fraud@asiamail.com&SHIPTOFIRSTNAME=SHIPTOFIRSTNAME&SHIPTOLASTNAM
E=SHIPTOLASTNAME&SHIPTOMIDDLENAME=SHIPTOMIDDLENAME&SHIPTOPHONE=650-555-
0124&SHIPTOPHONE2=650-555-0125&SHIPTOSTATE=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&VENDOR=TESTBillUSPosta
lAddressCheckReject&ZIP=60649"
```

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.

```
"TRXTYPE=A&ACCT=5105105105105100&AMT[8]=$1000.00&BROWSECOUNTRYCODE=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&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=PayPal&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 SHIPTOSTREET 2&SHIPTOZIP=60649&SS=565796510&STATE=CA&STREET=123 Main St.&BILLTOSTREET2=123 SHIPTOSTREET
2&TAXAMT=1.01&TENDER=C&USER=TESTHighRiskZIPCheckReject&VENDOR=TESTHighRiskZIPCheckReject&ZIP=60649"
```

Expected Response Message

```
resp msg=RESULT=125&PNREF=VB0A25031523&RESEMSG=Declined by Fraud
Service&PREFPMSG=Reject HighRiskZIPCheck
!!ERROR 13:55:6 result=125 TRXTYPE=A!!
```


D

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 Customer Service to request deactivation.

PayPal deactivates the service. Any remaining transactions settle normally.

Index

A

- Accepted transactions 18
- Account Number Velocity Filter 60
- Active mode 13
- APIs
 - documentation 23
 - downloading 23
- AVS Failure Filter 57
- AVSADDR 40
- AVSZIP 40

B

- BIN Risk List Match Filter 60

C

- Card Security Code Failure Filter 58
- communications errors 47
- configuring filters 12
- credit card fraud 11

D

- deactivation 81
- deploying filters 15
- documentation
 - API 23
- downloading APIs 23

E

- E-mail Service Provider Risk List Match Filter 62
- enrollment requirements 9

F

- Filter Scorecard 20
- filter types
 - High-risk Address 60
 - High-risk Payment 57
 - Unusual Order 55

filters

- Account Number Velocity 60
- AVS Failure 57
- BIN Risk List Match 60
- Card Security Code Failure 58
- configuring 12
- defined 11
- E-mail Service Provider Risk List Match 62
- examples 12
- Freight Forwarder Risk List Match 61
- Geo-location Failure 63
- IP Address Match 62
- IP Address Velocity 64
- parameters 26
- Product Watch List 56
- required transaction data 23
- response string 28
- Shipping/Billing Mismatch Filter 56
- testing 69
- Total Item Ceiling 55
- Total Purchase Price Ceiling 55
- USPS Address Validation Failure 61
- ZIP Risk List Match 61
- Freight Forwarder Risk List Match Filter 61

G

- Geo-location Failure Filter 63

H

- hacking 11
- High-risk Address Filters 60
- High-risk Payment Filters 57

I

- instant fulfillment 12
- IP Address Match Filter 62
- IP Address Velocity Filter 64

K

knowledgebase URL 8

L

logging transaction information 36

O

Observe mode 13, 14

P

Payflow parameters

 RESULT 47

PNREF 39

 format of value 41

PNREF value 40

Product Watch List Filter 56

R

recurring transactions 12

rejected transactions 18

rejecting transactions 20

RESPMSG 40

RESPMSG value 41

responses 28

 credit card transaction 39

RESULT 39

RESULT value 41

RESULT values

 communication errors 47

Reviewed transactions 18

reviewing transactions 18

risk lists 54

S

Shipping/Billing Mismatch Filter 56

T

Test phase 13

testing 14

 filters 69

Total Item Ceiling Filter 55

Total Purchase Price Ceiling Filter 55

transaction response

 PNREF parameter 40

 RESPMSG parameter 41

 RESULT parameter 41

transaction status values 19

transactions

 logging 36

 rejecting 20

U

Unusual Order Filters 55

USPS Address Validation Failure Filter 61

V

VERBOSITY parameter 28

Z

ZIP Risk List Match Filter 61