Visa PIN Security Program Frequently Asked Questions

1. **Q. Which Visa Rule applies to PIN Security and where can I find it?**
   A. Visa Rule ID# 151014-100512-0027086 is in the "Visa Core Rules and Visa Product and Service Rules" which can be found on www.visa.com. Use the search function on the website to enter the document name and locate the latest version.

2. **Q. Where can I find a copy of the Visa PIN Security Program Guide?**
   A. The Visa PIN Security Program Guide is currently a Visa Confidential document and can be downloaded from the Visa Online website www.visaonline.com. A public version of the document should be published in October 2015 on the www.visa.com/pinsecurity webpage.

3. **Q. Do Visa PIN Security Program participants need to be registered with Visa?**
   A. Yes, Encryption Support Organizations (ESOs), Third-Party Service (TPS) providers and VisaNet Processors must be registered by sponsoring financial institutions. For additional information contact:
   - AP and CEMEA: Agents@visa.com
   - Canada and U.S.: AgentRegistration@visa.com
   - LAC: AgentRegistrationLAC@visa.com

4. **Q. Who do I contact to confirm that my company is a validating PIN Security Program participant?**
   A. If you are unsure of your status please contact your regional PIN risk representative, email addresses are listed below in Question 30.

5. **Q. I do not currently process PIN transactions. However, I want to start processing PIN transactions for other Visa clients. Do I need to be registered as a PIN Security Program participant and have an onsite review performed before I can begin processing for others?**
   A. You will need to inform Visa of your intention first and an onsite review must be conducted by an approved Visa PIN Security Assessor. Upon completion of all validation and registration requirements, your organization will be included on the Global Registry of Service Providers and you may begin PIN processing services on behalf of other Visa clients. Contact your regional Visa risk representative for more information.

6. **Q. I have an existing Visa endpoint and currently acquire non-PIN transactions. What is required if I want to start acquiring PIN transactions?**

   A. All VisaNet Processors adding PIN acquiring services for the first time must inform Visa of their intention and first have an onsite review conducted by an approved Visa PIN Security Assessor. Upon completion of all validation you may begin PIN processing services. This applies to any VisaNet endpoint owner, old or new. Contact your regional Visa risk representative for more information.

7. **Q. Where can I find all of the documents for the Visa PIN Security Program requirements?**
   A.

   1.) VisaOnline

   Visa Online is your online destination for doing business with Visa. It has the PIN Security Program Guide. Visit VisaOnline to download the latest version.

   2.) Visa.com/PINSecurity

   Visa maintains a publically available webpage that contains links to Visa program requirements, FAQs, PIN SAQs, compliance validation information and other resources that are beneficial to all PIN program participants.

   3.) PCISecurityStandards.org

   The PCI Security Standards Council maintains a document library website where the PCI PIN Security Requirements are published. Select the PTS tab from the "Documents Library." If you cannot locate something, contact your regional PIN Security Representative.

8. **Q. What happens if I do not validate according to the Visa PIN Security Program requirements?**
   A. Visa will work with all validating PIN security participants to ensure that they can secure sensitive PIN information. Existing entities that are not able to meet the program requirements are required to provide remediation plans to Visa.

   Any client who sponsors a validating participant that does not validate compliance and does not provide remediation plans will be subject to non-compliance assessments as follows:

Violation	Non-Compliance Assessment
Initial violation and each month of unaddressed violations, up to 4 months after the initial violation	USD 10,000 per month
Violations after 4 months and each month thereafter	USD 25,000 per month

9. **Q. How will differing interpretations of the Payment Card Industry (PCI) PIN Security Requirements be resolved?**
   A. Requests for clarification of the PCI PIN Security Requirements or PCI PIN Transaction Security Point of Interaction (POI) requirements should be directed to the PCI Council at pcipts@pcisecuritystandards.org.

   Clarification on Visa's PIN Entry Device (PED) requirements, including encrypting PIN pads (EPP) or TDES mandates, and program requirements should be directed to your local Visa PIN risk representative.

