



Small Merchant Security Program Requirements – UPDATE

SUMMARY

As part of a broader effort to mitigate small merchant breaches, Visa Payment System Risk established new data security program requirements for U.S. and Canadian acquirers. Visa announced the new mandates for acquirers on 29 October 2015 via the *Visa Business News*. To provide acquirers and merchants with additional time to adhere with program requirements, Visa is adjusting compliance deadlines as follows:

- **(NEW)** 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).

Note that single-use terminals without Internet connectivity are considered low risk and may be excluded from these requirements.

As part of this expansion of the merchant data security validation requirements, Level 4 merchants now may also qualify for the Visa Technology Innovation Program (TIP) which recognizes and acknowledges merchants that take action to prevent counterfeit fraud by investing in EMV technology or PCI SSC-validated point-to-point encryption (P2PE) solutions. Participation in TIP allows qualifying merchants to discontinue the annual PCI DSS validation assessment.

To qualify for TIP and receive its benefits, a merchant must meet 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 EMV chip-reading terminals
 - OR
 - A [PCI SSC-validated P2PE solution](#)

OBJECTIVE

Based on recent forensic investigations, small merchants remain a target of hackers attempting to compromise payment data. Additionally, 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 that integrators and resellers use 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.

In 2015, Visa recommended that clients ensure that their merchants and merchants' agents use POS integrators and resellers selected from the list of PCI SSC QIR companies. 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, making it easy for acquirers and merchants to identify and select a partner.

Visa is establishing these requirements for acquirers to ensure their small merchants are taking steps to secure their environment.

KEY MESSAGES

- Using secure acceptance technologies and approved QIR companies is important to mitigate counterfeit fraud. Visa encourages using a multi-layered approach to security, and all parties must carefully consider their security investments to meet their risk management needs.
- Recent forensic investigations confirm that small merchants remain a target of hackers attempting to compromise payment data and that there are links between improperly installed POS applications and merchant payment data environment breaches.
- 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, making it easy for acquirers and merchants to identify and select a partner.
- Visa is establishing these requirements for acquirers to ensure their small merchants are taking steps to secure their payment environment.

Small Merchant Security Program – Frequently Asked Questions

Small Merchant Security Requirements

Q: What is required from acquirers based on this announcement?

- **(NEW)** 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 QIR professionals for 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).

Note that single-use terminals without Internet connectivity are considered low risk and may be excluded from these requirements.

Q: Do these requirements apply to all merchants?

No. Merchants using single-use terminals without Internet connectivity are considered low risk and may be excluded from these requirements.

Additionally, if a merchant does not use a third party for POS application or terminal installation, integration or maintenance, the requirement to use a QIR does not apply.

Q: Why is Visa establishing these requirements now?

Based on recent forensic investigations, small merchants remain a target of hackers attempting to compromise payment data. Additionally, 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 that integrators and resellers use 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.

In 2015, Visa recommended that clients ensure their merchants and merchants' agents use POS integrators and resellers selected from the list of PCI SSC QIR companies. 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 DSS compliance. Additionally, integrators and resellers that complete the program are included on the PCI SSC's online list of approved qualified providers, making it easy for acquirers and merchants to identify and select a partner.

Visa is establishing these requirements for acquirers to ensure their small merchants are taking steps to secure their environment.

Q: Why is the requirement to use a PCI QIR limited to Level 4 merchants?

Integrators and resellers that provide POS system installation and ongoing system management primarily work with level 4 merchants. Generally, larger merchants self-manage acceptance environments or structure enterprise-wide contracts to include direct servicing from large POS vendors and cover the security of these controls within their overall PCI DSS compliance plan. Additionally, based on forensic investigation findings, the breaches linked to insecure integrator and reseller practices are affecting small merchants. (For example, 80 percent of small merchant breaches are associated with insecure POS implementation and servicing by integrators and resellers.) The Visa requirement for Level 1, 2 and 3 merchants to annually validate PCI DSS compliance or participate in TIP has been in place for many years to address many common security vulnerabilities.

