Fraud Management Filters

For Professional Use Only
Currently only available in English.

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

Last updated: June 23, 2009

Fraud Management Filters

Document Number: 10060.en_US-200906

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

This document describes Fraud Management Filters.

Intended Audience

This document is intended for merchants implementing the PayPal Fraud Management Filters.

Revision History

Revision history for *Fraud Management Filters*.

TABLE P.1 Revision History

Date	Description
06/23/09	Updated to note that configuration of Fraud Management Filters is required before they take effect.
01/31/09	Updated to show correct filters and include IPN and API programming examples. This manual is for Canada, UK, and US.
09/30/08	Updated to show new free filters.
04/18/08	Second draft.
12/20/07	First draft.

1 Introducing Fraud Management Filters

PayPal Fraud Management Filters enable you to identify potentially fraudulent transactions. You must configure Fraud Management Filters to meet your needs; they are not active until you configure them.

- Fraud Management Filters Overview
- Fraud Management Filters Examples
- Merchants With Third-Party Shopping Carts

Fraud Management Filters Overview

PayPal provides many Fraud Management Filters, which make it easier for you to detect and respond to fraudulent transactions. You must configure the filters before they take effect.

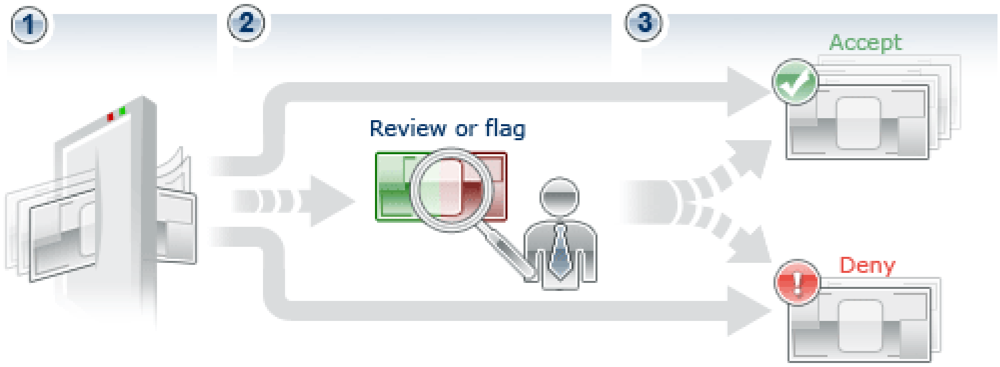
Fraud management filters (FMF) provide you with tools, called filters, that can identify potentially fraudulent transactions. The kinds of filters can be divided into the following categories:

- Basic filters include filters that screen against the country of origin, the value of transactions, and such. PayPal provides basic filters for business accounts and Website Payments Pro accounts.
- Advanced filters include filters that screen credit card and addresses information, filters that screen against lists of high-risk indicators, and filters that screen additional transaction characteristics. Website Payments Pro merchants can upgrade to use advanced filters.

  NOTE: Using advanced filters may incur additional charges.

Fraud Management Filters checks for payment characteristics that may indicate fraudulent activity. You set up Fraud Management Filters to provide the tightest control possible over payments so that you can deny payments that are likely to result in fraudulent transactions and accept payments that are not typically a problem. Payments that may require further investigation or intervention, such as comparing prior orders or contacting the customer for more information, can be flagged or put on hold or pended for review.

The following diagram, conceptually shows how Fraud Management Filters work in three steps:



1. Configure your Fraud Management Filters to flag, hold for review, or deny riskier payments.
2. Based on your settings, your filters review incoming payments.
3. Your filters automatically, flag, deny, or hold payments for review; typically, most payments are accepted because they do not show characteristics indicating fraud

A flexible fraud management configuration enables you to select the filters to use and to test your strategy before denying payments or pending transactions for review. Advantages of using Fraud Management Filters include

- time savings from having the computer do more to review transactions, and review them consistently, which allows you to focus on transactions that are truly risky
- cost savings from identifying potentially risky transactions, which reduces chargebacks and lowers your cost of doing business
- more accepted payments because you apply rules evenly with greater accuracy

Fraud Management Filters Examples

These examples show ways to configure Fraud Management Filters to flag or review transactions and accept or deny payments. You must configure your filters before they take effect.

Consider an example using four of the many kinds of filters provided by PayPal:

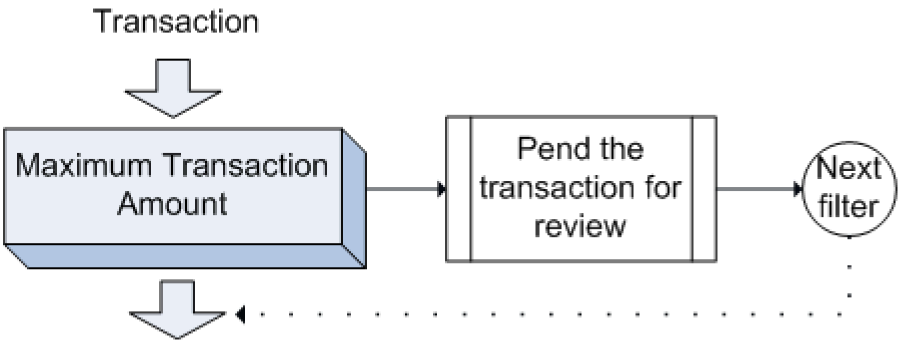
- Maximum Transaction Amount filter, which identifies transactions whose value exceeds a specified amount
- Country Monitor filter, which identifies transactions based on the country of origin
- Card Security Code Mismatch filter, which identifies transactions with differences in the credit card security code
- Total Purchase Price Minimum filter, which identifies transactions that are less than a specified amount

The Maximum Transaction Amount filter and the Country Monitor filters are examples of basic filters, which are available to business account holders and Website Payments Pro merchants. The Total Purchase Price Minimum filter and Card Security Code Mismatch filter are examples of advanced filters, which are available to Website Payments Pro merchants at additional cost.

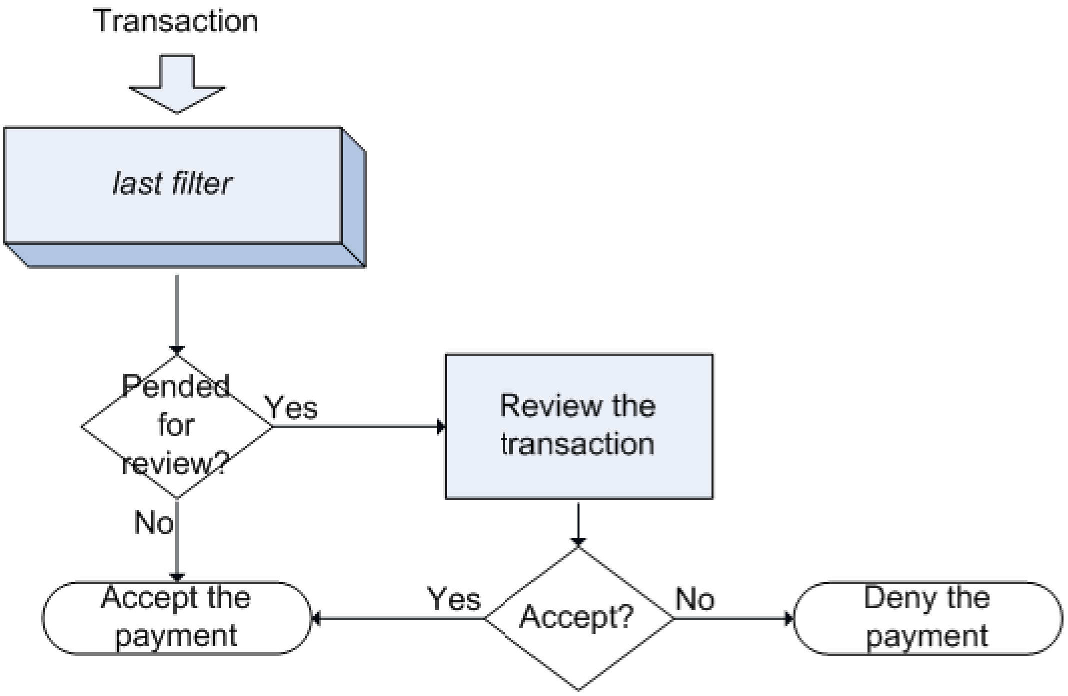
Reviewing High-Value Transactions

In this example, consider a scenario in which your average transaction amount is $100 and you seldom expect orders over $1,000. Although you have received large orders before, you want to verify for yourself that the order is legitimate and not an attempt to defraud you of merchandise. In this case, you could set the Maximum Transaction Amount filter to **Review** for transactions over $1,000.

The following diagram shows the effect of pending a transaction:



A transaction is pended when the maximum transaction amount specified by the filter is exceeded, which in this example is $1,000, meaning that these transactions await a decision whether to accept or deny the payment. Other filters execute because the payment has neither been accepted or denied. When there are no more filters to execute and another filter has not caused the payment to be denied or approved, a pended transaction is ready to be reviewed. The following diagram shows this logic:

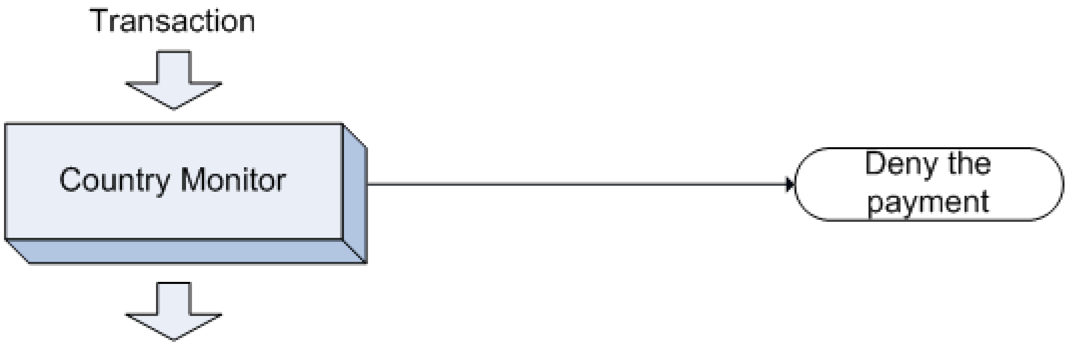


You can review a transaction and accept or deny a payment

- from the PayPal website. You examine the transaction details.
- from your website or application, by using the `ManagePendingTransactionStatus` API operation; for more information, see the *Name-Value Pair API Developer Guide and Reference* or *SOAP API Developer Reference*.
- from your shopping cart vendor, if they provide this feature for you.

Denying Transactions From High-Risk Countries

In this example, consider a scenario in which your experience indicates that transactions originating from some countries have always been attempts to defraud. You can set the Country Monitor filter to deny payments from these countries, as shown in the following diagram:

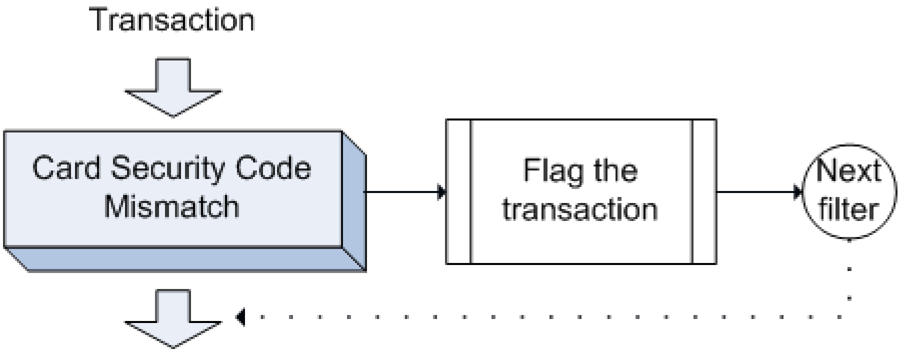


Filtering stops if the payment is denied. If the transaction originates from a country not on the list, filtering continues.

Flagging Transactions With Invalid Card Security Codes

In this example, consider a scenario in which your experience indicates that customers routinely mistype their credit card security code; however, in some cases, it is not an honest mistake and can indicate fraud. Before you decide to review or deny this kind of payment, you may decide to flag them first. After reviewing the flagged transactions, you can decide if further action is necessary.

