# Visa PIN Security Program

Webinar
May 2015

# Disclaimer

The information or recommendations contained herein are provided "AS IS" and are intended to be information about Visa's PIN Security program only. When implementing any new strategy or compliance program, you should consult with your internal experts and legal counsel to determine what Visa Rules, laws, and regulations may apply to your specific circumstances. The actual benefits of these recommendations or programs may vary based upon your specific business needs.

Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free.

To the extent permitted by applicable law, Visa shall not be liable for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

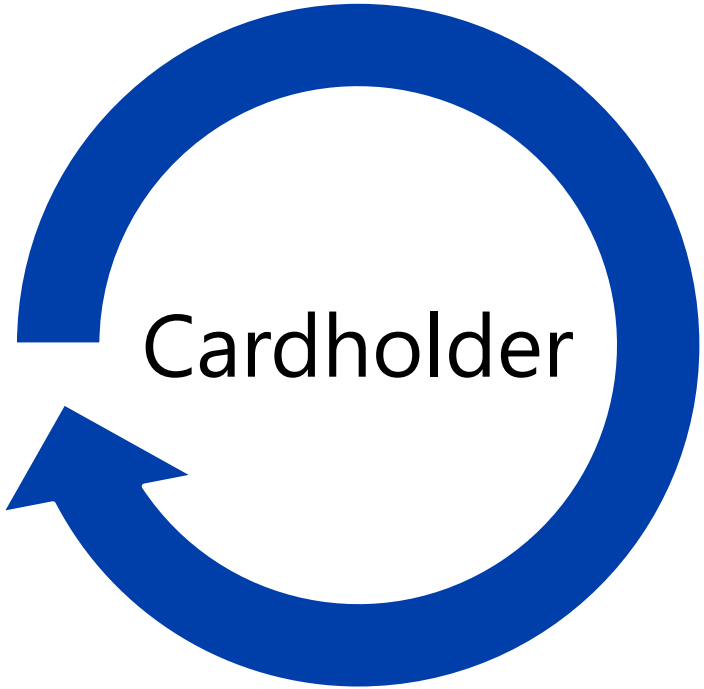
# Agenda

- Objectives
- Visa Rules on PIN Security
- Visa's PIN Security Program Framework
  - PIN Security Program Participants
  - PIN Security Program Requirements
  - Visa Approved Security Assessors
  - Global Registry of Service Providers
  - Summary
- Validation Deadlines
- PIN Security Program Enforcement Plan
  - Plan Outline
  - Remediation Options
- Additional Resources
- Q&A

# Objectives

- Review components of Visa PIN Security Program framework
- Ensure your understanding of validation requirements for 2015
- Examine the PIN Security Program requirements
- Compare the PCI PIN Security Requirements Version 1 and Version 2
- Revisit the Visa PED requirements and mandates
- Introduce the PIN Security Program enforcement plan

# The Importance of PIN Security




- Trust
- Loyalty
- Confidence

# Visa Rules on PIN Security

# Visa Core Rules on PIN Security

## PIN Security Program Requirements

An Acquirer or its agent processing PINs for Visa Transactions must comply with the security requirements specified in the PIN Management Requirements Documents and Visa PIN Security Program Guide. ID#: 151014-100512-0027086

See "PIN Security Non-Compliance Assessments" for noncompliance assessments for failure to comply.

