Europe PIN Security Program Modifications Frequently Asked Questions

1. **Q. When do the changes to the Visa Europe PIN Security Program go into effective?**
   A. Effective dates for the program modifications are as follows:

January 1, 2018	• Submission of Self-Assessment Questionnaires (SAQs) to Visa discontinued • Visa to update the Visa Security Assessor List with assessors from the Europe region
April 2018	• Communicate to Europe stakeholders PIN Security Program changes • Visa to contact Validating and Non-Validating Participants regarding revised compliance validation requirements • Visa to contact existing Europe PIN Participants to close open PIN assessment findings
May 2018	• Visa to host a webinar to review program changes • Visa to publish a revised version of the *PIN Security Program Guide* and FAQ
July 2018	• Changes to Visa in Europe PIN Security Program become effective • Validating Participants contract directly with PIN Security Assessors (SAs) for on-site PIN assessment services • Visa Approved Security Assessors track remediation efforts for on-site assessments and provide attestation of compliance to Visa • Visa to add Validated Participants that have demonstrated compliance to Visa PIN Security requirements on the Global Registry of Service Providers

2. **Q. Changes to Europe Visa PIN Security Program, including changes to on-site assessments, become effective in July 21, 2018. What if I am scheduled for an on-site PIN assessment before July 2018?**
   A. Validating Participants may continue with existing on-site assessments that have been previously scheduled. Validating PIN Program Participants that are not performing an onsite assessment before July 21st, will receive a letter in April with information about the program changes and their organization's next validation due date.

3. **Q. Since submitting a PIN Self-Assessment Questionnaire (SAQ) is no longer required, what happens to previously submitted SAQs that had open findings?**
   A. For SAQs and on-site PIN assessments performed during or prior to 2017, Visa notify these organizations directly with instruction to close existing issues.

4. **Q. When does the new validation requirements become effective?**
   A. Validation requirement modifications will take place according to the following timeline:

   - ***SAQs:*** Effective January 1, 2018, submitting PIN SAQs to Visa is no longer required. Organizations identified as Non-Validating Participants should continue to evaluate their PIN security posture using the SAQ template or an equivalent process but the results do not need to be sent to Visa.

   - ***On-site PIN assessments:*** Effective July 21, 2018, on-site PIN assessments are to be performed by an approved PIN SA listed on Visa Approved Security Assessor List . Visa will contact Europe PIN Participants

individually on how the program changes affect their existing validation and what is required under the revised program.

5. **Q. I prepared my SAQ and attestation for 2018. Can I still send it to Visa?**
   A. Unless specifically requested, Visa no longer requires organizations to submit SAQs to us. However, organizations must retain their SAQs or equivalent validation evidence. Per Visa rules, all organizations handling PIN data must comply with the PCI PIN Security Requirements. Visa may request evidence of PIN compliance at any time.

6. **Q. How often must on-site PIN Security assessments be performed to demonstrate compliance to the Visa PIN Security Program?**
   A. All Validating Participants must perform an on-site PIN assessment, performed by an approved Visa PIN SA, at least once every 24 months. Visa will notify Validating Participants of their initial validation due dates.

7. **Q. What is a validation date?**
   A. Each Validating Participant has a validation date. The validation date is the deadline for the program participant to submit their evidence of compliance to Visa.

8. **Q. How do I know my validation date?**
   Validation dates will depend on when the Validating Participant performed their last compliance assessment. The table below provides guidance on the validation dates. **Visa will notify each Validating Participant of their initial validation date under the new program.**

PIN Program Participant	2017 PIN Security Report Accepted By Visa	PIN Program Participant Listed on Global Registry	Next Validation Due Date
Performed onsite PIN assessment and compliant with requirements in 2017.	mm dd, 2017 E.g., August 31, 2017	Yes	mm dd, 2019 E.g., August 31, 2019 (24 months after receiving the previous attestation of compliance.
Did not perform PIN onsite assessment in 2017 **OR** **Did not complete required remediation in 2017.**	No	No*	Visa will notify each Validating Participant of their initial validation due date under the new program but initial validation is due no later than **December 31, 2019.**

Note: Validating Participants are encouraged to schedule their onsite assessment early, with sufficient time to prepare and perform the assessment and remediate any non-compliant findings before the compliance validation date deadline to avoid non-compliance assessment or escalations.

****Validating Participants will not be listed on Visa's Global Registry of Service Providers until their attestation of compliance is received by Visa.***

9. **Q. How will differing interpretations of the Payment Card Industry (PCI) PIN Security Requirements be resolved?**
   A. Requests for clarification of PCI PIN Security Requirements should be directed to the PCI SSC at pcipts@pcisecuritystandards.org. Clarification on Visa PIN Entry Device (PED) requirements or compliance validation requirements should be directed to your regional Visa Risk Representative.

10. **Q. Do all non-compliant findings need to be resolved before an organization is listed on the Global Registry of Service Providers?**
    A. Yes. All non-compliant findings must be resolved and verified by the security assessor. Visa will only list organizations that have validated full compliance with stated security requirements.

11. **Q. Are on-site assessments required for financial institutions that process only their own BINs?**
    A. No. Financial Institutions that process PIN data for only their own BINs or acquiring services are not considered Validating Participants and are not required to submit to evidence of compliance to Visa

    However, all organizations are expected to comply with the PCI PIN Security requirements and as such, Visa encourages Non-Validating Participants to perform appropriate due diligence to ensure ongoing compliance with stated requirements.

