Risk Management | Data Security 26 March 2015

Technology Innovation Program Expanded to Merchants That Implement Point-to-Point Encryption

AP, Canada, CEMEA, LAC, U.S. | *Acquirers, Issuers, Processors, Merchants, Agents*

The Technology Innovation Program (TIP) recognizes and acknowledges merchants that take action to prevent counterfeit fraud by investing in EMV technology, specifically through purchasing, deploying and enabling EMV point-of-sale (POS) terminals. Participation in TIP allows qualifying merchants to discontinue the annual Payment Card Industry Data Security Standard (PCI DSS) validation assessment. Qualifying merchants can reap meaningful savings and have the opportunity to reinvest those savings into additional secure acceptance technology.

Effective 1 April 2015, Visa will expand TIP qualification to merchants that have invested in a validated point-to-point encryption solution. Qualifying solutions are those that are included on PCI SSC's list of Validated Point-to-Point Encryption Solutions or independently validated by a PCI SSC Qualified Security Assessor point-to-point encryption company. Point-to-point encryption helps to secure a merchant's acceptance environment by removing or devaluing cardholder data. Visa recognizes the security value this technology brings to the POS acceptance environment.

Expanded Support for Merchants to Maintain Security

Visa requires all organizations that store, transmit or process cardholder data to comply with the PCI DSS, including merchants that may participate in TIP. PCI DSS compliance is the foundation of Visa data security programs and is critical to protecting sensitive cardholder data from compromise. Visa also supports and encourages the use of payment technologies that eliminate cardholder data, secure data in storage and transit and/or devalue remaining information via dynamic authentication.

Many merchants invest time and money in the purchase, deployment and enablement of EMV POS terminals and/or in the implementation of point-to-point encryption solutions. These merchants have also consistently invested in annual PCI DSS compliance assessments, which may include the engagement of a Qualified Security Assessor and can represent a significant expense. Visa is expanding TIP to help merchants reduce these costs.

Minimum Merchant Qualification Requirements

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

- Confirm that sensitive authentication data (i.e., the full contents of magnetic stripe, CVV2 and PIN data) are not stored subsequent to transaction authorization, as defined in the PCI DSS.
- Ensure that at least 75 percent of all transactions originate through one of the following secure acceptance channels:

    - Enabled and operating chip-reading terminals (U.S. merchants must meet the volume criteria with dual-interface contact / contactless terminals)[1]

    - Validated point-to-point encryption service[2] **(NEW)**

- Not be involved in the breach of cardholder data. A breached merchant may qualify for TIP if it has subsequently validated PCI DSS compliance.

Merchants that do not meet the program's qualification requirements, including merchants whose transaction volume is primarily from e-commerce and mail order / telephone order acceptance channels, are still required to validate PCI DSS compliance annually in accordance with Visa compliance programs. As a reminder, merchants must not request or use a Visa account number for any purpose other than as payment for goods and services, as specified in the *Visa Cole Rules and Visa Product and Service Rules* (ID#: 0008585).

To participate in TIP, acquirers must submit a program application to Visa to enroll each qualifying merchant. At its sole discretion, Visa will review applications and provide acquirers with confirmation of approved merchant participation. Visa will provide acquirers with additional program details and application materials as well as confirm each acquirer's ongoing reporting responsibilities.

[1] Chip-enabled terminals must have current, valid EMV approval and pass Acquirer Device Validation Toolkit (ADVT) / Contactless Evaluation Toolkit (CDET) / Visa payWave Test Tool (VpTT) testing requirements, as applicable.

[2] The point-to-point encryption solution must be included on the PCI SSC list of validated solutions or independently validated by a PCI SSC Qualified Security Assessor point-to-point encryption company.

PCI DSS Compliance Requirements

Although Visa may eliminate the annual validation requirement for TIP-qualifying merchants, all merchants are still required to maintain ongoing PCI DSS compliance. Acquirers retain full responsibility for merchants' PCI DSS compliance, and for any fees that may be assessed in the event of an account data breach event. Visa reserves the right, in its discretion, to require that acquirers submit timely validation of PCI DSS compliance on behalf of their compromised entities or of any entity that is determined to present a security risk to the Visa system. If risk conditions change in any market, Visa may re-evaluate the need for merchants to validate PCI DSS compliance. In addition, Visa may rescind participation in TIP if it determines that a participant does not meet all program requirements.

To ensure the protection of vulnerable static data that remains in the payment system, merchants can limit the availability of all payment card data within their environment using technologies such as encryption and tokenization, which may also aid in PCI DSS compliance. Visa best practices for the use of each of these technologies are available on the Cardholder Information Security Program web page. CVV2 validation and Verified by Visa are also beneficial for combating card-absent fraud by effectively limiting cross-channel contamination between a compromised face-to-face environment and subsequent card-absent fraud.

Finally, and in accordance with the PCI DSS, all merchants must establish and annually test an incident response plan that outlines the steps to take in the event of a suspected account data compromise. This plan must be consistent with the Visa *What To Do If Compromised* procedures document.

About EMV and Point-to-Point Encryption Technologies

EMV transactions include a chip-generated, dynamic data element that is unique for every transaction. This dynamic data element prevents the successful creation of counterfeit cards, even if the authentication data is compromised. EMV transactions reduce the fraud value of cardholder data and help prevent the compromise of

sensitive authentication data. The use of validated point-to-point encryption solutions help secure a merchant's acceptance environment through removing or devaluing cardholder data.

Dynamic authentication and data devaluation are critical advancements in preventing counterfeit fraud and important elements of Visa's multi-layered approach to security. However, no single solution is a silver bullet for fraud mitigation and the industry must continue to protect sensitive data aggressively. Merchants should give careful thought to their approach for security, and base their decisions on cost, necessity, industry requirements, regulations and likely trends. Security investments must likewise be considered in the context of a business's tolerance for risk from losses.

Additional Resources

Documents & Publications

"Visa Introduces Technology Innovation Program for Merchants," *Visa Business News*, 9 February 2011

Visa Best Practices for Data Field Encryption

Visa Best Practices for Tokenization

Online Resources

Cardholder Information Security Program web page

PCI Security Standards Council web page

For More Information

Contact your Visa representative. Third party agents should contact their issuer or acquirer.