White Paper

Authorize.Net
a CyberSource solution

Fighting Online Fraud

Maintaining tight security, including using both standard and advanced fraud detection and prevention tools, is crucial to maintaining a successful business. No merchant can afford to overlook the need for protection against fraud and other types of abuse. This document details the tools and security best practices that Authorize.Net recommends to merchants for detecting, preventing, and managing transaction fraud.

The Fight Against Online Transaction Fraud

In the faceless world of the Internet, online transaction fraud is one of the greatest challenges for merchants. According to the results of the 13th annual CyberSource Online Fraud Report, U.S. merchants lost an estimated $3.4 billion to fraud in 2011. Advanced solutions are needed to protect merchants from this constantly evolving threat. The Authorize.Net Advanced Fraud Detection Suite™ (AFDS) arms you with advanced filters and tools, providing a customizable solution to combat today's most common types of fraud.

All Merchants Are Potential Targets

Regardless of size, transaction volume or Internet expertise, all e-commerce merchants are susceptible to falling prey to any of the various types of online transaction fraud. Hackers and fraudsters are becoming more sophisticated and skillful at manipulating Internet protocols, Web languages and infrastructures to discover any weakness they can exploit. Thousands of online merchants experience suspicious transaction activity and other types of account abuse each day—and it can happen to you.

Standard Verification Tools Are Not Enough

Standard verification tools developed to assist merchants with screening transactions, such as the Address Verification System (AVS) and Card Code Verification (CCV), though essential, are limited as to the level of protection they can provide. Fraudsters have learned how to interpret AVS and CCV responses and are not usually deterred by the use of these tools. As a result, using these verification tools exclusively for protection against fraud is insufficient. Merchants now need to look to additional, more advanced solutions designed to fight fraud—such as the Advanced Fraud Detection Suite.

www.authorize.net
P.O. Box 8999, San Francisco, CA 94128-8999
Toll-free at 866-437-0491 E-mail: sales@authorize.net

Common Types of Fraud

Knowing what you're up against is the key to a strategic defense. Online merchants most often face two types of transaction fraud.

Verification Fraud

The most common type of fraud is verification fraud. Fraudsters can easily obtain or generate potentially legitimate credit card numbers. By submitting orders using a merchant's payment form, they can determine whether that information is valid. At this point, they are not seeking financial gain, only information. But for merchants who suddenly experience thousands of invalid transactions, the repercussions can be costly.

Settlement Fraud

Once fraudsters have confirmed the validity of a credit card, they can then use it to purchase goods from a merchant. Fraudsters will usually attempt to get a merchant to ship large amounts of a product to a location different from the billing address of the cardholder. Their motive is to steal as much as they can as quickly as possible. By the time the chargebacks come rolling in, merchants are left holding the bag.

Combat Online Fraud Using AFDS

By supplementing standard payment gateway features such as AVS and CCV, AFDS helps create an umbrella of protection for your business. With customizable filters and tools, AFDS provides you with a greater degree of control over your incoming transactions, and can potentially prevent costly authorization and chargeback fees, as well as the inventory loss that often results from fraudulent transactions. Benefits of AFDS include:

- **Customizable Filters** – Configure AFDS's filters based on your business's processing trends.
- **Pending Review** – Prevent per-transaction fees by holding, reviewing and declining transactions prior to authorization.
- **Advanced IP Address Tools** – Allow or block transactions from specific IP addresses, regions and countries.
- **Suspicious Transaction Search** – Use unique filter-specific criteria to search for transactions that have triggered a filter.
- **Suspicious Transaction Reports** – Intuitive reporting allows you to research transactions that have triggered one or more filters.
- **Control Response to Customers** – Choose from standard customer responses or create your own response for transactions that have tripped one or more filters.
- **E-mail Notification** – Receive real-time e-mail notification each time a suspicious transaction triggers one or more filters.

How AFDS Works

AFDS includes multiple filters and tools that work together to evaluate transactions for indicators of fraud. Their combined logic provides a powerful and highly effective defense against fraudulent transactions.

+ **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, preventing high-volume attacks common with fraudulent transactions.
+ **Shipping-Billing Mismatch Filter** - Identify high-risk transactions with different shipping and billing addresses, potentially indicating purchases made using a stolen credit card.
+ **Transaction IP Velocity Filter** - Isolate suspicious activity from a single source by identifying excessive transactions received from the same IP address.
+ **Suspicious Transaction Filter** - Reviews highly suspicious transactions using proprietary criteria identified by Authorize.Net's dedicated Fraud Management Team.
+ **Authorized AIM IP Addresses** - Allows merchants 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.
+ **Enhanced AVS Handling Filter** - Customize how to handle transactions that return AVS mismatch codes, including the ability to decline or hold transactions for manual review. Allows you to protect your business from fraudulent transactions while saving legitimate orders from being rejected.
+ **Enhanced CCV Handling Filter** - Like the AVS Filter, customize how to handle transactions that return CCV response codes, including the ability to decline or hold transactions for manual review.
+ **Shipping Address Verification Filter** - Verify 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. This helps to determine whether or not the order is shipping to the country from which it originated.
+ **Regional IP Address Filter** - Flag orders coming from specific regions or countries. You can choose to customize the filter actions based on an entire geographic area, or select country by country how to process transactions flagged by the filter.