12. **Q. What if I am a new VisaNet Processor (VNP) but will only process my own BINs. Do I need to perform an on-site assessment?**
    A. VNPs establishing new connections with Visa, whether client/members or third parties, must adhere to the requirements for new VNPs. All new VNPs are required to perform an on-site PIN Security assessment. To obtain information about becoming a VNP, send an e-mail to NewEndPointInquiries@visa.com for additional information.

13. **Q. Why did Visa change its PIN Security Program?**
    A. Visa is continually evolving its Payment System Risk programs to maintain the security of the payment system and address current threats. The new PIN Security Program validation requirements are risk-based and focus on third parties processing PIN data and performing cryptographic key management on behalf of Visa clients.

14. **Q. Who is required to comply with the PCI PIN Security requirements?**
    A. All PIN acquiring organizations and their sponsored agents that process Visa cardholder PIN data and organizations that are involved with encryption key management must comply with the PCI PIN Security Requirements, Visa PED usage and TDES mandates. All organizations must perform appropriate due diligence to ensure compliance. However, only entities identified as Validating Participants must submit compliance validation documentation to Visa.

    Note: *Visa may require evidence of PIN security compliance or request an on-site PIN Security assessment of any organization (Validating or Non-Validating Participants) to ensure the security of the payment system.*

15. **Q. What if my participant status changes? For example, what if a financial institution that processed PIN data for themselves starts processing PIN data on behalf of other financial institutions?**
    A. An on-site PIN Security assessment by a Visa approved PIN SA is required before a financial institution can begin processing PIN data for another financial institution. Contact your regional Visa Risk Representative for additional information.

16. **Q. As a Validating Participant, can I have my organization's internal audit or security group perform the on-site PIN Security assessment?**

A. No, Validating Participants must use a Visa Approved Security Assessor (PIN SA) for its onsite assessment. The Visa Approved Security Assessor List can be found on www.visa.com/pinsecurity .

17. **Q. Will Visa pay for the on-site PIN Security assessment?**
    A. No. Any fees and/or expenses associated with the on-site assessment are between the Validating Participant and the PIN SA.

18. **Q. Can I use the same PIN SA every review cycle?**
    A. No, a SA Company and individual PIN SA are limited to assess the same organization for the same compliance program for only two consecutive review cycles. Any exceptions must be explicitly authorized in advance and in writing by your regional Visa Risk Representative.

19. **Q. Will the PIN SA be listed on the PCI Security Council website?**
    A. No. At this time, the list of Visa PIN SAs is only available on the Visa website. The Visa Approved Security Assessor List can be found on www.visa.com/pinsecurity

20. **Q. Can an organization be listed on the Global Registry of Service Providers even if it is a Non-Validating Participant?**
    A. Yes, an organization not formally identified as a Validating Participant may undergo an on-site assessment performed by an approved Visa PIN SA to demonstrate its PIN compliance and be listed on the Global Registry of Service Providers. Contact your regional Visa Risk Representative for additional information.

21. **Q. What happens if I do not validate according to these requirements?**
    A. Validating Participants that do not perform an on-site assessment or cannot comply with stated security requirements by the validation deadlines will be removed from the Global Registry of Service Provider and sponsoring Visa clients may be subject to non-compliance assessments.

    Sponsoring clients of Non-Validating Participants that do not maintain compliance with stated security requirements are also subject to non-compliance assessments.

22. **Q. Do Visa PIN Participants need to be a registered agent?**
    A. Yes, Encryption Support Organizations (ESOs), Third-Party Service (TPS) providers and VNPs must be registered by sponsoring financial institutions. For additional information contact:

    - ESO and TPS: AgentRegistration@visa.com
    - VNP: NewEndPointInquiries@visa.com
    - Visa in Europe ESO and TPS: Agentcompliance@visa.com

23. **Q. Can I get an extension to complete validation if I cannot meet the validation deadline?**
    A. No. Validating Participants are required to validate compliance by their initial validation due date and again every 24 months. Attestations of compliance submitted after an organization's deadline may result in removal from the Global Registry of Service Providers.

24. **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 Validating Participant and have performed an on-site assessment before I can begin processing for others?**

A. Yes, you will need to inform Visa of your intention first. An on-site assessment must be conducted by a PIN SA. 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.

25. **Q. I am a principal licensee and I process PIN transactions for our organization's associate and sponsored clients. Am I a Validating Participant?**

A. No, as the associates and sponsored clients are sponsored by your organization, you assume the risk and responsibility for your clients.

26. **Q. I am a principal licensee and I process PIN transactions for associate and sponsored clients of other principle licensees. Am I a Validating Participant?**

A. Yes, as the associates and sponsored clients are sponsored by other organization, you would be a third party and do not assume the risk and responsibility for these transactions.

27. **Q. I am a Validating Participant, and also provide a point-to-point encryption (P2PE) solution to clients. Can I arrange to combine both the PCI PIN and PCI P2PE assessments?**

A. Potentially yes. Visa would need to understand what PIN services are being provided and need to be assessed under each standard. The Validating Participant would need to confirm that the security assessor is authorized to perform both types of assessments. Contact your Visa Risk Representative with full details of your services for a definitive answer.

28. **Q. With the integration of Visa Inc. and Visa in Europe PIN programs, are there changes to the PIN Entry Device (PED) requirements?**

A. There are no changes to the existing PED requirements for each regions. Review the *Visa PIN Security Program Guide*, Appendix B- Visa PED Requirements, Purchase, Usage and Sunset Dates for more information.

29. **Q. Who should I contact with questions?**

A. Each Visa region manages PIN Participants for their region. Contact your local Visa Risk Representative at the following e-mail addresses:

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