White Paper

Authorize.Net
a CyberSource solution

Security Best Practices

Maintaining tight security, including using both standard and advanced fraud detection and prevention tools, is crucial to maintaining a successful business. No merchant can afford to overlook the need for protection against fraud and other types of abuse. This document details the tools and security best practices that Authorize.Net recommends to merchants for detecting, preventing, and managing transaction fraud.

Built-In Fraud Prevention Tools

Several basic fraud prevention tools are included with your payment gateway account. It is strongly recommended that you use and customize these essential tools as well as implement adequate fraud detection and prevention policies and practices within your business to protect your account from transaction fraud.

Warning: Failure to adequately implement fraud prevention tools could result in losses for your company. Settings for standard account security tools must be properly implemented. For questions or assistance establishing your fraud prevention settings, please contact Authorize.Net Customer Support.

Address Verification Service

The Address Verification Service (AVS) is a security system designed to combat one of the most common forms of online credit card fraud. AVS compares the billing address information provided by the customer with the billing address on file at the customer's credit card issuer. The payment gateway receives an AVS response code and then either accepts or declines the transaction according to your configured settings.

More information on AVS is available in the Address Verification Service help file located in the Merchant Interface Online Help Files.

Card Code Verification

A customer's card code is a three- or four-digit security code printed on a credit card's signature panel in reverse italics, or following the full number on the front of the card. Similar to AVS, Card Code Verification (CCV) compares the customer's card code with the card code on file at the credit card issuer. The payment gateway receives the card code verification response code from the customer's bank and either accepts or declines the

transaction according to your configured settings. Since the card code should only be known to the person in possession of the physical credit card, these additional numbers provide an extra measure of security against unauthorized credit card transactions.

More information is available in the Card Code Verification help file located in the Merchant Interface Online Help Files.

Multiple User Accounts

The Multiple User Accounts feature allows you to strengthen account security and streamline transaction management by creating unique user accounts with distinct login IDs and passwords for each employee who accesses the Merchant Interface. Each user's account is assigned a specific set of permissions or actions that the user is permitted to perform within the Merchant Interface. These permissions restrict access to Merchant Interface features on a need-to-use basis, making business operations more secure and efficient.

WebLink Best Practices

WebLink is a legacy integration method and is no longer fully supported by Authorize.Net. If you are using WebLink to connect to the Authorize.Net Payment Gateway, it is strongly recommended that you convert to using either the Advanced Integration Method (AIM) or Simple Integration Method (SIM). Both offer increased security options and customization.

However, if you prefer to continue using WebLink as your integration method, you should apply the following best practices specific to the WebLink connection method.

+ Referrer URLs – A Referrer URL is a required security feature in order to process transactions via WebLink. A Referrer URL is the authorized Web page address from which transactions are submitted to the payment gateway from your Web site (for example, https://www.merchantyourwebsite.com/paymentform.html). All URLs from which you submit transactions must be listed on the "Referrer URLs" page of the Merchant Interface. The payment gateway will reject transactions from unlisted URLs.
+ Password-Required Mode – The Password-Required Mode setting is not compatible with WebLink. It should be turned off for your account in order to successfully submit transactions to the payment gateway.

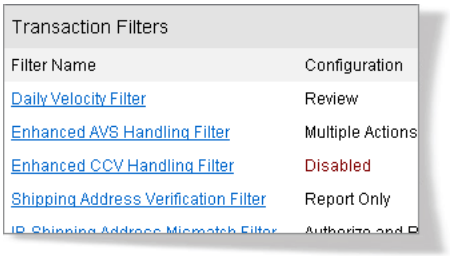
More information is available in the Merchant Interface Online Help Files.

Password-Required Mode

Password-Required Mode is a required security setting for merchants who submit transactions via AIM, SIM, or exclusively via Virtual Terminal or Batch Upload. When placed in Password-Required Mode, the payment gateway requires an authentication value for each transaction submitted for your payment gateway account. Any transaction submitted without proper authentication will be rejected by the payment gateway.

If you integrate to the payment gateway via a shopping cart or third party solution, please contact your solution provider to confirm that you are passing your payment gateway transaction key or fingerprint with every transaction.

More information is available in the Password-Required Mode help file located in the Merchant Interface Online Help Files.



