White Paper

Authorize.Net
a CyberSource solution

Developer Security Best Practices

The importance of strong security cannot be overvalued for any successful business. A security breach can result in significant financial loss, irreparable damage to reputation or worse.

Information security should therefore be of the utmost concern when developing computer applications that handle, process, or store consumer information. This document provides information about payments industry security initiatives and other best practices that are recommended to developers for incorporating the highest levels of data protection in their various payment applications.

Payments Industry Security Initiatives

The Card Associations employ stringent data protection compliance requirements for merchants and merchant service providers, including businesses or other parties that provide payment processing solutions to merchants. Two specific programs, the Payment Card Industry (PCI) Data Security Standard and the Payment Applications Best Practices (PABP), are vital to the long term success of your business. Authorize.Net encourages you to read the following sections thoroughly so as to understand both PCI and PABP and their specific requirements for you and your merchants.

Payment Card Industry (PCI) Data Security Standard

The PCI Data Security Standard is an industry-wide program implemented in December 2004 that incorporates the various cardholder security programs previously created by Visa, MasterCard, Discover, and American Express. PCI is designed for merchants and merchant service providers (including developers) that handle, process, and/or store cardholder information. Recognizing that a merchant's security needs vary according to its size and the number of transactions it processes, the PCI Data Security Standard has been divided into separate levels of required merchant and developer compliance.

To support your efforts to optimize security, Authorize.Net has partnered with TrustWave, a leading data security and compliance services provider that offers convenient and affordable PCI compliance tools. For more information about TrustWave's services and

pricing options, please visit http://www.authorizenet.trustkeeper.net. You will need to register in order to log in. You can also learn more about the required levels of PCI compliance at http://www.atwcorp.com/pciDataSecurityStandard.php.

To optimize security and reliability, Authorize.Net strongly recommends that all merchants and service applications strive to become compliant with the PCI Data Security Standard.

Please note that the following information is only a summary of the PCI Data Security Standard requirements. This information is not comprehensive and should not be substituted for official PCI documentation. For more information about the PCI Data Security Standard, see https://sdp.mastercardintl.com/pdf/pcd_manual.pdf or http://www.usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|Service%20Providers.

Build and Maintain a Secure Network

Requirement 1 - Install and maintain a firewall configuration to protect data

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.

Requirement 2 – Do not use vendor supplied defaults for system passwords and other security parameters

When installing any system on a network you should change the vendor-supplied default passwords. Using strong passwords that are difficult to guess or generate can significantly decrease the chances of confidential information becoming compromised. For additional information about password security, please read the Authorize.Net Password Policy White Paper at http://authorize.net/upload/images/Files/White%20Papers/PasswordPolicy.pdf/.

Protect Cardholder Data

Requirement 3 - Protect stored data

Ideally, storing sensitive customer information should be avoided. However, if you must store this information, it should be encrypted or masked in a secure database on a server that is not directly connected to the Internet. Remember that the payments industry requires certification of security compliance of all service providers and merchants that store or process sensitive customer information.

Requirement 4 - Encrypt transmission of cardholder data and sensitive information across public networks

All sensitive information must be encrypted when transmitted over the Internet. To protect communications, it is highly recommended that you use at least a 128-bit Secure Sockets Layer (SSL) digital certificate. Confidential information such as

cardholder data should never be sent via unencrypted e-mail or communicated using other insecure methods.

Maintain a Vulnerability Management Program

Requirement 5 - Use and regularly update anti-virus software
Using anti-virus and spyware software is an important way to protect your network and computer systems from outside threats. This software should be updated on a regular basis.

Requirement 6 – Develop and maintain secure systems and applications
Optimize performance and systems protection by maintaining compatibility with service and security updates and patches. Remember also to reinstall service and security updates when reinstalling software or restoring backed-up drives.

Implement Strong Access Control Measures

Requirement 7 – Restrict access to data by business need-to-know
Share access to network drives and individual computers only with trustworthy users on a need-to-know basis. Especially avoid sharing access to files that store passwords and other confidential or sensitive information.

