Security “Best Practices” White Paper

Introduction

Suspicious Internet transactions come in many forms and require proactive measures to detect, prevent, and manage. The Payment Gateway recommends some best practices in suspicious transaction detection, prevention, and management that are currently available to you in the Payment Gateway tool set.

Best Practices

- **Connect to the Payment Gateway using Advanced Integration Method (AIM) (previously known as ADC Direct Response).** The Payment Gateway promotes Advanced Integration Method (AIM) (previously known as ADC Direct Response) as the preferred connection method for processing transactions. Using AIM, you can connect your server directly to the system’s gateway server to process transactions in real-time. With proper use of this method, you can retain full control of the data that is used in the processing of the transaction, and keep the customer on your own Website during the entire transaction. Please note that, in order to implement AIM effectively, it is recommended that the scripts responsible for submitting sensitive account information to the Payment Gateway (i.e., your Login ID and password) be stored on a server separate from the one that hosts your payment form and other Web pages.

  If you are currently using the WebLink or Relay Response connection methods, you are strongly encouraged to convert to AIM or Simple Integration Method (SIM). Released in part to accommodate for the eventual discontinuation of WebLink and Relay Response, SIM is an increased security option for merchants that cannot easily establish a secure sockets layer (SSL) connection to the Payment Gateway. Please refer to the AIM/SIM Conversion Guide for more information about converting to a new connection method.

- **Consider using an alternative hosting solution.** If you cannot easily integrate to the AIM or SIM connection methods, you should seriously consider using an alternative web hosting solution. Authorize.Net-certified shopping carts are an ideal solution because they meet the highest security standards for submitting transactions to the Payment Gateway. Using an Authorize.Net-certified shopping cart allows you to submit transactions securely without having to upgrade web systems and security. View the list of Authorize.Net-certified shopping carts at http://www.authorize.net/alliances/carts.php.

  You may also consider using HyperMart’s QuickCharge solution. QuickCharge allows you to use a HyperMart-hosted payment form for collecting payment information, and submits transaction information securely and directly to the Payment Gateway. For more information about QuickCharge, please see HyperMart’s QuickCharge FAQ at http://www.hypermart.net/t/quickcharge/faq.

- **Change your Payment Gateway password on a regular basis.** Your password should be at least six characters long, contain upper and lowercase characters, and contain at least one number. It is confidential and should be shared only with those who have a need to access your Payment Gateway account. You can change your Payment Gateway password at any time by selecting "Change Password" in the Security section of the Merchant Interface Settings menu.

- **Implement standard Internet transaction screening tools (such as Address Verfication System (AVS) and Card Code Verification).** These two tools are standard industry practices and will greatly assist you in combating suspicious transactions (see below for more information).

- **Implement the proper security settings for your connection method.** Your Payment Gateway account includes built-in security features customized for each connection method, such as Referrer URLs or Password-Required Mode. These features should be used appropriately in conjunction with your connection method to optimize the security and performance of your account (see below for more information).

- **Monitor your batches.** You should always be aware of the transactions that are being processed through your account. Know the time that your transactions are settled and always review transactions before settlement occurs. Monitor unsettled transactions and void any suspicious transactions on your account. Constant monitoring is the first step in the detection of suspicious transaction activity.

- **Be suspicious of transaction amounts that are not in the usual range of your customers' average ticket.** Suspicious transactions may consist of random amounts ranging from one dollar to thousands of dollars. Amounts are typically whole numbers and are multiples of 1, 10 or 100. Carefully monitor your account for this type of activity and void any transactions you find suspicious for your business.

- **Monitor all international transactions.** Be aware of the differences between international and domestic transactions and pay special attention to all international transactions. Information passed with an international transaction (such as the format of a cardholder's address) differs from the information passed with a domestic transaction.

  Note: Some tools, such as the AVS Filter, do not screen international transactions, therefore, manual monitoring is highly recommended.

Standard Features Offered to All Merchants

- **Card Code Verification.** Card Code (CVV2/CVC2/CID) is a three-digit security code that is printed on credit cards. The value appears in reverse italic at the top of the signature panel on the back of the card, or on the front of the card just above the end of the credit card number. These additional numbers provide an extra measure of security against unauthorized credit card transactions. The credit card would need to be present for the purchaser to know the Card Code number, as it is not stored on any system outside of the credit card issuer. The Payment Gateway allows you to customize your account so that the system rejects transactions where the Card Code provided by the cardholder is invalid. By using Card Code verification, you are able to make a more informed decision about whether to accept a particular credit card transaction.

More information is available through the Merchant Interface Online Help Files and the Implementation Guides in the Documentation and Reference Guides section of the Help Menu.

