Small Merchant Security Program – QIR Requirement Clarifications

AUGUST 2016

SUMMARY

As part of a broader effort to mitigate small merchant breaches, Visa established new data security program requirements for U.S. and Canadian acquirers. Visa announced the following requirements and associated deadlines in January 2016:

- Effective 31 March 2016, acquirers must communicate to all Level 4 merchants that beginning 31 January 2017, they must use only Payment Card Industry (PCI)-certified Qualified Integrators and Reseller (QIR) professionals for point-of-sale (POS) application and terminal installation and integration.
- Effective 31 January 2017, acquirers must ensure that Level 4 merchants using third parties for POS application and terminal installation and integration engage only PCI QIR professionals.
- Effective 31 January 2017, acquirers must ensure Level 4 merchants annually validate PCI DSS compliance or participate in the Technology Innovation Program (TIP).

KEY CLARIFICATIONS

A number of complex business models are used in today's payment eco-system to support merchant acceptance. To assist acquirers with ensuring compliance with the Small Merchant Security Program, Visa is providing the following program clarifications.

- Vendors that do not sell, support or service PA-DSS validated POS applications are not currently eligible to participate in the PCI QIR program. As a result, the requirement to complete the PCI QIR certification for purposes of complying with Visa's program does **not** apply to these vendors. *Note that although these organizations are not eligible to participate in the PCI QIR program, Visa strongly encourages acquirers and merchants ensure these organizations use secure practices if the organization provides service or support to a merchants POS environment via remote access.*

- The requirements and associated deadlines for use of a QIR do **not** apply to the following:

    - Merchants using single-use terminals without Internet connectivity.
    - Merchants not using a third-party for POS application, installation, integration or maintenance.
    - Merchants with IP-based terminals who do not work with vendors accessing the POS environment via remote access.

- The requirement for an organization to complete the PCI QIR certification for purposes of complying with Visa's program does **not** apply for the following:

    - Vendors that support ancillary applications integrated into the POS systems, but which are properly segmented from the payment processing operations are not subject to the requirement. (Examples may include companies that support inventory management systems, reservation systems, etc.)
    - Vendors providing simple plug-and-play devices for merchants which will not allow remote access into the POS environment.
    - An acquirer or their affiliated business unit. (As a best practice, an acquirer may also choose to complete the QIR certification in order to be included on the PCI SSC's list of QIR companies, making it easy for merchants to identify their secure provider.)

ADDITIONAL INFORMATION

- 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 protects against payment data breaches and facilitates a merchant's PCI Data Security Standard (PCI DSS) compliance. Additionally, integrators and resellers that complete the program are included on the PCI SSC's online list of approved qualified providers as well as the Visa Global Registry of Service Providers, making it easy for acquirers and merchants to identify and select a partner.

- Although some organizations providing integrator/reseller services may not be eligible to participate in the PCI QIR program, Visa strongly encourages acquirers and merchants ensure these organizations use secure practices if the organization provides service or support to a merchants POS environment via remote access. All acquirers and merchants must maintain compliance with PCI DSS.

- As a reminder, Visa will not proactively enforce or measure compliance with the new requirements at an individual merchant level. In the event of a compromise linked to a merchant's non-compliance with Visa rules or PCI DSS, acquirers may be subject to non-compliance assessments.

- If an acquirer or its merchant(s) will not meet the established requirements and/or deadlines, it is not necessary to seek a formal waiver as Visa will not proactively enforce compliance or assess proactive non-compliance assessments. In the event of a compromise linked to a merchant's non-compliance with Visa rules or PCI DSS, acquirers may be subject to non-compliance assessments.

- As a reminder, all organizations that store, transmit or process cardholder data must comply with PCI DSS.