Mitigating Large Merchant Data Breaches

August 28, 2013

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. 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 to a client or any third party 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

- Global Threat Landscape
- Common Security Deficiencies
- Intruder Footprints and Attack Prevention
- Secure Technologies
- Q&A

Visa Global Security Summit

The Visa Global Security Summit is a must-attend event for executives from business, government, academia and law enforcement. The conference will explore the intersection of technology and security, and participants will offer diverse perspectives on how industry and government can collaborate to address cyber security issues.

- Pre-Summit Risk workshops for acquirers, merchants, and processors: Oct 1st
- General Session: Oct 2nd

Register at: https://www.cvent.com/events/visa-global-security-summit/registration-e3c000e253d34af6872c03cd5126c32e.aspx

Visa's Multi-Layered Strategy

Mitigating fraud through continuous leadership, coordination and investment

Maintaining and enhancing stakeholder trust in Visa as the most secure way to pay and be paid

Security Vulnerabilities and Prevention Strategies

Ingrid Beierly

PCI DSS Requirements

Commonly Identified Security Deficiencies

	Vulnerability	Applicable Requirement
Network Security	Default or no firewall / router rules	Requirement 1
	No DMZ	Requirement 1
	Insecure remote access, no 2-factor authentication	Requirement 8
Host-based Security	Insecure operating systems and databases	Requirement 6
	No patching	Requirement 6
	No or outdated anti-virus signatures	Requirement 5
	No password management or access control lists (ACL)	Requirement 7
	Use of default or shared usernames and passwords	Requirement 2
	No system logging	Requirement 10
	No file integrity monitoring	Requirement 10
Application Security	SQL injection / other web-based exploits	Requirement 6
	No secure coding, independent code review, or penetration testing process in place	Requirement 6
Incident Response	No incident response plan	Requirement 12
General	No monitoring of systems, logs, access control, etc.	Requirement 10

- **Lack of network segmentation has contributed to multiple location breaches**

Source: Data breach forensic reports

Identified Security Vulnerabilities

	Vulnerability
Malware (RAM scraper, Key Logger)	RAM scraper is the #1 malware used by hackers to steal full track data in memory
	Citadel malware is used to steal VPN credentials and exploit the payment card environment
Insecure Web Applications	Web Management Console is accessible from the Internet
	SQL injection and xp_cmdshell vulnerabilities
	ColdFusion vulnerabilities
Insecure Domain Controllers	Use of weak password hash algorithm
	Unrestricted logon rights for privileged accounts stored in the local SAM
	Allowing Internet access
Storage of Prohibited Data	Troubleshooting/debug mode is enabled
	Secure delete is not used to remove data
	No enterprise-wide cardholder data scans are conducted to identify cardholder data storage

Source: Data breach forensic reports

Indicators of a Compromise (IOC)

File Name	Purpose	File Size (bytes)	MD5 Hash
System32.exe	Backdoor	618570	b9cf8e70681755c1711c38944695eeaa
Svcsec.exe	Backdoor	614474	25f7b169b43c4d5db472afb0ee09b035
CiscoSvc.exe	Memory Parser	N/A	9f456687aad8d329e347fb00fe01e6b4 a3224de91bab9d0c22498853de86808d
CiscoLog.exe	Memory Parser	N/A	4b9b36800db395d8a95f331c4608e947
oposvc.exe	Memory Parser	69632	dd90c44afa5da730b8cb979667ae8fd3
apve.exe	Citadel variant	274432	f45c85e5b1a46dd773d2dc907f782f2c

Source: Data breach forensic reports

Attack Prevention: Security Strategies and Actionable Items

- The following slides will cover strategies and actionable items for these security domains:
  - Network Security
  - Point-Of-Sale Security
  - Secure Web-based Applications
  - Administrator Accounts
  - Incident Response

Network Security Actionable Items

- Segregate the payment processing network from other non-payment processing networks
- Implement strict inbound and outbound filtering on the firewall rule sets (critical on outbound traffic)
- Perform penetration testing to identify security gaps
- Identify systems (such as jump servers) that have access to the payment card and ensure systems are secure
- Deny Remote Desktop Protocol (RDP) logons
- Secure domain controllers (DCs) and implement a process to have a repeatable and secure deployment of DCs

