Visa in Europe PIN Security Program Changes

Richard Trim – Security & Third- Party Risk – Visa Europe
Janet Cookson – Global PIN Security Program Manager

May 24, 2018

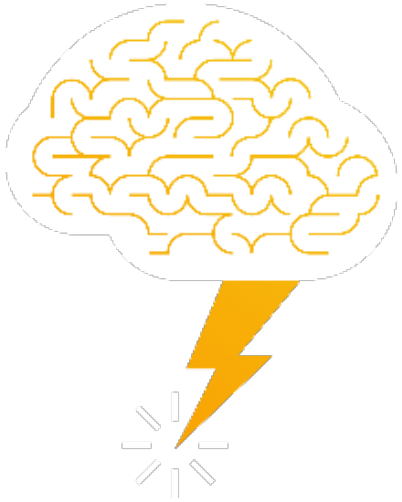
Agenda

- Introduction
- Evolution of Visa PIN Security Program
- PIN Program Participant Redefined
- Discontinue Submission of PIN SAQ
- PIN Security Assessors
- Global Registry of Service Providers
- Validation Cycle
- Question and Answer

Forward-Looking Statements

“This presentation contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995 that relate to, among other things, our future operations, prospects, developments, strategies, business growth. Forward-looking statements generally are identified by words such as "believes," "estimates," "expects," "intends," "may," "projects," “could," "should," "will," "continue" and other similar expressions. All statements other than statements of historical fact could be forward-looking statements, which speak only as of the date they are made, are not guarantees of future performance and are subject to certain risks, uncertainties and other factors, many of which are beyond our control and are difficult to predict. We describe risks and uncertainties that could cause actual results to differ materially from those expressed in, or implied by, any of these forward-looking statements in our filings with the SEC. Except as required by law, we do not intend to update or revise any forward-looking statements as a result of new information, future events or otherwise.”

Before we begin, let’s take a poll!



Introduction

Visa PIN Security Program Objective:

- *Ensure cardholder PINs are secure*
- *Engage with stakeholders to comply with security requirements*

Changes to Existing Visa in Europe PIN Program Include:

- *Redefine PIN Participants That Must Validate Compliance*
- *Elimination of PIN Security Self-Assessment Questionnaire Submission*
- *Introduction of PIN Security Assessors (SA)*
- *Validation Cycle Every 24 Months*
- *Compliant Entities Listed On Global Registry of Service Providers*

Further Drive PIN Security Through a Risk-Based, Prioritized Approach That Focuses On Third Parties

Visa PIN Program Evolution

1995

- Visa establishes PIN Security & Key Management Compliance Program

2011

- PCI Council adopts Visa PIN Security Requirements

2013

- Visa Inc. Implements Changes to the PIN Security Program

Jan 2018

- Europe Discontinue SAQ Submissions

Apr-May 2018

- Publish VBN Announcing Program Changes
- Notify existing participants
- Webinar
- Publish Program Guide & FAQ

July 2018

- Europe Program Changes Become Effective
- Contract directly with Approved SA for on-site reviews
- SA track remediation and submit attestation to Visa
- Compliant PIN Participants listed on Visa Global Registry of Service Providers

Visa PIN Security Program: Indemnification

Visa Core Rules - PIN Security Program Requirements

- All PIN acquiring entities in the payment system must comply with Visa's PIN Security Program
- A Sponsoring Acquirer is responsible for its agent PIN Security compliance
- Sponsoring Acquirers may be subject to non-compliance assessments

PIN Participants Redefined

Validating PIN Participants

- **PIN Acquiring Third-party VisaNet Processors**
  - Entities directly connected to VisaNet providing PIN Acquiring Third-Party processing services
- **PIN Acquiring Member Service Provider VisaNet Processors**
  - Entities directly connected to VisaNet providing PIN Acquiring processing services on behalf of other Financial Institutions
- **PIN Acquiring Third-Party Servicers (TPS)**
  - Type of Agent that performs PIN Acquirer processing not directly connected to VisaNet
- **Encryption and Support Organizations (ESO)**
  - Type of Agent that manages cryptographic keys on behalf of other agents, Banks, merchants and processors