Authorize.Net also offers a new **Daily Velocity Filter** at no charge. The Daily Velocity Filter allows you to specify a threshold for the number of transactions allowed per day, a useful tactic to identify high-volume fraud attacks.

www.authorize.net
P.O. Box 8999, San Francisco, CA 94128-8999
Toll-free at 866-437-0491 E-mail: sales@authorize.net

Additional Recommended Resources

The Authorize.Net Document Library at http://www.authorize.net/resources/documentlibrary/ features several valuable white papers and reports.

+ The **Security Best Practices White Paper** details several payment gateway tools and recommended security practices for merchants to detect, prevent, and manage online transaction fraud.
+ The **Password Policy White Paper** provides critical information on protecting your account from unauthorized access by implementing a strong password policy.
+ The **CyberSource 2011 Online Fraud Report** is the industry's most respected online fraud study.

A video tutorial on setting up, and the benefits of using, AFDS is available in the Authorize.Net video library at http://www.authorize.net/videos.

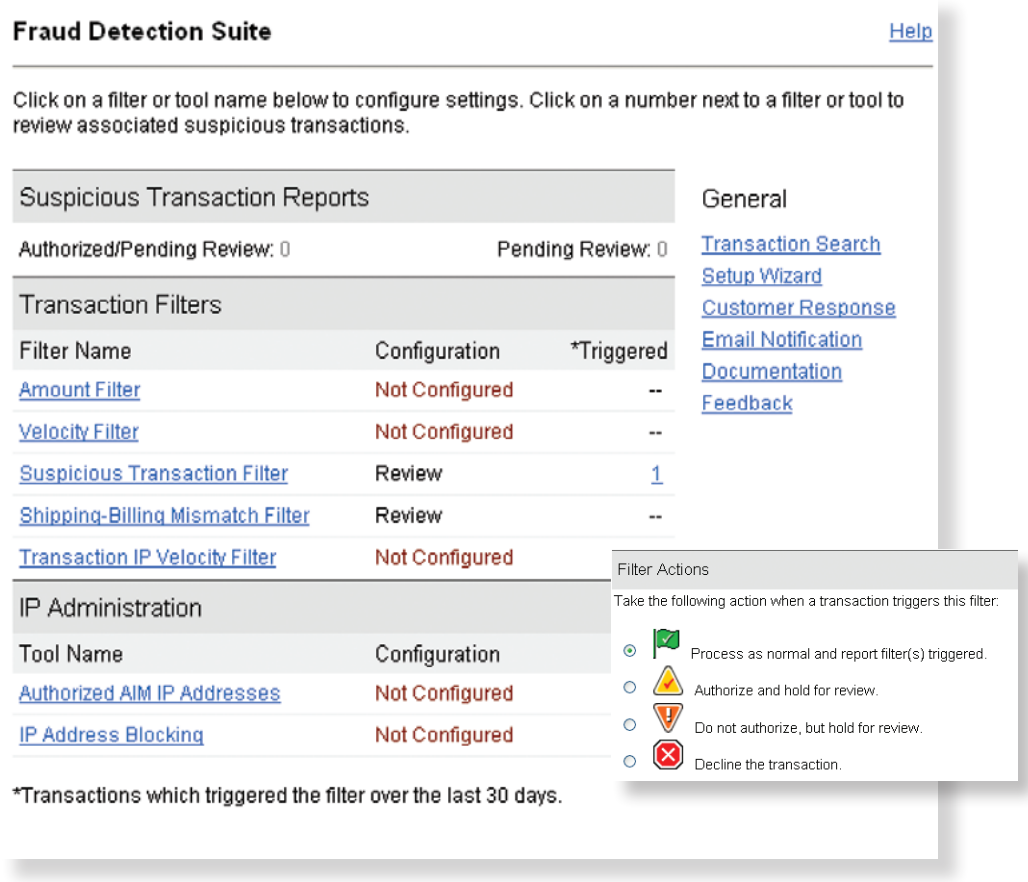
Conclusion

For too many merchants, online transaction fraud is far too real and devastating. Fraudsters are constantly working on new techniques to hone their craft which is why Authorize.Net is dedicated to providing merchants with tools like AFDS. It is essential that you take advantage of these tools to protect your business as carefully and strategically as possible.

By protecting your business today using every tool and best practice available to you, including the Advanced Fraud Detection Suite, you can help prevent becoming another statistic in the war against online transaction fraud.

www.authorize.net
P.O. Box 8999, San Francisco, CA 94128-8999
Toll-free at 866-437-0491 E-mail: sales@authorize.net

Authorize.Net®
a CyberSource solution



AFDS includes multiple filters and tools that work together to evaluate transactions for indicators of fraud. Their combined logic provides a powerful and highly effective defense against fraudulent transactions.

About Authorize.Net®

Authorize.Net, a CyberSource solution, provides secure, reliable, payment gateway solutions that enable merchants to authorize, settle and manage electronic transactions anytime, anywhere, via websites, retail, mail order/telephone order (MOTO) call centers and on wireless devices. Authorize.Net is sold through an extensive network of reseller partners and financial institutions that offer its industry leading payment services to their merchant customers.

www.authorize.net
P.O. Box 8999, San Francisco, CA 94128-8999
Toll-free at 866-437-0491 Email: sales@authorize.net

WP-FRAUD-0712