Point-Of-Sale (POS) Security Actionable Items

- Implement point-to-point encryption (P2PE) PEDs
  - EMV capability
  - Secure Reading and Exchange of Data (SRED)
  - Hardware-based encryption
- Install PA-DSS compliant payment applications
- Deploy the latest version of operating systems and ensure it is up-to-date with security patches, anti-virus, FIM, HIDS
- Perform a binary or checksum comparison
- Disable unnecessary ports and services, null sessions, default users and guests
- Enable logging of events and make sure there is a process to monitor logs on a daily basis

POS Security (cont.)

- Implement least privileges and access controls lists (ACLs) for users and applications on the system
- Implement a security policy that includes operating system security configuration to include the following:
  - Security installation guide
  - Password management guide to manage users on the system
  - Mechanism to ensure consistent security baseline on critical systems
- Implement an enterprise-wide cardholder data scan to identify storage of clear-text data and perform a secure delete of any data identified

Secure Web-based Applications Actionable Items

- Perform detailed and manual web application penetration testing against applications in your environment
- Review all web-based management consoles and ensure it is configured in a secure manner
- Ensure all web servers are hardened and up-to-date with the latest security patches and hotfixes
- Implement a Web Application Firewall (WAF) to help mitigate web-based attacks
  - A combination of insecure code and dangerous stored procedures could execute statements at a higher level privilege

Administrative Accounts Actionable Items

- Use two-factor authentication when accessing the payment processing networks
- Limit administrative privileges on applications
- Periodically review systems (local and domain controllers) for unknown and dormant users
- Apply same security on database users
- Do not use weak encryption algorithm for passwords (e.g., NTLM)

Incident Response Actionable Items

- Deploy Security Information and Event Management (SIEM)
- Review logs and offload to a dedicated server (e.g., syslog and in a secure location where hackers can't tamper with logs)
- Invest in an incident response team
  - Knowledge
  - Training
  - Certification
- Test your incident response plan
- Implement Indicators of Compromise (IOC) signatures on your solution

Secure Technologies and U.S. Authentication Roadmap

Tia D. Ilori

Secure Technologies

Advance cardholder data security through the use of robust technologies design to further protect customer data:

- **EMV Chip Technology**
  - Protects against counterfeit cards by replacing static data with dynamic
- **Point-to-Point Encryption (P2PE)**
  - Protects cardholder data from the point of data entry to the payment card processor
  - Shields against malware that “sniffs” and “captures”
- **Tokenization Technology**
  - Replaces cardholder data with surrogate values, or “tokens”
  - Allows merchants to limit or eliminate the storage of cardholder data

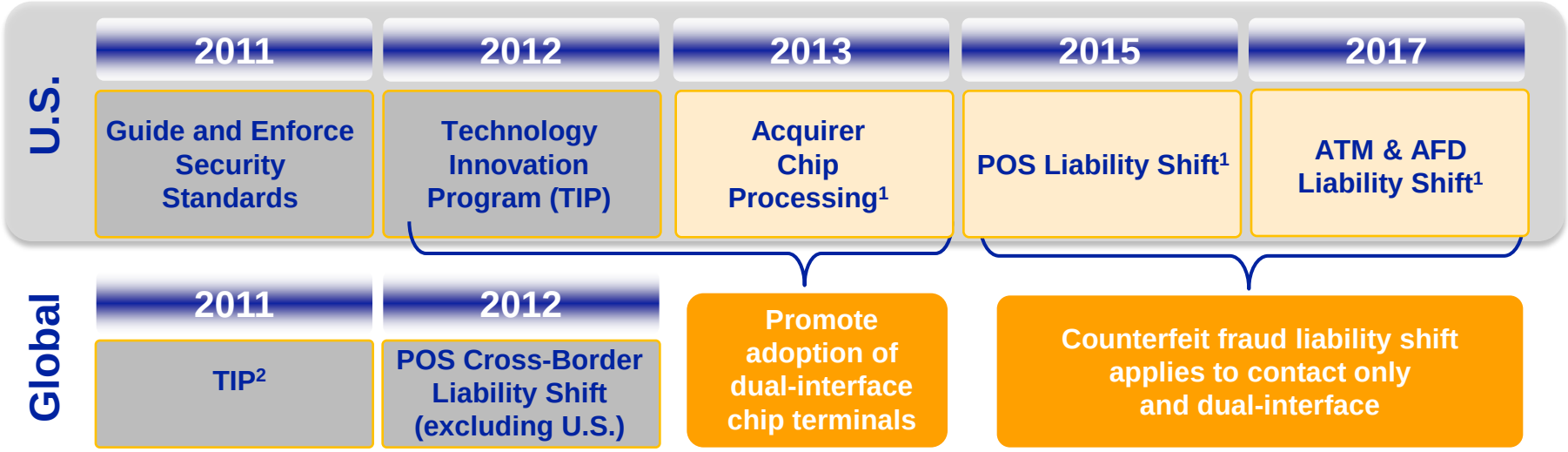
If properly implemented, all three can reduce the scope of PCI DSS compliance.

