

E-Commerce Payment Card Security

By Gideon T. Rasmussen, CISSP, CISA, CISM, CIPP
Enterprise Information Management
Bank of America

E-commerce merchants conduct business over the Internet by definition. As such, they are vulnerable to attack from remote locations around the world. This article provides guidance for protecting e-commerce websites in accordance with the PCI Data Security Standard (PCI DSS) and information security best practices.

Organized Crime and Incident Trends

In August 2008, it became apparent organized crime had targeted merchants in a sophisticated conspiracy. An 11 person group was charged with the theft of 41 million card numbers from 10 merchants.

Internet-connected merchants are becoming increasingly attractive targets for such criminal enterprises, now that most large merchants no longer store magnetic stripe (track) data in brick and mortar locations. Websites are preferable targets, due to the relative anonymity of remote attacks. In addition to the obvious trend of web application security vulnerabilities and associated compromises, [Visa compromise statistics](#) document an even split between physical and web stores in 2007. E-commerce merchants are in the crosshairs of sophisticated criminal organizations.

Anatomy of an Incident

Hackers attack via common infrastructure and web application vulnerabilities. They use newly discovered exposures such as the Kaminsky Domain Name Service Vulnerability, which caused administrators to scramble to patch affected systems recently. Hackers also use obscure, legacy attacks such as session replay (where the hacker provides an authorized user with a session id, monitors for its use and hijacks the session). They follow trends, such as compromise of data in transmission across internal private networks.

A compromise may be detected by the merchant, a service provider or Visa common point of purchase fraud investigations. Visa has documented the following indications of a security breach:

- Unknown or unexpected outgoing Internet network traffic from the cardholder environment
- Presence of unexpected IP addresses on store and wireless networks
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Failed login attempts in system authentication and event logs
- Vendor or third-party connections to the cardholder environment without prior consent and/or a trouble ticket
- SQL Injection attempts in web server event logs
- Authentication event log modifications (i.e. unexplained event logs being deleted)



-
- Suspicious after-hours file system activity (i.e. user login or activity to POS server after-hours)
 - Presence of .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data.

The card organizations (Visa®, MasterCard®, etc.) expect merchants to be 100% compliant with the PCI DSS at all times. Non-compliant and compromised merchants are subject to fines, loss of tiered interchange discounts, legal liability, reputation damage and resulting loss of business. Merchants may need to reimburse processors for fines up to \$500,000 by Visa if not PCI compliant at the time of an incident, and may also be required to pay for fraud losses resulting from compromised card account details –loss recovery charges may exceed PCI non-compliance fines.

E-commerce Security Best Practices

1. Comply with the PCI Data Security Standard (DSS). Use the PCI DSS as a reference document. It contains PCI requirements and testing procedures used by assessors. Additional PCI guidance can be found in [Navigating the DSS](#) and PCI information supplements.

2. Protect card data in storage and transmission. Render card numbers unreadable anywhere they are stored (DSS requirement 3.4). Options for secure storage include strong encryption, truncation, and hashing. Use strong encryption to safeguard card data in transmission across public networks (requirement 4.1). As a best practice, encrypt card data across internal networks between web, application and database servers. Merchants with limited security resources and expertise should consider outsourcing the processing, transmission, and storage of cardholder data to a PCI compliant service provider. Doing this can significantly simplify a merchant's data security risk profile and compliance deliverables, but in no way removes the need for merchants to remain vigilant regarding cardholder data security.

3. Do not store prohibited data. E-commerce merchants often provide the ability for customers to store their card number in order to make future transactions. Under PCI standards, it is forbidden to store CVV2 data (the three digit number on the back of a card). Hackers can use CVV2 codes combined with card numbers to conduct fraudulent transactions. Per Visa, "CVV2 may be used in the initial authorization request to set-up a recurring transaction for an Internet or telephone order. However, CVV2 is not required for subsequent transactions."

4. Focus on data flow. Ensure appropriate controls are in place anywhere card data is stored, processed or transmitted. This key DSS directive is absolutely critical to keeping card data secure.

5. Implement world class network security. The DSS provides detailed requirements for network security via router and firewall configurations, demilitarized zone networks, databases on an internal network, etc. Follow those directives to the letter. As a best practice, use network segmentation to isolate card data internally.

6. Harden systems against attack. Configure operating systems and commercial applications in accordance with industry standard hardening guides. Install anti-virus and malware protection software. Install relevant security patches within 30 days.

7. Actively manage software development. Develop custom applications in accordance with an industry standard methodology. Refer to the [Secure Software Development Life Cycle Processes](#) document as a resource. Ensure the security team is involved in development initiatives. Hire developers with secure coding experience. Establish a targeted security awareness program for developers.