In this case, you could set the Card Security Code Mismatch filter to **Flag**, which would flag the transaction:



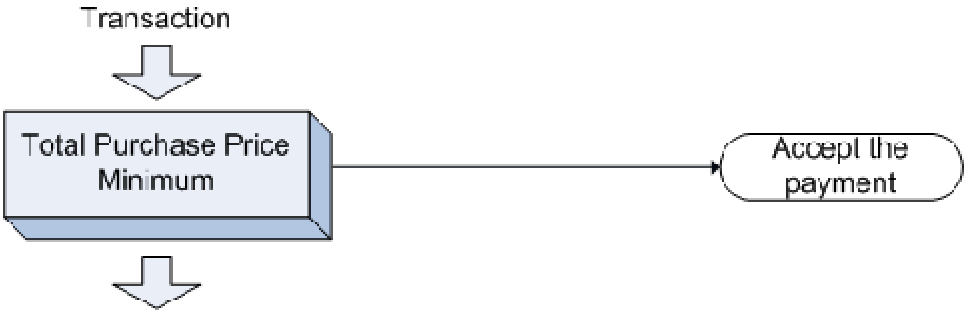
Regardless of whether the transaction has been flagged, the next enabled filter is applied. Flagging a transaction does not approve or deny a payment or pend the transaction for review.

Accepting Transactions Using the Total Price Minimum Filter

For the purpose of thinking about the operation of filters, the Total Price Minimum filter determines the universe of payments on which the other filters operate. If the Total Price Minimum filter is not enabled, the Fraud Management Filters universe includes all payments; otherwise, the Fraud Management Filters universe includes all payments above the amount specified by this filter.

NOTE: This filter is also the only filter that uses **Accept** to indicate that the filter does not deny payments less than the specified amount.

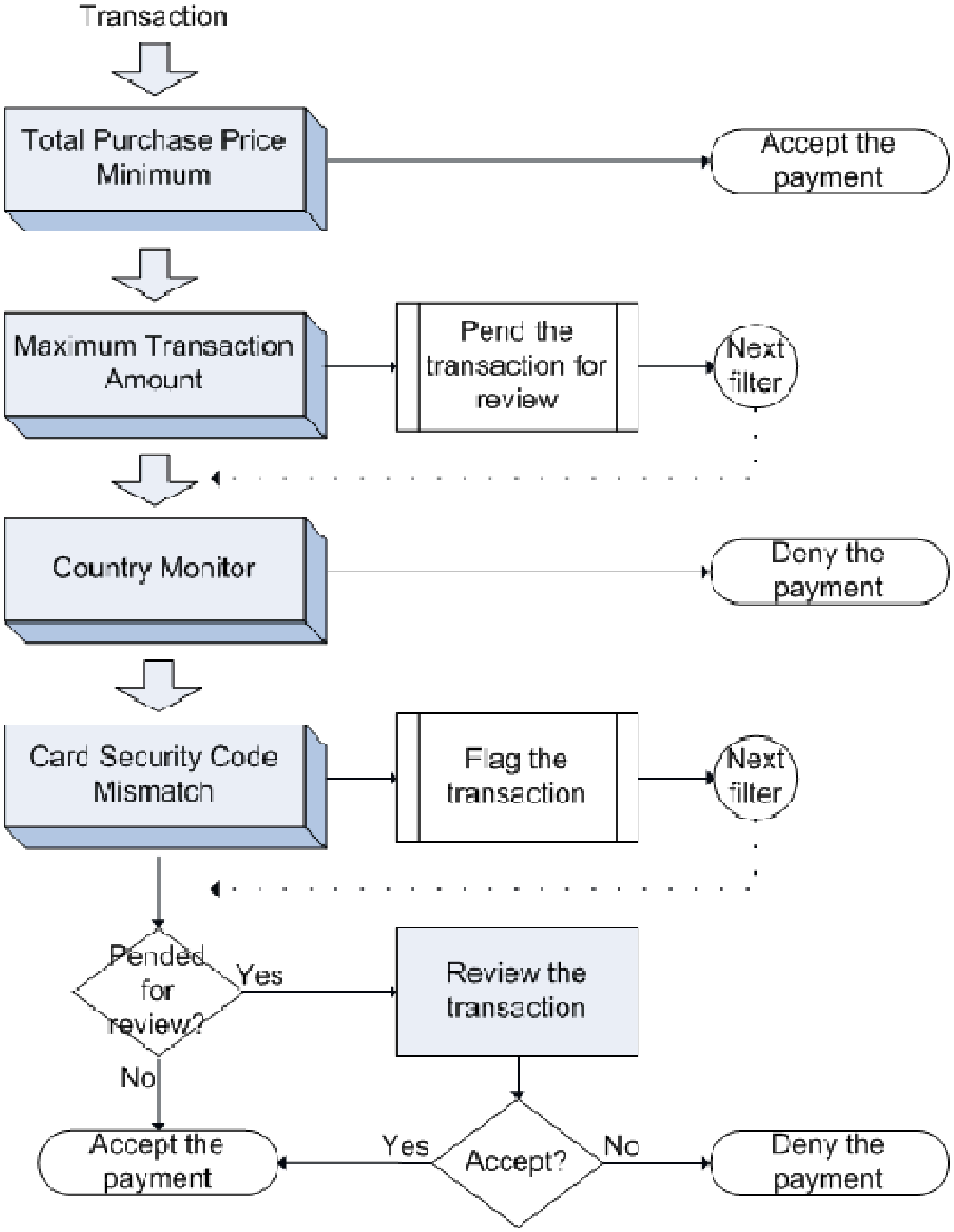
Consider the following example in which the Total Price Minimum filter is set to **Accept** for $10, In this case a $10 payment will be accepted and other filters will not be executed. If the payment was for $11, other filters execute.



Using Multiple Filters

If you enable more than one filter, the filters are applied in the order determined by the kind of payment method until one of them causes the payment to be accepted or denied. If all filters have been applied and the transaction has not been pended for review, it is automatically accepted. For information about the order in which filters are applied, see Fraud Management Filters Operating Principles.

Consider the four filters in the following diagram, which are shown in the order used for Direct Credit Card and Virtual Terminal payments.



1. If the total amount of the transaction is less than the amount specified by the Total Purchase Price Minimum filter, the payment is accepted and processing stops; otherwise, the next filter is applied.

2. If the total amount of the transaction is greater than the amount specified by the Maximum Transaction Amount filter, the transaction is pended awaiting review; regardless of whether the transaction is pended, the next filter is applied.
3. If the transaction's country of origin matches a country specified by the Country Monitor filter, the payment is denied and processing stops; otherwise, the next filter is applied.
4. If the customer's credit card security code does not match a valid code, the Card Security Code Mismatch filter flags the transaction and processing continues; the next filter is applied.
5. When there are no more filters to apply and the transaction has not been pended, the payment is accepted; otherwise, you must decide whether to accept or deny the payment.

Modifying the Examples to Meet Your Needs

These examples use specific filters, which are set to take specific actions. Your needs dictate how you use these and other filters to reduce risk to a manageable level without significantly increasing the effort required to process an order.

You need not use the same filters shown in the examples and you can take different actions if you do use them. The following items are just some of the alternatives for you to consider:

- You may decide not to use the Total Purchase Price Minimum filter or use it with a lower transaction value.
- You may decide to pend transactions from high-risk countries rather than deny their payments.
- You may decide to flag high-value transactions rather than pend them for review.

Setting up Fraud Management Filters requires both experimentation and iteration.

Merchants With Third-Party Shopping Carts

Merchants that use a shopping cart provider, should consult with their vendor about their level of support for Fraud Management Filters.

You can use Fraud Management Filters with a third-party shopping cart. You should check with your vendor about their level of support for Fraud Management Filters because the business procedures you use to review transactions may be different depending on your shopping cart's level of support.

For example, your cart vendor may support all features of Fraud Management Filters, in which case, you would review and accept or deny payments from their service. If your cart vendor does not provide any additional support for Fraud Management Filters, you will need to log onto PayPal to review and accept or deny payments or provide your own solution using the PayPal API to develop a custom application.

2 Setting Up Fraud Management Filters

You must set up Fraud Management Filters after you sign up for them.

- Configuring Your Fraud Management Filters
- Fraud Management Filter Settings
- Fraud Management Filters Setup Strategy

Configuring Your Fraud Management Filters

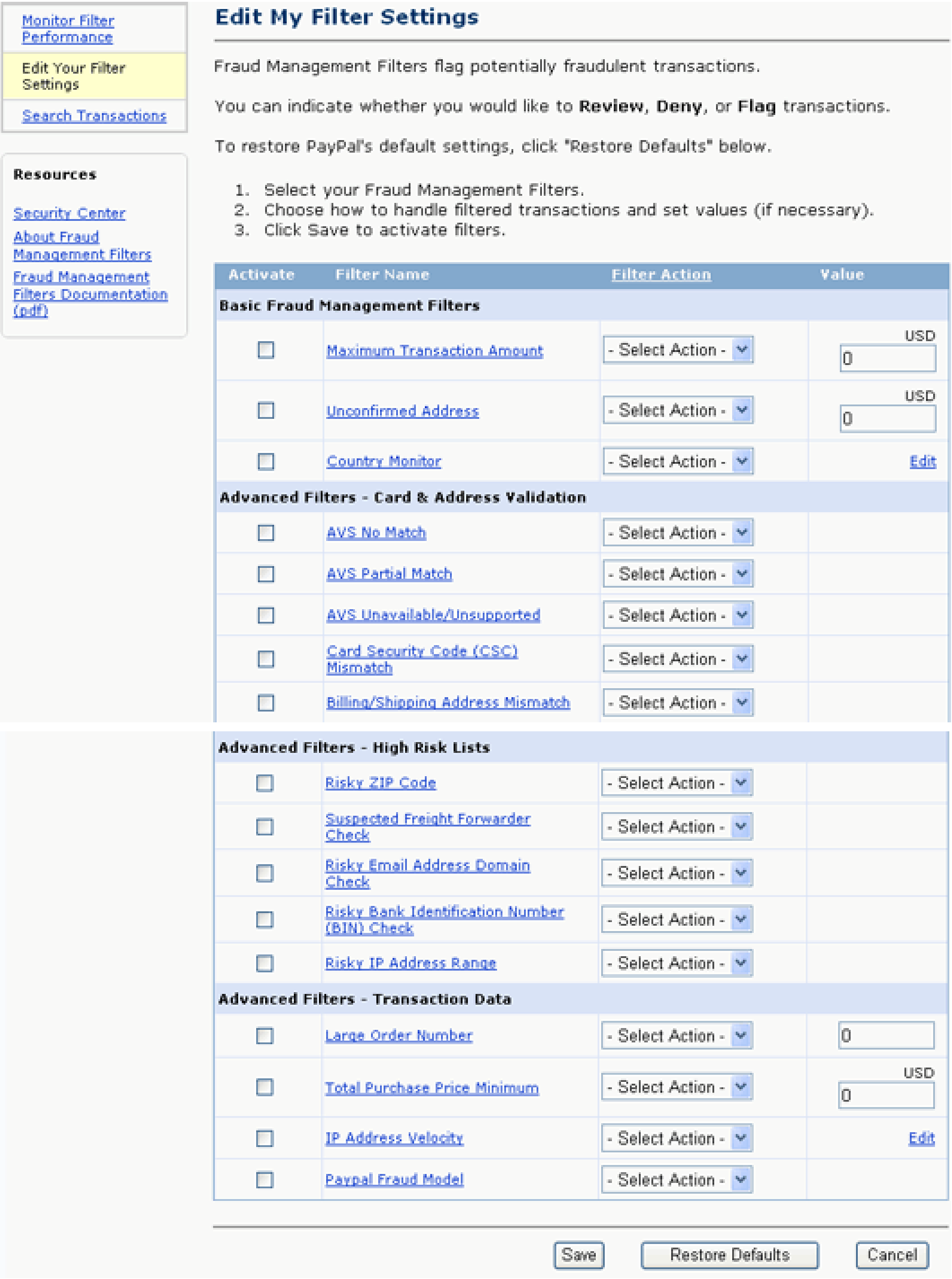
Configuring Fraud Management Filters to enable filters that are predictive of fraud requires both experimentation and iteration. By default, Fraud Management filters are not configured to identify potentially fraudulent transactions.

IMPORTANT: By default, Fraud Management Filters are not configured. You must configure your filters before they take effect.

You configure PayPal Fraud Management Filters to accept as many payments as possible automatically, deny payments that are clearly associated with fraud, and review the payments that are outside your normal experience but may or may not indicate an attempt to defraud.

When you first start, you should consider using filters only to flag payments; in which case, the payment is accepted but you can easily locate and view the payment later. If you notice that a filter configuration is predictive of fraud, you can either change the filter configuration to review the payment or to deny the payment. If you choose to review the payment, you may want to incorporate the review into your normal workflow. If a filter is not predictive of fraud, you can deselect the filter.

To configure Fraud Management Filters, select **Fraud Management Filters** from your Profile. Then enable the filters you want to use from the Edit My Filter Settings page:



Monitor Filter Performance

Edit Your Filter Settings

Search Transactions

Resources

Security Center

About Fraud Management Filters

Fraud Management Filters Documentation (pdf)

Edit My Filter Settings

Fraud Management Filters flag potentially fraudulent transactions.