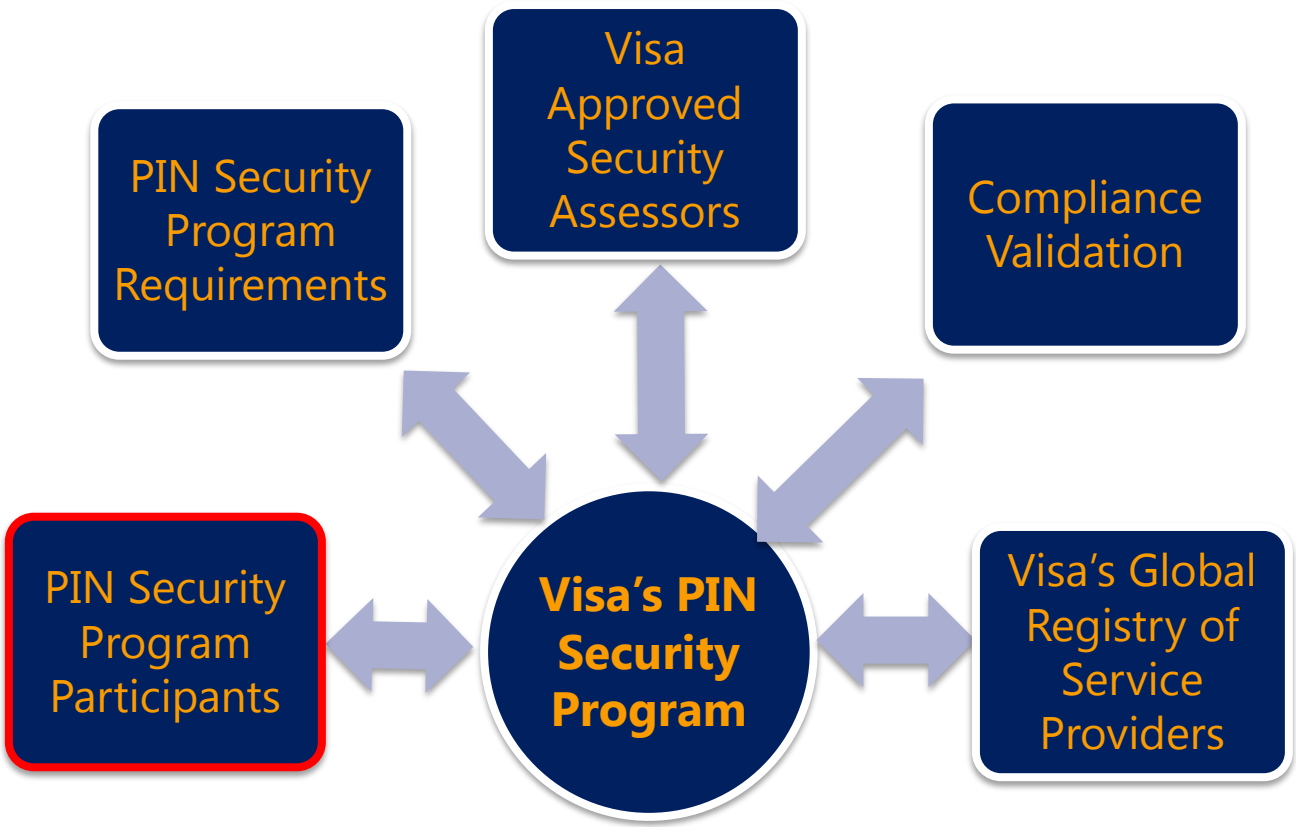
Visa Rules are publically available:

www.Visa.com, http://usa.visa.com/download/about_visa/15-October-2014-Visa-Rules-Public.pdf

Visa PIN Security Program Guide available on www.VisaOnline.com

# Visa PIN Security Program Framework

# Visa PIN Security Program Framework



# Visa PIN Security Program Framework

PIN Program Participants

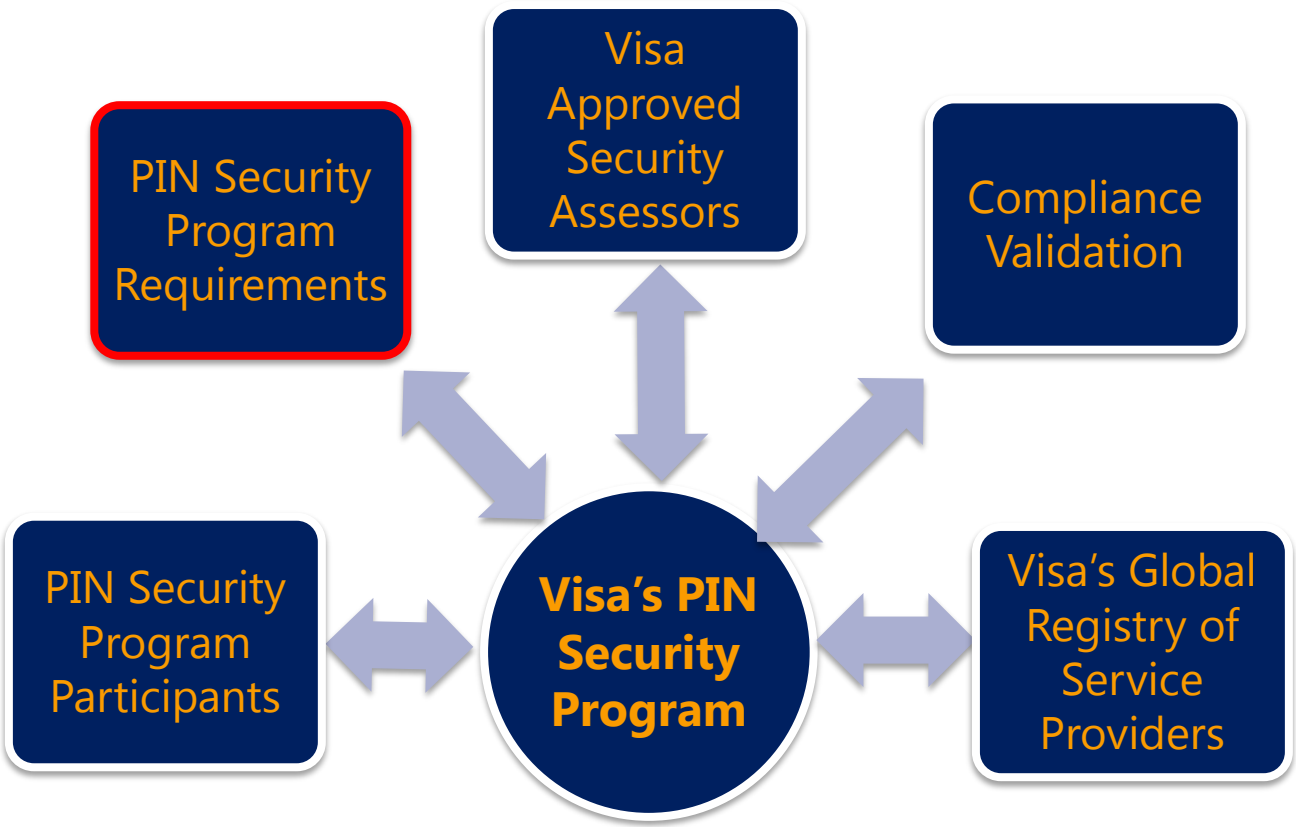
## PIN Security Program Participants, Validating Participants

