

# Fraud Detection Suite

## Protecting Your Business From Fraud

Fraud detection and prevention is crucial to maintaining a successful Web business. No merchant can afford to overlook the need for protection against fraud.

### The Fight Against Online Transaction Fraud

In the faceless world of the Internet, online transaction fraud is one of the greatest challenges for Web merchants. Advanced solutions are needed to protect merchants from the constantly evolving problem posed by fraud. The Fraud Detection Suite arms merchants with advanced filters and tools, providing them with a customizable solution to combat the most common types of online transaction fraud facing merchants today.

### All Merchants Are Potential Targets

Regardless of size, transaction volume or Internet expertise, all Web 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 Web 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, though essential, are limited as to the level of protection they can provide. Fraudsters have learned how to interpret AVS and Card Code Verification 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 Fraud Detection Suite.

(Continued on Page 2)

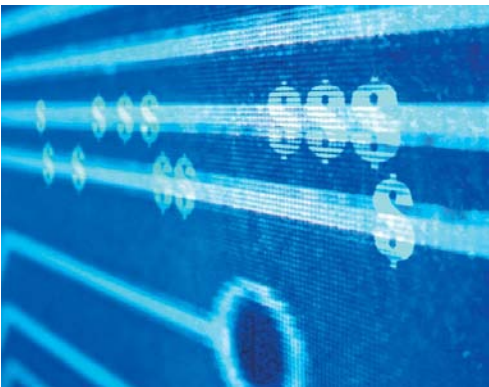


## Common Types of Fraud

Knowing what you're up against is the key to a strategic defense. Web 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 at a merchant's online store, they can determine whether that information is valid. At this point, they are not seeking financial gain, only information. But for merchants the repercussions can be costly.



### Settlement Fraud

Once fraudsters have a valid source of money, 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 the Fraud Detection Suite

In addition to using the standard security tools already built into the payment gateway, such as AVS and Card Code Verification, merchants can now implement an advanced fraud prevention solution. Complete with customizable filters and tools, the Fraud Detection Suite can provide merchants with a greater degree of control over the decision whether or not to accept a transaction, and could prevent costly authorization and chargeback fees, and the possible loss of inventory that often result from fraudulent transactions.

## Conclusion

Online transaction fraud is real. To an unprotected merchant the effects of fraud can be devastating. It is essential that merchants protect their online business as carefully and strategically as they would a retail store. In addition to industry standard security practices and verification tools, solutions such as the Fraud Detection Suite are necessary to provide advanced protection from online transaction fraud. Sign up today!



- + **Suspicious Transaction Reports** – Includes the ability for merchants to hold transactions for manual review, either before or after authorization.
- + **Customizable Filters** – Customizable settings allow merchants to configure their filters based on their processing trends, including four options for handling suspicious transactions.
- + **Advanced IP Address Tools** – Includes flexible tools enabling merchants to allow or block transactions from specific IP addresses.
- + **Quick Reports** – Simply click the hyperlinked number next to each filter to generate quick reports for transactions that have triggered one or more filters in the past 30 days.

### Fraud Detection Suite [Help](#)

Click on a filter or tool name below to configure settings. Click on a number next to a filter or tool to review associated suspicious transactions.

| Suspicious Transaction Reports  |                |                    | General<br><a href="#">Transaction Search</a><br><a href="#">Setup Wizard</a><br><a href="#">Customer Response</a><br><a href="#">Email Notification</a><br><a href="#">Documentation</a><br><a href="#">Feedback</a> |
|---|----------------|--------------------|---|
| Authorized/Pending Review: <a href="#">5</a> Pending Review: <a href="#">15</a> |                |                    |   |
| Transaction Filters   |                |                    |   |
| Filter Name   | Configuration  | *Triggered         |   |
| <a href="#">Amount Filter</a>   | Decline        | <a href="#">2</a>  |   |
| <a href="#">Velocity Filter</a>   | Review         | --                 |   |
| <a href="#">Suspicious Transaction Filter</a>                                   | Review         | <a href="#">15</a> |   |
| <a href="#">Shipping-Billing Mismatch Filter</a>                                | Review         | <a href="#">5</a>  |   |
| <a href="#">Transaction IP Velocity Filter</a>                                  | Not Configured | --                 |   |
| IP Administration   |                |                    |   |
| Tool Name   | Configuration  |                    |   |
| <a href="#">Authorized AIM IP Addresses</a>                                     | Not Configured |                    |   |
| <a href="#">IP Address Blocking</a>   | Enabled        |                    |   |

\*Transactions which triggered the filter over the last 30 days.

- + **Pending Review** – Prevent bank and payment gateway per-transaction fees by holding, reviewing and declining transactions prior to authorization.
- + **Suspicious Transaction Search** – Use unique filter-specific criteria to search for transactions that have triggered a filter.
- + **Control Response to Customer** – Allows merchant to choose from three standard customer responses or create their own response for transactions held for merchant review.
- + **Email Notification** – Receive real-time email notification each time a suspicious transaction triggers one or more filters.