VISA BULLETIN

29 January 2015

PCI PIN SECURITY REQUIREMENTS UPDATED

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

Summary

To enhance validation methods and improve consistency with compliance assessments, the Payment Card Industry Security Standards Council (PCI SSC), which manages security standards for the payment card industry, has published version 2.0 of the PCI PIN Security Requirements. The new requirements were published and became effective December 2014.

PCI PIN Security Requirements Updates

The PCI SSC updates provide a complete set of requirements for the secure management, processing and transmission of PIN data during online and offline payment card transaction processing at ATMs and point-of-sale (POS) terminals. This latest version is designed to:

- Improve acquirer and agent understanding of PCI PIN Security Requirements
- Provide detailed testing procedures to ease compliance testing and ensure consistent validation methods
- Enhance requirements for deployed points-of-interest (POI) devices
- Improve organization of "Remote Key Distribution Using Asymmetric Techniques Operations" and "Certification and Registration Authority Operations" requirements

Compliance Effective Dates

Until 30 June 2015, organizations may perform their 2015 PIN security assessments to validate PIN compliance using version 1.0 or version 2.0 of the PCI PIN Security Requirements. **Effective 1 July 2015**, all PIN security compliance assessments must be started according to version 2.0.

Visa reminds clients and acquiring third party agents that process or handle PIN data or perform cryptographic key management activities that they must comply with the PCI PIN Security Requirements and adhere to all applicable Visa Core Rules and Visa Product and Service Rules pertaining to PIN Security (ID#: 0027086), Plus System, Inc. Operating Regulations and Interlink Network, Inc. By-Laws and Operating Regulations.

Visa PIN Security Program Participants[1]

As communicated in the 11 December 2014 edition of the Visa Business News, organizations identified as Visa PIN Security Program Participants must perform their onsite security assessment by their respective validation deadlines but **no later than 31 December 2015**.

All other organizations that process PIN data must comply with the PCI PIN Security Requirements but are not required to perform an onsite assessment using a Visa Approved PIN Security Assessor. Visa recommends that these organizations verify their compliance by performing a self-audit, either with forms available from the Visa PIN website or by using an internal or external auditor to conduct an onsite review. Organizations must retain results from the self-audit or company-initiated onsite review as evidence of compliance. Visa reserves the right to request evidence of PIN compliance at any time.

Visit the Visa PIN Security website for more information on validation deadlines or contact your regional Visa PIN Risk Representative.

[1] These PIN program compliance validation requirements are applicable to Visa Inc. regions only. As a separate company, Visa Europe maintains its own rules. Specific compliance validation deadlines and non-compliance assessments do not apply to Visa Europe clients or their sponsored agents.

Additional Resources

Online Resources

Visit the Visa PIN Security web page

Visa Global Registry of Service Providers

Payment Card Industry Data Security Standard

The following documents are available at the PCI Standards & Documents Library under the PTS tab:

- PIN Security Requirements, v2.0
- PIN Security Requirements Modifications: Summary of Changes v 1.0 to 2.0

For More Information

For more information on the Visa PIN Security Program, PIN participant status or validation deadlines, email your regional Visa risk representative:

- AP and CEMEA: pinsec@visa.com
- Canada and U.S.: pinna@visa.com
- LAC: pinlac@visa.com
- Global: pin@visa.com