- **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 members.
- **PIN Acquiring Client VNP acting as a Service Provider*** – A Visa member or member-owned entity that is directly connected to VisaNet and provides PIN acquiring processing services to members.
- **PIN Acquiring Third-Party Servicers (TPS)*** – A third-party agent that stores, processes, or transmits Visa account numbers and PINs on behalf of Visa members.
- **Encryption and Support Organizations (ESO)** – A non-member organization that deploys ATM, POS, or kiosk PIN acceptance devices which process and accept cardholder PINs and/or manage encryption keys (i.e., key injection facilities (KIFs)).

*These entities must validate PCI-DSS annually

If you are unsure of your status please contact your regional PIN Risk representative

# Visa PIN Security Program Framework



# Visa PIN Security Program Framework


## PIN Security Program Requirements

- PCI PIN Security Requirements
- Visa PIN Entry Device (PED) Requirements
  - PCI-PTS Approved Devices
  - PCI PIN Transaction Security Point of Interaction (POI) Modular Security Device Requirements
- Visa Triple Data Encryption Standard (TDES) Requirements

# Visa PIN Security Program Framework

PIN Security Program Requirements

## PCI PIN Security Requirements

- The minimum security requirements for PIN-based interchange transactions including minimum acceptable requirements for securing PINs and encryption keys
- Core requirements and additional information for Remote Key Distribution, Certification Authorities and Key-injection Facilities
- Latest Version 2 includes Testing Procedures document to assist with assessments
- The PCI PIN Requirements are maintained by PCI Security Standards Council
  *Can be found on the PCI SSC website:* *www.pcisecuritystandards.org*
- Select PCI Standards & Documents > Documents Library> PTS

*Questions?? Send an email to* ***pcipts@pcisecuritystandards.org***



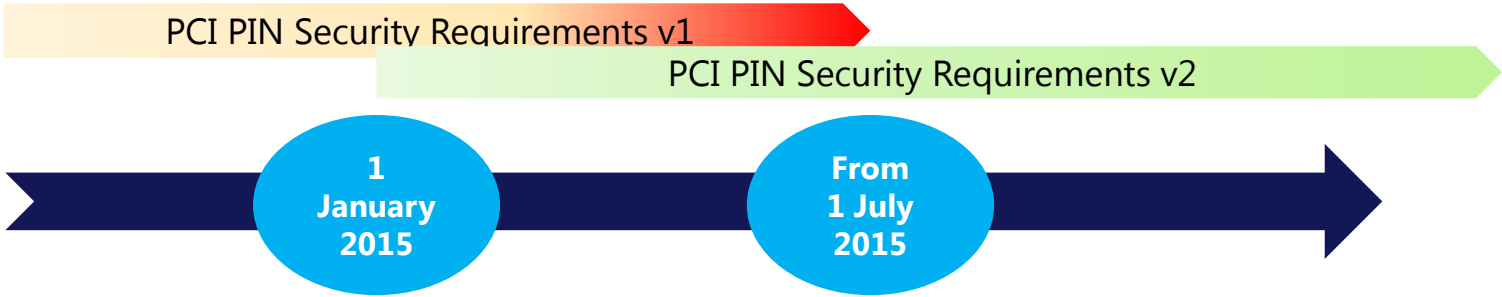


VISA

# Visa PIN Security Program Framework

PIN Security Program Requirements

## PCI PIN Requirements Version Timeline




- **Timeline set by Visa**

- **Improvements to Version 2**
  1. Detailed testing procedures to ensure consistent validation
  2. Enhanced requirements for deployed points-of-interaction (POI) devices
  3. Improved organization of "Remote Key Distribution Using Asymmetric Techniques Operations" and "Certification and Registration Authority Operations" requirements

