Changes to the PIN Security Program in Europe

As part of the integration efforts to include the Europe region in Visa security programs, the following information outlines upcoming changes to the PIN Security Program in Europe. These changes will simplify and unify PIN security validation across all regions and provide greater transparency into the security status of PIN program participants.

Mark Your Calendar:

- PIN Security Program changes go into effect **(21 July 2018)**

These modifications are intended to drive PIN security through a risk-based, prioritized approach that focuses on entities that process PIN data or perform key management activities on behalf of Visa clients. In summary, Visa will:

- Discontinue the requirement to submit PIN Security Self-Assessment Questionnaires (SAQs) to Visa.
- Introduce a new PIN security assessor (SA) model that enables members to engage with assessors directly for on-site reviews.
- Create a global list of approved and compliant PIN program participants, which provides a platform for program participants to promote their secure PIN services.

As part of this effort, Visa will publish an updated version of the *Visa PIN Security Program Guide* and notify existing Europe PIN program participants about how the program changes will affect their current compliance validation requirements. To help organizations prepare for these changes, Visa will hold a regional webinar in the coming weeks.

PIN Security Program Changes Defined

Unless specifically noted, program changes are **effective 21 July 2018**.

- **Requirement to Submit PIN Security SAQs Removed**

  Effective immediately, PIN program participants are no longer required to submit their annual PIN Security SAQs to Visa as part of compliance validation. All compliance validation obligations will be completed through on-site reviews performed by a Visa-approved SA.

  Visa will contact existing PIN program participants to close open items that were identified as part of previous reviews.

- **New Categories for PIN Program Participants**

  The PIN Security Program will recognize two types of PIN program participants: validating PIN participants and non-validating PIN participants.

  Validating PIN Participants

  As the name implies, entities identified under this category must validate PIN compliance to Visa by performing an on-site PIN security assessment conducted by a Visa-approved SA. Validating PIN participants must perform their on-site assessment every 24 months.

  The following types of organizations are considered validating PIN participants:

  - **PIN-acquiring third-party VisaNet processor (VNP)**: A third-party VNP entity that is directly connected to VisaNet and provides acquiring PIN processing services to Visa clients.

  - **PIN-acquiring client VisaNet processor acting as a service provider**: A Visa client or client-owned entity that is directly connected to VisaNet and provides PIN acquiring processing services to Visa clients.

  - **PIN-acquiring third-party servicers (TPS)**: A PIN-acquiring agent that stores, processes or transmits Visa account numbers and PINs on behalf of Visa clients.

  - An **Encryption and Support Organization (ESO)** is an entity that does one of the following:

    - Performs cryptographic key management services such as key injection facilities and remote key injections on behalf of Visa clients

    - Services and/or deploys client ATM, POS or kiosk PIN entry devices (PEDs) which process and accept cardholder PINs

    PED manufacturers and third-party certificate authorities that handle various cryptographic key management responsibilities for clients are also ESOs.

  Other third-party entities that are not identified above but perform PIN translation, key management and/or manage ATM or POS devices for Visa members may also be subject to the PIN Security Program requirements and classified as validating PIN participants. Acquirers should contact their regional Visa risk representative to review applicable requirements.

  Non-validating PIN Participants

  All other organizations that are not classified as validating PIN participants are considered non-validating PIN participants. This includes Visa clients, merchants and other organizations that acquire PIN transactions and/or perform key management services for only their own acquiring or issuing business. Non-validating PIN participants must also comply with the PIN Security Program requirements but will perform their own appropriate due diligence to ensure compliance. This may include performing self-assessments or on-site audits using an internal or external resource. Individuals performing the compliance reviews for non-validating PIN participants must have adequate knowledge of the Payment Card Industry (PCI) PIN Security requirements but do not need to be Visa-approved SAs.

  PIN security compliance evidence and results for non-validating PIN participants do not need to be submitted to Visa, but must be retained by the organization as evidence of PIN security compliance. Visa recommends that all organizations use the PCI PIN Security Assessment template (available at the Visa PIN Security website) or other compliance validation tools to measure and maintain ongoing PIN security for their own organization, sponsored merchants, agents and ATM portfolios.

Visa reserves the right to re-categorize non-validating PIN participants as validating participants that must demonstrate compliance as risks emerge. In these cases, organizations will be notified in writing by Visa that they are validating PIN participants.

Note: The Visa Rules require all entities that process Visa cardholder PIN data to comply with the PCI PIN Security requirements, the Visa PED usage mandates and the Triple Data Encryption Standard (TDES) mandates. Visa reserves the right to obtain evidence of an organization's PIN security compliance or require an on-site audit of an organization at any time.

- **Updates to PIN Security Program Guide**

  In the coming weeks, the existing *Visa PIN Security Program Guide* that details the requirements for validating and non-validating PIN participants will be updated to include information for Europe. The *Visa PIN Security Program Guide* is available on the Visa PIN Security website.

- **New PIN SA Model Introduced**

  Europe will align with the PIN SA model used by enabling validating PIN participants to contract and engage directly with Visa-approved SAs for on-site PIN reviews, thereby streamlining the process.

  SAs will be responsible for issuing a letter of findings directly to the validating PIN participant and, if necessary, validate that any remediation efforts are compliant. Once the validating PIN participant has remediated all non-compliance findings, the SA will provide the validating PIN participant the final report and provide Visa with an Attestation of Compliance (VAOC) signed by both the SA and the validating PIN participant executive management. Visa will no longer manage remediation of non-compliance issues.

  Any professional fees and expenses associated with on-site assessments by an SA will be paid by the validating PIN participant directly to the SA. Visa will no longer charge fees to program participants or SAs for on-site PIN reviews.

  Only PIN SAs identified on the Visa Approved Security Assessors List are authorized to perform on-site PIN security assessments for validating PIN participants.

- **Global Registry of Service Providers**

  The Visa Global Registry of Service Providers is a public, global listing of service providers and agents that have successfully validated compliance with the Visa security requirements and compliance programs. When validating PIN participants have submitted their compliance information to Visa, the Global Registry of Service Providers will be updated to include compliance information for the validating PIN participants.

Client Responsibilities

These program changes do not impose new requirements for Visa clients. Visa clients must continue to:

- Ensure that their acquiring third party agents that process or handle PIN data comply with the PCI PIN Security requirements and adhere to the Visa Rules.

- Ensure that their own processing environments that handle PIN data comply with the PCI PIN Security requirements.
- Perform the necessary due diligence prior to engaging any third party agent, and maintain policies and procedures to provide the correct level of oversight and control of the agent.

Visa will host a regional webinar for acquirers, PIN program participants and relevant stakeholders to provide additional information about the program revisions and to answer any questions. Visa will contact program participants directly with information about the webinar date and how the program's changes specifically affect their organization.

For more information on the PIN Security Program, contact your regional Visa risk representative at the following email addresses:

- **Europe:** VisaEuropePIN@visa.com
- **Global:** PIN@visa.com