Visa Best Practices for P2PE and Tokenization – www.visa.com/cisp

Authentication Roadmap

U.S. EMV chip roadmap supports three primary opportunities

1. **Build framework** for mobile payments and future innovation leveraging EMV infrastructure for both contact and contactless payments
2. **Support interoperability and improve authorization decisions** as EMV adoption continues to grow worldwide
3. **Reduce reliance on static data** and incidence of counterfeit fraud



[1]Dates and/or timelines may change
[2]Visa Europe announced a corresponding program

EMV Chip Technology

Chip cards, also known as smart cards, can be contact or contactless

- A chip card is simply a plastic card containing an integrated circuit
- The chip is usually powered by the reader and relies on a reader to function
- Contact cards communicate with the reader over a contact plate. The plate must come into contact with the terminal usually via a dip reader
- Contactless cards communicate via radio frequency (RF) and must contain an antenna
- Dual interface cards combine both technologies and can communicate either way

Secure Technologies

P2PE / Tokenization

- Encryption is designed to protect cardholder data from the point of data entry to the payment card processor
  - Designed to protect cardholder data in transit
  - Protects against malware that “sniffs” and “captures” cardholder data transmitting
  - Uses a key management feature making cardholder data unreadable to anyone that does not have a special “key”
- Tokenization defines a process through which PAN data is replaced with a surrogate value known as a “token.”
  - Designed to work in concert with encryption to eliminate storage of cardholder data.
  - Allows merchants to limit the storage of cardholder data to within the tokenization system
  - The security of an individual token relies on the infeasibility to determine the original PAN