Requirement 8 – Assign a unique ID to each person with computer access
To prevent unauthorized access to sensitive information, make sure that all user access is authenticated or password-protected. User login IDs and passwords should be encrypted and stored in a secure location.

Requirement 9 – Restrict physical access to cardholder data
Be sure hard copies of sensitive information are securely stored and locked in the appropriate storage rooms, file cabinets, and desk drawers. Restrict all access to hard copy files to a need-to-know basis.

Regularly Monitor and Test Networks

Requirement 10 – Track and monitor all access to network resources and cardholder data
Create and record an audit trail of all individual access to cardholder data and other sensitive information. This audit trail should cover a period of at least one year (the most recent 12 months).

Requirement 11 – Regularly test security systems and processes
Frequently test the functionality of your security setup (controls, restrictions, connections). Check your entire network for vulnerabilities at least once a quarter and after installing new software or otherwise changing the network.

Maintain an Information Security Policy

Requirement 12 – Maintain a policy that addresses information security
Create a security policy for employees to follow that is specific and understandable. This policy should be reviewed by all staff at least once a year.

Payment Applications Best Practices

Though Authorize.Net highly recommends that all merchant service providers comply with PCI, compliance is not generally required of most payment applications vendors and developers. However, Visa recognizes that payment applications are a key component of data security and has therefore developed the Payment Applications Best Practices (PABP)—a set of 13 industry security standards that assist software vendors with creating and maintaining secure payment applications. While PABP is not yet required by the payments industry, it is anticipated that it will be in the near future. Therefore, it is highly recommended that you comply with the practices listed below.

To help you increase the data security of your payment applications Authorize.Net has partnered with AmbironTrustWave to offer low rates to our affiliated software vendors for PABP compliance validation. Vendors that complete the validation process are listed on Visa's website as certified payment applications. To learn more about the PABP validation process, please see http://www.atwcorp.com/pabp/authorizenet.

Please note that the following information is only a summary of PABP standards. This information is not comprehensive and should not be substituted for official PABP documentation. For more information about PABP compliance, please see Visa's site at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_Payment_Application_Best_Practices.pdf?it=c|/business/accepting_visa/ops_risk_management/cisp_payment_applications%2Ehtml|Payment%20Applications%20Best%20Practices.

1. Do not retain full magnetic stripe or CVV2 data
Do not store sensitive authentication data after transaction authorization (not even if encrypted).

2. Protect stored data
Mask sensitive cardholder data when displayed and when stored. Protect encryption keys against disclosure and misuse, and implement key management processes and procedures, including the generation, distribution, management, and storage of secure keys.

3. Provide secure password features
Require a unique username and complex password for all users with access to computers, servers, and databases with payment applications, including administrative access and especially access to cardholder data. Application passwords should be complex and if possible, encrypted.

4. Log application activity
Log all computer and network access by individual users, and implement functionality to link those activities to individual users. Implement an automated audit trail to track and monitor access.

5. Develop secure applications
Develop Web software and applications based on secure coding guidelines and industry best practices. Emphasize information security throughout the software development life cycle and routinely review custom application code to identify possible vulnerabilities.

6. Protect wireless transmissions
Securely encrypt all wireless transmissions of cardholder data over both public and private networks.

7. Test applications to address vulnerabilities
Establish a process to regularly test applications and identify potential security vulnerabilities. Develop and deploy security patches in a timely and secure manner.

8. Facilitate secure network implementation
Implement payment applications in a secure network environment. The applications should not interfere with the use of network address translation, port address translation, traffic filtering network devices, anti-virus solutions, patch or update installation, or hardware or software encryption.

9. Cardholder data must never be stored on a server connected to the Internet
Do not configure a database server and Web server to reside on the same server or in the "demilitarized zone" (DMZ) with the Web server.

10. Facilitate secure remote software updates
If software updates are delivered via remote access into customers' systems, instruct customers to provide access to the system only when needed and to disable the connection immediately after downloads are complete. Alternatively, if delivered via virtual private network (VPN) or other secure connection, software vendors should advise customers to properly configure a personal firewall to secure "always-on" connections.

