worldpay

eComm Fraud Toolkit Info

Just because a credit card network/company returns a valid authorization for a purchase does not always mean that completing the transaction is in your best interest. There are multiple reasons you may wish to decline a sale on a particular card at a particular time. In many cases there are indicators that the transaction could be or likely is fraudulent. Acting to stop these transactions at submission prevents loss, as well as reducing the number fraud related chargebacks in the future. Worldpay offers a robust fraud solution, the Fraud Toolkit, to assist you in reducing the number of possibly fraudulent transactions inflicted upon you by bad actors.

The Fraud Toolkit has three tiers or levels of implementation, each providing more rigorous examination of transaction properties and data points, as well as valuable information and guidance. The table below provide an overview of the tool provided at each level. The items highlighted in blue require the inclusion of a small snippet of code on your checkout page.

TABLE 1 Fraud Toolkit Implementation Levels

Filter/Feature	Essential	Extended	Premium
AVS Filter	X	X	X
CVV No-Match Filter	X	X	X
International BIN Filter	X	X	X
Prepaid Non-Reloadable Filter	X	X	X
Prior Chargeback Filter	X	X	X
Prior Fraud Advice Filter	X	X	X
Card Velocity Filter	X	X	X
Email Velocity Filter	X	X	X
Phone Velocity Filter	X	X	X
IP Velocity Filter	X	X	X
Device Velocity Filter	X	X	X
IP Address, Geolocation, and Proxy Detection		X	X
Merchant Customizable Rules Template		X	X

TABLE 1 Fraud Toolkit Implementation Levels (Continued)

Filter/Feature	Essential	Extended	Premium
ThreatMetrix Cybercrime Dashboard		X	X
(Asynch) Transaction Review Queues		X	X
Rule Management and Portal Training		X	X
Standalone Transaction API Access		X	X
Cybercrime Industry Report (Quarterly)		X	X
Access to Fraud Consultant			X

Essential Tier

The Essential tier includes a suite of eleven Fraud Filters that you can apply individually or in combination. Nine of the eleven filters, based on card/submitted data, potentially require no additional integration on your part, assuming you already submit the necessary information. The remaining two filters require you to add a a small snippet of code on your checkout page.

Prepaid Card Filtering

Many merchants engaged in recurring payment, installment payment, or deferred billing experience some loss due to fraud schemes that make use of prepaid cards. Consider the case of a consumer using a prepaid card with a balance of $100 to make a purchase that involves an initial charge of $50 followed by three installments of $50 each. The authorization would be approved for the initial transaction, and the card might have adequate balance for an additional charge, but if the consumer was attempting to defraud the merchant or simply used the card for other purchases, the card may not have sufficient balance for any additional payments. While the Prepaid Indicator feature provides you with the information necessary to make a decision at the time of the sale, and to request a secondary or different payment method, instead you may wish to have Worldpay filter these transactions automatically when you send the Authorization transaction.

If you elect to use the Prepaid Card Filtering Service, you can select one of two methods of implementation. Using the first filtering method, our system declines all Authorization and Sale transactions when the consumer uses a prepaid card. Upon a decline, the system returns a Response Reason Code of **309 - Restricted Card - Prepaid Card Filtering Service**. This method also allows you to disable the filtering logic on a transactional basis by including the `<prepaid>` element set to a value of **false**, allowing you to accept any prepaid card for these transactions.

The second method of implementing the Prepaid Card Filtering Service is per transaction. To enable the filter on a particular transaction, set the `<prepaid>` element to a value of **true**. This method is useful to a merchant who offers products with both one-time payments and installment payments. For products involving a single payment, you may want to allow the use of prepaid cards, while for the product with multiple payments you may want to filter prepaid cards.

> **NOTE:** Within either implementation method, you can elect to filter all prepaid cards, or only non-reloadable prepaid cards. Please speak to your Implementation Consultant for additional information about setting these global parameters.

International BIN Filtering

An examination of your historical fraud data may show a high percentage of fraudulent transactions originating with certain international cards. You can limit your exposure to this type of fraud by taking advantage of the International Card Filtering Service. This feature allows you to filter MasterCard and Visa cards originating in either all foreign countries or selected foreign countries based upon the country of the card issuer.

If you elect to use this feature, when you submit an Authorization/Sale transaction, the system determines the country of origin of the card. If the card originates outside the United States and you have elected to filter all international cards, the system declines the transaction. Likewise, if you have elected to filter a specific country or countries and the card originates from a designated country, the system declines the transaction. Upon a decline, the system returns a Response Reason Code of **312 - Restricted Card - International Card Filtering Service**.