Visa Merchant Data Secure

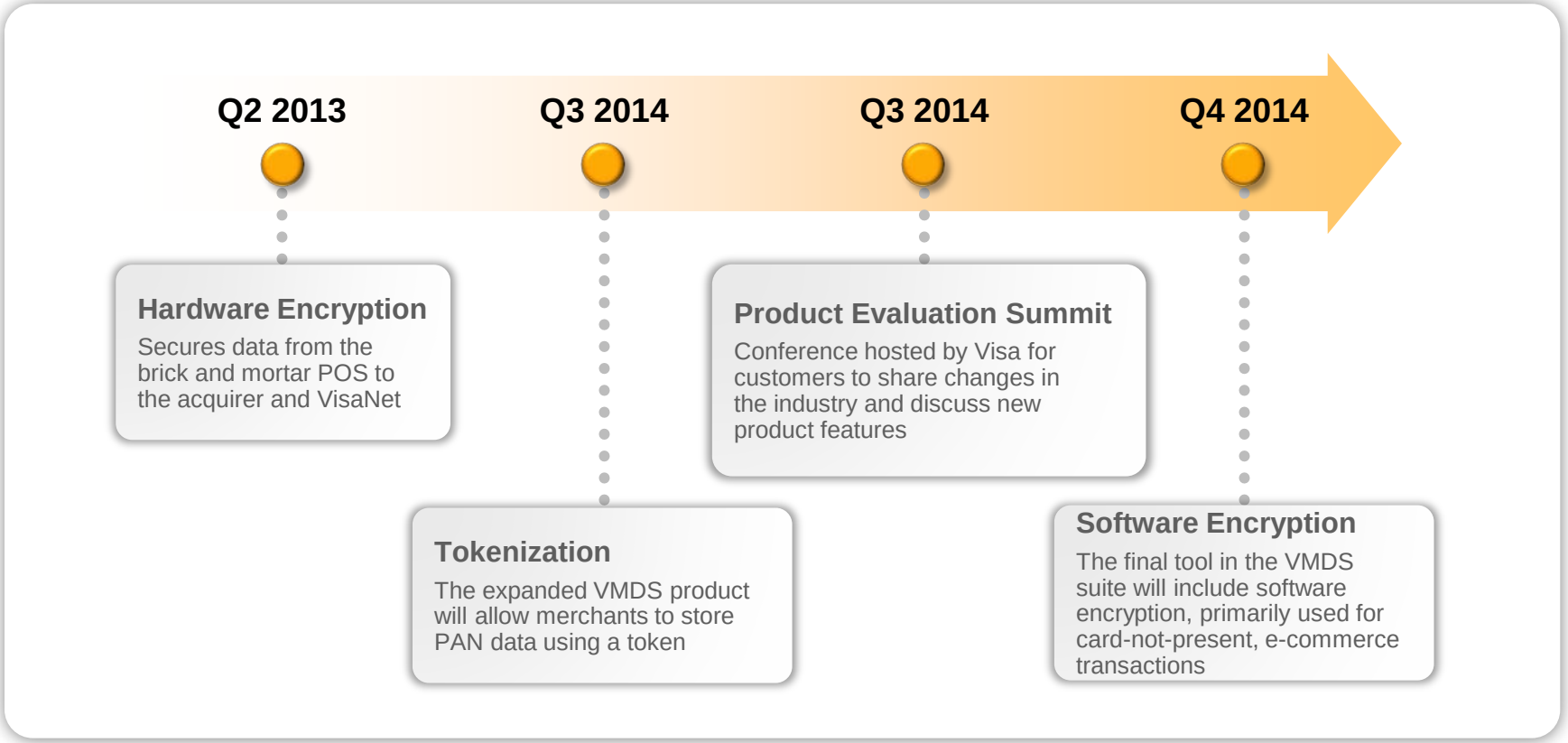
Visa Merchant Data Secure with Point-to-Point Encryption (VMDS with P2PE) is being developed to:

- Protect Sensitive Card Data Information
- Encrypt from the POS to a Card Network
- Integrate Seamlessly into Existing Business Processes
- Encrypt All Card Brand Data in Transit
- Be a Leading Industry Standard
- Offer Scalable Technology and Be Flexible for All Merchant Sizes

Proposed service in development and presented for discussion purposes only; service functionality, features and timelines subject to change by Visa at any time.

Roadmap for Development

Visa plans to expand the VMDS Product Suite by providing customers with solutions for enterprise security



Proposed service in development and presented for discussion purposes only; service functionality, features and timelines subject to change by Visa at any time.

Visa Ready Program mPOS Overview

Foster innovation by making it easier to navigate the complexities of the payment ecosystem and develop best in class offerings

- Innovative payment methods like mobile Point-of-Sale devices being introduced in marketplace
- Visa Ready provides guidance for vendors to meet Visa's requirements for a reliable, convenient, and secure mobile point of sale experience
- Mobile payment application vendors submit solution to participating third-party lab for evaluation and approval
- Financial institutions and merchants can benefit from certified Mobile Payment Acceptance Solutions
- Visa Ready mPOS solutions can be found at https://technologypartner.visa.com/mPOS/default.aspx

Visa Secure Technology Webinar

Encryption and Tokenization: Protecting Customer Data

- **Wednesday, September 18, 2013 - 10:00 am Pacific time**
- **Tia D. Ilori | Americas Payment System Security**
- **Sue Zloth | Global Acquirer Processing**

When a customer swipes, dips or types their payment card information, they want to trust that their personal and financial information will be safe. Recently, enterprise data breaches have exposed millions of cards to hackers, bringing into question this trust.