11. Facilitate secure remote access to applications
If employees, administrators, or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. The application should allow for technologies with tokens, or VPN with individual certificates.

12. Encrypt sensitive traffic over public networks
Use strong cryptography and encryption techniques (at least 128 bit) such as SSL, Point-to-Point Tunneling Protocol (PPTP), or Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks. Never send cardholder information via unencrypted e-mail.

13. Encrypt all non-console administrative access
Use appropriate technologies for Web-based management and other non-console administrative access. Telnet or remote login must never be used for administration.

Additional Best Practices

Connect to the Payment Gateway Using Advanced Integration Method (AIM)

The recommended method of integration for all Card Not Present (CNP) merchant business models is AIM. AIM offers the most flexible integration, allowing merchants to host their own secure payment form and send transactions to the payment gateway using an end-to-end Secure Sockets Layer (SSL) connection.

Authorize.Net also provides a Card Present (CP) integration method designed for developers and providers of retail point-of-sale (POS) systems and payment solutions. This method connects via AIM using an SSL connection. CP solutions may be developed so that retail and mobile merchants need only to purchase a ready-to-install POS solution or device.

For detailed information about AIM and CP integration, please see the Authorize.Net Implementation Guides at http://developer.authorize.net/guides/.

Log Out of All Secure Connections

It is a good practice to completely log out of any secure website (such as the Authorize.Net Merchant Interface) and close the browser window if you will not be using the site for an extended period of time. Failure to close the browser window may result in the login session remaining open.

Use Network Blocks and Filters

Set network parameters that block or filter unwanted files such as adult content, spam, pop-ups, spyware, viruses, and illegal downloads. Monitor employee use of the Internet, including excessive use of bandwidth, personal surfing, and inappropriate viewing and downloading.

Access the Interface Appropriately

Be sure that the Merchant Interface is accessed appropriately via methods documented and supported by Authorize.Net. For example, shortcuts such as "screen-scraping" programs are potentially insecure and may break during payment gateway updates. Additionally, cookies must be enabled in order to access the Merchant Interface.

Authorize.Net®
a CyberSource solution

Implement Optimal Website Programming

Optimize the security of your checkout pages. For example, if you host a payment form page, implement controls to restrict its use to one authorization per order session. Also, if your merchants use the GET method to return their customers to their website from a receipt page, you should convert to the POST method. The POST method uses hidden fields, thus better protecting transaction information.

Educate Merchants about Security Best Practices

Your merchants also have a great responsibility to implement and maintain optimal security for their businesses. Authorize.Net offers a wide range of built-in features and value-adding products that increase security and diminish the risk of fraud. For more information about these features and products, and other general security best practices, refer your merchants to our Security Best Practices White Paper at http://www.authorize.net/files/securitybestpractices.pdf.

Support Advanced Fraud Detection Solutions

Support API fields for built-in and value-added fraud prevention solutions such as Address Verification Service (AVS), Card Code Verification (CCV), and the Authorize.Net Fraud Detection Suite (FDS). Encourage your merchants to implement these solutions for their payment gateway accounts. More information about these solutions is available in the Merchant Interface Online Help Files and Implementation Guides at http://developer.authorize.net/guides/.

Become a Certified Authorize.Net Developer or Solutions Provider

Developers that are, or plan to become, compliant with payments industry security initiatives and best practices can easily become certified Authorize.Net Developers or Solutions Providers. Certified Authorize.Net Developers and Solutions Providers are promoted to thousands of merchants who access the Authorize.Net website every day. For more information about our developer and solutions certification programs, see http://www.authorize.net/solutions/partnersolutions/.

About Authorize.Net®

Authorize.Net, a CyberSource solution (Nasdaq: CYBS), provides secure, reliable, payment gateway solutions that enable merchants to authorize, settle and manage electronic transactions anytime, anywhere, via Web sites, 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-DEVSEC-0712