



Visa Announces Updates to PIN Security and Key Management Compliance Validation Program

Related Information

[Visa Business News Archive](#)

[Key Dates](#)

[Visa Online](#)

The *Payment Card Industry (PCI) PIN Security Requirements* is a comprehensive set of internationally aligned security requirements for safeguarding PIN data acquired at point-of-sale (POS) and ATM devices. Visa established the PIN Security and Key Management Compliance Program in 1995, based on the original *Visa Consolidated PIN Security Requirements*. In 2004, these requirements were aligned with MasterCard as the *PCI PIN Security Requirements*, which define secure cryptographic key management standards for the protection of PINs.

In addition to the *PCI PIN Security Requirements*, the Visa PIN Security and Key Management Compliance Program includes the *PCI POS PIN Entry Device (PED) Security Requirements* and the *PCI Encrypting PIN Pad (EPP) PED Security Requirements*, which define device attributes for physical and logical (functional) security characteristics. The PCI Security Standards Council adopted the PCI PED testing program in 2008 and plans to adopt the *PCI PIN Security Requirements*.

Visa is committed to protecting the Visa payment system and appreciates the efforts made by Visa clients to enhance PIN security. Compliance with the *PCI PIN Security Requirements* results in benefits beyond simply securing PIN data, as sound security practices help to protect organizations from adverse financial and reputational consequences associated with PIN data compromises.

Compliance with the *PCI PIN Security Requirements* and applicable PCI PED requirements (outlined in Appendix A of the *PCI PIN Security Requirements*) is currently required of any entity that accepts and processes Visa, Plus or Interlink PINs.

PIN Security and Key Management Compliance Framework

Visa has implemented a PIN Security and Key Management compliance framework within its regions, which establishes global validation requirements for PIN accepting/processing entities. This new framework establishes:

- A risk-based approach to identify program participants and validation levels for ATM and POS acceptance channels, and
- Common validation requirements comprised of on-site PIN security field reviews conducted by Visa or a delegated entity and the submission of PIN security self-attestations.

This compliance framework is based on the current risk environment that exists for cardholder PINs accepted at ATMs and POS PEDs. Visa will inform clients of any future changes to this PCI PIN validation framework based on further analysis of exploited vulnerabilities, emerging risks and threats to the payment system.

Global ATM and POS Levels and Validation Requirements

In addition to mandates for complying with the *PCI PIN Security Requirements* and PCI PED usage requirements, Visa has defined minimum validation levels based on connectivity, the number of PIN accepting devices, potential risk, and exposure introduced into the Visa payment system. The following tables define minimum ATM and POS PIN levels and validation requirements for *PCI PIN Security Requirements* and PCI PED compliance validation.

ATM Validation Levels

Validation Level	ATM Level Description	Validation Action	Validated By	Frequency
Level 1	<ul style="list-style-type: none"> Third party VisaNet processors Service providers (downstream processors) Certificate authorities Financial institution ATM acquirers deploying more than 250 ATMs Encryption Support Organizations (ESOs) with more than 1,000 devices supported annually 	Field review	Visa Field Reviewer	Every 5 years
		AND		
		Self-attestation	Internal or independent auditor and signed by an officer of the company	Annually
Level 2	<ul style="list-style-type: none"> Financial institution VisaNet processors Financial institution ATM acquirers deploying between 25–249 ATMs ESOs supporting fewer than 1,000 devices annually 	Self-attestation	Internal or independent auditor and signed by an officer of the company	Annually
Level 3	<ul style="list-style-type: none"> Financial institution ATM acquirers deploying fewer than 25 ATMs Sponsors of third party agent-deployed ATMs Visa affiliate endpoints* 	Attend Visa webinar OR Visa training OR Self-attestation	Internal or independent auditor and signed by an officer of the company	Every 3 years

*Includes Visa Debit Processing Service

POS PIN Validation Levels

Validation Level	POS PIN Level Description	Validation Action	Validated By	Frequency
Level 1	<ul style="list-style-type: none"> Acquiring VisaNet processors Financial institutions performing PED injections Service providers (downstream processors) Certificate authorities ESOs supporting more than 1,000 devices annually 	Field review	Visa Field Reviewer	Every 5 years
		AND		
		Self-attestation	Internal or independent auditor and signed by an officer of the company	Annually
Level 2	<ul style="list-style-type: none"> Merchants driving their own PEDs (Host Security Modules) and/or performing PED injections ESOs supporting fewer than 1,000 devices annually 	Self-attestation	Internal or independent auditor and signed by an officer of the company	Annually

Visa reserves the right to escalate any ATM or POS participant to a higher validation level or frequency. Additionally, new VisaNet processors must undergo a PIN security field review prior to processing production PIN-based traffic.

