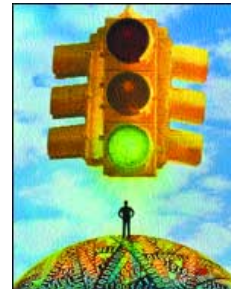


FRAUD AND RISK MANAGEMENT (FRISK)

The proprietary FRISK risk management system from CCNJ provides a sophisticated suite of fraud detection and prevention options. Each transaction submitted can be filtered through a comprehensive series of fraud detection rules to determine potential risk. Configuration of these rules is under your complete control using our user-friendly Online Merchant Center merchant administration web site.

The Fraud Protection utility within the CCNJ system allows you implement safety precautions when accepting mail order/telephone orders (MO/TO) or Internet transactions. Due to the inherent risk associated with these transaction types, it is recommended that you begin to develop a negative database to help you identify and prevent high-risk transactions.

This feature works with the automated Address Verification System (AVS) to help you avoid charge backs and fraudulent transactions. High-risk Customers can be disallowed from purchasing items based on credit card number, name, and country.



Fraud Protection Tools

- Credit Card Numbers - You may block any credit card you wish. You may look up credit card numbers of problem clients with the Account Management and Reports tools. Enter the credit card number exactly as it appears on the card or in a report. Click Add and the credit card will be added to your negative database and will be prevented from making future purchases.
- Name - Adding a customer name to your database is performed in the same manner as adding credit card numbers. Occasionally you may wish to add the name of a problematic company or customer to your list, so that they will be prevented from purchasing regardless of form of payment.
- Country - You can enable the blocking of orders from certain countries to which you do not wish to ship or accept credit cards. This feature may be very useful due to the limited recourse you may have legally and with credit card disputes originating from purchases made by foreign customers. To enable the blocking of a specific Country simply select that feature from the bottom of the Fraud Protection console and then use the arrow to the right of the entry box to scroll through the list of countries. When you have found the country you wish to block simply click on it. You may also type the abbreviations if necessary.

Automatic Merchant Fraud Protection

In addition to the merchant-initiated protection mechanisms described in this section, several automatic features have been incorporated into the Merchant Fraud Protection module to block out customers exhibiting suspicious buying behaviors, including -

- A feature to block a credit card that is submitted and declined twice within 24 hours using different expiration dates.
- A feature to check City and State entries for validity against the zip code entered.
- A feature to check area codes for validity against the zip code entered.

SSL Technology

The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on their SSL capabilities.

SSL comes in two strengths, 40-bit and 128-bit, which refer to the length of the "session key" generated by every encrypted transaction. The longer the key, the more difficult it is to break the encryption code.

Most browsers support 40-bit SSL sessions, and the latest browsers, including Netscape Communicator 4.0, enable users to encrypt transactions in 128-bit sessions - trillions of times stronger than 40-bit sessions.

Configuration of these rules is under your complete control using our user-friendly CCNJ merchant administration web site.

Credit Cards, NJ

p. 201.645.0132 | f. 201.490.5451

e. info@creditcardsnj.com | w. www.creditcardsnj.com

FRISK features

- Negative Account Blocking - Reject transaction from known fraudulent account numbers.
- Cramming Protection - Prevent the use of credit card or ACH number generating schemes by limiting the number of transactions allowed from a given IP address.
- Domain Blocking - Filter transactions by the Internet domain associated with the customer's email address.
- Country Blocking - Filter transactions by the Internet domain associated with the customer's country code.
- Prevent Duplicate Transactions - Track recent transactions to ensure the same transaction is not authorized more than once. This eliminates problems due to "double clicking" the transaction submit button as well as duplicate submittal of batch transactions.
- IP Activity Limit - Limit the number of accepted transactions from a given IP address.
- Large Transaction Notification - This feature examines the transaction amount after the transaction has been accepted. When the amount exceeds an amount specified by the merchant an e-mail is sent notifying the merchant that the amount has exceeded the threshold. The merchant can then review the transaction, refuse the sale before any products are shipped, and credit back the consumer at a later time.
- Address Verification (AVS) - AVS matches the known address information associated with the given credit card number against the billing address information provided by the user. If the information does not match, the transaction is declined. The merchant has the option of choosing the level of match required for an approved transaction.
- CVV2 - CVV2, or Card Verification Value 2, is a number that is printed, not imprinted, on Visa and MasterCard. This number is never transferred during card swipes and should only be known by the cardholder, the person holding the card in their hand.
- Reject Free Email Address - checks the e-mail address of the consumer against a database of free e-mail providers. Transactions in which the email domain of the consumer is in this database are declined.

Credit Cards, NJ

p. 201.645.0132 | f. 201.490.5451
e. info@creditcardsnj.com | w. www.creditcardsnj.com