
Visa Introduces Technology Innovation Program for Merchants

Visa is introducing the Technology Innovation Program (TIP) to recognize and acknowledge merchants in Visa Inc. regions outside of the United States that have taken action to prevent counterfeit fraud by investing in EMV technology.

The program specifically benefits those merchants that have made progress towards purchasing, deploying and enabling EMV point-of-sale (POS) terminals. Effective 31 March 2011, Visa will allow qualifying merchants outside of the United States to discontinue their annual Payment Card Industry Data Security Standard (PCI DSS) revalidation assessment. Visa Europe has announced a similar program for acquirers and merchants in its geographical markets. Details of the Visa Europe TIP program can be obtained by contacting Visa Europe Customer Support via email at customersupport@visa.com or datasecuritystandards@visa.com.

Background

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

Visa data security compliance programs help to reduce the compromise of sensitive cardholder data. Visa required all Level 1 and Level 2 merchants outside of the United States to validate PCI DSS compliance by 30 September 2010.¹ As of 31 December 2010, 76 percent of Level 1 merchants in Visa Inc. regions had validated their compliance with the PCI DSS. The majority of remaining merchants report that they will validate compliance within 12 months. Importantly, 99 percent of Level 1 and Level 2 merchants in all Visa Inc. regions have also validated that they do not store prohibited data (i.e., the full contents of magnetic stripe, CVV2 or PIN data).

Many merchants have invested time and money in the purchase, deployment and enablement of EMV POS terminals. These merchants have also invested in annual PCI DSS compliance assessments, which may require the use of a Qualified Security Assessor and can be a significant expense. Visa is introducing the Technology Innovation Program to assist merchants in reducing the costs associated with annual PCI DSS validation.

About the Visa Technology Innovation Program

TIP is part of Visa's ongoing strategy to protect the payment system and advance security practices that will help secure cardholder data. This program rewards and further encourages the use of EMV technology as it decreases the value of transaction data to criminals.

Effective 31 March 2011, this program will allow qualifying merchants outside of the United States to discontinue their annual PCI DSS revalidation assessment. Qualifying merchants can reap meaningful savings, and will have the opportunity to re-invest those savings into additional technology to support dynamic data processing.

Despite industry interest in chip and dynamic data authentication, the program is not currently available in the United States because recent debit card regulation has cast uncertainty in the marketplace. Visa Inc. may consider implementation of TIP in the United States at a later date based on evolving environmental circumstances.

¹ These validation deadlines did not apply to acquirers and merchants residing within Visa Europe.

Note: Visa Europe has announced a similar program for acquirers and merchants in its geographical markets. Details of the Visa Europe TIP program can be obtained by contacting Visa Europe Customer Support via email at customersupport@visa.com or datasecuritystandards@visa.com.

Minimum Merchant Qualification Standards

To qualify for the program and receive its benefits, merchants must meet **all** of the following criteria:

1. The merchant must have validated PCI DSS compliance previously **or** have submitted to Visa (via their acquirer) a defined remediation plan for achieving compliance based on a gap analysis.
2. The merchant must have confirmed that sensitive authentication data (i.e., the full contents of magnetic stripe, CVV2 or PIN data) is not stored, as defined in the PCI DSS.
3. At least 75 percent of the merchant's transaction count must originate from enabled chip-reading device² terminals (i.e., contact and/or dual interface contact/contactless terminals).
4. The merchant must not be involved in a 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 EMV terminalization requirements, including merchants whose transaction volume is primarily from e-commerce and Mail Order/Telephone Order (MO/TO) acceptance channels, are still required to validate their PCI DSS compliance annually in accordance with Visa compliance programs.

Visa will work directly with acquirers to confirm eligible merchants and validate acquirer reporting responsibilities.

Visa Inc. reminds acquirers that a merchant must not request or use a Visa account number for any purpose other than as payment for goods and services, per the *Visa International Operating Regulations*.

Merchants Must Maintain PCI DSS Compliance

Although Visa may waive the annual validation requirement for qualifying merchants, all merchants are still required to maintain on-going PCI DSS compliance. Acquirers retain full responsibility for merchants' PCI DSS compliance, as well as responsibility for any fees, fines or penalties, which may be applicable in the event of a data breach.

Visa reserves the right to require full PCI DSS validation of compromised entities. If risk conditions change dramatically, Visa may re-evaluate the need for merchants to validate PCI DSS compliance.

To ensure the protection of vulnerable static data that remains in the payment system, merchants may seek to limit the availability of all payment card data within their environment through other complementary technologies such as data field encryption and/or tokenization, which may also aid in their PCI DSS compliance. Visa recommended best practices for the use of each of these technologies are available at www.visa.com/cisp.

Visa Inc. also reminds acquirers of the benefits of the use of CVV2 and Verified by Visa in combating card-not-present (CNP) fraud within in their merchant portfolio, especially in the case of fraud that may be perpetrated using account number and expiration date only. The use of either technology can effectively limit cross-channel contamination between the compromise of a face-to-face environment and subsequent fraudulent use in the CNP space.

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 Visa Inc.'s *What To Do If Compromised* procedures document, which is also available for download at www.visa.com/cisp.

² Chip-enabled terminal devices must have current, valid EMV approval **and** pass Visa Acquirer Device Validation Toolkit (ADVT) / Visa payWave Test Tool (VpTT) implementation requirements as applicable.

Program Implementation Plan and Market-Specific Application

To address country-specific threat environments, Visa may adopt a country-specific approach to drive PCI DSS compliance and EMV technology implementation (e.g., requiring different degrees of compliance validation). If it is necessary to implement the program with unique or additional qualification criteria, Visa will notify acquirers in the affected country or region.

Impact

Many merchants have already made the investment to transition to EMV terminals, in addition to their annual PCI DSS compliance validation. TIP will provide qualifying merchants with a return on that investment, as well as the opportunity to continue to process dynamic data transactions.

While Visa may waive the requirement for some merchants to annually validate PCI DSS compliance, acquirers must continue to communicate to their merchants the importance of maintaining on-going PCI DSS compliance and the need to protect static cardholder data.

Visa will work closely with acquirers on the continued monitoring of merchants' PCI DSS compliance and EMV terminalization efforts.

About EMV Technology and Dynamic Authentication

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 which benefits all stakeholders.

Dynamic authentication is a critical advancement in preventing counterfeit fraud and an important element of Visa's multi-layered approach to security. EMV chip technology is a proven platform that allows the payment card industry to facilitate dynamic data and enable payment innovations. However, the EMV chip alone is not a silver bullet for fraud mitigation and the industry must continue to protect sensitive data aggressively.

All participants in the payment system must continue to protect sensitive static card account information (including PINs) vigilantly and adhere to industry data security standards such as the PCI DSS, PCI PIN Transaction Security and the Payment Application Data Security Standard (PA-DSS).