You can indicate whether you would like to **Review**, **Deny**, or **Flag** transactions.

To restore PayPal's default settings, click "Restore Defaults" below.

1. Select your Fraud Management Filters.
2. Choose how to handle filtered transactions and set values (if necessary).
3. Click Save to activate filters.

Activate	Filter Name	Filter Action	Value
Basic Fraud Management Filters			
□	Maximum Transaction Amount	- Select Action -	USD 0
□	Unconfirmed Address	- Select Action -	USD 0
□	Country Monitor	- Select Action -	Edit
Advanced Filters - Card & Address Validation			
□	AVS No Match	- Select Action -	
□	AVS Partial Match	- Select Action -	
□	AVS Unavailable/Unsupported	- Select Action -	
□	Card Security Code (CSC) Mismatch	- Select Action -	
□	Billing/Shipping Address Mismatch	- Select Action -	
Advanced Filters - High Risk Lists			
□	Risky ZIP Code	- Select Action -	
□	Suspected Freight Forwarder Check	- Select Action -	
□	Risky Email Address Domain Check	- Select Action -	
□	Risky Bank Identification Number (BIN) Check	- Select Action -	
□	Risky IP Address Range	- Select Action -	
Advanced Filters - Transaction Data			
□	Large Order Number	- Select Action -	0
□	Total Purchase Price Minimum	- Select Action -	USD 0
□	IP Address Velocity	- Select Action -	Edit
□	Paypal Fraud Model	- Select Action -	

NOTE: The available filters are determined by agreement between the merchant and PayPal. You may not be granted access to all filters.

Fraud Management Filter Settings

You can configure Fraud Management Filters to accept or deny a payment and to review or flag a transaction.

Setting	Description
Accept	Accept the payment. This setting is only used by the Total Price Minimum filter, which causes PayPal to accept transactions that fall below a minimum transaction amount, regardless of the setting of any other filter.
Deny	Deny the payment. You should only use this setting if you are certain you want the filter to disqualify the payment. For example, you might deny payments from countries for which it is too difficult to conduct business.
Review	Pend the payment for your review. Use this setting when you want to evaluate the transaction and make an explicit decision whether to accept or deny the payment.
Flag	Accept the payment and flag it for later examination. Use this setting for testing a filter or when you are not sure you want review the payment but want an easy way to locate the payment should you decide to look at it.

Fraud Management Filters Setup Strategy

You enable the Fraud Management Filters that your experience suggests will be most predictive of fraud. By default, Fraud Management Filters are not enabled.

Consider an example in which your experience indicates that orders whose total amount exceed a threshold amount are unusual. It may indicate that the buyer does not really care about the size of the order because the order is not actually legitimate; in this case, it could be an attempt to obtain merchandise by fraud.

Depending on how much you rely upon the belief that a specific transaction characteristics are indicitive of fraud, you specify one of the following actions on the Edit My Filters Settings page:

- Flag the transaction, in which case the transaction is accepted; however, you can conveniently view the transaction on PayPal later and, if you believe that the transaction might be fraudulent, you can reverse the payment and not ship the requested merchandise.
- Review the transaction if it exceeds the threshold amount, in which case the transaction is marked as pending. You explicitly accept or deny the payment before deciding whether to ship the requested merchandise. Specifying a review is similar to flagging the payment, except that you must make an explicit decision whether to accept or deny the payment; it is not automatically accepted.

- Deny the payment. This operation is automatic; however, because the action results in the loss of revenue if the payment is actually legitimate, you should choose this action only after careful consideration.

In the case of the size of the transaction, and with many other filters, can choose a threshold for which the specified action applies; for example, you can flag, review, or deny transactions over a specified amount.

You should set up your Fraud Management Filters so that most transactions pass through your filters and payments are accepted automatically. Your goal is to minimize the risk of a fraudulent transaction against the cost of denying a legitimate payment and to minimize the time required to review transactions.

To meet this goal, you typically experiment with the filters available to you and the actions to take. Before you set up a filter to deny payments or pend transactions for review, you can set the filter to flag the transaction, which allows you to identify the transactions before taking more severe actions. PayPal also provides you with feedback on the operation of each filter.

3 Using Fraud Management Filters

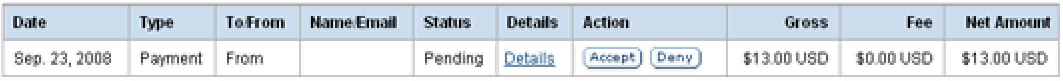
You can use PayPal to monitor transactions for fraud and determine the effectiveness of your Fraud Management Filters.

- Accepting and Denying Payments
- Monitoring Fraud Management Filters Performance
- Using Fraud Management Filters with Virtual Terminal
- Using Payment Fraud Search

Accepting and Denying Payments

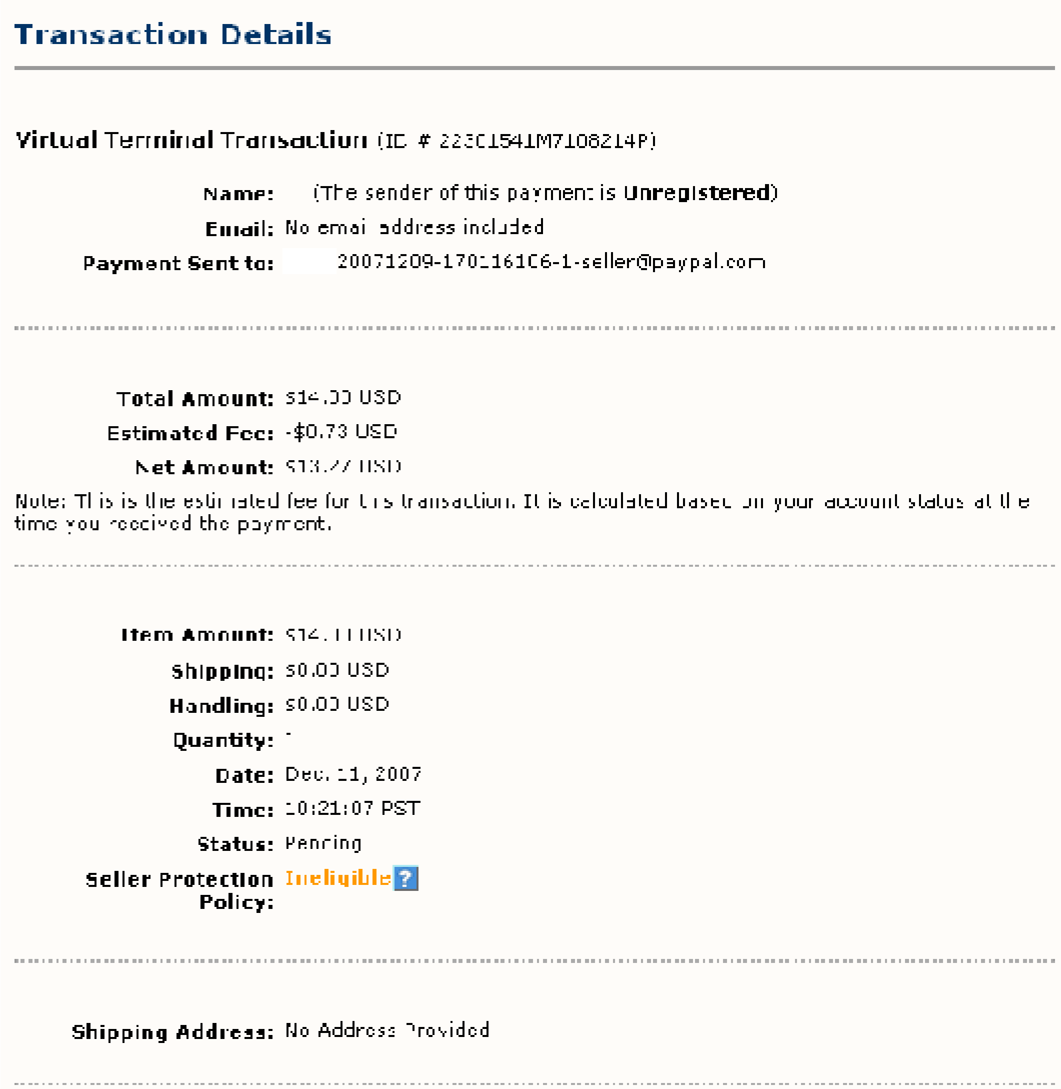
You can use the Fraud Management Filters-related features from the Transaction History page.

You can accept or deny a pending payment from the Transaction History page,:



Date	Type	To/From	Name/Email	Status	Details	Action	Gross	Fee	Net Amount
Sep. 23, 2008	Payment	From		Pending	Details	Accept Deny	$13.00 USD	$0.00 USD	$13.00 USD

You can also view the transaction details to help you make a decision about whether to accept or deny a payment as shown below. The reason that the transaction is pending, waiting for your review is explained at the bottom of this page:



Transaction Details

Virtual Terminal Transaction (ID # 223C1541M7108214P)

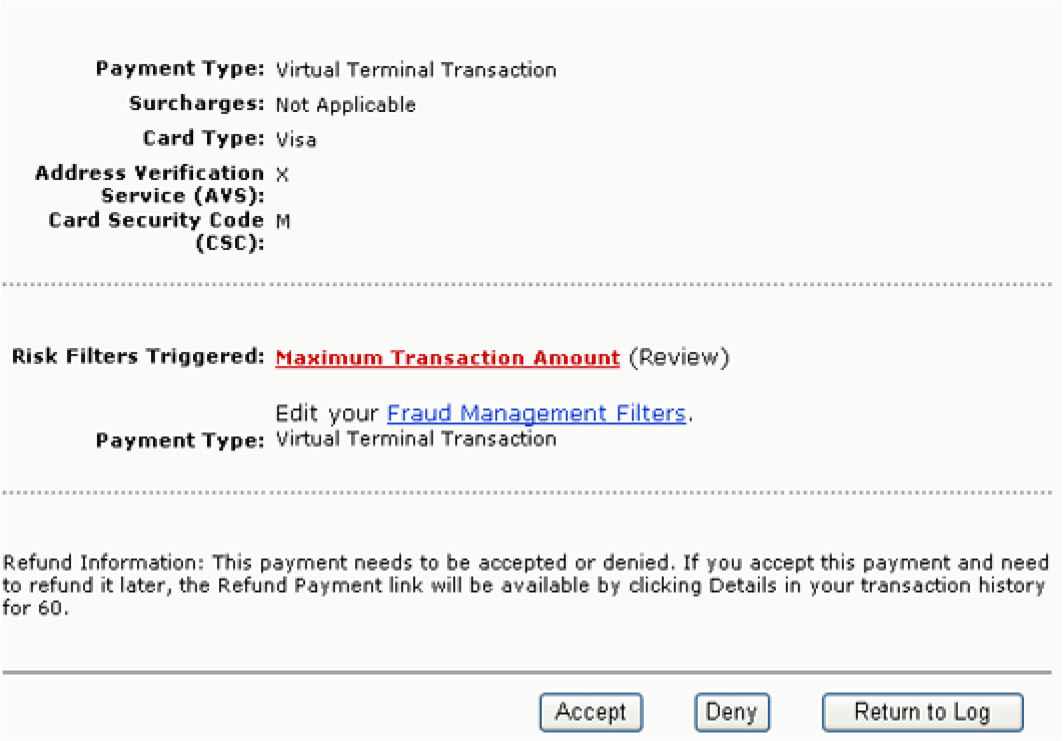
Name:	(The sender of this payment is **Unregistered**)
Email:	No email address included
Payment Sent to:	20071209-170116106-1-seller@paypal.com

Total Amount:	$14.00 USD
Estimated Fee:	-$0.73 USD
Net Amount:	$13.27 USD

Note: This is the estimated fee for this transaction. It is calculated based on your account status at the time you received the payment.

Item Amount:	$14.00 USD
Shipping:	$0.00 USD
Handling:	$0.00 USD
Quantity:	1
Date:	Dec. 11, 2007
Time:	10:21:07 PST
Status:	Pending
Seller Protection Policy:	Ineligible ?

Shipping Address:	No Address Provided



Payment Type:	Virtual Terminal Transaction
Surcharges:	Not Applicable
Card Type:	Visa
Address Verification Service (AVS):	X
Card Security Code (CSC):	M

Risk Filters Triggered: Maximum Transaction Amount (Review)

Edit your Fraud Management Filters.

Payment Type: Virtual Terminal Transaction

Refund Information: This payment needs to be accepted or denied. If you accept this payment and need to refund it later, the Refund Payment link will be available by clicking Details in your transaction history for 60.

