Top Three E-commerce Vulnerabilities and Acquirer Actions to Ensure Their Merchants Protect Online Data

Recent breaches have highlighted common security weaknesses that continue to affect merchants and have begun to affect industries beyond traditional e-tailers, including online gaming networks, social media websites and educational institutions. These vulnerabilities affect all e-commerce environments, regardless of whether the merchant hosts its own payment processing pages or outsources this function. However, many of these vulnerabilities can be addressed with basic planning and measures.

As part of its ongoing, industry-leading data security education and awareness programs, Visa has identified three common security vulnerabilities that have been exploited in e-commerce merchant data breaches and is providing recommended strategies to minimize risk.

- **Structured Query Language (SQL) Injection**: A common hacking technique in which malicious code is used to access the databases of websites that don't have proper input validation. The malicious code returns unintended values or error messages to the hacker, who can then use the information to access the database, retrieve and modify data, insert malware or exploit other weaknesses. SQL injection can be mitigated by various methods, including:
    - Validating all user input values by testing type, length, format and range.
    - Limiting or eliminating error code responses to external system users.
    - Strengthening database security by disabling default or unnecessary stored procedures, disabling direct SQL queries, installing the latest security patches and protecting database and local administrative accounts.
- **Cross-Site Scripting**: A hacking technique in which malware is used to hijack user sessions, redirect users or take over the user's browser. Like SQL injection, cross-site scripting targets websites that don't have proper input validation. Such an attack can be mitigated by:
    - Encoding the Web page output based on input parameters.
    - Filtering input parameters for special characters.
    - Filtering output based on input parameters for special characters.
- **Authentication and Session Management Flaws**: These weaknesses range from unprotected usernames or passwords in databases and application timeouts that are not properly set, to exposed session IDs in the website URL. Other vulnerabilities include weak password creation rules, poor password change or recovery features, and weak session IDs. Authentication and session management flaws can be minimized by:
    - Implementing strong authentication and session management controls, which can be found on the Application Security Verification Standard page at the Open Web Application Security Project (OWASP) website.

For more information on common coding vulnerabilities, review the 2011 CWE / SANS Top 25 Most Dangerous Software Errors and the CERT Secure Coding Standards.

Understanding the Risks

Acquirers should understand their full risk exposure and address data security concerns with e-commerce merchants by first determining the complexity of the merchant's online payment-card-processing environment and then applying the following best practices:

- E-commerce merchants that do not have in-house expertise or resources should consider fully outsourcing their payment-card processing operations to a service provider validated by the Payment Card Industry Data Security Standard (PCI DSS). By using a fully outsourced service provider, the merchant does not store cardholder data in electronic format and does not process or transmit any cardholder data on their systems or premises. This option also greatly reduces the PCI DSS validation requirements for an e-commerce merchant.

  Acquirers should ensure service providers are listed in *Visa's Global Registry of Service Providers—PCI DSS Validated Entities*.

- E-commerce merchants that purchase payment application software, such as a shopping cart, and integrate it with their website should ensure the software is on the PCI Security Standards Council's list of validated payment applications or is compliant with the PCI Payment Application Data Security Standard (PA-DSS).

  Acquirers should make sure merchants comply with these requirements.

- E-commerce merchants that custom design their payment applications or have developed in-house applications should conform to industry best practices for application development such as the OWASP Top 10, a document that identifies the most critical Web-application security flaws and outlines ways to remediate those vulnerabilities. Preventing common coding vulnerabilities is also referenced in the PCI DSS Requirement 6.5.

  Acquirers should ensure merchants are not storing the Card Verification Value 2 (CVV2) after the authorization of a transaction. Storing CVV2 after authorization is a violation of the PCI DSS and *Visa International Operating Regulations* (ID#: 050411-010410-0002228).

Additionally, merchants can help further secure sensitive cardholder information by implementing point-to-point encryption or tokenization. Point-to-point encryption is designed to protect cardholder data from the point of data entry to the payment card processor. By making data unreadable to anyone without the decryption keys, point-to-point encryption can protect against malware that tries to "sniff" and "capture" the data in transit. Tokenization replaces data such as the payment card account number with a randomly generated surrogate value. This token can then be used for payment card functions such as returns and chargebacks, so the merchant does not need to retain the full account number. Implementing such technologies can also help reduce merchants' PCI DSS compliance and validation scope, thereby potentially helping simplify compliance with PCI DSS requirements.

Although point-to-point encryption and tokenization provide an additional layer of security and can potentially remove payment card data from the merchant's scope, the PCI DSS remains the best protection against account data compromise. To mitigate network intrusions, acquirers should ensure their merchants comply with the PCI DSS and encourage them to implement secure technologies to further protect or eliminate vulnerable data from payment card environments.

Acquirers are reminded to comply with *Visa International Operating Regulations* governing Verified by Visa Acquirer and Merchant Requirements (ID#: 160312-010410-0004616), as well as regional rules that mandate PCI DSS compliance.