

Advanced Fraud Detection Suite

Protect your business against
payments fraud



FRAUD MANAGEMENT

You may not think your business is big enough to be the target of fraudsters. But they're out there. Fraudsters are relentless and many of them quite savvy. However, there are actions you can take to protect your business. With 13 configurable fraud filters, the Advance Fraud Detection Suite (AFDS) helps you identify, manage, and prevent suspicious and potentially fraudulent transactions.

Don't let payment fraud jeopardize your business, take back control.

Filters to help fight fraud

Authorize.net's configurable fraud filters are specifically designed to identify, manage and prevent costly fraudulent transactions. The filters focus on four major categories:

Velocity

Daily Velocity Filter

Allows you to specify a threshold for the number of transactions allowed per day.

Amount Filter

Set lower and upper transaction amount thresholds to restrict high-risk transactions often used to test the validity of credit card numbers.

Hourly Velocity Filter

Limit the total number of transactions received per hour

Transaction

Suspicious Transaction Filter

Reviews highly suspicious transactions using proprietary criteria identified by Authorize.net's dedicated Fraud Management Team.

Enhanced AVS Handling Filter

Compares the address submitted with an order to the address on file with the customer's card issuer.

Enhanced CCV Handling Filter

CCV uses a card's three- or four-digit number to validate customer information on file with the card issuer.

IP

Transaction IP Velocity Filter

Isolate suspicious activity from a single source by identifying excessive transactions received from the same IP address.

Authorized AIM IP Addresses

Allows merchant submitting Advanced Integration Method (AIM) transactions to designate specific server IP addresses that are authorized to submit transactions.

IP Address Blocking

Block transactions from IP addresses known to be used for fraudulent activity.

Regional IP Address Filter

Flag orders coming from specific regions or countries.

Shipping

Shipping Address Verification Filter

Verifies that the shipping address received with an order is a valid postal address.

IP Shipping Address Mismatch Filter

Compare the shipping address provided with an order to the IP address of where the order originated from.

Shipping-Billing Mismatch Filter

Identify high-risk transactions with different shipping and billing addresses

What actions can be taken if the above filters are violated?

Process as normal and report filter(s) triggered

When this action is selected, transactions that trigger this filter are processed as normal, but are also reported in the Merchant Interface as triggering this filter. This action is useful if you want to “test” your filter settings.

Do not authorize, but hold for review

When this action is selected, transactions that trigger this filter are placed in the Pending Review state prior to being sent for authorization. Once in Pending Review, you will have 5 days to manually review and either approve or decline the transaction. Once you approve the transaction, it is sent for authorization. If no action is taken in the 5-day period, the transaction will expire. This action is useful if you want to review transactions prior to authorization to avoid incurring any associated authorization fees.

Authorize and hold for review

When this action is selected, transactions that trigger this filter are sent for authorization, and upon successful authorization are placed in the Authorized/Pending Review state. Once in Authorized/Pending Review, you will have 30 days to manually review and either approve or void the transaction. If no action is taken in the 30-day period, the transaction will expire. This action is useful if you want to review authorized transactions prior to submitting for settlement.

Decline the transaction

When this action is selected, transactions that trigger the filter will be declined automatically prior to authorization. This is the most severe action you can take for a transaction.

NOTE

In the event that a transaction triggers more than one filter, and each filter is configured with a different action, the most severe filter action will be applied to the transaction. For example, you might configure filter A to decline all triggered transactions, and filter B to authorize but hold all triggered transactions. If a transaction triggers both filters A and B, it will be declined rather than authorized and held for review.



How can I configure my Advanced Fraud Detection Suite?

Utilizing our setup Wizard is a simple and efficient way to configure your Advanced Fraud Detection Suite™ (AFDS).

To access the Wizard, please follow these steps:

1. Log into your Merchant Interface.
2. Click Advanced Fraud Detection Suite in the main left side menu
3. Click Setup Wizard
4. Follow every step in the Wizard, so your settings will be successfully applied.

How can existing users receive e-mail notifications for Advanced Fraud Detection Suite filters?

1. Log into your Merchant Interface.
2. Click User Administration in the main left side menu.
3. Click the name of the contact for which you would like to setup e-mail notifications.
4. Click Edit Profile Information.
5. Check the box for AFDS Per Suspicious Transaction.
6. Click the Submit button when you have finished making changes.



NOTE

Although these per-transaction notifications provide information regarding how suspicious transactions are handled, you should not rely solely on them for information about transaction statuses.

The AFDS is applicable for all business types and sizes – preventing even one instance of fraud can be the difference in saving your business on any given day.

Oftentimes small and medium business believe they are not the target of fraudsters, but in reality they are just as vulnerable as large businesses.