FRAUD PROTECTION TOOLS AND PROCESSING CONTROLS

Fraud Protection is an integral and built-in piece of the eProcessing Network secure product offering. ePN is committed to providing secure systems and payment applications that meet or exceed compliance with the Payment Card Industry Data Security Standards (PCI-DSS). We believe it to be so essential, that it’s included with every type of merchant gateway account our company offers, because you can never put a price on peace-of-mind.

Benefits for your Business

- AVS, or Address Verification System verifies whether the Street address and Zip code entered by your customer is the same as what the cardholder’s issuing bank has on file.
- CVV2/Card Verification Code lets a merchant verify that the cardholder does in fact have the card in his or her possession.
- Block Specific Integrations - allows merchants to specify which integration types to allow (i.e. Web Order Forms, TDBE/API, Shopping Carts, etc.).
- Disable Refunds - allows merchants to specifically decline any refunds coming from an API.
- Block specific IP Addresses - merchants can restrict all access to the TDBE/API or Authorize.Net™ integration.
- Velocity Controls - allows merchants to specify the maximum number of approved or declined transactions per IP address within a specified time period (i.e. minutes). This feature deters hackers and fraudsters from using your website to test a list of stolen or fraudulent credit card numbers.
- Customized Control - allows merchants to determine if a transaction should be handled as a ‘Sale,’ ‘Auth Only’ or ‘Auth Convert’.
- Convert transactions - allow transactions to convert automatically to ‘Sale’ (or leave as ‘Outstanding’) depending on (18) different AVS and (6) CVV2 criteria.

For more information on Fraud Protection Tools and Processing Controls, visit us online at eProcessingNetwork.com