Monitoring Fraud Management Filters Performance

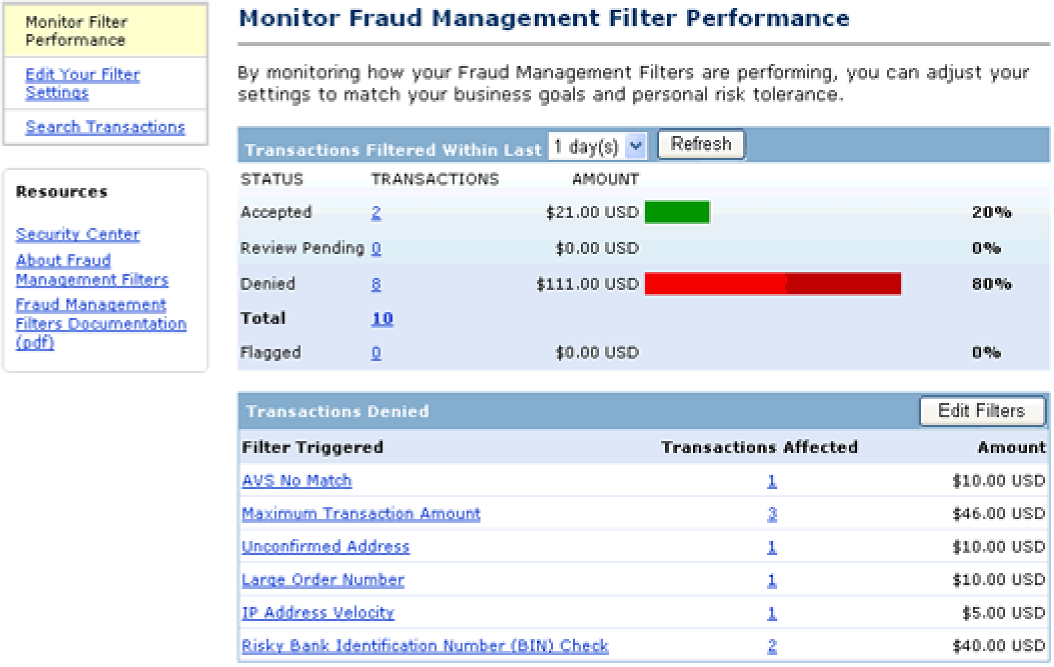
You can monitor the effect of choosing various Fraud Management Filters.

The Fraud Management Filters Performance Monitor enables you to graphically view the monetary effect of your filter settings. You can use the monitor to quickly review the effect of your filter settings and make decisions to balance risk and convenience.

The monitor presents three bars that shows activity for the time period that you specify:

- the monetary volume and percentage of payments accepted after Fraud Management Filters have been applied
- the monetary volume and percentage of payments that are pending review
- the monetary volume and percentage of payments denied after Fraud Management Filters have been applied

The Performance Monitor also shows the number and total monetary effect of the filters that have been triggered during the specified time period.



Monitor Filter Performance
Edit Your Filter Settings
Search Transactions

Resources

Security Center
About Fraud Management Filters
Fraud Management Filters Documentation (pdf)

Monitor Fraud Management Filter Performance

By monitoring how your Fraud Management Filters are performing, you can adjust your settings to match your business goals and personal risk tolerance.

Transactions Filtered Within Last 1 day(s) Refresh

STATUS	TRANSACTIONS	AMOUNT		
Accepted	2	$21.00 USD	🟩	20%
Review Pending	0	$0.00 USD		0%
Denied	8	$111.00 USD	🟥	80%
Total	**10**			
Flagged	0	$0.00 USD		0%

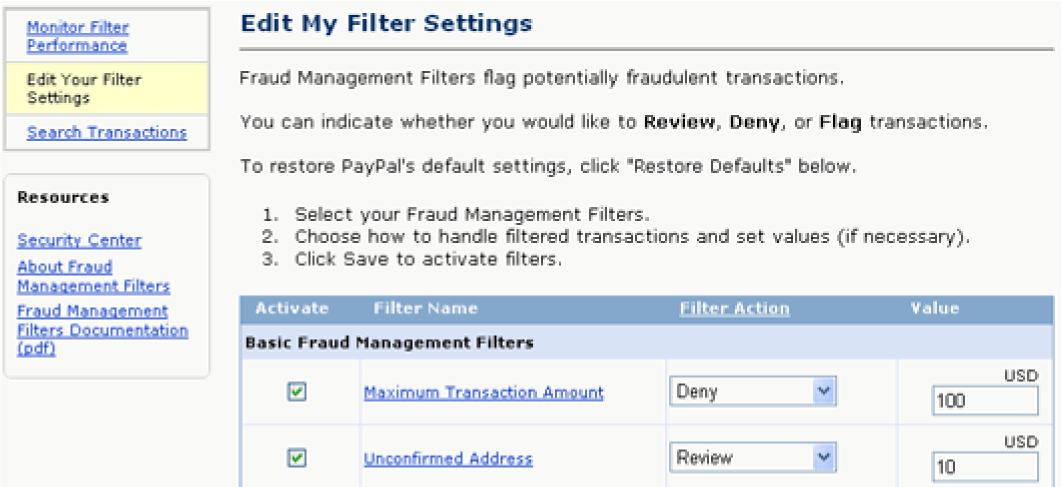
Transactions Denied — Edit Filters

Filter Triggered	Transactions Affected	Amount
AVS No Match	1	$10.00 USD
Maximum Transaction Amount	3	$46.00 USD
Unconfirmed Address	1	$10.00 USD
Large Order Number	1	$10.00 USD
IP Address Velocity	1	$5.00 USD
Risky Bank Identification Number (BIN) Check	2	$40.00 USD

Using Fraud Management Filters with Virtual Terminal

You can use Fraud Management Filters to manage risk while using Virtual Terminal.

Consider an example in which your Fraud Management Filter settings are set to deny payments over $100 and to review payments of $10 or more if the address has not been confirmed:



Monitor Filter Performance
Edit Your Filter Settings
Search Transactions

Resources

Security Center
About Fraud Management Filters
Fraud Management Filters Documentation (pdf)

Edit My Filter Settings

Fraud Management Filters flag potentially fraudulent transactions.

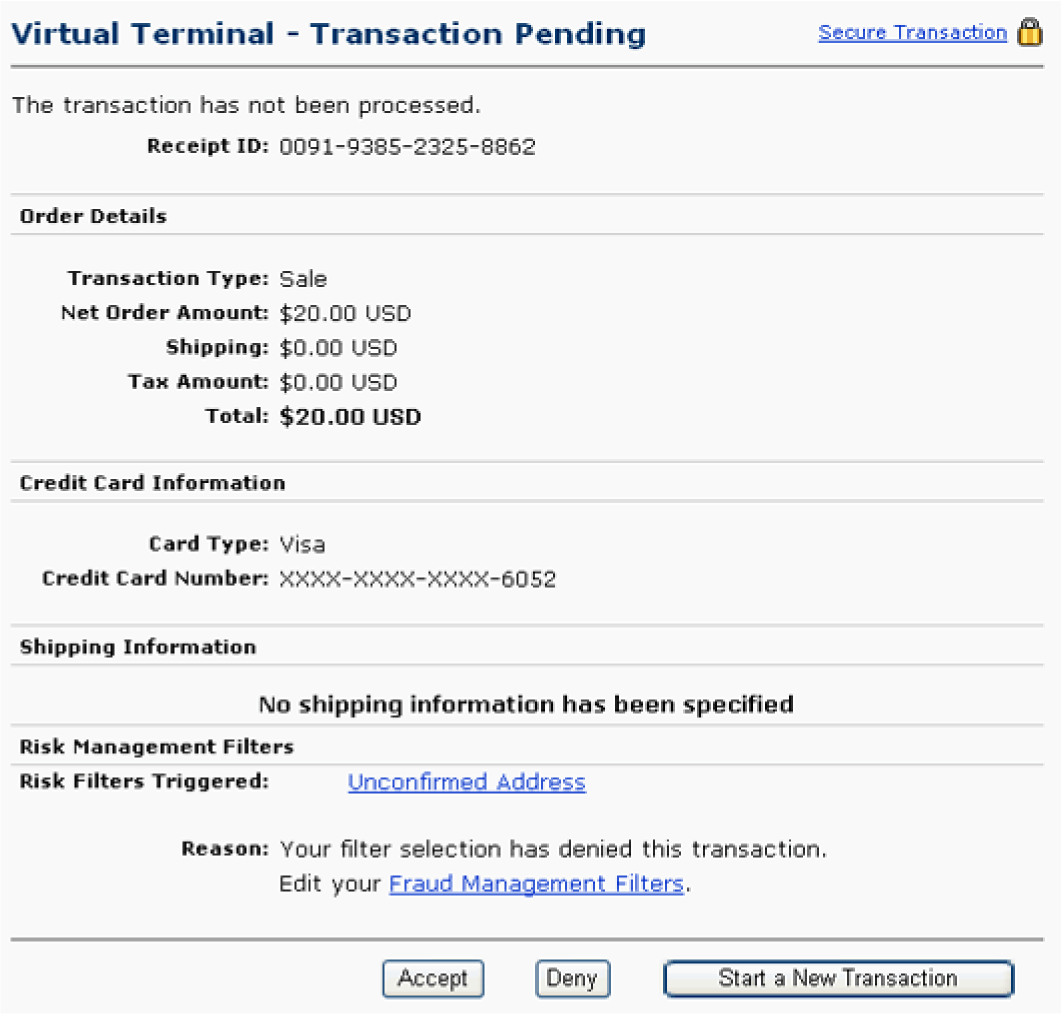
You can indicate whether you would like to **Review**, **Deny**, or **Flag** transactions.

To restore PayPal's default settings, click "Restore Defaults" below.

1. Select your Fraud Management Filters.
2. Choose how to handle filtered transactions and set values (if necessary).
3. Click Save to activate filters.

Activate	Filter Name	Filter Action	Value
Basic Fraud Management Filters			
☑	Maximum Transaction Amount	Deny	USD 100
☑	Unconfirmed Address	Review	USD 10

When you enter a transaction for $20 net using Virtual Terminal, the payment is pended and you are prompted to accept or deny the transaction:



Virtual Terminal - Transaction Pending

Secure Transaction

The transaction has not been processed.

Receipt ID: 0091-9385-2325-8862

Order Details

Transaction Type: Sale
Net Order Amount: $20.00 USD
Shipping: $0.00 USD
Tax Amount: $0.00 USD
Total: **$20.00 USD**

Credit Card Information

Card Type: Visa
Credit Card Number: XXXX-XXXX-XXXX-6052

Shipping Information

No shipping information has been specified

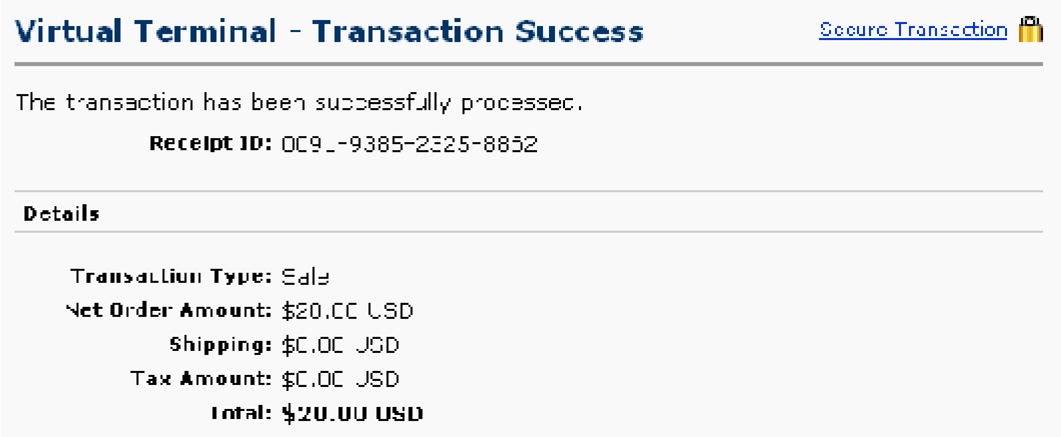
Risk Management Filters

Risk Filters Triggered: Unconfirmed Address

Reason: Your filter selection has denied this transaction.
Edit your Fraud Management Filters.

NOTE: You are not required to accept or deny the payment immediately. You can start a new transaction, in which case, you can view the transaction history or details and accept or deny the original payment later.

