Issuers and Payment Card Industry Security Standards

This Frequently Asked Questions (FAQ) document provides guidance for issuers on Visa data security programs and Payment Card Industry (PCI) standards that may be applicable within an issuer environment:

Topics include:

- PCI Data Security Standard (DSS)
- PCI Payment Application Data Security Standard (PA-DSS)
- PCI Software Security Framework
- PIN Management Requirements
    - PCI PIN Security Requirements
    - PCI PTS Point of Interaction (POI) Modular Security Requirements
    - Visa Hardware PIN Entry Device (PED) Requirements

Frequently Asked Questions

Issuers and the PCI DSS

Q: Are issuing banks required to comply with the PCI DSS?

- Yes. All organizations, and their Agents, that store, process or transmit Visa account data are required to comply with the PCI DSS. *(Visa Rules ID#0002228).* This is inclusive of issuers.

Q: Are issuing banks required to validate PCI DSS compliance with Visa?

- Visa-issuing members that are directly connected to VisaNet and that process on behalf of other Visa members must validate PCI DSS compliance and provide attestations to Visa for new connection requests.

  As a best practice, Visa recommends issuers, even if not directly connected to VisaNet, validate compliance to ensure they have the appropriate security controls in place. This validation may be performed by a PCI Qualified Security Assessor or internal resources. The PCI SSC offers PCI DSS training and certification through the Internal Security Assessor (ISA) Training Program to assist with an internal assessment process and has other educational resources available on their website at *www.pcisecuritystandards.org.*

Q: Are third party processors and agents required to comply with the PCI DSS?

- Yes. All third party processors and agents that provide payment-related services to Visa clients (issuers and acquirers) must annually validate PCI DSS compliance and provide attestations to Visa. Visa clients, including issuers, must register their third-party processors and agents with Visa and provide the necessary oversight to ensure these third parties adhere to the requirements of *Visa Third Party Agent Program*.

Q: Can issuing banks be PCI DSS compliant if they store sensitive authentication data (SAD)?

- Yes. PCI SSC provides guidance that clarifies that companies that perform, facilitate or support payment card issuing services are permitted to store SAD, **if there is a legitimate business need to store such data.**

Q: Which of the PCI DSS requirements pertain to ATM vendors, ATM owners and ATM processors?

- Regarding ATM provisioning or ATM servicing, there are many different service option configurations and managed services; each case may have a unique configuration. For each entity that deploys, services or provisions ATMs, Visa recommends contracting with an approved PCI Security Standards Council (SSC) Qualified Security Assessor (QSA) to determine the applicability of the PCI DSS requirements to the defined in-scope environment.

Q: Are ATMs within the scope of the PCI DSS?

- Yes. PCI DSS applies to any entity that stores, processes or transmits cardholder data. The ATM network and the physical environment in which it resides must also comply with the PCI DSS. It is critical to ensure that access to the ATM processing environment is protected to guard against ATM Cashout-type attacks.

Q: Can ATMs be PCI DSS compliant if those ATMs store sensitive authentication data (SAD)?

- SAD may only be retained if it is stored securely, in accordance with the PCI DSS, and if there is a legitimate business reason to do so. It is recommended that financial institutions that have managed ATM application logs that store sensitive authentication data work with their managed service provider to ensure that sensitive cardholder data is protected throughout its life cycle (which may include research and resolution activities), and that technologies such as data field encryption or tokenization are used.

Q: For Visa's PCI DSS compliance validation requirements, are banks that acquire ATM transactions (i.e., cash disbursements only) considered to be merchants?

- In accordance with Visa-defined merchant[1] PCI DSS compliance validation levels, a bank that acquires ATM transactions (i.e., cash disbursements only) **is not** considered to be a merchant. However, a bank offering product sales (e.g., postage stamps) via an ATM **is** considered to be a merchant, and all such transactions acquired by all participating ATMs must be aggregated to determine the merchant level and any validation requirements.

  Banks must ensure that their merchants comply with Visa's Account Information Security (AIS)

[1] A "merchant" is any business entity that accepts Visa payment cards as a form of payment for goods or services rendered.

program and validate at the appropriate merchant level.

Q: For Visa's PCI DSS compliance validation requirements, are issuing banks with branches that process cash advances considered to be merchants?