# Visa PIN Security Program Framework

PIN Security Program Requirements

## Visa PIN Entry Device (PED) Requirements

| Device / Expiration | Purchase | Deployment and Usage | Visa Inc. Sunset Mandate |
|---|---|---|---|
| PCI PED V1.x<br>April 2014 | No | Allowed if purchased prior expiration date | **Recommend device replacement** |
| PCI PED V2.x<br>April 2017 | Yes | | Recommend device replacement |
| PCI PTS POI V3.x<br>April 2020 | Yes | | |
| PCI PTS POI V4.x<br>April 2023 | Yes | | |

***Full Visa PED Requirements can be found at www.visa.com/PINsecurity***

***Review the Visa Compromised PIN Entry Device List www.visa.com/PINsecurity***





VISA

# Visa PIN Security Program Framework


## PCI-PTS Version 1 Devices

**Expired PCI PTS POI V1 PED devices** should be removed from the payment system as soon as possible.

- V1 PEDs were introduced in 2004 and built to address attacks that were known over 10 years ago.
- They are no longer able to withstand current attack vectors.
- A number of device compromises reported.

**Pre-PCI PED devices**, just say no! Mandated sunset date has passed, 31 December 2014

**Note to Security Assessors* – If there are version 1 devices for organizations you assess ensure you check purchase dates on receipts are prior to 30 April 2014.

# Visa PIN Security Program Framework

PIN Security Program Requirements

## PCI PIN Transaction Security Point of Interaction Modular Security Device Requirements (PCI PIN, PTS POI )

- Complete list of security requirements that terminals are evaluated against to obtain Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) device approval
- Latest Version 4 of PCI PTS POI released June 2013
- Pertinent to the Device Testing and Approval Program

## Approved PTS Device List

- Always refer to the list when investing in new equipment.

***www.pcisecuritystandards.org/approved_companies_providers/approved_PIN_transaction_security.php***

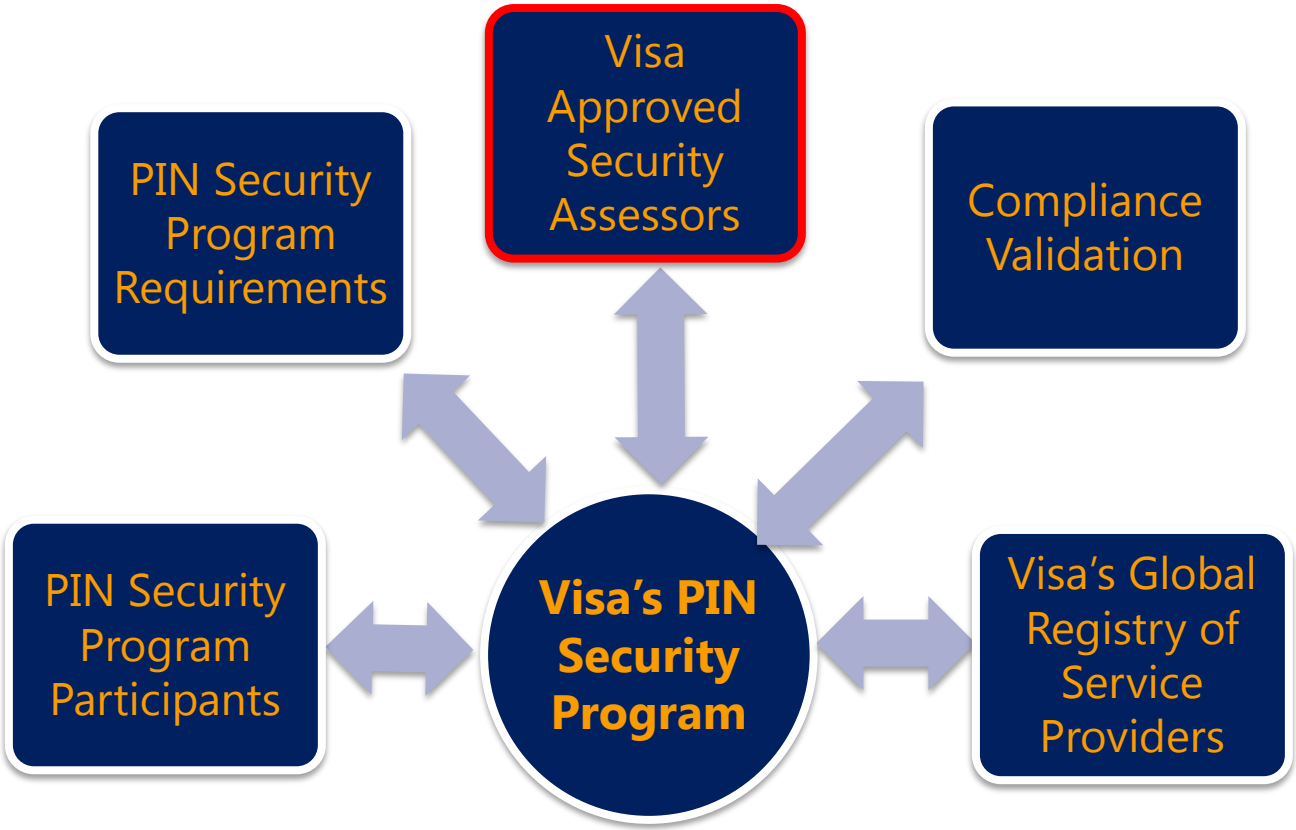
# Visa PIN Security Program Framework


## Visa TDES Requirements

- All ATMs and POS PIN acceptance devices must use TDES to protect PINs
- US only - Effective 1 July 2010, Automated Fuel Dispensers (AFDs) must use Tripe DES or Single DES Derived Unique Key Per Transaction to protect PINs. Sunset dates for SDES DUKPT to be decided

Note: It is not too early to start thinking about AES.