If you accept the payment, Virtual Terminal processes the transaction normally:



Virtual Terminal - Transaction Success

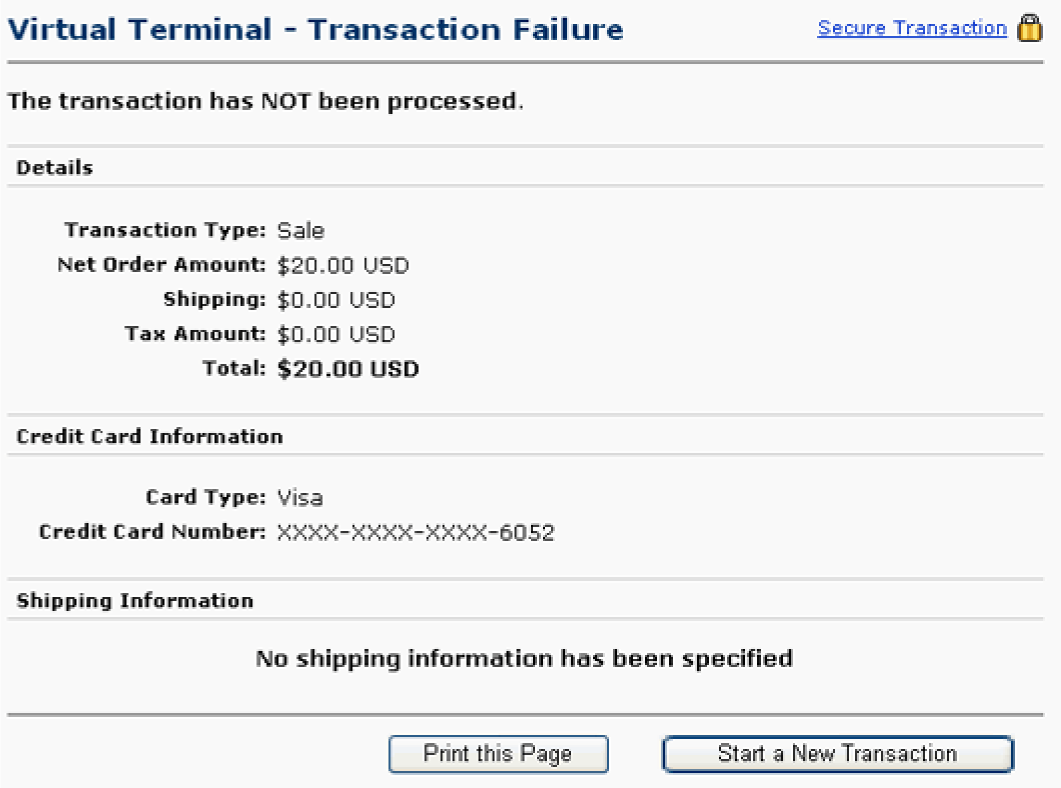
The transaction has been successfully processed.

Receipt ID: 0C9_-9385-2325-8852

Details

Transaction Type: Sale
Net Order Amount: $20.00 USD
Shipping: $0.00 USD
Tax Amount: $0.00 USD
Total: **$20.00 USD**

If you deny the payment, Virtual Terminal does not process the transaction.



Virtual Terminal - Transaction Failure

The transaction has NOT been processed.

Details

Transaction Type: Sale
Net Order Amount: $20.00 USD
Shipping: $0.00 USD
Tax Amount: $0.00 USD
Total: **$20.00 USD**

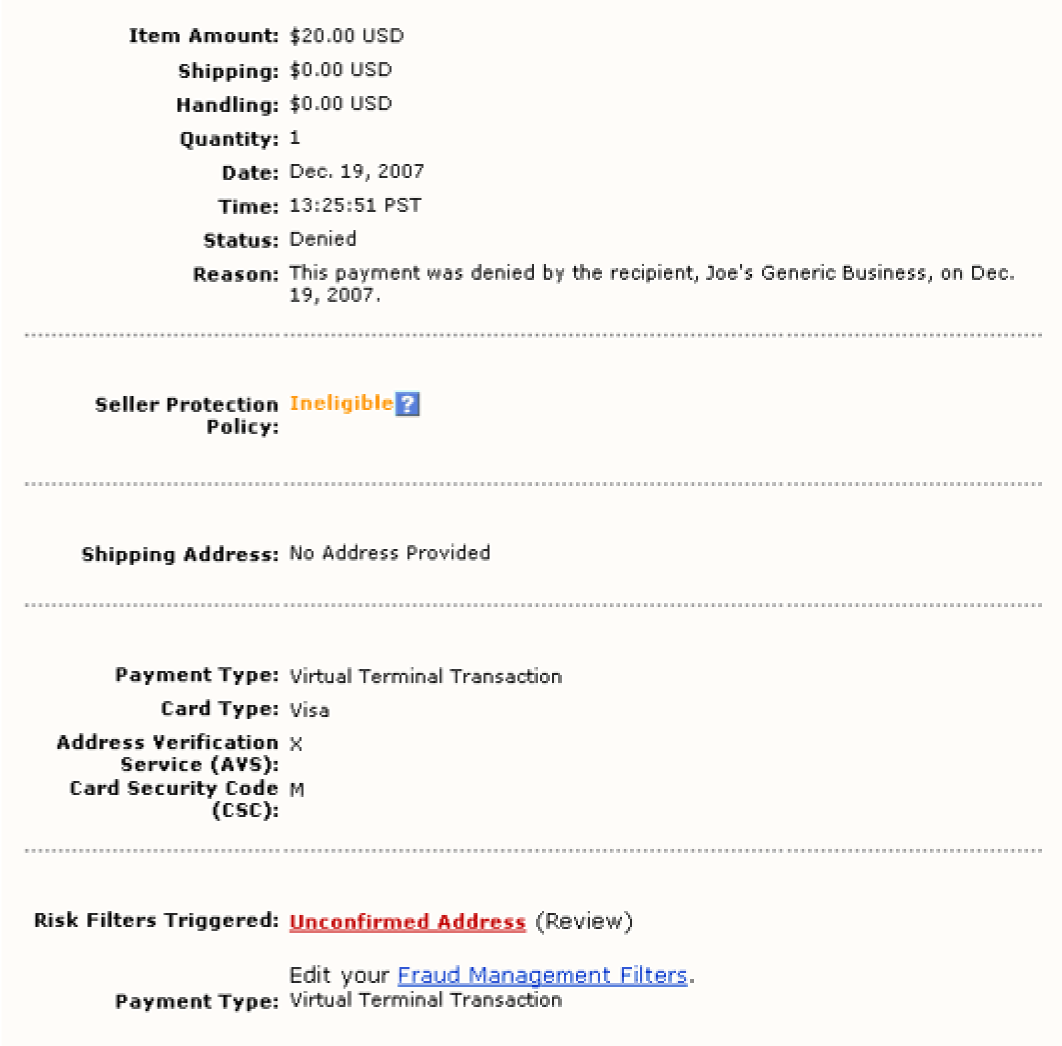
Credit Card Information

Card Type: Visa
Credit Card Number: XXXX-XXXX-XXXX-6052

Shipping Information

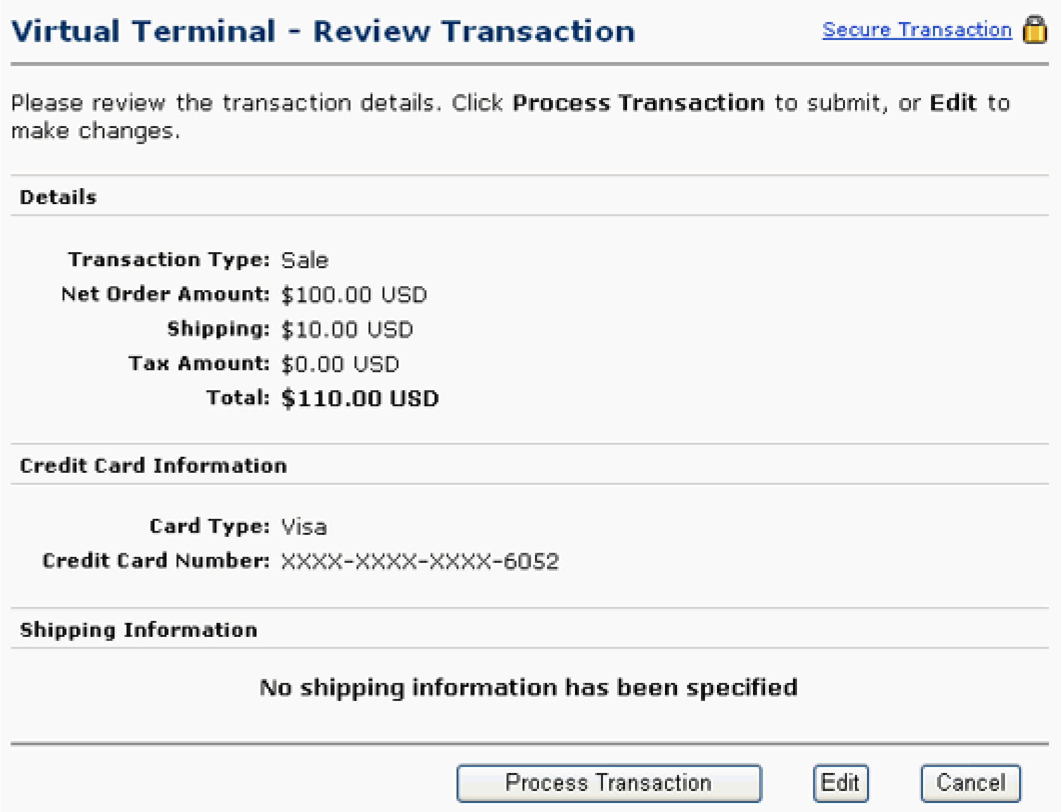
No shipping information has been specified

For more information, you can review the transaction details:



Item Amount:	$20.00 USD
Shipping:	$0.00 USD
Handling:	$0.00 USD
Quantity:	1
Date:	Dec. 19, 2007
Time:	13:25:51 PST
Status:	Denied
Reason:	This payment was denied by the recipient, Joe's Generic Business, on Dec. 19, 2007.
Seller Protection Policy:	Ineligible ?
Shipping Address:	No Address Provided
Payment Type:	Virtual Terminal Transaction
Card Type:	Visa
Address Verification Service (AVS):	X
Card Security Code (CSC):	M
Risk Filters Triggered:	Unconfirmed Address (Review) Edit your Fraud Management Filters.
Payment Type:	Virtual Terminal Transaction

Consider another Virtual Terminal transaction, this one in which the total payment amount is $110:



Virtual Terminal - Review Transaction

Please review the transaction details. Click **Process Transaction** to submit, or **Edit** to make changes.

Details

Transaction Type:	Sale
Net Order Amount:	$100.00 USD
Shipping:	$10.00 USD
Tax Amount:	$0.00 USD
Total:	**$110.00 USD**

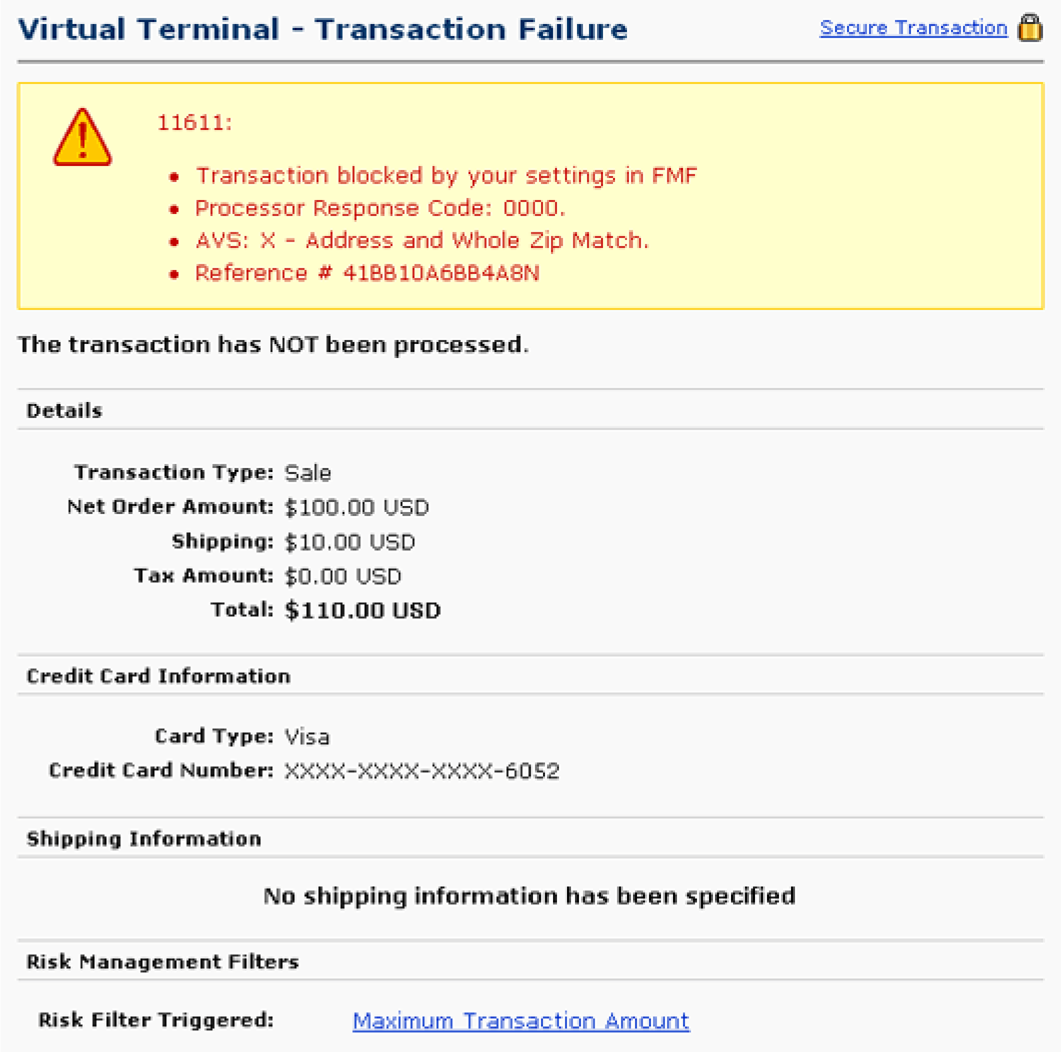
Credit Card Information

Card Type:	Visa
Credit Card Number:	XXXX-XXXX-XXXX-6052

Shipping Information

No shipping information has been specified

In this example, the maximum amount filter automatically denies the payment because it exceeds $100.