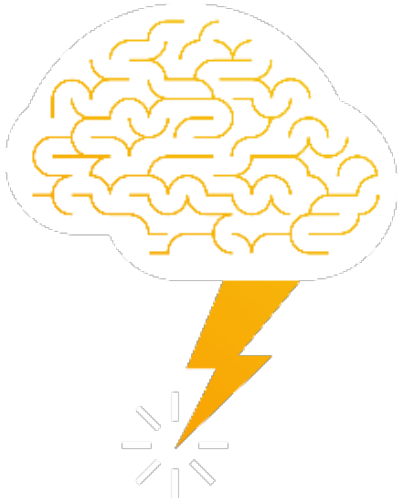
PIN Participants Redefined

Non-Validating PIN Participants

- **Clients, merchants and other organizations that acquirer PIN transactions and/or perform key management for their own acquiring business.**
  - Must fully comply with Visa PIN Security Program Requirements
  - Perform ongoing due diligence to ensure continued compliance
  - Retain results but do not submit results to Visa

Visa reserves the right to request evidence of PIN compliance or request an onsite assessment be performed at any time.

Let’s take a poll to see how we’re doing so far



Discontinue Submission of PIN SAQ

- Effective January 1, 2018, PIN program participants are no longer required to submit annual PIN Security SAQs (Self-Assessment-Questionnaire) to Visa
- Visa recommends continued use of SAQ or equivalent processes to measure internal compliance
- The SAQ template available: *http://www.visa.com/pinsecurity*

Attestation of Compliance (SAQ)

PCI PIN SECURITY REQUIREMENTS

Compliance Statement

I, _____
(print or type name and title)

(check one)

☐ am an **internal auditor** for _____ and I have no operational responsibility for matters referenced in the PIN Security Requirements Self-Audit.

☐ am an **independent auditor** employed by _____ and hired by _____ to complete the PIN Security Requirements Self-Audit and the Compliance Statement.

I do hereby attest that the above-referenced organization is:

(check one)

☐ **In full compliance** with the PIN Security Requirements Self-Audit.

☐ **Not in full compliance** as indicated by the attached Audit Exception Form(s).

Signature: _____ Date: _____

Officer Attestation:

I, _____
(print or type name and title)

I do hereby attest that the above-referenced organization is:

(check one)

☐ **In full compliance** with the PIN Security Requirements Self-Audit.

☐ **Not in full compliance** as indicated by the attached Audit Exception Form(s).

Signature: _____ Date: _____

PIN Security Assessors (PIN SA)

- Possess the required knowledge, skill and experience in PIN security
- Pass necessary background checks and adhere to professional/business ethics policy
- PIN Program Participants contract directly with Visa-approved a PIN SA for on-site PIN reviews
- Any professional fees/expenses are settled between the program participant and PIN SA
- Visa is removed from assessment process

On-site PIN assessments must be performed by an approved Visa PIN SA

www.visa.com/pinsecurity Select the Visa Approved Security Assessor List

PIN SA Responsibilities

- Contract directly with PIN participant to perform on-site assessment
- Schedule, plan and perform on-site assessment
- Release assessment reports to PIN participants upon completion of on-site assessments
- Validate remediation activities to ensure issues have been resolved
- Submit Visa Attestation of Compliance (VAOC) when compliance is achieved
- An individual PIN SA or PIN SA Company must not assess the same entity more than every 2 review cycles unless approved by Visa

PIN SA are the point of contact for interpretation or technical guidance on requirements

List of Visa Approved PIN SAs

www.visa.com/pinsecurity Select the Visa Approved Security Assessor List

Visa Approved Security Assessors (SA) List
Last Updated: 16 April 2018

Defined program participants that are required to validate compliance to one or more of the following Visa security programs; Access Control Server (ACS), Approved Vendor Program (AVP) and PIN Security must use a Visa Approved Security Assessor (SA) identified on this list for their onsite validation review. Program participants are not required to use Approved SAs for any off-year or mid-year validation efforts. Furthermore, organizations that are not defined program participants and are not required to submit compliance validation to Visa, may use internal audit staff or other qualified assessors for security reviews. Sponsored entities that are not designated program participants, should contact their sponsoring financial Institution for further guidance.

Contact the regional Visa Risk Representative for additional information on program compliance requirements.

PLEASE NOTE: Visa no longer manages security assessors for 3DS Security Assessments (formerly called ACS). ACS Service Provider onsite assessments must be performed by a PCI 3DS QSA. Please visit the PCI SSC Assessor website to identified an approved 3DS QSA. https://www.pcisecuritystandards.org/assessors_and_solutions/3ds_assessors.