8. Evaluate web-facing applications. DSS requirement 6.6 provides two options: conduct code reviews or implement application firewalls. Clarification within an [information supplement](#) lists four methods to meet the code review option:

-
- Manual review of application source code
 - Proper use of automated application source code analyzer (scanning) tools
 - Manual web application security vulnerability assessment
 - Proper use of automated web application security vulnerability assessment (scanning) tools

Most significantly, the list can be used to mitigate risk above-and-beyond minimum DSS requirements. For example, conduct code reviews and use an application vulnerability scanning tool.

9. Perform penetration testing. Establish a penetration testing program in accordance with DSS requirement 11.3. Refer to the related [information supplement](#). Adopt a well regarded penetration testing methodology such as the Open Source Security Testing Methodology Manual (OSSTMM) or the Information System Security Framework (ISSAF). Penetration testing is critical to the security of networked devices and web applications. If your staff does not have the requisite experience, outsource to a qualified security firm.

10. Conduct network scans. DSS requirement 11.2 mandates quarterly network scans, conducted by an Approved Scanning Vendor. Conduct scans after any significant changes in the network as well. For improved security posture, increase scan intervals to once a month. Scanning once a quarter may leave a vulnerability undiscovered for 90 days, increasing the risk of compromise.

11. Use secure payment applications. Use software from Visa's List of Validated Payment Applications as a best practice. Each application listed has been assessed for compliance with Payment Application Best Practices (PABP). Install payment applications in accordance with vendor instructions to avoid insecure configurations such as leaving full debug logging enabled.

12. Review the list of non-compliant payment applications. Request a copy of Visa's List of Payment Applications Storing Prohibited Data from your acquiring bank. The applications listed are designed to improperly store sensitive authentication data subsequent to transaction authorization (including CVV2 data). Hackers have awareness of these applications and actively seek to compromise them.

13. Refer to the SANS Institute Top 20 and OWASP Top 10. The SANS Top 20 is a list of critical vulnerabilities that require immediate remediation. It includes advice for addressing vulnerabilities; including how to protect against zero day attacks. The Open Web Application Security Project (OWASP) Top 10 is a list of common web application vulnerabilities, included within DSS requirement 6.5. Monitor for updates to OWASP outside of the two year DSS revision cycle.

14. Have emphasis on detective controls. A layered monitoring program is necessary to detect attacks and provide forensic information for incident response. If an incident occurs, the goal should be to detect it early on and limit further data compromise. Imagine the damage if an incident goes undetected for months or a year. Detective controls include centralized audit logs, log monitoring, file integrity monitoring and intrusion detection software.

15. Monitor for new threats and vulnerabilities. New vulnerabilities are detected daily. Subscribe to Computer Emergency Response Team (CERT) advisories, the SANS @RISK Consensus Security Alert, BugTraq and vendor security alerts.

16. Thoroughly evaluate service providers. Merchants are liable when card data is shared with a service provider. Therefore, it is prudent to thoroughly evaluate their security controls based upon services provided. If the organization is not listed on Visa's List of Compliant Service Providers, ask to review a PCI Report on Compliance. If a report is not available, evaluate the provider based upon applicable PCI requirements and security controls associated with their custody of card data.

17. Evaluate custom application functionality. Conduct a review of existing card applications. Determine if authorized access to card data is appropriately restricted by business need. For example, if an end user's duties only require access to one card number at a time, ensure controls are in place to limit access by those constraints.

18. Implement fraud detection measures. Monitor access to card data for fraudulent activity. Normal business activities have an expected pattern of behavior. Configure monitoring to alert when expected thresholds are exceeded. For example, alert if an authorized user accesses twice their normal amount of data.

19. Establish an incident response program. Establish an incident response program using NIST 800-61 or CERT's Handbook for Computer Security Incident Response Teams. Incorporate requirements from Visa's What to Do if Compromised document.

20. Conduct risk assessments. Identify emerging threats and vulnerabilities and mitigate risk as appropriate. Refer to NIST 800-30 and [Beyond Minimum Compliance](#) for PCI risk management recommendations. Consider recommendations from the [SANS Internet Storm Center](#) describing how to "build a web site that shall not be broken into, no matter what".

As you can see, ecommerce security is a highly technical domain, requiring a variety of disciplines. If your organization does not have a specific skill set in-house, either hire qualified personnel or engage a service provider with the required expertise. Organized crime is spending significant resources to compromise payment cards. Do not leave card data at risk. Too much is at stake.