- In accordance with Visa-defined merchant PCI DSS compliance validation levels, banks that process cash advances **are not** considered to be merchants. Banks must ensure that cash advance transactions are properly coded in accordance with Visa Rules.

Q: For Visa's PCI DSS compliance validation requirements, are issuing banks that accept payment cards for products or services (such as account fees or mortgage payments) considered to be merchants?

- In accordance with Visa-defined merchant PCI DSS compliance validation levels, bank branches that accept Visa- or Interlink-branded cards as payment for products or services are considered to be merchants. All such transactions acquired by participating bank branches must be aggregated to determine the merchant level and any validation requirements.

  Additionally, if a branch accepts Interlink (PIN required), the bank must comply with the Visa PIN Security Program.

Issuers and the PA-DSS / Software Security Framework (SSF)

Q: Are ATMs within the scope of the PA-DSS?

- The PA-DSS applies to payment applications that store, process or transmit cardholder data as part of authorization or settlement. As a best practice, ATM core processing applications should adhere to the PA-DSS.
  Some ATM vendors have included PA-DSS approved applications on the *List of Validated Payment Applications*. To further protect the ATM environment, members are encouraged to work with vendors to purchase and install PA-DSS validated applications only.
  Note: *Existing PA-DSS payment applications will eventually be replaced by the application and the validation programs within the PCI Software Security Framework (SSF). Acceptance of new PA-DSS application validations will continue until June 30, 2021, and all PA-DSS validated payment applications will remain current and continue to be governed under the PA-DSS program until the expiry date for those applications is reached (October 2022 for payment applications validated to PA-DSS v3.2).*

Issuers and PIN Security

Q: Are issuing banks with Visa / Plus-accepting ATMs required to comply with the PIN Management Requirements Documents?

- Yes, compliance with the PCI PIN Security Requirements is required of all Visa / Plus members that acquire interchange PIN-based transactions (including any ATM that is owned or branded by the financial institution that accepts Visa or Plus products regardless of the vendor,

processor, independent sales organization (ISO), ATM connectivity, or agent used to manage or deploy / support the ATM). These requirements do not apply when only "on us" transactions are performed.

The Encrypting PIN Pads (EPPs) that are used in ATMs must be evaluated against and comply with the PCI PTS POI Modular Security Requirements. Compliant devices are listed as an approved device on the PCI SSC website. Review the *Approved PIN Transaction Security Devices* list to confirm that approved versions of the devices have been deployed.

PIN entry devices, including EPPs that have an expired PCI PTS security approval, must abide by the Visa Hardware PIN Entry Device Requirements for purchasing, usage, deployment and sunset/retire dates for expired devices. Visa Hardware PIN Entry Device Requirements can be found in Visa PIN Security Program Guide, Appendix B.

Q: Do issuing banks with Visa / Plus-accepting ATMs need to validate to the PIN Management Requirements Documents with Visa?

- Issuers that manage their own ATMs are required to comply with the PCI PIN Security requirements but are not considered a Validating PIN Participant and are not required to validate. However, Issuers do have responsibility for ongoing PIN security and are encouraged to review the Visa PIN Security Program Guide available on the Visa PIN website, www.visa.com/pin. Also available on Visa Online is the Issuer PIN Security Guidelines which are tailored to an issuer's environment.

Q: Do issuing banks that acquire Visa / Plus ATM transactions need to comply with the PCI DSS and Visa PIN Security Program if ATM driving, processing and maintenance is performed by a third party processor or agent?

- Yes, ATM owners and sponsors must ensure that their ATMs comply with applicable PCI DSS Requirements and the PIN Management Requirements Documents regardless of an ATM's connectivity or the processor or agent used to maintain and support an ATM.

Q: How can ATM deployers and their agents ensure that EPPs purchased are approved for use?

- ATM owners and their agents should review the *Approved PIN Transaction Security Devices* list to confirm that a device matches all of the following items as listed: model name, hardware number, firmware number, and, if applicable, application number and loader version.

When making purchasing decisions, ATM owners and their agents should be aware that some vendors may sell the same model EPP in both approved and unapproved versions. Note: EPPs that have an expired PCI PTS security approval must abide by the Visa Hardware PIN Entry Device Requirements for purchasing, usage, deployment and sunset/retire dates for expired devices. Visa Hardware PIN Entry Device Requirements can be found in Visa PIN Security Program Guide, Appendix B.