# Visa PIN Security Program Framework

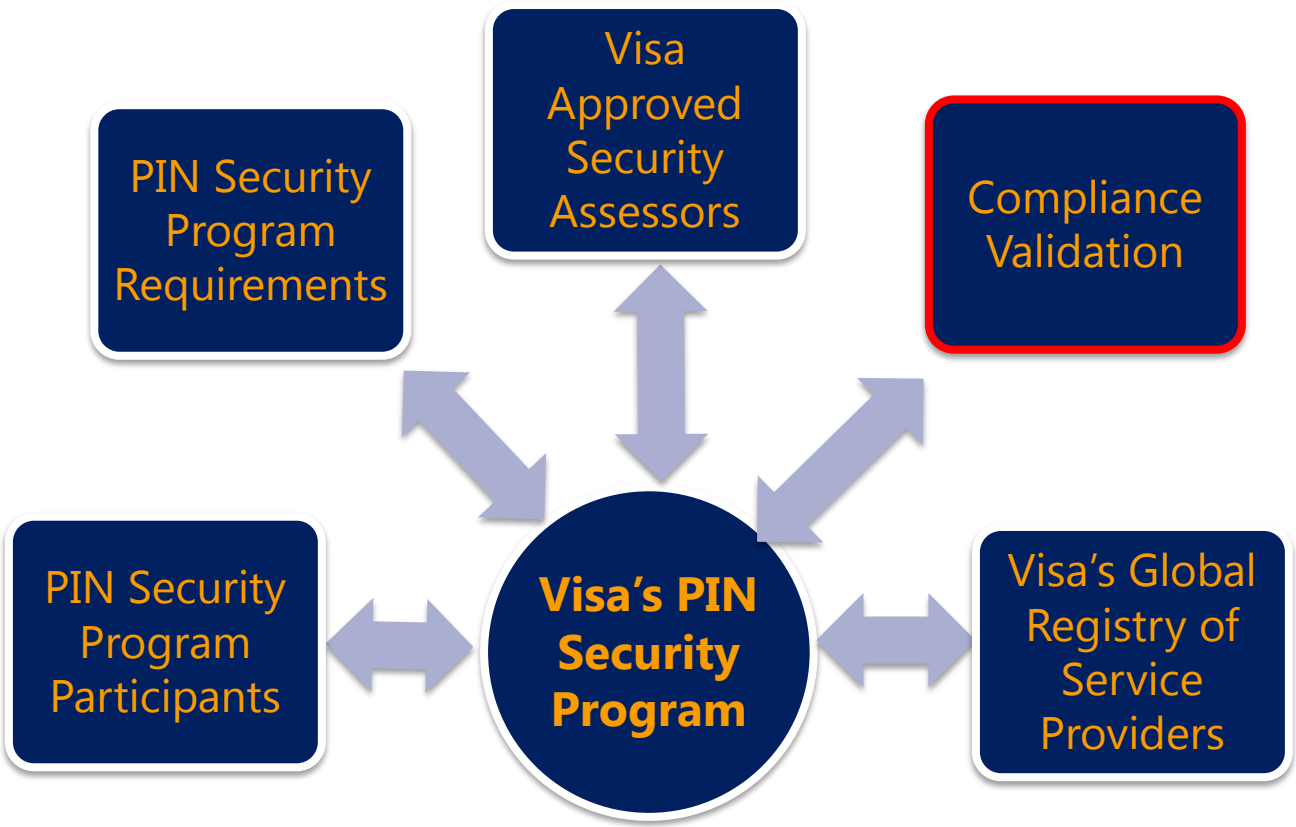


# Visa PIN Security Program Framework


## Visa Approved Security Assessors

- **Who are they?**
  - Companies that Visa has approved for onsite PIN assessments
  - Experienced security professionals
- **What they can do**
  - Perform onsite PIN security assessments
  - Provide consultation on improving your security position and track remediation outstanding issues
- **What they cannot do**
  - Market or sell services that influence the results of your onsite PIN assessment
- **Where can I find them?**
  **http://usa.visa.com/download/merchants/sa-global-list.pdf**

