

Checks performed by the Innovative Gateway Solutions fraud screening system

- Allows country ids to be blocked based on information entered by the user in their country code selections. Some country codes are also blocked by default by the Gateway. For information on this or to have a transaction allowed to one of these countries contact security@innovativegateway.com.
- Requires valid formatting of the Email address. Forces the use of name@domain with validity checks on the root domain.
- Screens IP numbers entered in the negative IP database. The gateway tracks known hacker IPs and allows the merchant to add IPs that they would also like blocked from their own site.
- Requires name for purchaser. If required by the merchant for address verification settings.
- Requires area code to exist in state entered. If required by the merchant for address verification settings.
- Requires zip code to exist in state entered. If required by the merchant for address verification settings.
- Duplicate transaction in last 2 min. If required by the merchant for address verification settings.
- Blocking of Post Authorizations that do not have a corresponding Pre Authorization in our systems. To do this the merchant must either use the merchant reports with the built-in buttons or submit a transaction that has the approval code and transaction codes from the Pre Authorization that is being Post Authorized.
- CVV2 standard. The verification is CVV2 certified and capable of using the CVV2 standard.
- Mod 10 check on card number. Simple check to ensure the credit card number is in an accurate range of possible numbers.
- Obscenity in any text entered.
- Blocking credits that do not have an exact match for previous transaction of the same value or more. This blocking mechanism works in the same manner as the pre authorization and post authorization process.
- The bank gets daily reports that show possible fraudulent transactions. Using these reports the bank can quarantine transactions and later release them once they have been verified. This prevents charge backs without interfering with the flow of money.
- The gateway monitors for multiple user ids being used from a single ip. When an attempt to login with more than one user id from the same ip is found the IP can be blocked by the gateway to prevent further hack attempts from this IP number.
- The gateway monitors for multiple IPs from different subnets using a single user id. When an attempt to login with more than one ip with the same user id is found the username can be blocked by the gateway to prevent further hack attempts using this name.
- The gateway tracks all data posted to its servers for review. This allows the systems to capture data for analysis that was not intended to be used for transaction processing.
- Force connection from 128bit cipher strength SSL to all servers outside of the main website.
- The gateway gives the merchant the ability for to block any of the information listed above for their entries, for the their entries plus the gateway entries, or for all entries in the system including those entered by other merchants.
- Merchants must register the IPs of the servers that will connect to the gateway servers for running transactions against their merchant account. The gateway allows eight by default but the merchant can request others be added.
- Merchant must register a phrase for use in retrieving lost passwords. This prevents others from easily impersonating the merchant and changing the password to something the merchant does not know.

- Passwords are randomly assigned at setup and expire every 45 days. These passwords must be at least 9 digits in length, contain uppercase, lowercase and numeric characters.
- No reports contain the full credit card number. Only the first 10 digits are given in the reports. This must be combined with the emails sent to the merchant as verification to get the full credit card number of any transaction. The merchant is expected to track the credit card numbers on their systems if they need them.
- The most sensitive functions of the merchant require a login even if the merchant is already logged in. This prevents a malicious internal employee from obtaining or changing information when a user is logged in but away from their desk.
- Historical data is kept online for six months and is then moved to offline servers for archival. Reports can be obtained from this historical data by emailing archives@innovativegateway.com with a request for the report needed.

Planned enhancements to the fraud screening system

- Certificate level authentication of machine connecting to the gateway transaction processes and merchant menus
- Ability for merchants to force a transaction failure when AVS information is incorrect