

Internet Fraud Screening - Innovative Fraud Screening Tool (IFST)

With the increasing concerns over Internet credit card fraud, Innovative Gateway Solutions has developed special security measures which substantially reduce the likelihood that a merchant will receive a fraudulent credit card order.

Our Basic Innovative Fraud Screening Tool functions are applied automatically and included with all our services. Our system requires some parameters that make the process slightly more difficult to implement but considerably more functional in real protection of the merchant from Fraud.

IFST's design allows it to be applied to merchants by setting. A merchant, while defaulting to full security, may optionally not participate in all IFST functionality checks. Making a decision to not participate in all checks provided, while very unwise, is possible. In order to protect the systems some checks are applied system wide and the merchant is not allowed to opt out of them.

IFST was designed on the foundation of 16 basic checks and measures. These measures are listed in list a.

Innovative Fraud Screening Tool's Basic Functions (list a)

Check	Description
Credit Card Number (MOD 10) Validation	All cards are initially checked to be MOD 10 compliant
Required Data Field Checking (Based on settings set by the merchant)	Merchants are allowed to choose what parts of the AVS information they collect and check. The default is for all fields to be required. The type of information that merchants can ask for are : <ul style="list-style-type: none">• Address, City, State, Zip• Phone• EMail
Proprietary Data Encryption	The passwords are encrypted in the gateway databases and the merchant account name and password are encrypted in any cookies sent to the browsers of the merchant.
Credit Card Type Validation	Card number must match the type of card chosen
Negative Credit Card Screening. (Merchant can add individual entries)	Card numbers can be black listed by the gateway or by an individual merchant. Once they are black listed they can be excluded by all members of the gateway or by individual merchants.
Negative BIN Number Screening (Merchant can add individual entries)	BIN numbers are used for screening cards originating in countries that are issued in countries with unacceptable fraud rates

Duplicate Order Checking	No order can be a duplicate within a span of 2 min. This stops a hacker from entering the same transaction over and over without changing the basic information of the transaction.
E-mail Address Filtering	EMail addresses or email domains can be black listed by the gateway or by an individual merchant. Once they are black listed they can be excluded by all members of the gateway or by individual merchants.
Country Filtering	Country codes can be filtered by merchants to not allow any transaction from a country. This is based on the country code entered by the purchaser.
Area Code/State Matching Check	Area codes are matched to the state of the address. The merchant can choose to reject transactions when the area code does not match the state.
Zip Code/State Matching Check	Zip codes are matched to the state of the billing address. The merchant can choose to reject transactions when the Zip code does not match the state.
Internal Intrusion Detection System Built Around All Transaction Processes	Using a sophisticated array of hardware and software the gateway scans for intrusions by hackers that are posing as a user that they are not.
Multiple Login Checking For Abnormal Usage of Merchant Id	Fraud reports run daily and alert security staff when a merchant id is used for login from more than one domain or IP subnet. This allows the gateway to spot multiple logins being performed by a single user.
Velocity Checking (Built on historical averages and average ticket volume expected)	Fraud reports run daily that alert security staff when a single transaction is greater than or equal to the expected monthly volume of a merchant. This allows the merchant to look for charges that are unusually high but do not exceed the max. allowed by the gateway.
Required passwords	All transactions can only be run with valid passwords for the merchant. The password is used to keep hackers from guessing the merchant account name.
Random assignment of passwords and account names	The merchant account name and password are chosen by random systems at the time of setup. This keeps merchants from accidentally choosing a password or account name that is easy to guess.
Password difficulty	The passwords used by merchants must contain upper case, lower case and numerics
Password history	Passwords are stored historically in encrypted form so they can not be reused
Password expiration	Passwords automatically expire after 45 days. A warning is sent to the merchant so they change them before they expire so there is not interruption of service on transactions.
Multi-encryption method	All merchants are based on different encryption keys to protect against cross merchant hacking

In-active to active merchant change	Innovative Gateway Solutions fraud reports look for merchants that have been inactive and suddenly run multiple transactions
Amount screening	Transactions are not allowed to be run between the amounts of 1.00 and 2.00. These are common amounts used by hackers looking only to verify the card number.
Security logging	Innovative Gateway Solutions monitors all traffic. A log of all transactions is kept and a log of all security clearance requests is kept. The merchant can query their particular security audit report so they can determine if someone who is not authorized is signing on to use their account.
IP Address Filtering (Merchant can add their own entries)	IP numbers or subnets can be black listed by the gateway or by an individual merchant. Once they are black listed they can be excluded by all members of the gateway or by individual merchants. Merchant entries can not be excluded by the gateway as a whole unless the gateway security staff moves the excluded information to the excluded list. This is to protect against wide scale blocking and abuse of valid IP numbers.

Merchants can choose to perform various Address Verification Systems (AVS) checks prior to running the transaction. This process would allow the merchant to exclude transactions where any combination of the following rules were broken.

1. Match street address to zipcode
2. Match city to zipcode
3. Match zipcode to state
4. Match city to state

It is not advisable to use this process to halt transactions but if a merchant has a high incidence of fraud they may want to hold transactions for review that do not meet these 4 basic AVS checks.

In addition our systems have many robust tools designed to monitor activity on our systems. These are monitored 24 hours a day and you can sleep easy knowing our security team is watching your transaction processes.