# Visa PIN Security Program Framework



# Visa PIN Security Program Framework


## Compliance Validation

### Validating Participants

- Onsite assessment every 24 months
  - Onsite assessment performed by Visa approved security assessor identified on the Visa Approved Security Assessor list http://usa.visa.com/download/merchants/sa-global-list.pdf
- SA sends Visa Attestation of Compliance to Visa

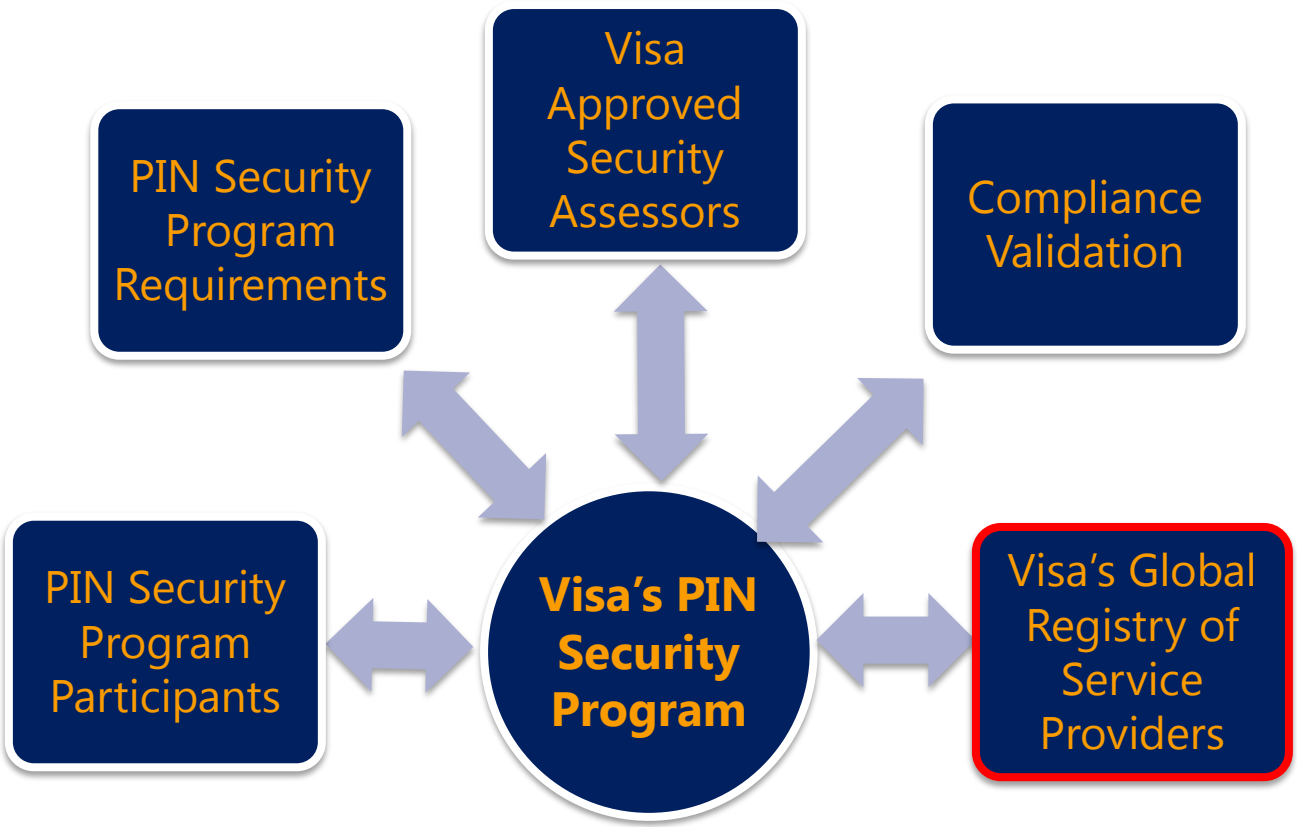
# Visa PIN Security Program Framework


## Compliance Validation

### Non-Validating Participants

- Must comply with the program requirements
- Performs self-assessment . Internal or external resource knowledgeable with PCI PIN security requirements. Does not need to be a Visa approved security assessor
- Not required to submit validation materials to Visa but must retain results as evidence of compliance
- Visa reserves the right to request evidence of PIN compliance at any time

# Visa PIN Security Program Framework



# Visa PIN Security Program Framework

Visa's Global Registry of Service Providers

## Visa's Global Registry of Service Providers

Key Features and Benefits

- Business information and type of services offered by agents
- Compliance validation details for agents

**Marketing Opportunity**

Provides listed agents with access to a new communication channel to promote their payment-related services to potential clients worldwide.

**Competitive Edge**

Serves as a platform where agents can proclaim their status and differentiate themselves from other agents.