Company Name	Security Assessor Name and Contact Information	Location	Market(s)	Supported Languages	Approved to Perform the Following Services			
					PCI DSS QSA	AVP-Logical*	AVP-Physical	PIN
1st Secure IT, LLC	Abelardo Rodrigues (954) 818-9045 ARodrigues@1stsecureit.com	Florida, U.S.A.	Global	English, Spanish, Portuguese	X			X
1st Secure IT, LLC	Raul Mejia (52 1) 55 66306384 rmejia@1stsecureit.com	Mexico City, Mexico	Global	English, Spanish, Portuguese	X			X
Adsigo AG	Dr. Stephan Engelke +49 176 1235 0901 stephan.engelke@adsigo.com	Hamburg, Germany	Global	English German	X			X

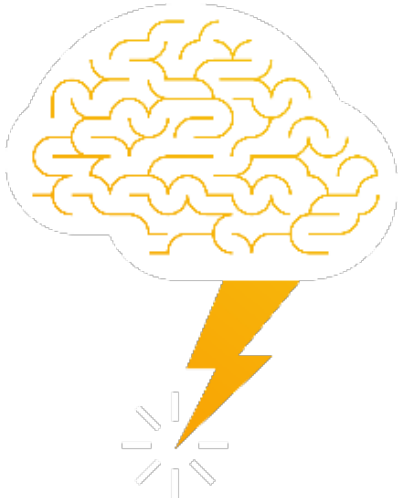
Schedule assessments early to ensure sufficient time to perform review & remediation by validation due date

Validation Cycle

- Must perform onsite review every 24 months
- Visa will recognize compliant PIN reviews performed in 2017
- All others, validation cycle begins July 21st 2018 and validation deadline is December 31st 2019
- Initial validating due date defined by Visa
- Next validation cycle begins when Visa Attestation of Compliance (VAOC) is received by Visa
- VAOC must be submitted by the entity's validation deadline
- VAOC must be submitted to be listed on Global Registry of Service Providers

Acquirers may be subject to a non-compliance assessment for its or its agent's failure to comply with security requirements or validation dates.

Let’s take a poll to see how we’re doing so far



Onsite Review Performed & Remediation Completed in 2017*

Old Framework		New Framework	
Visa performed onsite review	Remediation completed	Global Registry Listing	Next Visa AOC submission date
In 2017	In 2017	Yes	24 months from receipt of previous VAOC

For Example:

February 10, 2017	November 20, 2017	July 21st 2018 When Program becomes Effective	November 2019

