VISA SECURITY BULLETIN

29 October 2015

NEW SMALL MERCHANT DATA SECURITY REQUIREMENTS

Distribution: Acquirers, Processors, Merchants, Agents
Who should read this: Compliance, Information Security, Data Security

Summary

According to recent forensic investigations, small merchants remain targets of hackers who are attempting to compromise payment data. As part of an effort to secure the payment system and mitigate the risk of small merchant compromises, Visa is establishing requirements for U.S. and Canada acquirers to ensure that their small merchants take steps to secure their point-of-sale (POS) environment.

Merchants Must Use Qualified Integrators and Reseller (QIR) Professionals

Systems can fall out of compliance with the PCI DSS. PCI DSS Version 3.1, Requirement 6 states:

Effective 31 March 2016, acquirers must require all newly boarded Level 4 merchants[1] to use only Payment Card Industry (PCI)-certified QIR professionals from the QIR Companies list at the PCI Security Standards Council (PCI SSC) website for POS application and terminal installation and integration.

Effective 31 January 2017, acquirers must also ensure that all existing Level 4 merchants use PCI-certified QIR professionals from the QIR Companies list for servicing POS applications and terminals.

[1] Level 4 merchants include owner-operated locations of franchise or corporate organizations. Franchisors or corporate organizations must continue to validate as a merchant or service provider based on their designation and/or level.

About the QIR Program

Earlier this year, Visa recommended that clients ensure their merchants and merchants' agents use POS integrators and resellers selected from the PCI SSC QIR Companies list. Using organizations (i.e., payment application developers, integrators and resellers) that have completed the PCI SSC QIR training program helps improve security by ensuring that payment applications and terminals are installed and integrated in a manner that mitigates payment data breaches and facilitates a merchant's PCI Data Security Standard (DSS) compliance. Additionally, integrators and resellers that complete the program are included on the PCI SSC's online list of approved qualified providers and may be listed in the Visa Global Registry of Service Providers through completion of the Visa Merchant Servicer Self-Identification Program, making it easy for acquirers and merchants to identify and select a partner.

Forensic investigators have identified links between improperly installed POS applications and merchant payment data environment breaches. Specifically, forensic reports note security protocol gaps in remote-access services used by integrators and resellers to provide monitoring and software support (e.g., default or shared remote-access IDs without two-factor authentication or regular password changes). For merchants, these gaps create a significant risk of payment data compromise through malware exposure.

Visa and the PCI SSC have partnered to promote the QIR program and are extending the offer of an exclusive discount for integrators and resellers that enroll in the program by **31 December 2015**. Organizations can use the exclusive Visa promotional code VISA50%OFF to receive the discounted pricing. Promotion details are as follows:

• Discounted price is US $197.50 per professional

• Sponsor companies must apply and be approved through the standard QIR program process

New Visa Payment Security Compliance Validation Program Requirements for Level 4 Merchants

Using QIR companies provides small merchants some protection against a common vulnerability exploited by criminals. However, this alone will not prevent small merchant compromises. As such, Visa is expanding its PCI DSS validation program to include Level 4 merchants. **Effective 31 January 2017**, acquirers must ensure their Level 4 merchants validate full PCI DSS compliance annually.

Level 4 merchants may qualify for the Visa Technology Innovation Program (TIP), which recognizes and acknowledges merchants that take action to prevent counterfeit fraud and compromise by investing in EMV technology or validated point-to-point encryption (P2PE) solutions. Participation in TIP allows qualifying merchants to discontinue the annual PCI DSS validation assessment. Qualifying merchants can reap meaningful savings and have the opportunity to reinvest those savings into additional secure acceptance technology.

To qualify for TIP and receive its benefits, a merchant must meet all of the following criteria:

- Ensure that sensitive authentication data (i.e., the full contents of magnetic-stripe, Card Verification Value 2 and PIN data) is not stored subsequent to transaction authorization, as defined in the PCI DSS.

- Ensure that at least 75 percent of all transactions originate through the following secure acceptance channels:
    - Enabled and operating chip-reading terminals
    - Validated P2PE solution

Small Merchant Security Best Practices and Bi-Annual Acquirer Reporting

In support of the new requirements, Visa will provide acquirers with resources and best practices for management of small merchant security as well as more detailed instructions for reporting on Level 4 TIP-qualifying merchants. Visa will update the Biannual Acquirer Reporting template to capture

additional information regarding merchants' use of QIRs, chip terminals, P2PE solutions and service providers. Visa will distribute details on the revised reporting template to clients in the coming months.

As a reminder, Visa requires that clients, their merchants and agents comply with the PCI DSS and all relevant policies, as well as the validation and reporting requirements outlined in Visa data security compliance programs, including the Cardholder Information Security Program, provided in the Visa Rules (ID#s: 0002228 and 0008031).

In cases of suspected or confirmed loss, theft or compromise of Visa account information, clients must comply with Visa's *What To Do If Compromised* requirements. This may include the engagement of a PCI Forensic Investigator to perform a forensic investigation of the client, its merchants or agents (including QIR companies), if necessary. Clients may be subject to non-compliance assessments for failure to comply with these requirements.

Risk Management Benefits

Selecting and using approved QIR companies and implementing one or more of the abovementioned security controls helps clients and merchants improve security, reduce compromise risk through payment data devaluation and meet Visa security program requirements.

Visa appreciates clients taking the necessary actions to ensure merchants meet the requirements. Although using secure acceptance technologies and approved QIR companies are important for preventing counterfeit fraud and compromise, no single solution or action can completely secure the payment environment. Visa encourages using a multilayered approach to security, and all parties must give careful consideration to their security investments to meet their risk management needs.

Additional Resources

"Cybercriminals Targeting Point of Sale Integrators," *Visa Security Alert*, 5 June 2015

Visa What To Do If Compromised

PCI SSC List of QIR Companies

Visa Global Registry of Service Providers

Visa Payment Security website

Payment Card Industry Security Standards Council website

For more information, please contact Visa Risk Management: cisp@visa.com