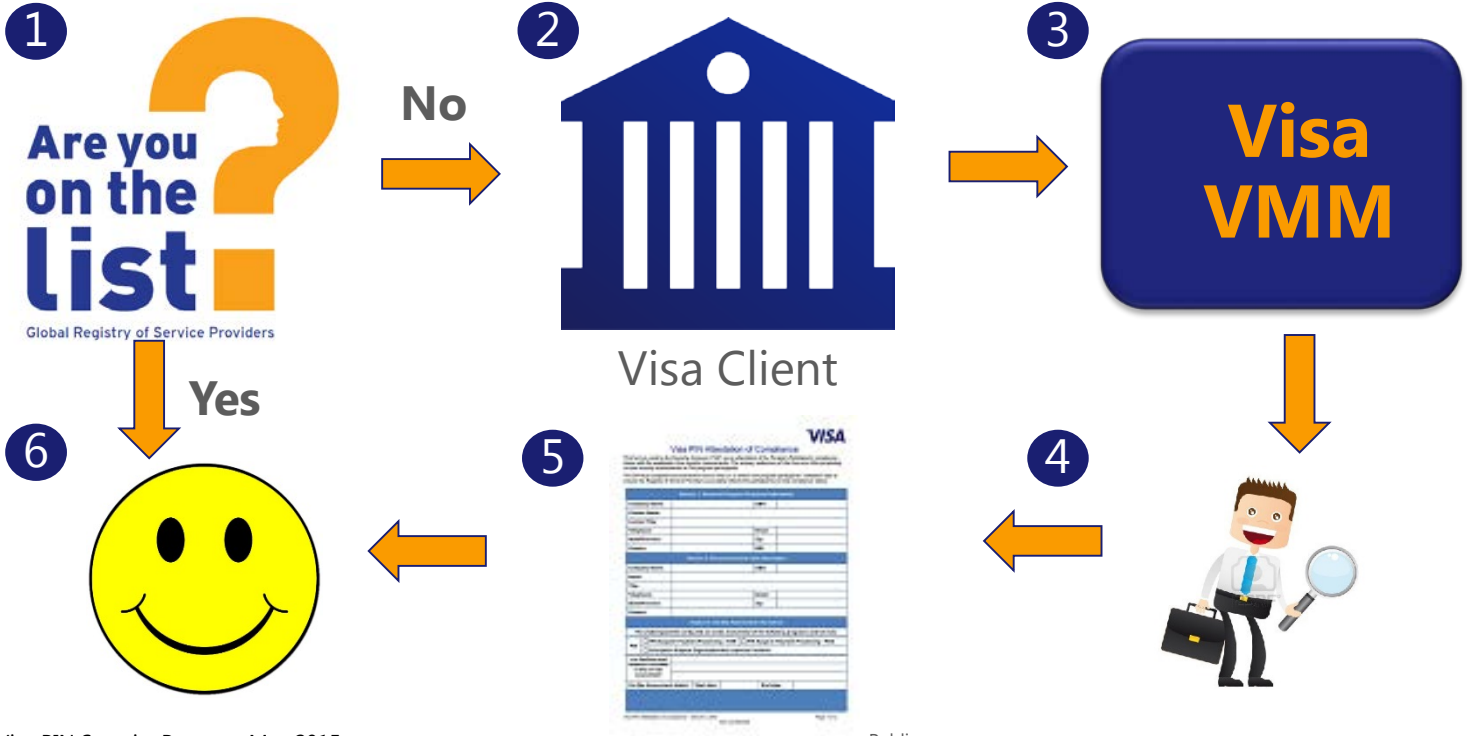
**Improved Communication with Visa**

Informs agents by providing access to Visa security alerts, bulletins, publications and invitations to Visa events and conferences.