As a reminder, all organizations that store, transmit or process Visa payment data must comply with PCI DSS, regardless of whether they are subject to validation requirements.

Q: Why do the new requirements only apply in the U.S. and Canada?

Visa is introducing these requirements in the U.S. and Canada because these countries have experienced the largest number of small merchant breach incidents. Visa will continue to evaluate whether the requirements should be expanded to acquirers in other countries.

Q: What is the most common attack related to small merchants and integrators / resellers?

The most common security protocol gaps occur in remote access services that integrators and resellers use 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.

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 DSS compliance. Additionally, integrators and resellers that complete the program are included on the PCI SSC's online [list of approved qualified providers](#), making it easy for acquirers and merchants to identify and select a partner.

Payment Card Industry Qualified Integrator and Reseller Program (PCI QIR)

Q: There are currently very few companies on the list of PCI QIR. What is Visa doing to increase the number of providers ahead of the mandate?

Visa partnered with the PCI SSC to promote the PCI QIR program and negotiated an exclusive discount for integrators and resellers enrolling in the program by 31 December 2015. Organizations could use the exclusive Visa promotional code, VISA50%OFF, to receive the discounted pricing of \$197.50 per attendee. Note that sponsor companies must apply and be approved through the standard QIR Program participation process.

The Payment System Risk team also has an ongoing communications campaign to reinforce data security best practices across all stakeholder groups and to reinforce the importance of ensuring integrators and resellers go through the PCI certification program. The communications effort includes publishing articles in industry publications, hosting educational webinars, etc. Additionally, Visa is working with a number of industry associations and large integrator/reseller organizations to drive participation in the PCI QIR Program.

Finally, Visa is working with the PCI SSC to update validation documentation to allow merchants to identify QIRs directly in the Self-Assessment Questionnaire or Report on Compliance. Updated documentation is targeted for publication in early 2016.

Q: Where can acquirers and merchants find additional information about the PCI QIR Program and the certified providers?

The PCI SSC manages the PCI QIR program and maintains the list of certified QIR companies at https://www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php

Q: How do merchants know if the integrator / reseller has completed the PCI QIR certification program?

The PCI SSC manages the PCI QIR program and maintains the list of certified QIR companies at https://www.pcisecuritystandards.org/approved_companies_providers/qir_companies.php

Additionally, the QIR must complete a QIR Implementation Statement confirming the payment application was installed and configured in a manner that supports PCI DSS compliance. A copy of the QIR Implementation Statement must be delivered to the customer no later than ten (10) business days after installation is complete, and a copy must be retained by the QIR company with their work papers.

Note: The customer may request that the QIR company to complete work beyond what is required to install the payment application; this is outside the scope of the QIR Program. Any such work does not form part of the Qualified Installation.

Q: How does an integrator / reseller get certified? What is the process?

The PCI SSC manages the PCI QIR program. Detailed information about the course, including the training schedule, pricing, registration and qualification criteria are all included at https://www.pcisecuritystandards.org/training/qir_training.php

Q: How can a terminal service provider or large-scale reseller that works with hundreds or thousands of integrators get certified?

The PCI SSC provides an opportunity for organizations working with large populations of integrators / resellers to qualify for a QIR Licensing Option. This allows the larger organization to obtain a license to provide the QIR training to their integrators and resellers with certification testing completed through the PCI SSC. Organizations interested in the QIR Licensing Option should contact PCI SSC directly at qir@pcisecuritystandards.org.

Q: What kinds of companies are required to participate in the QIR Program?

The QIR Program is designed to educate, qualify and train organizations involved in the implementation, configuration, support and/or maintenance of POS payment applications on behalf of merchants or service providers. The program focuses on ensuring that QIR companies install and configure payment applications into customer environments in a manner that supports PCI DSS compliance.

The types of services offered that qualify a company for the QIR program include any of the following:

- Configuring and/or installing POS software, payment applications or terminals for merchants

- Supporting or servicing POS software, payment applications or terminals for merchants – including accessing these systems remotely for troubleshooting, delivering system updates or offsite support.