Virtual Terminal - Transaction Failure

11611:

- Transaction blocked by your settings in FMF
- Processor Response Code: 0000.
- AVS: X - Address and Whole Zip Match.
- Reference # 41BB10A6BB4A8N

The transaction has NOT been processed.

Details

Transaction Type:	Sale
Net Order Amount:	$100.00 USD
Shipping:	$10.00 USD
Tax Amount:	$0.00 USD
Total:	**$110.00 USD**

Credit Card Information

Card Type:	Visa
Credit Card Number:	XXXX-XXXX-XXXX-6052

Shipping Information

No shipping information has been specified

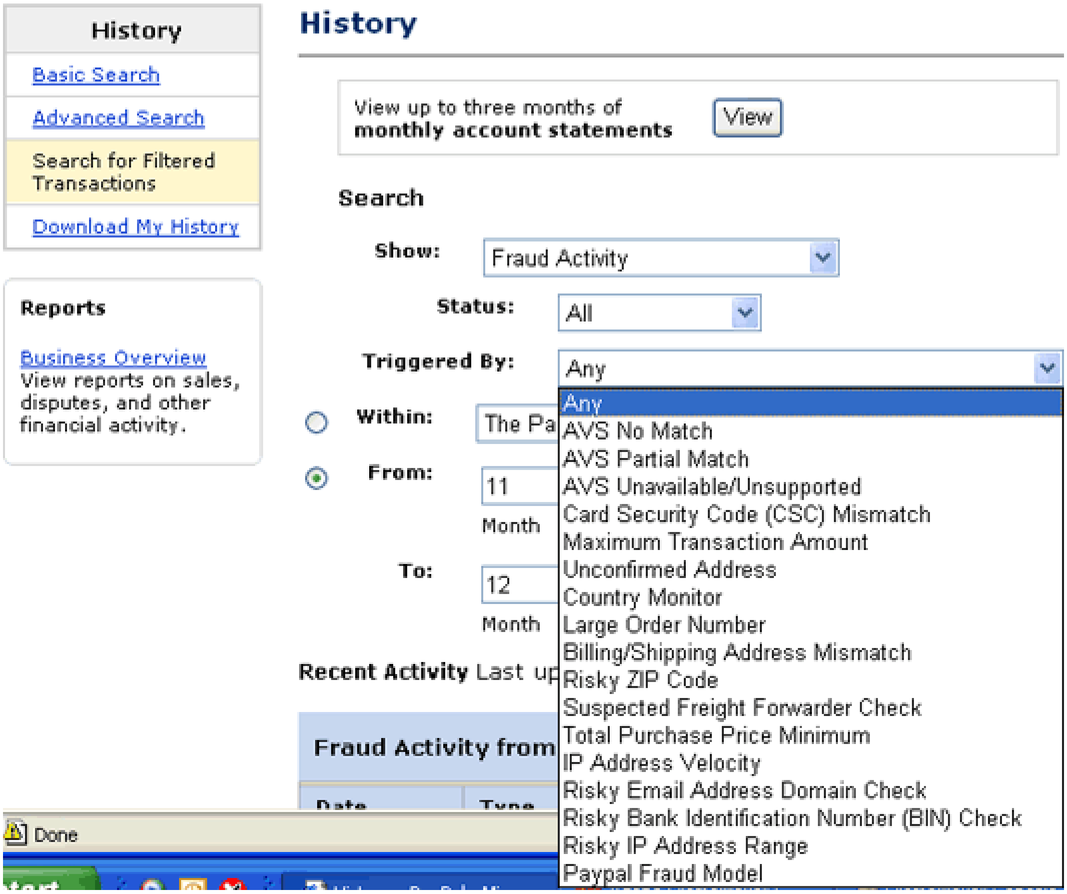
Risk Management Filters

Risk Filter Triggered:	Maximum Transaction Amount

Using Payment Fraud Search

You can use the Fraud Management Filters transaction search capability to help detect payment fraud.

You can search the transaction history for filtered transactions. To search, select Fraud Activity as the history you want to show and select any of the triggers shown below:


History
Basic Search
Advanced Search
Search for Filtered Transactions
Download My History
Reports
Business Overview
View reports on sales, disputes, and other financial activity.
History
View up to three months of
monthly account statements
View
Search
Any
AVS No Match
AVS Partial Match
AVS Unavailable/Unsupported
Card Security Code (CSC) Mismatch
Maximum Transaction Amount
Unconfirmed Address
Country Monitor
Large Order Number
Billing/Shipping Address Mismatch
Risky ZIP Code
Suspected Freight Forwarder Check
Total Purchase Price Minimum
IP Address Velocity
Risky Email Address Domain Check
Risky Bank Identification Number (BIN) Check
Risky IP Address Range
Paypal Fraud Model
Recent Activity Last up
Fraud Activity from
Date
Type
Done

Show: Fraud Activity

Status: All

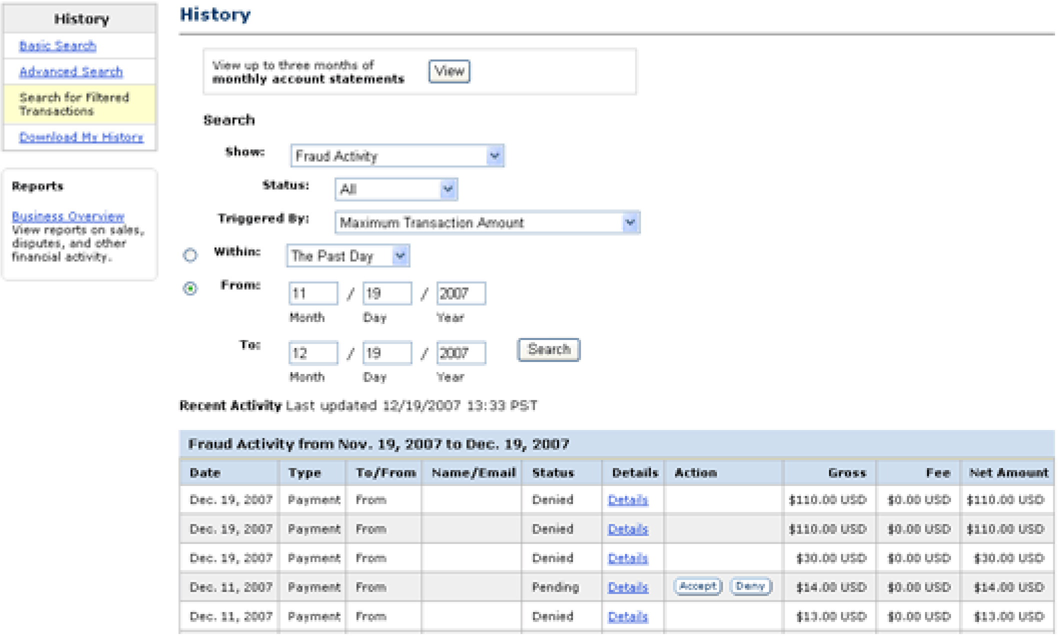
Triggered By: Any

○ Within: The Pa

● From: 11 Month

To: 12 Month

The following search presents the results of a search for potentially fraudulent payments detected by the Maximum Transaction Amount filter, including both those that have been denied or pended for your review:



History

Basic Search

Advanced Search

Search for Filtered Transactions

Download My History

Reports

Business Overview
View reports on sales, disputes, and other financial activity.

History

View up to three months of **monthly account statements** View

Search

Show: Fraud Activity

Status: All

Triggered By: Maximum Transaction Amount

○ Within: The Past Day

● From: 11 / 19 / 2007 (Month Day Year)

To: 12 / 19 / 2007 (Month Day Year) Search

Recent Activity Last updated 12/19/2007 13:33 PST

Fraud Activity from Nov. 19, 2007 to Dec. 19, 2007

Date	Type	To/From	Name/Email	Status	Details	Action	Gross	Fee	Net Amount
Dec. 19, 2007	Payment	From		Denied	Details		$110.00 USD	$0.00 USD	$110.00 USD
Dec. 19, 2007	Payment	From		Denied	Details		$110.00 USD	$0.00 USD	$110.00 USD
Dec. 19, 2007	Payment	From		Denied	Details		$30.00 USD	$0.00 USD	$30.00 USD
Dec. 11, 2007	Payment	From		Pending	Details	Accept Deny	$14.00 USD	$0.00 USD	$14.00 USD
Dec. 11, 2007	Payment	From		Denied	Details		$13.00 USD	$0.00 USD	$13.00 USD

You can examine the transaction details of these payments in the same way as any other transaction. You can also accept or deny pended payments listed in the history.

4 Customizing Websites to use Fraud Management Filters

You can detect and manage Fraud Management Filter results using IPN and the PayPal API. All merchants using IPN or the PayPal API must ensure that their systems can handle transactions pended by Fraud Management Filters.

- Using Fraud Management Filters With IPN
- Fraud Management Filters API Prerequisites
- Detecting Pending Transactions Using the PayPal API
- Handling FMF Errors in Payment API Operations
- Migration From Risk Controls

Using Fraud Management Filters With IPN

Fraud Management Filter actions are reported in IPN payment messages only when a filter causes the payment to be pended awaiting your review or a when you accept or deny a filter-pended payment. Filter actions are not reported when filters flag payments for review, allow payments to be accepted, or cause them to be denied.

When a payment occurs, an IPN message shows the transaction's payment status as `Completed`, regardless of whether a Fraud Management Filter was activated or not. There is no special notification for transactions that are flagged by a Fraud Management Filter. If a Fraud Management Filter is set to `Deny`, PayPal does not send an IPN message when the filter actually causes the payment to be denied.

When a transaction is pended, however, PayPal sends an IPN message containing one or more `fraud_management_pending_filters_`*n* variables, which identify the filters that caused the payment to be pended, where `n=1` specifies the first filter, and so on. In addition, the `payment_status` variable is set to `Pending`. The following example shows an IPN message in which two filters cause the transaction to be pended:

```
txn_type = virtual_terminal
payment_date = 17:11:42 Jul 15, 2008 PDT
last_name =
receipt_id = 3075-7371-4622-1677
residence_country = US
pending_reason = address
item_name =
payment_gross = 3.33
mc_currency = USD
business = acqrte_1215804264_biz@gmail.com
payment_type = instant
verify_sign = APYUGJhXGkUmvFnZf4I5co6CedKKAowZjfT4T7GXWJMDnZ0uFLkcq.oH
payer_status = unverified
test_ipn = 1
fraud_management_pending_filters_1 = Maximum Transaction Amount
tax = 0.00
txn_id = 5XN64179EB804362B
fraud_management_pending_filters_2 = Unconfirmed Address
quantity = 1
first_name =
receiver_email = acqrte_1215804264_biz@gmail.com
payer_id = PUWAJRBB8NM74
receiver_id = 2RXLTRMGT3M2G
item_number =
payment_status = Pending
shipping = 0.00
mc_gross = 3.33
custom =
charset = windows-1252
notify_version = 2.4
```

NOTE: If the transaction is for an authorization or an order, the `auth_status` variable may also be set to `Pending`.