- **Address Verification System (AVS).** Address Verification System (AVS) compares the billing address information provided by the customer online with the billing address on file at the customer's credit card issuing bank. The Payment Gateway reports the AVS response code to you, the Merchant, (match or no match) and, after screening for the AVS response codes that you have chosen to allow pass through the system, accepts or rejects transactions accordingly.

  Note: AVS does not screen international transactions. If the customer's credit card issuing bank is of non-US origin, it is not supported by AVS.

  More information is available through the Merchant Interface Online Help Files and the Implementation Guides in the Documentation and Reference Guides section of the Help Menu.

- **Referrer URLs (REQUIRED).** A Referrer URL is any Web page address from which your site processes its Authorize.Net transactions. In other words, if your customer links to the Payment Gateway's secure Payment Form from a certain page on your site, you will designate the URL *for that particular page* (e.g., https://www.mywebsite.com/paymentform.html) as a Referrer URL. This URL must be listed in the "Referrer URLs" area of the Merchant Interface. The Payment Gateway then will reject attempts to process transactions from any other URL. The Payment Gateway allows you to specify multiple Referrer URLs.

  Note: Referrer URLs are *required* for all Merchants who connect to the Payment Gateway via the WebLink connection method. DO NOT use this feature if you connect via Advanced Integration Method (AIM) (previously known as ADC Direct Response) or Simple Integration Method (SIM). To use the Referrer URL feature in conjunction with a shopping cart, please contact your shopping cart provider to verify that they are not using Advanced Integration Method (AIM) or Simple Integration Method (SIM) to connect to the Payment Gateway.

  More information is available through the Merchant Interface Online Help Files and the Implementation Guides in the Documentation and Reference Guides section of the Help Menu.

- **Password-Required Mode.** Password-Required Mode is a highly recommended (and eventually will be a required) security feature for any Merchant who uses the Advanced Integration Method (previously known as ADC Direct Response) or Simple Integration Method (SIM) to process transactions through the Payment Gateway. When an account is designated as Password-Required, no transaction can be processed without initially providing the account password. This mode prevents transactions from being completed with only the Login ID.

  Note: DO NOT use this feature with the WebLink connection method. To use Password-Required Mode in conjunction with a shopping cart, please contact your shopping cart provider and have them enable your cart to pass your Payment Gateway password (or fingerprint for SIM) with every transaction.

More information is available through the Merchant Interface Online Help Files and the Implementation Guides in the Documentation and Reference Guides section of the Help Menu.

Additional Suspicious Transaction Detection and Prevention Tools

The Payment Gateway offers a wide range of prevention and detection tools. Some of these tools are included in the standard Payment Gateway and others are additional services that may be subscribed to in order to further help you prevent, manage, and detect suspicious transactions. (These services are provided at an extra charge.)

- **Transact-Secure** (http://www.authorizenet.com/support/transact-secure.php)
  The Transact-Secure solution prevents purchaser identification fraud by empowering you, the Merchant, to automatically perform real-time multi-tiered authentication of the purchaser’s identity during checkout. Fraudsters are prevented from committing credit card and eCheck.Net fraud during checkout, and purchasers are prevented from committing “friendly fraud” by later denying their transactions. Every transaction authenticated by Transact-Secure is guaranteed up to $5,000.00. In the event that a transaction results in ID fraud, the Merchant will be reimbursed 100% of the transaction.

- **FraudScreen.Net** (http://www.authorizenet.com/support/fraudscreen.php)
  The FraudScreen.Net service is powered by HNC’s eFalcon product. HNC is the industry leader in transaction fraud scoring. HNC utilizes dozens of online, offline, and positive and negative databases to score each transaction (0 - 1000) for the probability of fraud. This service enables Merchants to set a rejection threshold for transactions based on a real-time score returned from the Payment Gateway.

Some Standard Computer Security Best Practices

Listed below are some standard computer industry security best practices.

- **Install a Firewall.** Firewalls are special servers that monitor the activity of external connections, primarily the Internet, to an internal network of servers. Firewalls help to eliminate the threat of any undetected external activity, and safeguard your network and connections from outside vulnerabilities.
- **Store all sensitive or confidential information separate from Web servers.** Customer information in particular, such as credit card numbers, should be stored in a secure database on a server that is not connected to the Internet. It is also a good idea to encrypt all stored information.
- **Use good Anti-virus software and update it regularly.** Anti-virus software is another important way to protect your network and computer systems from outside vulnerabilities. This software should be updated on a regular basis.
- **Regularly download and install security updates.** For server and individual computer operating system software, you can optimize performance and systems protection by maintaining compatibility with service and security updates. Remember also to reinstall service and security updates when reinstalling software.

- **Avoid file sharing.** Share access to network drives and individual computers only with needed, trustworthy users. Especially avoid sharing access to files that store passwords and other confidential or sensitive information
- **Avoid idle Internet connections.** Disconnect when you are finished using the Internet. This also eliminates the possibility of undetected outside vulnerabilities.