You can override your settings on a transactional basis by including the `<international>` element set to **false** when you submit the Authorization/Sale transaction. In this case, the system ignores the filtering service and processes the transaction normally.

Prior Chargeback Filtering

If you elect to use the Chargeback Filter Service, there are two configuration options. You can elect to filter all transactions using a card for which you received a chargeback, or you can elect to filter only the subset of transactions for which you received a fraud related chargeback (determine by the associated chargeback reason code). In both cases, the system checks your historical data to see if you received an applicable chargeback from the same account within the last 90 days. Upon a decline, the system returns a Response Reason Code of **308 - Restricted Card - Chargeback**.

Security Code No-Match Filter

The Card brands added the 3- or 4-digit security code to act as a verification that the person ordering your product in a card-not-present environment has physical possession of the card. While this validation can be a useful anti-fraud tool, typically, many issuing banks do not decline the transaction based upon a failure to match the security code. Declining the transaction is left to the discretion of the merchant.

> **NOTE:** Since American Express declines the transaction if the security code does not match, the Security Code No-Match filter does not apply to AmEx transactions. Transactions declined by AmEx for a failure to match the security code use the Response Code of 352 - Decline CVV2/CID Fail.
>
> Similarly, if Visa, MasterCard, or Discover decline a transaction based upon the security code results, Worldpay does not apply the filter and the transaction response contains the 352 Reason Code.

If you elect to use the Security Code No-Match Filter Service, the system takes action only if the issuer approves the submitted authorization/sale transaction, but includes a no-match code for the CVV2/CVC2/CID card validation check. In this case, the Worldpay declines the transaction with a Response Reason Code of **358 - Restricted by Worldpay due to security code mismatch**. The system also issues an Auth Reversal transaction on your behalf to remove the funds hold on the account.

Fraud Velocity Filtering

Often, when a person attempts to use a stolen credit card successfully, they will follow the initial purchase with a number of additional purchases within a short period of time. If you elect to use the Fraud Velocity Filter, the system filters the transaction based upon the number of previously approved Auth/Sale transactions plus the number of Auth/Sale transactions declined by another Basic Filter, for the same account within a configurable time period. Both the total number of transactions and the time period are configured in the Worldpay Merchant Profile.

Upon a decline, the system returns a Response Reason Code of **315 - Restricted Card - Auth Fraud Velocity Filtering Service**.

Prior Fraud Advice Filtering

Worldpay maintains a database of Fraud Advice information received from the Visa and MasterCard networks for transactions you processed in the last 200 days. If you use the Prior Fraud Advice Filter, the system compares the account information from the new transaction against the database of accounts with prior Fraud Advice and filters the transaction if there is a match.

Upon a decline, the system returns a Response Reason Code of **318 - Restricted Card - Auth Fraud Advice Filtering Service**.

AVS Filter

One of the fraud prevention tools provided by all card networks is an Address Verification System. By submitting the customer's address information in the `billToAddress` section of the cnpAPI message, you can verify that the address/zip code supplied by the consumer matches the issuer's records. The card networks, however, do not decline transactions based upon the failure to match the address or zip code. Using the AVS Filter, you can filter potentially fraudulent transactions based upon failure to match any of the following:

- the address
- the zip/postal code
- the address + zip/postal code (ANDed)
- the address or zip/postal code (ORed).

Upon a decline, the system returns a Response Reason Code of **319 - Restricted Card - Fraud AVS Filtering Service**.

Email Velocity Filter

Often, card testers or other bad actors submit a number of transaction using multiple cards, but with a common email address. The only requirement to make use of this filter is that you collect and include the consumer's email address with each transaction. We communicate the email address to our fraud partner, who tracks and analyzes the information. If the filter detects the same email used in the configured number of transactions within the configured period of time, the system declines new transactions (using the same email) on your behalf and returns Response Code **550 - Restricted Device or IP - ThreatMetrix Fraud Score Below Threshold**.

Phone Velocity Filter

Similar to email, card testers or other bad actors often submit a number of transaction using multiple cards, but with a common phone number. The only requirement to make use of this filter is that you collect and include the consumer's phone number with each transaction. We communicate the phone number to our fraud partner, who tracks and analyzes the information. If the filter detects the same phone number used in the configured number of transactions within the configured period of time, the system declines new transactions (using the same email) on your behalf and returns Response Code **550 - Restricted Device or IP - ThreatMetrix Fraud Score Below Threshold**.