Advanced Fraud Detection Suite™

Regardless of size, transaction volume or experience, all Web merchants are susceptible to various types of online transaction fraud. In addition to using the standard security tools already built into the payment gateway, you can implement more advanced fraud prevention solutions to further protect your account from fraudulent transactions.

Advanced Fraud Detection Suite (AFDS) is a low-cost, rules-based set of powerful filters and tools that allow you to identify, manage, and prevent suspicious and potentially costly fraudulent transactions. The AFDS filters and tools listed below can be customized to match your business needs and combat the most common types of online credit card fraud.

- Amount Filter – Uses lower and upper transaction amount thresholds to restrict high-risk transactions often used to test the validity of credit card numbers.
- Velocity Filter – Limits the total number of transactions received per hour, preventing high-volume attacks common with fraudulent transactions.
- Shipping-Billing Mismatch Filter – Identifies high-risk transactions with different shipping and billing addresses, potentially indicating purchases made using a stolen credit card.
- Transaction IP Velocity Filter – Isolates suspicious activity from a single source by identifying excessive transactions received from the same IP address.
- Suspicious Transaction Filter – Reviews highly suspicious transactions using proprietary criteria identified by Authorize.Net's dedicated Fraud Management Team.
- Authorized AIM IP Addresses – Allows merchants submitting AIM transactions to designate specific server IP addresses that are authorized to submit transactions.
- IP Address Blocking – Blocks transactions from IP addresses known to have been used in fraudulent activity.

AFDS is an extremely affordable and easy-to-implement option to help prevent costly transaction fraud from occurring on your account. You can sign up for AFDS through the Merchant Interface or call Sales Support at 866-437-0476. For more information, see the AFDS White Paper at http://www.authorizenet.com/files/fdswhitepaper.pdf or the AFDS Case Study at http://www.authorizenet.com/files/CS_FDS_0305.pdf.

Additional Best Practices

Adhere to the PCI Data Security Standard Requirements

The Payment Card Industry (PCI) Data Security Standard is an industry-wide program designed to significantly increase security for storing, transmitting, and processing cardholder data. To maximize your security, it is recommended that you thoroughly review and adhere to PCI requirements. For more information about the PCI Data Security Standard, please see http://www.usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html?it=l2|%2Fbusiness%2Faccepting_visa%2Fops_risk_management%2Fcisp_service_providers%2Ehtml|Merchants.

Since Authorize.Net is not directly involved with establishing, evaluating or validating merchant PCI compliance requirements, we have partnered with AmbironTrustwave, a leading provider of information security and compliance management solutions. Trustwave offers convenient PCI tools and validation services at a specially discounted price to Authorize.Net merchants. To register for AmbironTrustwave services, please visit http://authorizenet.trustkeeper.net.

To learn more about the different levels of PCI compliance and about Trustwave's services, please see http://www.atwcorp.com/pciDataSecurityStandard.php.

Connect to the Payment Gateway Using AIM

AIM is the preferred connection method for processing transactions. AIM allows you to host your own secure payment form and submit transactions to the payment gateway using an end-to-end secure sockets layer (SSL) connection. If you do not have an SSL certificate, Authorize.Net has partnered with Comodo, Inc., to offer SSL certificates to Authorize.Net merchants at a discounted price. For more information, please go to http://www.authorize.net/solutions/merchantsolutions/merchantservices/sslcertificates/.

If you are currently using WebLink to submit transactions to the payment gateway, you are strongly encouraged to convert to AIM. For more information on AIM, please see the Connection Methods Guide located at http://www.authorize.net/files/connectionmethodsguide.pdf.

Consider Using a Certified Third-Party Solution

If you cannot easily integrate to the payment gateway using AIM or SIM, you should seriously consider using a certified third-party solution, such as a certified shopping cart. Authorize.Net certified third-party solutions maintain the highest security

standards for submitting transactions to the payment gateway and allow you to submit secure transactions without having to do a lot of development and integration work yourself. View the list of Authorize.Net certified third-party solutions at http://www.authorize.net/cscdir.

Regularly Change Your User Account Password and Secret Question and Answer

You can significantly strengthen your payment gateway user account security by changing your password and secret question and answer at least every 45-60 days. Both your password and your secret answer are used to safeguard your user account and should NOT be shared with anyone.

For more information on password security, see our Password Policy White Paper at http://www.authorize.net/resources/files/PasswordPolicy.pdf.

Maintain Your API Login ID and Transaction Key Security

An account API Login ID and Transaction Key are required to process transactions through your payment gateway account.

