



Minimize Risks with Effective Fraud Detection Tools

Fraud Detection Suite™ (FDS) is a set of customizable, rules-based filters and tools that identify, manage, and prevent suspicious and potentially costly fraudulent credit card transactions. You can customize FDS filters and tools to match your business needs and control how suspicious transactions are handled.

Reduce Losses

Online fraud costs merchants billions of dollars each year. With FDS you can reduce the impact of fraud on your business.

- Protect profits by recognizing legitimate transactions, rather than refusing business due to a fear of potential fraud.
- Minimize authorization and chargeback fees as well as inventory loss.

Flexible and Customizable Settings

FDS allows you to customize individual settings according to your unique business needs.

- Filter actions control how suspicious transactions are processed - approve, hold for review or decline.
- Authorize or restrict transaction activity from specific Internet Protocol (IP) addresses.

Easy-to-Use Features

FDS includes a number of features designed to simplify the management of suspicious transactions.

- A setup wizard guides you through the configuration process.
- Look up suspicious transactions using the FDS search feature.
- Customize the response to customers whose transactions trigger an FDS filter.
- Receive email notification each time a transaction triggers one or more filters.

Robust Fraud Detection Filters

FDS 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 fraudulent transactions often used to test the validity of credit card numbers.
- **Velocity Filter** - Limit the total number of transactions received per hour, preventing high-volume attacks common with fraud.
- **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 addresses.
- **Suspicious Transaction Filter** - Identify highly suspicious transactions using proprietary criteria identified by our 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.