IP Velocity Filter

The IP Velocity filter is one of the two filter in the Essential tier that requires (see note below) the addition of a code snippet to your checkout page. This snippet, which you also need to implement for the higher tiers of Fraud Toolkit, allows our partner, to perform IP interrogation/piercing t determine the true IP Address of the device originating the order. As with the other velocity filters, if the filter detects the same IP Address used in the configured number of transactions within the configured period of time, the system declines new transactions from the same IP Address on your behalf and returns Response Code **550 - Restricted Device or IP - ThreatMetrix Fraud Score Below Threshold**.

> **NOTE:** Technically, you can make use of the IP Velocity filter without integrating the code snippet on your checkout page. Instead you can simply include the originating IP Address that you detect in your transaction. Please note that this method will likely be less effective than making use of the ThreatMetrix functionality, which includes IP piercing to determine the true IP of the consumer's device.

Device Velocity Filter

The Device Velocity filter is the second Essential tier filter in the that requires the addition of a code snippet to your checkout page. In this case, the snippet allows ThreatMetrix to construct a device fingerprint of the system originating the order. As with the other velocity filters, if the filter detects the same device used in the configured number of transactions within the configured period of time, the system declines new transactions from the same device on your behalf and returns Response Code **550 - Restricted Device or IP - ThreatMetrix Fraud Score Below Threshold**.

Application of Filters - Filtering Rules

> **NOTE:** You define Filter Rules as part of your Merchant Profile. Please consult with your Relationship Manager and/or your Implementation Consultant concerning the provisioning of Filter Rules.

While you can have all submitted transactions flow through the Fraud toolkit, you likely want to exercise a finer control over the application of the filters based upon a particular product, service or other criteria. The system provides you the flexibility of restricting which transactions are submitted to the filtering service and which filters the system applies to which groups. This is accomplished by defining Filtering Rules.

For each Filtering Rule you first define a subgroup of transactions by selecting one of the following Flow Selectors: Report Group, Billing Descriptor, orderSource, or MID (for Payment Facilitators, flow control by MID or orderSource only). You can apply only one selector per rule. After selecting a particular Flow Selector, you then select which filters to have applied to that subset of transactions. You can define the Filter Rules so that filters are ORed (transaction filtered when any one of the filters conditions met), or ANDed (transaction filtered when multiple filter conditions met). Table 2 defines five rules that a merchant might define.

TABLE 2 Example - Fraud Filtering Service Rules

Filter	Flow Selector	Filters
1	Report Group = "XYZ"	Prepaid
2	Report Group = "XYZ"	International
3	orderSource = "recurring"	Prepaid + Prior Chargeback
4	orderSource = "ecommerce"	Fraud Velocity + Security Code No-match
5	Billing Descriptor = "GoldMember"	Prepaid + International

Table 2 defines five Filter Rules that a merchant might use. These rules would be applied as follows:

- Filters 1 and 2 are applied to the subset of transactions that are members of Report Group XYZ and use the Prepaid and International Filters. Since the Filter Rules are defined separately, the rules are ORed. So, if a transaction uses either a Prepaid card or a card of International origin, the transaction is filtered.
- Filter 3 is applied to the subset of transactions that have an orderSource value set to recurring. These transactions are filtered only if both the criteria for the Prepaid Filter AND the Prior Chargeback Filter are met.
- Filter 4 is applied to the subset of transactions that have an orderSource value set to ecommerce. These transactions are filtered only if both the criteria for the Fraud Velocity Filter AND the Security Code No-Match Filter are met.

Filter 5 is applied to the subset of transactions that have an Billing Descriptor value set to GoldMember. These transactions are filtered only if both the criteria for the Prepaid Filter AND the International Filter are met.

Extended Tier

The Extended Tier include all of the Essential Tier filters, but offers an additional levels of fraud detection made available through Worldpay's partnership with ThreatMetrix. The addition of the same code snippet used for the IP and Device Velocity filters to your checkout page allows ThreatMetrix to gather additional data points, such as the consumer's device, proxy use, and location. Unlike the filters in the Essential Tier, which are basic accept/decline filters, the Extended Tier takes the data and compares the information to a rule list. Worldpay supplies an initial, Best Practices rules list designed for your business type (i.e., Retail, Digital, Non-profit, etc.), which you can modify and refine for you particular business model. Each rule, when triggered, add or subtract a preset value from the transaction score. If the score fall below a set threshold, the system declines the transaction, unless you prefer to make the final decision yourself. In either case, Worldpay returns the score and a list of triggered rules in the transaction response message.