Companies that support ancillary applications integrated into the POS systems but 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.)

Q: What if a service provider ships POS terminals to a merchant? Is that service provider in scope for the QIR program?

If the service provider is configuring the application within the terminal for the merchant and will support or service the terminal via remote access after installation, the service provider is in scope for the QIR Program and should complete the certification process.

An operator providing a merchant with a simple plug-and-play device for a merchant which will not allow for remote access into the POS environment is not in scope of the QIR program.

Q: If an acquirer or affiliated business unit is deploying, implementing or servicing POS software, payment applications or terminals for merchants, are they required to complete the QIR certification?

Generally, an acquirer or their affiliated business unit is considered by Visa to be a Third Party Agent. Third Party Agents are required to comply with PCI DSS based on their role of storing, transmitting or processing cardholder data. The PCI DSS is a comprehensive security standard and requires secure practices broader than what is required of QIR professionals. 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.

Visa Program Compliance and Enforcement

Q: How will Visa measure an acquirer's compliance with these requirements?

In support of the new requirements, Visa will provide acquirers with resources for managing small merchant security. Additionally, 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 2016.

Q: Is using a QIR company from the PCI SSC list sufficient to meet the Visa requirements or does the individual employee need to be certified?

Individual employees are not currently included on the PCI SSC QIR Companies list. Therefore, confirming that the integrator / reseller company is listed meets the Visa requirements. QIR companies are responsible for ensuring that employees performing installation services meet the QIR Program requirements.

Q: How do acquirers enforce the requirements?

Acquirers are responsible for ensuring their merchants meet all Visa security program requirements, regardless of merchant level or validation requirements. Acquirers must communicate the requirements to their merchant portfolio, track compliance and report to Visa through the biannual report.

Most acquirers already require small merchants to complete annual PCI DSS validation and update Visa on those security efforts through the biannual report. The new requirements ensure that all acquirers are subject to the same requirements and establish a level playing field to enforce small merchant security across the industry.

Q: What if an acquirer cannot meet the deadlines?

Visa requires that clients, their merchants and agents comply with PCI DSS and all relevant policies, as well as the validation and reporting requirements outlined in Visa data security compliance programs, including the Account Information Security Program. Clients may be subject to non-compliance assessments for failure to comply with these requirements.

Visa will continue to work closely with clients to ensure they understand the new requirements. Additionally, Visa will not proactively enforce or measure compliance with the new requirements at an individual merchant level. Visa will update the Biannual Acquirer Reporting template to capture additional data elements that help acquirers manage their programs / procedures in accordance with Visa program requirements. 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.

Q: Will Visa impose non-compliance assessments for Level 4 merchants not using QIR companies and/or not completing PCI DSS validation by the deadlines?

Visa will not proactively enforce or measure compliance with the new requirements at an individual merchant level. Visa will update the Biannual Acquirer Reporting template to capture additional data elements that help acquirers manage their programs / procedures in accordance with Visa program requirements. 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.

Q: What happens if a compromise is linked to insecure practices of an integrator / reseller?

In the event that a compromise of cardholder data is determined to be the result of an integrator / reseller's non-compliance with QIR Program requirements, the QIR may be de-listed (if they are a current program participant). Visa may also impose additional risk controls, if appropriate.

Q: What do acquirers need to do for Level 4 merchants that qualify for TIP?

Acquirers will not need to submit individual applications for Level 4 merchants that qualify for TIP. Visa will update the Biannual Acquirer Reporting template to capture additional information about merchants' use of QIRs, chip terminals, P2PE solutions and service providers, including merchants that qualify for TIP. Visa will distribute details on the revised reporting template to clients in 2016.

Q: Which P2PE solutions can a merchant use to qualify for TIP?

In order to meet Visa's requirements for TIP participation, merchants must use a PCI-validated P2PE solution. PCI-validated solutions are included on the PCI SSC's website:

- [Validated Point to Point Encryption Solutions](#)
- [Validated Point to Point Encryption Applications](#)