- The API Login ID validates a merchant's access to submit transactions to the payment gateway.
- The Transaction Key is similar to a password and is used to authenticate transactions submitted from authorized users.

Because your API Login ID and Transaction Key are highly sensitive security values that allow you to submit transactions to the payment gateway, they should be not be shared with anyone and should be stored securely. Your Transaction Key should be changed regularly to further strengthen the security of your account.

If you have reason to believe that your API Login ID has been compromised, or you suddenly experience an unusual amount of suspicious transaction activity, call Customer Support at 877-447-3938 immediately to have it reset. You will need to update your Web site integration with the new API Login ID immediately to avoid a disruption in your transaction processing.

More information is available in the API Login ID and Transaction Key help file located in the Merchant Interface Online Help Files.

Require Complete Order Information

Although a customer may legitimately submit different billing and shipping information, such informational discrepancies can indicate a fraudulent transaction. Therefore, consider requiring complete order information, e.g., a full address and phone number, and be cautious about accepting orders with different shipping and billing addresses or urgent shipping instructions. Do everything you can to validate the order before processing, even if it means calling the customer for confirmation.

You can automate this fraud prevention process by signing up for AFDS and configuring the Shipping-Billing Mismatch Filter.

Monitor Your Transactions

Constant monitoring is the first step toward detecting suspicious transaction activity, particularly if you accept international transactions. It is highly recommended that you regularly review transactions, monitor unsettled transactions, and void any suspicious transactions before your account's daily transaction cut-off time. Be especially aware if your account receives a higher-than-usual number of transactions, transactions with random amounts ranging from one penny to thousands of dollars, or transactions with differing billing and shipping addresses. These types of transaction activity can be a signal that online credit card fraud is being attempted against your account. If you suspect this is the case, place your account in Test Mode or contact Customer Support for additional help.

You can automate several of these transaction monitoring processes by signing up for AFDS and configuring the Amount, Velocity and Transaction IP Velocity Filters.

Computer Security Best Practices

The following standard computer security best practices can further protect your transactions and business.

Install a Firewall

A firewall is a hardware or software solution that monitors the activity of external connections (primarily the Internet) to an internal network of servers. Firewalls help to eliminate unauthorized or unwanted external activity and safeguard your network and connections from outside threats.

Store All Sensitive or Confidential Information Separate from Web Servers

For maximum information security, you should never store sensitive customer information, such as credit card numbers. If for some reason it is necessary to store this data, do so in a secure, encrypted database on a server that is not connected to the Internet. If sensitive information is stored in hard copy, thoroughly shred and dispose of the information on a regular basis.

Use Anti-Virus Software and Update It Often

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

Software performance and security can be optimized by installing all service and security updates. If you ever need to reinstall your software, remember to reinstall all updates.

Authorize.Net®
a CyberSource solution

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 Sending or Requesting Confidential Information via Insecure Methods

As a standard security practice, legitimate businesses will never request confidential information (such as credit card information or passwords) from you in an e-mail or online chat session. Your business should also never request or submit confidential information via e-mail or other insecure methods. If you receive a communication requesting you to submit confidential information in an insecure manner, always call the soliciting business to confirm the request before responding.

Helpful Web Sites

Authorize.Net recommends that you regularly visit the Web sites listed below to remain current with the latest fraud prevention best practices and resources.

- Authorize.Net Fraud Prevention Center: http://www.authorize.net/resources/fraudprevention/
- Federal Trade Commission: http://www.ftc.gov/bcp/edu/microsites/idtheft/business/index.html
- U.S. Department of Justice: http://www.usdoj.gov/criminal/fraud/internet/
- Better Business Bureau: http://www.bbbonline.org/
- Internet Crime Complaint Center: http://www.ic3.gov/
- Identity Theft Resource Center: http://www.idtheftcenter.org

About Authorize.Net®

Authorize.Net, a CyberSource solution, provides secure, reliable, payment gateway solutions that enable merchants to authorize, settle and manage electronic transactions anytime, anywhere, via websites, retail, mail order/telephone order (MOTO) call centers and on wireless devices. Authorize.Net is sold through an extensive network of reseller partners and financial institutions that offer its industry leading payment services to their merchant customers.

www.authorize.net
P.O. Box 8999, San Francisco, CA 94128-8999
Toll-free at 866-437-0491 E-mail: sales@authorize.net

WP-SECBP-0712