If a transaction has been pended, PayPal sends an IPN message when the payment has been accepted or denied. The following example shows an IPN message indicating that a pended transaction has been accepted:

```
txn_type = virtual_terminal
payment_date = 17:11:42 Jul 15, 2008 PDT
last_name =
receipt_id = 3075-7371-4622-1677
residence_country = US
item_name =
payment_gross = 3.33
mc_currency = USD
business = acqrte_1215804264_biz@gmail.com
payment_type = instant
verify_sign = AFcWxV21C7fd0v3bYYYRCpSSRl31AjcbYkD.VCCBmpD4lZq.yYTxBKkr
payer_status = unverified
test_ipn = 1
fraud_management_pending_filters_1 = Maximum Transaction Amount
tax = 0.00
txn_id = 5XN64179EB804362B
fraud_management_pending_filters_2 = Unconfirmed Address
quantity = 1
receiver_email = acqrte_1215804264_biz@gmail.com
first_name =
payer_id = PUWAJRBB8NM74
receiver_id = 2RXLTRMGT3M2G
item_number =
payment_status = Completed
payment_fee = 0.45
mc_fee = 0.45
shipping = 0.00
mc_gross = 3.33
custom =
charset = windows-1252
notify_version = 2.4
```

The following example shows an IPN message indicating that a pended transaction has been denied:

```
txn_type = virtual_terminal
payment_date = 17:09:40 Jul 15, 2008 PDT
last_name =
receipt_id = 0739-3836-3393-2098
residence_country = US
item_name =
payment_gross = 2.11
mc_currency = USD
business = acqrte_1215804264_biz@gmail.com
payment_type = instant
verify_sign = AFcWxV21C7fd0v3bYYYRCpSSRl31ASrKFBPwac7aQm47p8CMLrdParSt
payer_status = unverified
test_ipn = 1
fraud_management_pending_filters_1 = Maximum Transaction Amount
tax = 0.00
txn_id = 53R82724RM1848354
fraud_management_pending_filters_2 = Unconfirmed Address
quantity = 1
first_name =
receiver_email = acqrte_1215804264_biz@gmail.com
payer_id = PUWAJRBB8NM74
receiver_id = 2RXLTRMGT3M2G
item_number =
payment_status = Denied
shipping = 0.00
mc_gross = 2.11
custom =
charset = windows-1252
notify_version = 2.4
```

Fraud Management Filters API Prerequisites

If your website uses PayPal APIs and you want to use FMF, you must detect transactions that have been pended by Fraud Management Filters.

IMPORTANT: To use Fraud Management Filters with the PayPal API, you must use version 52.0 or higher of the PayPal API.

To detect transactions that have been pended by Fraud Management Filters, you must ensure that your website meets the following criteria:

- You must handle `Pending` in the pending status of a response as representing a successful payment.
- You must handle the `SuccessWithWarning` acknowledgement status in the response to any of the following API operations that you use: `BillUser` `DoDirectPayment` `DoExpressCheckoutPayment` `DoReferenceTransaction`

Any of these APIs could return a `SuccessWithWarning` status indicating that the transaction was pended.

IMPORTANT: You may lose payment transactions if you do not handle `SuccessWithWarning` acknowledgements.

- You must capture and evaluate the return code associated with a `SuccessWithWarning` acknowledgement.
- If you process authorizations or orders, you must be able to analyze the short message associated with a capture failure

  Because a payment cannot be captured until it is taken out of the pending state, a capture failure may occur because the transaction was pended or it may occur for some valid reason. You must be able to distinguish between different kinds of failures.
- Your shipping process must not allow shipping before the payment has been accepted.

  If the payment status is `Pending`, you must ensure that you do not ship merchandise until you review the transaction. You can use the PayPal website or the `ManagePendingTransactionStatus` PayPal API operation to either accept or deny pending transactions.

  NOTE: Pending payments are held 30 days unless explicitly denied or accepted. After 30 days, a pending payment is automatically reversed.
- If you use Direct Payment Recurring Billing (for Website Payments Pro merchants), your subscription creation process must handle a `SuccessWithWarning` acknowledgement and associated return codes. Specifically, it must handle the situation in which only the first payment is pended; payments thereafter will not be placed in pending.

If you cannot accept these prerequisites; for example, if your shipping process would require substantial rework, you can still use Fraud Management Filters to flag or deny riskier payments, which provides you with additional risk review options, without changing your site. In this case, do not set any Fraud Management Filters to Review.

NVP Example

For a pended transaction, the NVP response would contain `PAYMENTSTATUS` set to `Pending` and the response would also contain the following fields:

```
ACK=SuccessWithWarning
L_ERRORCODE0=11610
L_SHORTMESSAGE0=Payment%20Pending%20your%20review%20in%20Fraud
%20Management%20Filters
L_LONGMESSAGE0=
L_SEVERITYCODE0=Warning
```

SOAP Example

The SOAP response would contain `PaymentStatus` set to `Pending` and the response would also contain the following fields:

```
...
<ack>
 <__value__>
  <m__value>SuccessWithWarning</m__value>
 </__value__>
</ack>
...
<errors>
 <com.paypal.soap.api.ErrorType>
  <shortMessage>Payment Pending your review in Fraud Management
   Filters</shortMessage>
  <longMessage></longMessage>
  <errorCode>
   <m__value>11610</m__value>
  </errorCode>
  <severityCode>
   <__value__>
    <m__value>Warning</m__value>
   </__value__>
  </severityCode>
  <____hashCodeCalc>false</____hashCodeCalc>
 </com.paypal.soap.api.ErrorType>
</errors>
...
```

Detecting Pending Transactions Using the PayPal API

You must detect an acknowledgment status of `SuccessWithWarning` and an error code of 11610 to identify a pending transaction. The payment status should be `Pending`.

The following simple example modifies the `DoExpressCheckoutPayment.jsp` sample in the NVP SDK to support Fraud Management Filters. It does not handle the possibility that more than one error code can be returned. The changes to the sample are noted:

```
...
String strNVPResponse = (String) caller.call( strNVPString);
NVPDecoder decoder = new NVPDecoder();
decoder.decode(strNVPResponse);
String strAck = decoder.get("ACK");
// BEGIN CHANGES FOR FRAUD MANAGEMENT FILTERS
String strErrorCode = decode.get("L_ERRORCODE0");
String strPaymentStatus = decode.get("PAYMENTSTATUS");
if (strAck.equals("SuccessWithWarning") &&
strPaymentStatus.equals("Pending") && strErrorCode.equals("11610"))
{
     // [insert code to record this transaction as pending "Review"]
}
else  // END CHANGES
if(strAck !=null && !(strAck.equals("Success") ||
strAck.equals("SuccessWithWarning")))
{
  session.setAttribute("response",decoder);
  response.sendRedirect("APIError.jsp");
  return;
}
...
```

Handling FMF Errors in Payment API Operations

When you use Fraud Management Filters programatically, you must check for errors reported by a filter in the response to the `DoDirectPayment`, `DoExpressCheckoutPayment`, `DoReferenceTransaction`, and `BillUser` API operations. If you enabled reporting of FMF details in the request to these API operations, the response identifies the filters that caused a transaction to be pended or denied when these actions occur.

To enable reporting of FMF filter information, set the `ReturnFMFDetails` flag to `1` (`true`) in your request to `DoDirectPayment`, `DoExpressCheckoutPayment`, `DoReferenceTransaction`, and `BillUser`. You must explicitly request FMF detail information or the response will not contain it.

NOTE: Fraud Management Filters operate whether or not you request FMF detail information.

Regardless of whether you return FMF detail information, you must check for errors. Specifically, you must check for acknowledgements of `Success` and `SuccessWithWarning` in the response; however, PayPal recommends that you check for all possible acknowledgement status values. You must check for errors codes 11610 and 11611, depending on the acknowledgement status:

- If the acknowledgement status is `SuccessWithWarning`, check for error code 11610, which indicates that one or more filters caused the transaction to be pended, awaiting your review

- If the acknowledgement status is not `Success` or `SuccessWithWarning`, check for error code 11611, which indicates that one or more filters caused the transaction to be denied

The following SOAP example shows typical error handling for Fraud Management Filters:

```
...
if (DPRes.Ack == AckCodeType.Success) // No error
{
  // Run success code
  // Let buyer know, mark the order as complete in database, etc.
}
else if (DPRes.Ack == AckCodeType.SuccessWithWarning) // May be pended
{
  // Test for pended transaction
  bool isFMFPended = false;
  for (int z = 0; z < DPRes.Errors.Length; z++)
  {
    if (DPRes.Errors[z].ErrorCode == "11610")
    {
      isFMFPended = true; // Transaction was pended
    }
  }
  if (isFMFPended == true)
  {
    // Keep information about filters causing transaction to be pended
    if (DPRes.FMFDetails.PendingFilters != null)
    {
      for (int x = 0; x < DPRes.FMFDetails.PendingFilters.Length; x++)
      {
        // Useful information to be kept:
        // DPRes.FMFDetails.PendingFilters[x].Description;
        // DPRes.FMFDetails.PendingFilters[x].Id;
        // DPRes.FMFDetails.PendingFilters[x].Name;
      }
    }
  }
}
else if (DPRes.Ack == AckCodeType.Failure ||
         DPRes.Ack == AckCodeType.FailureWithWarning) // Definite failure
{
  // Test for denied transaction
  bool isFMFDenied = false;
  for (int z = 0; z < DPRes.Errors.Length; z++)
  {
    if (DPRes.Errors[z].ErrorCode == "11611")
    {
      isFMFDenied = true; // Denied by FMF
    }
  }
  if (isFMFDenied == true)
  {
    // Keep information about filters causing transaction to be denied
    if (DPRes.FMFDetails.DenyFilters != null)
    {
      for (int x = 0; x < DPRes.FMFDetails.DenyFilters.Length; x++)
      {
        // Useful information to be kept:
        // DPRes.FMFDetails.DenyFilters[x].Description;
        // DPRes.FMFDetails.DenyFilters[x].Id;
        // DPRes.FMFDetails.DenyFilters[x].Name;
      }
    }
  }
}
else
{
  // Unexpected ACK type. Log response and inform the buyer that the
  // transaction must be manually investigated.
}
```

Migration From Risk Controls

Unlike Risk Controls, Fraud Management Filters do not return risk-related error codes for the `DoAuthorization` and `DoCapture` API operations. If you have previously programmed checks for risk controls after these operations, you may need to change your business logic.

You must handle error codes related to FMF in the response of the `DoDirectPayment`, `DoExpressCheckoutPayment`, `DoReferenceTransaction`, and `BillUser` API operations. These error codes are different than error codes associated with Risk Controls.

5 Fraud Management Filters Summary

Fraud Management Filters includes both basic and advanced filters.

- Kinds of Fraud Management Filters
- Basic Fraud Management Filters
- Advanced Fraud Management Filters

Kinds of Fraud Management Filters

The filters you can use are determined by agreement between you and PayPal.

PayPal provides basic and advanced filters:

- Basic filters are automatically available to any PayPal business account holder using Website Payments Standard, Website Payments Pro, Express Checkout, Virtual Terminal, or Email Payments. For more information about basic filters, see Basic Fraud Management Filters.
- Advanced filters are available to Website Payments Pro merchants as an inclusive upgrade from the basic filters; using them may incur additional charges.

  Advanced filters are ideal for merchants with a medium to high volume of transactions. You can use them to automate existing manual review processes. They are specifically developed to combat credit card fraud by detecting fraudulent patterns in credit card payments. For more information about advanced filters, see Advanced Fraud Management Filters.

IMPORTANT: You must have a business account to use Fraud Management Filters. Not all filters are available in each country or to each merchant. You can see your options by logging into PayPal and selecting Fraud Management Filters in the Profile.

Basic Fraud Management Filters

Basic Fraud Management Filters are filters that are available to all PayPal business account holders.

Maximum Transaction Amount Filter

This filter screens for payments above the specified amount by screening the total amount of the transaction, including tax, shipping, and handling fees. Transactions that exceed this maximum amount trigger this filter. An unusually high total amount can indicate potential fraudulent activity because fraudsters generally aren't price sensitive as they aren't paying with their own money. The Maximum Transaction Amount filter applies to all payments.

Unconfirmed Address Filter

This filter screens for payments above the specified amount when the shipping address entered by your customer has not yet been confirmed by PayPal as belonging to the PayPal account holder. A confirmed address is less likely to be used for fraudulent activity; however, there are many valid reasons why a customer's legitimate address may not be confirmed. For example, the customer may have recently moved or may live in a country where address confirmation is not available. Currently, only addresses in Canada, the United Kingdom, and the United States can be confirmed. You can also specify a maximum amount for the payment, in which amounts lower than the specified amount are not checked. The Unconfirmed Address filter applies to all payments.