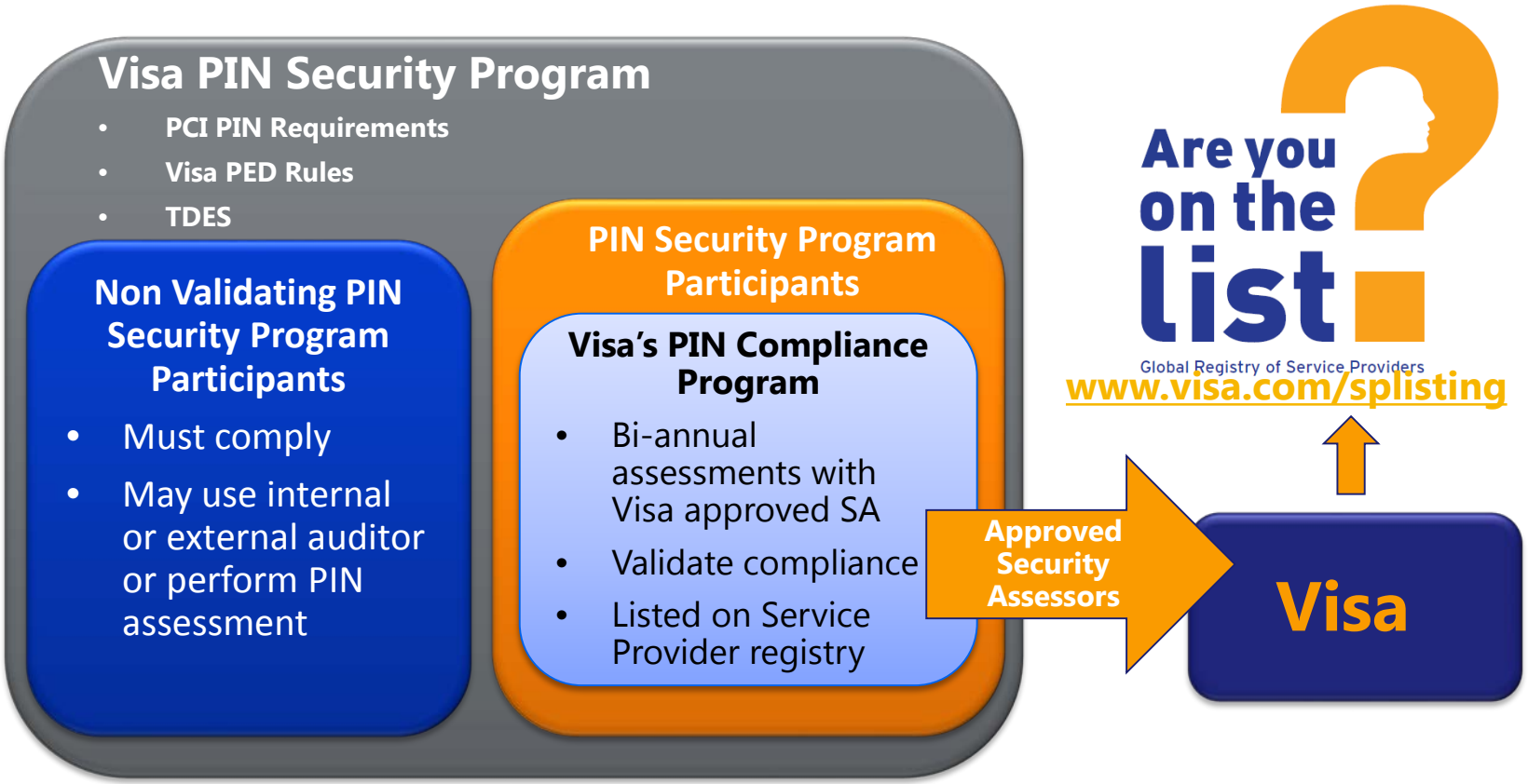
# Visa PIN Security Program Framework

Visa's Global Registry of Service Providers

## Steps to get on the Visa's Global Registry of Service Providers List



# Visa PIN Security Program Framework Summary



# Validation Deadlines for Visa PIN Security Program Participants

# Validation Deadlines for Visa PIN Security Program Participants

| Criteria | Validation Deadline |
|---|---|
| ➢ Have not performed a PIN Security onsite review before | 31 December 2015 |
| ➢ Performed an onsite review prior to 2013<br>**OR**<br>➢ Performed an onsite review in 2013 but did not complete remediation efforts | 31 December 2015 |
| ➢ Performed an onsite review in 2013<br>**AND**<br>➢ Achieved compliance | 24 months from date that compliance was achieved |
| ➢ Performed an onsite review from 2014 onwards | 24 months from the Visa Attestation of Compliance (VAOC) was issued |
| ➢ All others **OR** in doubt? | Check with Regional PIN Security Program Managers |

# PIN Security Program Enforcement Plan

# PIN Security Program Enforcement Plan

## Outline of the enforcement plan

- Effective 1 January 2016
- Affects PIN Security Program Participants who:
  - Do not have a VAOC, remediation plan, or compliance validation plan on file with Visa
  - Are not in compliance with the PIN Security Program Requirements, including PIN Security, Visa PED requirements and TDES requirements
- Noncompliance assessments will be applied to any client using a noncompliant agent on a monthly basis

**Note – PIN Security  Program Enforcement Plan does not supersede assessments pursuant to the Visa Rules for PIN Security noncompliance in the event of a PIN Compromise.*

# PIN Security Program Enforcement Plan

## Remediation and Compliance Validation Plan Options

- Need to be submitted before validation deadline to avoid noncompliance assessments
- Visa client will review and accept the remediation plan and provide a copy of the documentation to Visa PIN Risk representative
- Visa reserves the right to review and reject remediation plans

## Remediation Plan

- Identifies areas of noncompliance determined by the Visa Approved Security Assessor and action plan to correct
- Includes dates and 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

# Additional Resources

# Additional Resources

## PIN Security Website

- *www.visa.com/PINsecurity*
- PIN Security News
- Important Visa PIN Documentation
- PIN Security Program requirement documentation

## PCI PIN Training through the Visa Business School

- *www.visabusinessschool.com*

## Visa PIN Security Program Contacts

**Canada and US:** PINna@visa.com
**AP & CEMEA:** PINsec@visa.com
**Latin America:** PINlac@visa.com

Thank you for attending!

Questions?