Visa PIN Security Program Update

Summary:

Visa has announced the sunset of its PIN Security compliance program, effective October 1, 2023.

Q&A:

Q: Why is Visa sunsetting its PIN compliance program?

A: Visa's decision to sunset the compliance program reflects a shift towards a multi-layered security approach, recognizing the evolving landscape of payment security and where the risks of a PIN compromise sit comparatively to other emerging data compromise trends prevalent in the industry.

Q: Will acquirers, Third Party Agents, and Processors still be required to be compliant with PCI PIN Security requirements?

A: Yes, they remain responsible for protecting PIN data in accordance with industry security standards and Visa Rules at all times. Additionally, the sunset of the compliance program does not waive or alter any fees, non-compliance assessments or other liabilities associated with a compromise resulting from a violation of the Visa Rules which results in the loss of Visa account data with PIN. It is important to emphasize that Visa's decision to update its compliance program should not be misinterpreted as a reduced emphasis on the PCI PIN standard. Compliance with the industry standards is necessary to maintain a secure payment ecosystem.

Q: Will entities still be required to submit to Visa evidence of compliance with PCI PIN Security Requirements?

A: While Visa does not require scheduled submissions of validation of compliance with PCI PIN Security Requirements, acquirers, third-party agents, and processors, who are involved in handling PINs for Visa transactions or provide key management functions or support PIN entry devices, must maintain compliance with PCI PIN Security Requirements. This is achieved through a Qualified PIN Assessor (QPA) to carry out the assessment.

Q: Can entities validate compliance with PCI PIN Security Requirements through a self-assessment?

A: No, PCI PIN Security Attestation of Compliance requires a Qualified PIN Assessor to test and assess the requirements and controls and be conducted at least every 2 years.

Q: Does the program sunset affect the type of POI acceptance devices that can be used by merchants?

A: No. PCI PIN Security Requirements mandate that all cardholder-entered PIN must be entered in a device that is validated and approved against one of the following:

- One of the versions of the PCI PTS standard, as members of Approval Classes EPP, PED, SCRP or UPT (collectively known as POI Devices) and Approval Class HSMs, or
- FIPS 140-2 or FIPS 140-3 level 3 or higher

When the POI devices are purchased and owned by a merchant, the acquiring entity sponsoring the usage of the devices into a payment network ultimately bears the responsibility for any non-compliance.

Are acquirers expected to remove PTS devices with expired approvals from production?

A: Already deployed devices can remain in use beyond the expiration of their PCI PTS approval, but it is recommended that they are replaced as soon as they are added to the PCI's PIN Transaction Security Devices With Expired Approvals list.

Q: Will the sunset affect my listing on the Visa Global Registry of Service Providers?

A: Yes, since the PCI PIN validation documents will no longer be submitted to Visa, the existing entities listed on the Visa Global Registry will remain until the document expires and the information will subsequently drop from the site.

Q: What if I have additional questions?

A: Please contact your Visa Account Executive or Ecosystem Data Security team if you have additional questions.