The webinar will cover the following:

- How can a merchant be sure data is secure?
- What tools can merchants use to mitigate risk?
- How does EMV fit with Encryption and Tokenization?
- How do Encryption and Tokenization affect PCI compliance?

To register visit:
https://visa.adobeconnect.com/e4ay2jujycq/event/registration.html

Visa Global Security Summit

The Visa Global Security Summit is a must-attend event for executives from business, government, academia and law enforcement. The conference will explore the intersection of technology and security, and participants will offer diverse perspectives on how industry and government can collaborate to address cyber security issues.

- Pre-Summit Risk workshops for acquirers, merchants, and processors: Oct 1st
- General Session: Oct 2nd

Register at: https://www.cvent.com/events/visa-global-security-summit/registration-e3c000e253d34af6872c03cd5126c32e.aspx

PCI SSC Community Meeting

- **PCI Security Standards Council (SSC) North America Community Meeting**
- **September 24-26, 2013**
- **Las Vegas, Nevada**
- **Visa will host "office hours" throughout the community meeting**
  - Participating organization are encouraged to take advantage of this unique opportunity to engage with Visa representatives
  - For more information please visit https://www.pcisecuritystandards.org/communitymeeting/2013/north-america

Questions?

Appendix

What To Do If Compromised

- Take compromised system off the network
- If you must rebuild system, take a forensic image prior to rebuild
- Review firewall configuration and disable any unnecessary inbound and outbound traffic
- Pair down ACLs, ports and services between PCI and non-PCI environment
- Create strict ACLs segmenting public facing systems and backend database systems that house payment data (e.g., DMZ)
- Change all passwords on the network including applications and local accounts
- Review all access to the payment processing environment and terminate connectivity

What To Do If Compromised (cont.)

- Notify your acquiring bank
- Engage a PCI Forensic Investigator (PFI) https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php
- For more information, please refer to Visa's *What To Do If Compromised,* available at www.visa.com/cisp under the "If Compromised" section
- You can also contact Visa Fraud Control and Investigations at usfraudcontrol@visa.com or (650) 432-2978, option 4

Resources

Visa's U.S. Data Security Program

- Data Security Alerts, Bulletins and Webinars
- Data Security Best Practices
- Data Security Press Releases and Third Party Media Articles
- Global Registry of Service Providers – PCI DSS Validated Entities
- Technology Innovation Program
- PIN Security and Key Management Program
- What To Do If Compromised manual
- Responding to a Data Breach guidelines