10. **Q. Will Visa accept validations for PCI PIN Security Requirements v1 after July 1, 2015?**
    A. Yes. If a Visa approved Security Assessor started an onsite assessment before July 1, 2015, Visa will accept a v1 VAOC after July 1, 2015.

11. **Q. If my assessment began (interviews, etc.) prior to June 30, 2015 and the onsite visit occurs after June 30, 2015, will Visa still accept a v1 assessment?**
    A. Until June 30, 2015, organizations may perform their 2015 PIN security assessments to validate PIN compliance using version 1 or version 2.0 of the PCI PIN Security Requirements. Effective July 1, 2015, all PIN security compliance assessments must be started according to version 2.0. Contact your regional PIN representative for additional information.

12. **Q. Can I deploy my stock of expired v1 PTS POI PIN encryption devices**
    A. Expired devices may be deployed after the expiration date only if the device was purchased prior to the expiration date. Security assessors will look at purchase orders to determine compliance. See the Visa PIN Entry Device Requirements for more information.

13. **Q. When will Visa mandate sunset dates for expired v1 PTS POI PIN encryption devices?**
    A. Visa is aware that many organizations are investing in newer PEDs to support EMV conversations and take advantage of the new functionality that is available with the newer devices. Therefore Visa has not specified a sunset mandate that requires the removal of version 1 PTS devices from the payment system network. Visa anticipates version 1 devices to be replaced through attrition.

    However, depending on the rate of adoption of newer terminals, Visa may issue a mandate in the future. The full set of PED requirements can be found on Visa's PIN security website, www.visa.com/pinsecurity.

14. **Q. Is there a pre-PCI PED mandate coming for unattended devices?**
    A. Visa is aware that many organizations are investing in new technology and we expect that

through attrition these devices will be replaced. Visa may issue a mandate in the future. The full set of PED requirements can be found on Visa's PIN security website, www.visa.com/pinsecurity.

15. **Q. Can my organization's internal audit or security group perform the onsite PIN Security assessment?**
A. Maybe. Whether an internal auditor may perform your organization's onsite PIN assessment is dependent on the type of PIN program participant your organization is defined as.

Validating PIN Program Participants - No, onsite PIN security assessments must be performed by an approved Visa PIN Security Assessor. Review the Visa Approved Security Assessor List to identify and obtain contact information for assessors.

Non-Validating PIN Program Participants - Yes, you may use internal or external resources to perform the PIN security assessment. It is highly recommended to have the assessment performed by a qualified security professional.

16. **Q. What is the process that will be used to ensure that a company on the approved security assessor list is used?**
A. Visa will only accept validation materials (VAOC) from Visa approved security assessors.

17. **Q. Can my organization (a validating PIN program participant) use a security company or individual that is not listed on the Visa Approved Security Assessor List to validate compliance to Visa?**
A. No. Visa will only accept submissions from Visa approved security assessors. Visa has verified each assessor on the Visa Approved Security Assessor List and has a service agreement in place with them specifically for the Visa PIN Security Program.

18. **Q. How do I get added to Visa's Approved Security Assessor List?**
A. Visa's Approved Security Assessor list is managed for the purpose of having verified companies available to Visa PIN security program participants that need to validate compliance to Visa. If the respective Visa market requires more security assessors due to increase in demand, then Visa will add more assessors. Please contact your local Visa PIN risk representative for additional information.

19. **Q. Will Visa pay for the onsite PIN Security assessment?**
    A. No. Any fees and/or expenses associated with the onsite assessment are settled between the validating participant and the Visa approved security assessor.

20. **Q. Can I use the same Visa approved Security Assessor every review cycle?**
    A. An individual SA must not assess the same organization more than two consecutive review cycles unless approved or specifically directed by Visa. For more information contact your regional PIN Risk Representative.

21. **Q. Why are we limited to using the same Security Assessor twice? If we have used them twice, are we ever able to use them again?**
    A. Visa aligns with industry best practices regarding assessor independence. Once this requirement has been met, organizations may use a previously used Visa approved security assessor for the next two cycles.