NOTE: All payments made using debit cards, credit cards, and Virtual Terminal are considered to be from unconfirmed addresses.

Country Monitor Filter

This filter screens for payments from countries that you believe to pose an increased risk of fraud by screening a customer's IP address, billing address, and shipping addresses for matches with the countries you specify. Orders from customers in some countries can have a relatively higher incidence of fraud, especially where it is difficult to authenticate information about residents of the country. The Country Monitor filter applies to all payments.

Advanced Fraud Management Filters

Advanced Fraud Management Filters, which are optional, provide additional protection aimed at detecting fraud in credit card payments.

Advanced Fraud Management Filters are only available with Website Payments Pro. You can upgrade to these filters on PayPal. If you no longer want advanced fraud management filters, you can downgrade by contacting PayPal customer support.

Card and Address Validation Filters

You can filter transactions based on address information or credit card security code.

Address Verification Service No Match Filter

This filter screens for payments for which the billing address entered by your customer doesn't match the information maintained by the card issuer, as determined by the Address Verification Service (AVS). This filter corresponds to AVS response codes N or C. AVS compares the street number and zip code entered by the customer with information maintained by the card issuer. An AVS match helps verify that the customer using the credit card is the owner of the card. Failure to match may indicate that the address provided by the customer is fraudulent; however, no match may simply be the result of a typographical error. The Address Verification Service no match filter applies to Direct Credit Card and Virtual Terminal payments. Not all merchants are eligible for this filter; contact PayPal for more information if you want to use this filter.

Address Verification Service Partial Match Filter

This filter screens for payments for which the billing address entered by your customer doesn't completely match the information maintained by the card issuer, as determined by the Address Verification Service (AVS). This filter corresponds to AVS response codes A, B, P, W, and Z. AVS compares the street number and zip code entered by the customer with information maintained by the card issuer. A complete match helps verify that the customer using the credit card is the owner of the card. Failure to match may indicate that the address provided by the customer is fraudulent; however, a partial match may simply be the result of a typographical error. The Address Verification Service partial match filter applies to Direct Credit Card and Virtual Terminal payments. Not all merchants are eligible for this filter; contact PayPal for more information if you want to use this filter.

Address Verification Service Unavailable or Not Supported Filter

This filter screens for payments for which the Address Verification Service (AVS) is unable to verify the billing address. The filter corresponds to AVS response codes I, G, R, S, U and E. When AVS is not available to double-check the address, you may be more susceptible to fraud. Although AVS is supported by most credit cards in the United States, it is not supported by all cards worldwide. The Address Verification Service unavailable filter applies to Direct Credit Card and Virtual Terminal payments. Not all merchants are eligible for this filter; contact PayPal for more information if you want to use this filter.

Card Security Code Mismatch Filter

This filter screens for payments that do not include a correct Card Security Code. (This corresponds to Virtual terminal response code N.) The card security code is a three- or four-digit number usually found on the signature panel of a card. This fraud management tool has various names. Visa calls it CVV2, MasterCard calls it CVC2, and American Express calls it CID. The Card Security Code filter compares the number provided by the customer to the number on file with the issuer. A valid Card Security Code helps verify that your customer has a physical card with them when they place an order. An invalid code could be the result of a customer's typographical error or it could indicate that a fraudster did not have the card with them when they placed the order. The Card Security Code filter applies to Direct Credit Card and Virtual Terminal payments. Not all merchants are eligible for this filter; contact PayPal for more information if you want to use this filter.

Billing/Shipping Address Mismatch Filter

This filter screens for payments based on differences between the customer's billing and shipping addresses (street, state, zip code, and country). The filter checks relationships among the street address, city, state, and postal code and determines if a minor change is needed before filtering the transaction.

A billing/shipping address mismatch may indicate that the customer is shipping to an address different from the one the bill is sent to. A mismatch could be due to a fraudster using a stolen identity to complete a purchase; however, there are also legitimate reasons why a customer's shipping and billing address might not match. For example, your customer might be buying a gift for someone who lives at a different address or they might want to have a purchase delivered to their workplace. The billing/shipping address mismatch filter applies to Direct Credit Card and Virtual Terminal payments.

High Risk Lists Filters

You can filter transactions based on lists of risk criteria.

Zip Code Filter

This filter screens for payments with billing addresses that include a zip code with historically high rates of fraud. Zip codes are checked against a "Risk List" maintained by PayPal for US addresses. High-risk zip codes are determined through careful analysis of millions of e-commerce transactions. Because fraud tends to happen more often in densely populated areas like major cities, zip codes on the risk list are often for major cities. A matching zip code does not necessarily indicate a fraudulent purchase; however, it may indicate that you should pay special attention to the transaction. This filter applies to Direct Credit Card and Virtual Terminal payments.

Suspected Freight Forwarder Filter

This filter screens for payments whose shipping address is a known freight forwarder. Addresses are checked against a "Risk List" maintained by PayPal, which only applies to US shipping addresses. Freight forwarding services receive packages on behalf of a customer and forward them to another destination. There are legitimate uses for freight forwarding services; however, fraudsters can use a freight forwarder to mask their true locations. This filter applies to Direct Credit Card and Virtual Terminal payments.

Email Address Domain Filter

This filter screens for payments from email addresses with historically high instances of fraud. Email domains are checked against a "Risk List" maintained by PayPal. Fraudsters often use specific free email services because they don't require traceable billing information; however, free email services are also popular among legitimate customers. This filter applies to Direct Credit Card and Virtual Terminal payments.

Bank Identification Number Filter

This filter screens for payments from credit cards with Bank Identification Numbers (BIN) that have historically been associated with a relatively higher rate of fraudulent transactions. BINs, which identify the bank that issues the card, are checked against a "Risk List" maintained by PayPal. Some BINs carry a higher risk of fraud because the card issuer uses less stringent authentication policies before issuing cards. Cards from issuers with a large number of cards in circulation may also represent higher risk because more cards are available to fall into the hands of fraudsters. The bank identification number filter applies to Direct Credit Card and Virtual Terminal payments.

IP Address Range Filter

This filter screens for payments from IP addresses with historically high instances of fraud. IPs are checked against a “Risk List” maintained by PayPal. Historically, fraud is more likely to originate from compromised networks because fraudsters launch attacks from compromised computers or networks. To use this filter, you must send the customer’s IP address along with the rest of the transaction information. The IP address range filter applies to Direct Credit Card and Virtual Terminal payments.

Transaction Data Filters

You can filter transactions based on transaction data.

Large Order Number Filter

This filter screens for payments based on the number of items a customer purchases by identifying transactions that exceed the specified number of items purchased at your business. Fraudsters usually try to purchase as much as they can before the stolen cards they use are cancelled. An unusually high item count may indicate potential fraudulent activity. Fraudsters frequently attempt to order large numbers of attractive items that can be easily resold. The large order number filter applies to Direct Credit Card and Virtual Terminal payments.

Total Purchase Price Minimum Filter

This filter overrides other filter actions if the transaction falls below a minimum total transaction amount, including tax, shipping, and handling fees. If the transaction amount is below the amount set for this filter, the payment is automatically accepted, overriding any other filter that would have set aside this transaction for your review.

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 amount you specify are accepted without further analysis. This filter applies to Direct Credit Card and Virtual Terminal payments.

IP Address Velocity Filter

This filter screens for multiple payments that originate from the same IP address by checking for repeated transaction attempts from the same computer or network. A high number of orders from a single IP address may be associated with a fraudster making repeated purchases on your website. A fraudster may repeatedly attempt transactions through an automated script that tests unknown card numbers or may attempt to make many small purchases through multiple stolen cards to bypass other filters.

Legitimate customers typically don’t perform multiple transactions in quick succession; however, some Internet Service Providers (ISPs) may use a single IP address for all of their customers’ computers. You can choose to ignore IP addresses from these ISPs so that payments originating with them will not be filtered. The IP address velocity filter applies to Direct Credit Card and Virtual Terminal payments.

PayPal Fraud Model Filter

This filter screens for payments that would have been declined by PayPal's fraud model. PayPal's fraud model identifies potentially risky transactions. It is updated dynamically to combat trends and patterns in fraudulent activity around the world. The PayPal fraud model filter applies to Direct Credit Card and Virtual Terminal payments. Not all merchants are eligible for this filter.

6 Fraud Management Filters Operating Principles

In addition to how you set up Fraud Management Filters, the operation of Fraud Management Filters depends on the kind of flow, the payment method, such as by Express Checkout, Direct Credit Card, or Virtual Terminal, and interaction with other PayPal fraud protection services.

- Fraud Management Filters Operation With Direct Credit Card and Virtual Terminal Payments
- Fraud Management Filters Operation With Other Payment Transactions
- Fraud Management Filters Pending State Operation

Fraud Management Filters Operation With Direct Credit Card and Virtual Terminal Payments

Both basic and advanced Fraud Management Filters can be used on Direct Credit Card or Virtual Terminal transactions.

For Direct Credit Card or Virtual Terminal transactions PayPal, applies the filters you enable in the following order:

1. Total Purchase Price Minimum filter
2. Maximum Transaction Amount filter
3. Unconfirmed Address filter
4. Country Monitor filter
5. Large Order Number filter
6. Billing/Shipping Address Mismatch filter
7. Zip Code filter
8. Suspected Freight Forwarder filter
9. IP Address Velocity filter
10. Email Address Domain filter
11. Bank Identification Number filter
12. IP Address Range filter
13. PayPal Fraud Model filter
14. Address Verification Service No Match filter

15. Address Verification Service Partial Match filter

16. Address Verification Service Unavailable or Not Supported filter

17. Card Security Code Mismatch filter

NOTE: For Canadian merchants, the Zip Code and Suspected Freight Forwarder filters only operate on US addresses. These filters are not available to UK merchants.

Fraud Management Filters Operation With Other Payment Transactions

For non-Direct Credit Card and non-Virtual Terminal transactions, only basic Fraud Management Filters are applied.

For other payment transactions, such as Express Checkout, PayPal applies the basic filters you enable in the following order:

1. Maximum Transaction Amount filter

2. Unconfirmed Address filter

3. Country Monitor filter

Fraud Management Filters Pending State Operation

Transactions that are set aside for review enter the pending state.

You can enable a filter by setting it to **Accept**, to **Deny**, **Review**, or to **Flag**. Payments awaiting review by you are marked by PayPal as *pending*. More than one filter can cause a payment to be pended awaiting your review; however, as soon as a filter causes a payment to be accepted or denied, all filtering stops. The filter actions to accept, deny, or pend a payment for review are mutually exclusive; PayPal can take only one of these actions for each transaction as it is processed by a filter.

NOTE: The **Review** setting for a filter enables payments to be set aside for your review. It is not the same as additional review actions that PayPal may take on your behalf to reduce fraud.

If you specify that a filter should flag a payment, the PayPal user interface marks the transaction when it is displayed in the PayPal website. A flagged payment is not pended. Another filter may cause a flagged payment to be accepted, denied, or pended.

When a payment is set aside for review, the associated transaction enters the pending state. You must accept for deny the payment before the transaction can complete.

NOTE: If you do not make a determination within 30 days, PayPal automatically returns the funds to the buyer.

Supported Transaction Flows for Review Action

The kind of flow determines whether a payment can be marked as pending your review; not all flows support the **Review** action. Only payments made during specific transaction flows can be set aside for review. Payments occurring outside of these flows are either accepted or denied. If the flow does not support the **Review** action, requests for review are ignored; however, these payments are flagged so that you can view them from the PayPal website. The following transaction flows enable PayPal to pend a payment for review:

- Web Site Payments Standard for Buy Now and shopping carts
- Express Checkout
- Virtual Terminal
- Mass Pay
- Credit Card Recurring Transactions
- Web Accept Express
- Send Money

Capturing Pending Payments

You cannot capture a payment that was placed in the pending state by Fraud Management Filters. For example, if the payment occurs as part of an authorization or order, you must accept the payment before it can be captured.

Interaction with Payment Receiving Preferences

Fraud Management Filters operates on a payment as soon as the transaction occurs. Other PayPal fraud protection services may not pend a payment until later in the process. A transaction could be pended for your review by Fraud Management Filters and then be pended for your review by another PayPal fraud protection service.

You can use Payment Receiving Preferences with Fraud Management Filters; however, you need to be aware that Fraud Management Filters pends a payment as the first step in processing a transaction while Payment Receiving Preferences may pend a payment during capture. Both Payment Receiving Preferences and Fraud Management Filters can pend a payment during a sale. For authorizations and orders, however, Fraud Management Filters can pend a payment and you can accept it just to have Payment Receiving Preferences pend the payment again during capture. In these cases, you must accept the payment twice.

Index