Visa Business News

PIN Security

1 April 2021

Updates to PCI PIN Security Requirements and PIN Security Program News

Global | *Acquirers, Issuers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: The Payment Card Industry Security Standards Council (PCI SSC) has published version 3.1 of the *PCI PIN Security Requirements*. The revised standard is effective immediately and organizations may validate to v3.0 or v3.1 through 30 September 2021. Beginning 1 October 2021, all new assessments must be performed against PCI PIN v3.1. In addition to alerting clients of the updated PIN security requirements, this article is also reminding stakeholders about other important PIN security news.

The *PCI PIN Security Requirements,* which is a Visa Supplemental Requirements document, defines technical and procedural controls to assist with the secure management, processing and transmission of cardholder PIN data during online and offline payment card transaction processing at ATMs and POS terminals. Visa requires compliance with these requirements.

Mark Your Calendar:

- Required validation to PCI PIN v3.1 **(1 October 2021)**

Visa encourages all stakeholders in the payment ecosystem to review the *PCI PIN Security Requirements—Summary of Requirements Changes from v3.0 to v3.1* and the updated *PCI PIN Security Requirements and Testing Procedures v 3.1*, both of which are available online from the PCI SSC Document Library (filter by PIN).

Changes to the PCI PIN v 3.1 security requirements are summarized below:

- Existing effective dates to support the new International Organization for Standardization (ISO) PIN Block Format 4 have been suspended until further notice.
- Effective dates have been updated for phases 2 and 3 of key block implementation to reflect a previously-issued PCI bulletin.
- Encrypted key loading dates have been aligned with a previously-issued PCI bulletin, which deferred the implementation dates by three years, and the applicability changed from point-of-interaction (POI) v3 and higher devices to POI v5 and higher devices.
- Language has been clarified on use of RSA keys sizes of 1024 and 2048 and SHA-1/SHA-2 when used for key distribution in accordance with Annex A.

The *PCI PIN Security Requirements and Testing Procedures v3.1* was published in March 2021 and is **effective immediately**. For entities that are required to submit validation documents to Visa, assessments can be performed against v 3.0 or v3.1 through 30 September 2021. **Effective 1 October 2021**, all new assessments must be performed to v3.1.

Note: Visa will no longer accept v 3.0 PIN Attestation of Compliance (AOC) documents **after 1 January 2022**.

Additional PIN Security Program News and Reminders

All stakeholders should be aware of the following news and reminders.

- **PCI PIN entry devices (PED) v3.0 security approval expires 30 April 2021**

  In March 2020, PCI SSC published a security bulletin informing the payment community that the PCI Council extended the PIN Transaction Security (PTS) POI v3.0 security approval expiration date for one year. As a reminder, the revised expiration date is now 30 April 2021.

  Visa's PIN Security Program requires industry participants to use PCI PTS devices for cardholder PIN entry.[1] PCI PTS devices are listed on the PCI Approved PTS Device List. Each device is assigned a 10-year security approval expiration date to correspond to the published security requirements that the device was evaluated against. For example, PED v3.0 devices were evaluated to security requirements that were published in 2010. Therefore the PED v3.0 security approval expiration date is 30 April 2021 (originally 30 April 2020).

  Understanding that attack vectors and threats evolve, the security approval expiration date is an indication the device may no longer be able to withstand modern day attacks, even though the device is still functional. Visa allows continued use of PEDs with expired security approvals, but recognizes that the risk of compromise and data loss increases following the security approval expiration date.

  Organizations that have PCI PTS PEDs with expired security approvals should refer to *Appendix B—Visa PED Hardware Requirements* in the *Visa PIN Security Program Guide*, (a Visa Supplemental Requirements document) to understand the requirements for devices with expired security approvals, including purchasing, deployment, usage and sunset / replacement dates for each version.

  [1] Approved PCI SPoC or Visa Ready solutions may be allowed for PIN entry on COTS devices. Contact your regional PIN Program Manager for additional information.

- **Key block effective dates have been extended**

  As announced in the 6 August 2020 edition of the *Visa Business News*, the PCI SSC has extended the effective dates of the PCI PIN key block requirements for Phase 2 and Phase 3. Visa's PIN Security Program and VisaNet requirements for exchanging keys in the key block format will align with the revised dates. Refer to the PCI SSC security bulletin that communicates the updated effective dates and previously published Visa technical letters outlined in the 6 August 2020 *Visa Business News* article for additional information.

- **PIN participants must rotate PIN assessors**

  Validating PIN participants are reminded to rotate their PIN assessor company and individual assessors after two consecutive review cycles for a given facility, unless approved or specifically directed by Visa. This practice helps with ensuring that assessments are performed in an objective and thorough manner.

  Refer to the *Visa PIN Security Program Guide* on the Visa PIN Security Program page to understand all requirements, including which organizations are required to validate PIN security compliance with Visa and the processes associated with the Visa PIN Security Program.

Client Responsibilities

Clients must continue to:

- Ensure that all agents are appropriately registered in the Visa Third Party Agent (TPA) Registration Program. Contact your regional Visa representative to obtain information about the registration process.
- Ensure that their acquiring TPAs that process or handle PIN data comply with the PCI PIN security requirements and adhere to the Visa Rules.
- Ensure that their own processing environments that handle PIN data comply with the PCI PIN security requirements.
- Perform the necessary due diligence prior to engaging any TPA, and maintain policies and procedures to provide the correct level of oversight and control of the agent.

Clients that use agents identified as validating PIN participants that have not performed an on-site PIN assessment or have areas of non-compliance may be subject to non-compliance assessments as defined in the Visa Rules.

For More Information

Merchants and third party agents should contact their acquirer.