In addition to the ThreatMetrix rules engine, you get access to the ThreatMetrix Portal allowing you to customize your rules list and scoring values. This level also allows you to white list/black list items, such as email addresses and phone numbers. Other items included in this tier are:

- ThreatMetrix Cybercrime Dashboard
- Asynchronous Transaction Review Queues
- Monthly Rules and Portal training
- API Access to Standalone Fraudcheck transaction.

Premium Tier

The Premium Tier provides all of the tools from the Essential and Extended Tiers, and most importantly, access to the Worldpay eComm Fraud Consulting service. With the service, the Fraud Consultant assigned to you helps analyze your transactional data, recommends rule changes to fine-tune your results, and advises you on fraud detection strategy.

Modifications to Your Web Page

For ThreatMetrix to gather information for analysis, you must add certain profiling tags (see example below) to selected pages served by you web application. These tags allow ThreatMetrix to collect information by loading objects used for detection into the consumer's browser. These tags are invisible to the consumer and add only a fraction of a second to your page's rendering time. Once loaded, these objects require only 3-5 seconds to gather profiling information from the consumer device.

Place the tags as early as possible on the page, inside the `<body></body>` tags of the HTML.

Example: ThreatMetrix Profiling Tags

> **NOTE:** Replace UNIQUE_SESSION_ID with a uniquely generated handle that includes the Worldpay supplied prefix.
>
> The value for ORG-ID is a Worldpay supplied value.
>
> The pageid tag is not used at this time. The value for PAGE-ID defaults to 1.
>
> For production, replace h.online-metrix.net with a local URL and configure your web server to redirect to h.online-metrix.net.

```
<!-Begin ThreatMetrix profiling tags below -->

<script type="text/javascript"
src="https://h.online-metrix.net/fp/tags.js?org_id=ORG_ID&session_id=UNIQUE_SESSION_ID&pageid=
PAGE_ID"></script>

  <noscript>

<iframe style="width: 100px; height: 100px; border: 0; position: absolute; top: -5000px;"
src="https://h.online-metrix.net/tags?org_id=ORG_ID&session_id=UNIQUE_SESSION_ID&pageid=PAGE_I
D"></iframe>

         </noscript>

<!- End profiling tags -->
```

cnpAPI Transactions

To subject a transaction to the advanced fraud checks performed by ThreatMetrix and retrieve the results, you simply submit the `<webSessionId>` element as part of your cnpAPI Authorization (or Sale) transaction. This session Id is the same unique value you assigned and sent to ThreatMetrix when your web page called the application (designated as UNIQUE_SESSION_ID in the ThreatMetrix Profiling Tags example). When we receive an Authorization/Sale that includes the `<webSessionId>`, our system automatically queries the ThreatMetrix platform for the associated results. The cnpAPI response message includes the `<advancedFraudResults>`

element containing the score and status and any triggered rules. The following two examples show a standard Authorization transaction, including a `<webSessionId>` and a **pass** response.

Example: Authorization including <webSessionId> Element

```
<cnpOnlineRequest  version="12.3" xmlns="http://www.vnativcnp.com/schema"
 merchantId="81601">
 <authentication>
   <user>User Name</user>
   <password>password</password>
 </authentication>
 <authorization id="002" reportGroup="001601">
   <orderId>10102013_sessionId_app</orderId>
   <amount>1002</amount>
   <orderSource>ecommerce</orderSource>
   <billToAddress>
     <name>John Doe</name>
     <addressLine1>15 Main Street</addressLine1>
     <city>San Jose</city>
     <state>CA</state>
     <zip>95032-1234</zip>
     <country>USA</country>
     <phone>9782750000</phone>
     <email>nobody@vantiv.com</email>
   </billToAddress>
   <card>
     <type>MC</type>
     <number>5405102001000003</number>
     <expDate>1115</expDate>
   </card>
   <advancedFraudChecks>
     <webSessionId>ASDFG-AXXXXAB999</webSessionId>
   </advancedFraudChecks>
 </authorization>
</cnpOnlineRequest>
```