*** Applies to Validating PIN Participants**

Onsite Review NOT Performed in 2017*

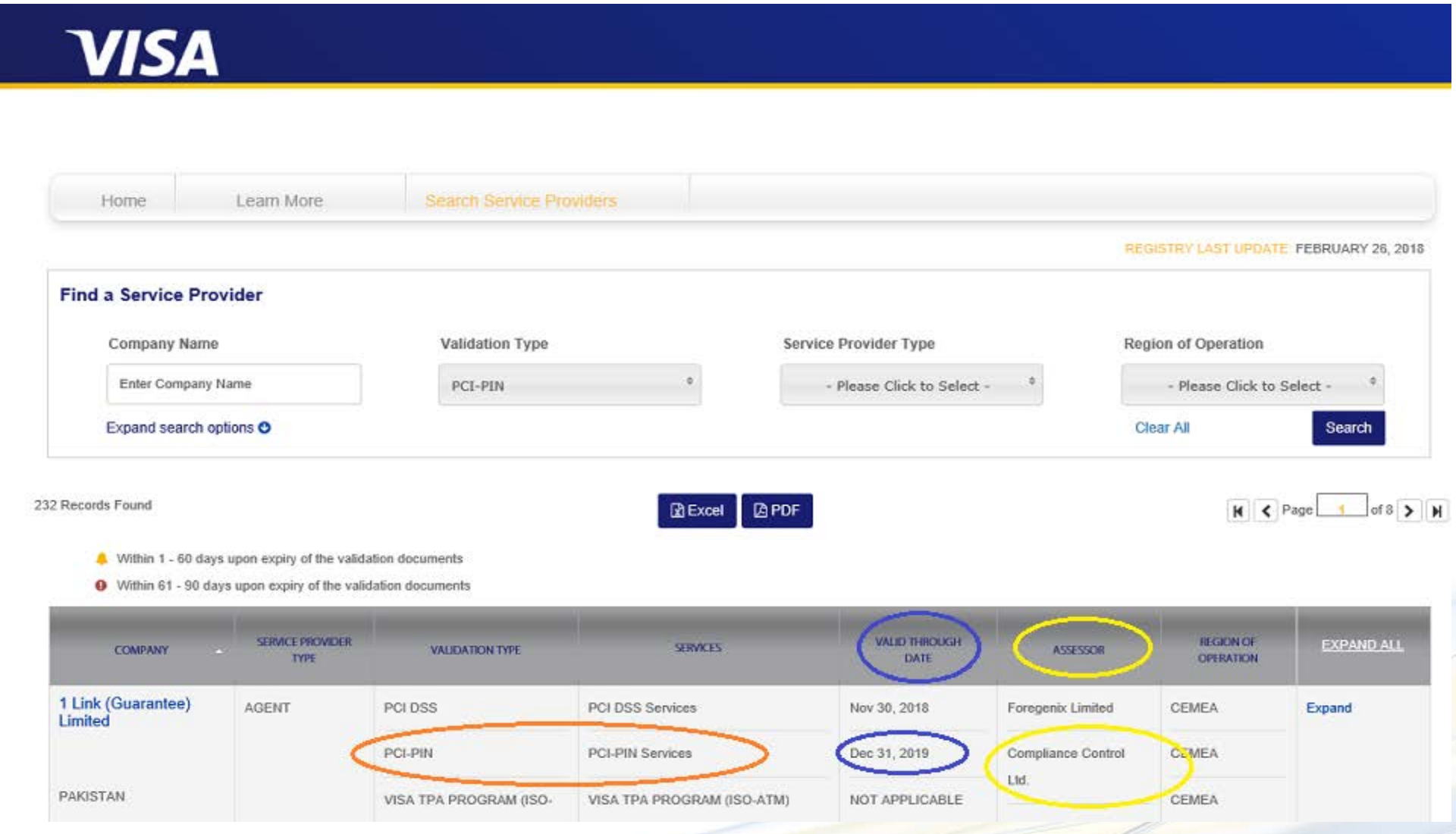
Old Framework	New Framework	
Visa Performed Onsite Review	**Initial Validation Due Date**	**Next Validation Due Date**
Prior to 2017 or Never	**Defined by Visa**	**24 months from receipt of initial VAOC**

For Example:

February 10th 2015	**March 30, 2019**	**March 30, 2021**

*** Applies to Validating PIN Participants**

Global Registry of Service Providers



www.visa.com/onthelist

Summary

Changes to Existing Visa in Europe PIN Program Include:

- *Redefine PIN Participants That Must Validate Compliance*
- *Elimination of PIN Security Self-Assessment Questionnaire Submission*
- *Introduction of PIN Security Assessors (SA)*
- *Validation Cycle Every 24 Months*
- *Compliant Entities Listed On Global Registry of Service Providers*

Visa Pin Program Contacts

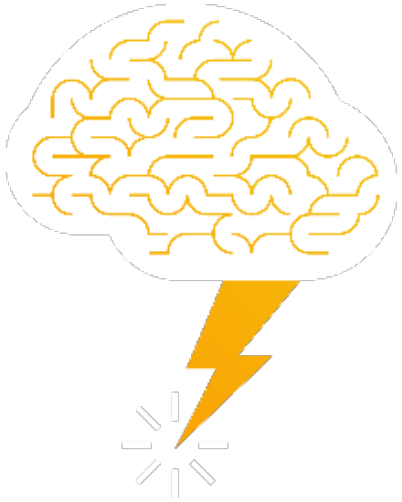
Visa in Europe	visaeuropepin@visa.com
AP & CEMEA	pinsec@visa.com
LAC	pinlac@visa.com
North America	pinna@visa.com
Global	pin@visa.com

Visa PIN Security Resources

www.visa.com/pinsecurity

- Visa PIN Security Program Guide
- Visa in Europe Program Changes
- PIN Security Alerts & Bulletins
- Listing of Pre-PCI Approved PEDs
- Visa What to do if Compromised

Let’s take a final poll!



Questions or Comments?

Note: This presentation will be posted on www.visa.com/pinsecurity