Issuers' Payment Card Industry Data Security Standard Frequently Asked Questions

This frequently asked questions (FAQ) document provides guidance for issuers and the ATM environment on Visa-specific programs that mandate compliance with the following Payment Card Industry (PCI) standards:

- PCI Data Security Standard (DSS)
- PCI Payment Application Data Security Standard (PA-DSS)
- PCI PIN Security Requirements
- PCI Encrypting PIN Pad (EPP) Security Requirements

In addition to reviewing this FAQ document, Visa encourages all payment system participants to review the *General PIN-Entry Device Frequently Asked Questions* document available at www.visa.com/cisp.

Issuer Members: PCI Data Security Standard FAQ

1. Are issuing banks required to comply with the PCI DSS?

Yes, all Visa issuing and acquiring members and their sponsored agents, processors and/or service providers that store, process or transmit card data are required to comply with the PCI DSS. Visa members must also ensure that their agents are in compliance with these data security requirements. *(Visa International Operating Regulations, ID#: 010410-010410-0008031)*

2. 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.

3. 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 annually validate PCI DSS compliance with Visa.

As a best practice, issuers not directly connected to VisaNet should also validate compliance. This validation may be performed by a QSA or an internal auditor. The PCI SSC offers PCI DSS training and certification through the Internal Security Assessor (ISA) Training Program.

4. Are third party processors required to comply with the PCI DSS and validate compliance with Visa?

Yes, third party processors that store, process or transmit Visa cardholder data are required to comply with the PCI DSS and validate compliance with Visa.

5. Can issuing banks be PCI DSS compliant if they store sensitive authentication data?

The PCI SSC has clarified that companies that perform, facilitate or support payment card issuing services are allowed to store sensitive authentication data **if there is a legitimate business need to store such data** *(PCI Data Security Standard, Requirement 3.2)*.

All other PCI DSS requirements apply to issuers. **Note**: An issuer must have a legitimate reason to store sensitive authentication data (sensitive authentication data cannot be stored solely because it is convenient), and must protect such data in accordance with the PCI DSS.

6. Are an issuing bank's ATMs within the scope of the PCI DSS?

Yes. The PCI SSC states that the PCI DSS applies to any entity that stores, processes or transmits cardholder data. The ATM's network and the physical environment in which it resides must also comply with the PCI DSS.

7. Are an issuing bank's 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.

8. Can an issuing bank's ATMs be PCI DSS compliant if those ATMs store sensitive authentication data?

Sensitive authentication data 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.

9. For Visa PCI DSS compliance validation requirements, are issuing banks that acquire ATM transactions (i.e., cash disbursements only) considered to be merchants*?

In accordance with Visa-defined merchant 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 identified as a Level 4 merchant based on the aggregate total of annual product sales transactions may decide at their own discretion to validate PCI DSS compliance.

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

10. For Visa 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.

11. For Visa 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 be in full compliance with the PCI PIN Security Requirements and the PCI POS PIN Entry Device Security Requirements.

Banks identified as Level 4 merchants based on the aggregate total of annual product sales transactions may decide at their own discretion to validate PCI DSS compliance.

Issuer Members: PCI PIN Security and PCI EPP FAQ

12. Are issuing banks with Visa / Plus-accepting ATMs required to comply with the PCI PIN Security Requirements and the PCI EPP Security Requirements?

Compliance with the PCI PIN Security Requirements is required of all Visa / Plus members that acquire interchange PINs (including any ATM that is owned or branded by the financial institution that accepts not "on-us" 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).

ATM deployers must also be in full compliance with the PCI EPP Security Requirements. For more information, refer to the *General PIN-Entry Device FAQ* document.

13. Do issuing banks with Visa / Plus-accepting ATMs need to validate PCI PIN security compliance and PCI EPP security compliance with Visa?

In the 18 November 2009 edition of the Visa Business News, Visa announced a new PIN security compliance validation framework in the article titled, "*Visa Announces Updates to PIN Security and Key Management Compliance Validation Program*". Financial institutions with ATMs should refer to this announcement and determine their compliance validation level.

In early 2010, Visa notified all Level 1 PIN Security Program participants of their Level 1 compliance level. These participants are required to annually submit a PIN Security Attestation of Compliance to Visa.

14. Do issuing banks that acquire Visa / Plus ATM transactions need to comply with the PCI PIN Security Requirements, the PCI DSS Requirements and the PCI EPP Security Requirements 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 PIN Security Requirements, the PCI DSS Requirements and the PCI EPP Security Requirements regardless of an ATM's connectivity or the processor or agent used to maintain and support an ATM.

15. What are the Visa requirements for the use of PCI-approved EPPs within ATMs?

Effective 1 October 2005, all newly deployed EPPs (including replacements or those in newly deployed ATMs) must pass testing by a PCI-recognized laboratory and be PCI-approved for new deployments. For more information, refer to the *General PIN-Entry Device FAQ*.

16. How can ATM deployers and their agents ensure that EPPs purchased comply with applicable PCI EPP Security Requirements?

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.