Example: Authorization Response including <advancedFraudResults> Element

```
    <cnpOnlineResponse version="12.3" xmlns="http://www.vantivcnp.com/schema"
    response="0" message="Valid Format">
      <authorizationResponse id="002" reportGroup="001601">
        <cnpTxnId>82823534116454639</cnpTxnId>
        <orderId>10102013_sessionId_app</orderId>
        <response>000</response>
    <responseTime>2018-10-08T21:36:50</responseTime>
    <postDate>2018-10-08</postDate>
    <message>Approved</message>
    <authCode>000003</authCode>
    <fraudResult>
      <avsResult>00</avsResult>
      <advancedFraudResults>
        <deviceReviewStatus>pass</deviceReviewStatus>
        <deviceReputationScore>50</deviceReputationScore>
        <triggeredRule>FlashImagesCookiesDisabled</triggeredRule>
      </advancedFraudResults>
    </fraudResult>
  </authorizationResponse>
</cnpOnlineResponse>
```

> **NOTE:** The other possible values for the **`<deviceReviewStatus>`** element are *fail*, *review*, *unavailable*, and *invalid_session*.
>
> The **`<deviceReputationScore>`** value can range from -100 to 100. The resulting pass, fail, or review value depends upon your profile settings.
>
> The <**`triggeredRule`**> element can occur multiple times, once for each rule triggered.

Information Only Option

If you wish to retain full control of the decision to accept or decline transactions, Worldpay offers the option of using the Advanced Fraud Tools in an Information Only mode. In this configuration, you receive the same information in the response as you would with the full implementation; however, Worldpay will not automatically decline transactions with a failing score.

If the authorization is declined by the network, you can choose to recycle the transaction or do nothing. If an authorization with a failing score receives approval from the network, it would be up to you to reverse the authorization should you decide not to proceed with the transaction. This is similar to the case of an approved transaction that has a status of Review, but you decide not to proceed. Issuing an authorization reversal allows you to avoid any misuse of Auth fees otherwise imposed by the card networks.

Fraud Check Transactions

If you wish to retrieve the Advanced Fraud results without introducing a Authorization or Sale transactions, use a Fraud Check transaction (example below). The standalone Fraud Check also allows you to check various types of account takeover and new account creation fraud. By submitting the `<eventType>` element, with or without the `<accountLogin>`, `<accountPasshash>`, and other information, you can check for the following scenarios:

<eventType>	Scenario Description
account_creation	Checks for evidence of new account creation fraud. We recommend you include the `<accountLogin>` element.
detail_changes	Checks for evidence of account takeover fraud, such as changes to billing address and other customer profile information. We recommend you include the `<accountLogin>` element, along with billing information and the `<accountPasshash>` element for password changes.
login	Checks for evidence of account takeover/hacking fraud. We recommend you include the `<accountLogin>` and `<accountPasshash>` elements.
payment (default)	Checks for evidence of traditional payment fraud. We recommend you include the `<accountLogin>` element.

Fraud Check transactions are only supported as Online transactions.

Example: Fraud Check Transaction

```
<cnpOnlineRequest  version="12.4" xmlns="http://www.vantivcnp.com/schema"
  merchantId="81601">
  <authentication>
    <user>User Name</user>
    <password>password</password>
  </authentication>
  <fraudCheck id="002" reportGroup="001601">
    <advancedFraudChecks>
      <webSessionId>ASDFG-AXXXXAB999</webSessionId>
      <customAttribute1>Attribute passed to Vantiv</customAttribute1>
      <customAttribute2>Attribute passed to Vantiv</customAttribute2>
      <customAttribute3>Attribute passed to Vantiv</customAttribute3>
      <customAttribute4>Attribute passed to Vantiv</customAttribute4>
      <customAttribute5>Attribute passed to Vantiv</customAttribute5>
    </advancedFraudChecks>
    <billToAddress>
      <name>John Doe</name>
      <addressLine1>15 Main Street</addressLine1>
      <city>San Jose</city>
      <state>CA</state>
      <zip>95032-1234</zip>
      <country>USA</country>
      <phone>9782750000</phone>
      <email>jdoe@Worldpay.com</email>
    </billToAddress>
    <shipToAddress>
      <name>Jane Doe</name>
      <addressLine1>15 Main Street</addressLine1>
      <city>San Jose</city>
      <state>CA</state>
      <zip>95032-1234</zip>
      <country>USA</country>
      <phone>9782750000</phone>
      <email>jdoe@vantiv.com</email>
    </shipToAddress>
    <amount>20000</amount>
    <eventType>detail_changes</eventType>
    <accountLogin>User1</accountLogin>
    <accountPasshash>passhashValueOfLength56or64or96or128</accountPasshash>
  </fraudCheck>
</cnpOnlineRequest>
```