Compliance Validation Time Frames and Fees

Visa will notify Level 1 PIN Security and Key Management Program participants or their sponsors of their participant status, deadlines for submitting the PIN Security Attestation of Compliance form, and/or scheduling of an on-site PIN security field review. Starting in 2010, entities that are identified as Level 1 participants will be assessed an annual compliance program participant fee of US \$2,000. Benefits associated with this fee include Visa PIN Security and Key Management training for participant staff and on-site PIN security field reviews of participants every five years. Level 1 participants may send one staff member to attend the one-day Visa PIN Security Key Management Training each year **or** one staff member to attend the three-day Visa PIN Security Compliance Validation Training every three years. Additional attendees will be charged at published rates.

Visa reserves the right to request validation of PIN security compliance for all Level 1, 2 and 3 participants at any time and will notify Level 2 and Level 3 participants or their sponsors of applicable validation reporting requirements. If entities do not comply with *PCI PIN Security Requirements*, PCI PED usage requirements and related validation requirements, Visa will impose appropriate risk controls up to and including expulsion from the Visa payment system.

This compliance framework is based on the current risk environment that exists for cardholder PINs accepted at ATMs and POS PEDs. Visa will inform clients of any future changes to this PCI PIN validation framework based on further analysis of exploited vulnerabilities, emerging risks and threats to the payment system.

Plus ATM Network Third Party Agent Controls

This communication establishes minimum criteria for program participation and validation and does not supersede any applicable earlier deadlines, related education, reporting or enforcement programs already in place for Plus ATM Network third party agents and sponsors. Clients are reminded that Plus Independent Sales Organizations, ESOs, third party servicers and staff from sponsoring client financial institutions are required to attend a Visa PIN Security Key Management Training at least once every three years. In 2004, this requirement was enacted to ensure that clients and their agents have the necessary skills to properly safeguard PIN data.

Related Documents

Additional information on Triple Data Encryption Standard (TDES), as well as *PCI PIN Security Requirements* and PED security, may be found in the following Visa publications and on Visa websites. In addition, Visa will offer ongoing PIN Security and Key Management trainings throughout 2010. For more information on these trainings, go to www.visa.com/cisp.

Web Resources:

- To assist clients and merchants with questions regarding AFDs and Visa PED testing requirements, please refer to the *Visa General PED FAQ* at www.visa.com/cisp.
- To assist clients and merchants with questions regarding TDES requirements, please refer to the *Visa TDES FAQ* at www.visa.com/cisp.
- For the most recent listing of PCI-approved PEDs and other PCI PED testing program information, visit www.pcisecuritystandards.org/pin.
- For *Payment Card Industry POS and EPP PIN Entry Device Security Requirements* manuals, visit www.pcisecuritystandards.org/pin.
- For the *Visa PIN Security Tools and Best Practices for Merchants* brochure, visit

www.visa.com/cisp or contact the Visa Fulfillment Center at (800) 235-3580. Reference document number VRM 08.05.07.

- For the *Payment Card Industry PIN Security Requirements* manual, visit www.visa.com/cisp or the “Risk Management” section of [Visa Online](#).

Publications:

- “2009 Visa PIN Security Update on Visa’s Compliance Policy to Facilitate Triple Data Encryption Standard Usage,” April 22, 2009, *Visa Business News*.
- “2010 Visa PIN Security and Key Management Training Series,” November 18, 2009, *Visa Business News*.
- “Visa Publishes U.S. List of Registered Encryption Support Organizations,” November 4, 2009, *Visa Business News*.
- “Reminder—PIN-Entry Device Testing Program Changes Effective December 31, 2007,” October 2007, *Visa Business Review*, Issue No. 071023.
- “Visa Announces a New Category for Unattended PIN Entry Devices,” June 2007, *Visa Business Review*, Issue No. 070619.
- “PIN Pad Found Vulnerable to Skimming Attacks,” March 2007, *Visa Business Review*, Issue No. 070327.
- “Visa PIN Security Initiatives and Controls for Merchants,” November 2006, *Visa Business Review*, Issue No. 061121.
- “PIN Security Best Practices for Merchants,” June 2006, *Visa Business Review*, Issue No. 060620.
- “Members Are Reminded that POS PIN Pads Susceptible to Skimming Attacks Must Be Replaced,” February 2006, *Visa Business Review*, Issue No. 060214.
- “PIN Security Best Practices for Merchants,” June 2006, *Visa Business Review*, Issue No. 060620.
- “Visa Announces Triple Data Encryption Standard Implementation Requirements,” August 16, 2005, *Visa Business Review*, Issue No. 050816.
- “Visa Announces Initial Triple DES Implementation Requirements,” August 2002, *Visa Business Review*, Issue No. 020813.

For More Information

For questions regarding the new Visa PIN Security and Key Management Compliance Validation Framework, e-mail pinusa@visa.com. For more information regarding the Visa PIN Security and Key Management Compliance Program or the PCI PIN Security Requirements, go to www.visa.com/cisp.