22. **Q. When identifying what an approved Visa PIN Security Assessor can/cannot do, can you provide any conflict of interest guidance on an approved Visa PIN Security Assessor providing a review and either the same Security Assessor or their organization providing security consulting.**
    A. An approved Visa PIN Security Assessor must not perform an audit of their own work or of an environment that they have helped to design and create. Visa approved security assessors must perform onsite assessments independently in both fact and appearance. If an organization previously engaged an approved Visa PIN Security Assessor or their company for security consulting, advisory roles or direct employment, then a conflict of interest may exist and the organization may need to engage a different Visa approved security assessor for onsite reviews.

    An approved Visa PIN Security Assessor may provide guidance on how to remediate any issues found during the onsite assessment without impairing their independence, however they cannot sell additional services to help you achieve compliance.

    If you are unsure if a conflict of interest exists please contact your local Visa PIN risk representative for clarification.

23. **Q. What if I want to buy additional services from my Visa approved security assessor?**
    A. You can freely buy services as long as they do not influence the outcome of your PIN security onsite assessment. An approved Visa PIN Security Assessor or their company should not require you to purchase any service in order for your company to pass the assessment.

24. **Q. Will the Visa approved security assessor be listed on the PCI Security Council website?**
    A. No. The list of Visa approved Security Assessors will be available on www.visa.com in the "Visa Approved Security Assessors (SA) List" document. Use the search function on the website to enter the document name and locate the latest version.

25. **Q. What if my participation status changes? For example, what if a financial institution starts processing PIN data on behalf of other financial institutions?**
    A. An onsite PIN Security review by an approved Visa PIN Security Assessor is required before a financial institution can begin processing PIN data for another financial institutions. Contact your local Visa PIN risk representative for more information.

26. **Q. Can an organization be listed on the Global Registry of Service Providers even if it processes its own PIN data?**
    A. Yes, an organization not formally identified as a validating participant may undergo an onsite review performed by an approved Visa PIN Security Assessor to demonstrate its PIN Security compliance. Once Visa receives the Visa Attestation of Compliance (VAOC), the organization will be listed on the Global Registry of Service Providers.

27. **Q. Can I get an extension to complete validation?**
    A. Participants are required to validate compliance every 24 months. Validating participants that expect to submit their validation materials late must inform Visa before their validation deadline. The PIN security program manager from Visa will request a remediation plan depending on the reason for late submission. The validation date will not be changed unless the company is removed from Visa's Global Registry of Service providers.

28. **Q. How do I know my validation date?**
    A. If you have not validated compliance since the end of 2012 then your validation deadline is December 31, 2015. If you validated your compliance to Visa at any time since the start of 2013 then your next validation date is the last day of the month you achieved compliance plus 24 months.

    Validated participants can also find their "valid through date" on Visa's Global Registry of Service Providers.

29. **Q. Are these program changes applicable to Visa Europe?**
    A. These program modifications are applicable to Visa Inc. regions only. Visa Europe maintains separate rules.

30. Q. Who should I contact with questions?

A. You may contact your Visa PIN risk representative at the following e-mail addresses:

- AP and CEMEA: pinsec@visa.com
- Canada and U.S.: pinna@visa.com
- LAC: pinlac@visa.com
- Global: pin@visa.com

31. Q. What is the difference of a remediation plan and compliance validation plan

A. When a validating participant is not able to meet their validation deadline they must submit either a remediation plan or a compliance validation plan.

Remediation Plan

- Identifies areas of noncompliance determined by the Visa approved security assessor and action plan to correct
- Includes dates of when noncompliance will be corrected

Compliance Validation Plan

- Identifies date when the compliance validation review will be performed
- Specifies the Visa Approved Security Assessor's name that is contracted to perform the review
- Visa will only accept Compliance Validation Plans until 31 December 2015

Either type of plan must be submitted to Visa before the validation deadline to avoid noncompliance assessments. Sponsoring Visa clients must first review and accept the remediation/compliance validation plan and provide a copy of the documentation to a Visa PIN Risk representative.

Visa reserves the right to reject remediation/compliance validation plans