Comments to cisp@visa.com

www.visa.com/cisp

Resources

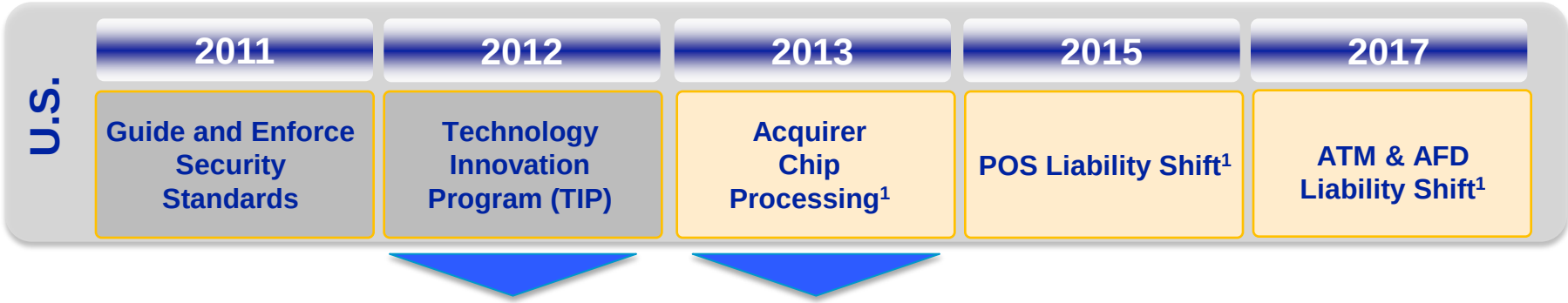
PCI Security Standards Council

- PCI Data Security Standard (DSS)
- Payment Application Data Security Standard (PA-DSS)
- PCI PIN Transaction Security (PTS)
- PCI Point-to-Point Encryption (P2PE)
- PCI DSS Applicability in an EMV Environment
- PCI DSS Tokenization Guidelines
- Self-Assessment Questionnaires (SAQ A, B, C, VC-VT, D, P2PE-HW)
- Qualified Security Assessor (QSA) List
- Approved Scan Vendor (ASV) List
- PCI Forensic Investigator (PFI) List
- FAQ Database

www.pcisecuritystandards.org

Encouraging Terminal Adoption

Building processing infrastructure for chip and mobile acceptance



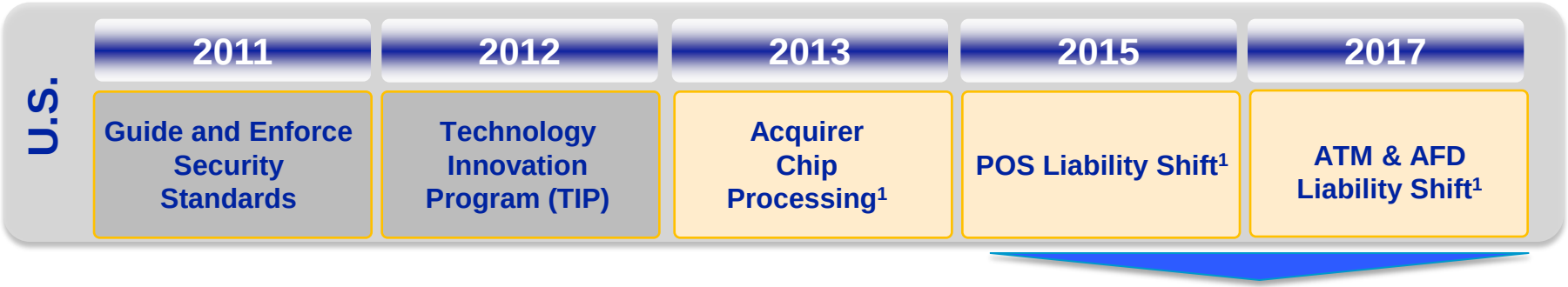
- TIP recognizes and incents merchant chip investments, while maintaining expectation for merchants to protect cardholder data
- Participation results in cost savings by waiving the annual PCI DSS validation exercise
- Eligible merchants must meet **all** of the minimum qualification criteria
  - PCI DSS compliance or remediation plan
  - No storage of prohibited data
  - At least 75 percent of merchants' transactions must originate from dual interface chip terminals and can process end-to-end chip transactions
  - No involvement in cardholder data breach[2]

- Mandate for U.S. acquirer processors and sub-processor service providers to support chip processing, effective April 1, 2013
- Acquirers must certify the ability to comply
- Visa will require support of Field 55 and additional related chip fields for VIP authorization messages between the acquirer and Visa
- Acquirers should also ensure downstream connections certify to their own platforms prior to the deadline

[1]Dates and/or timeline may change
[2]Merchants previously involved in a breach may qualify if they have completed subsequent PCI DSS validation

Managing Liability

Liability shift rewards the entity making the investment in EMV. It is not a mandate to issue or accept chip cards



- Visa intends to establish a U.S. liability shift for domestic and cross-border counterfeit POS transactions
- If a card is contact chip-capable and the merchant has not invested in chip, liability for counterfeit fraud will shift to the acquirer
- The chip card's counterfeit fraud protection plus the liability shift encourage issuer chip adoption by providing dynamic authentication that helps better protect all parties
- The liability shift does not cover
  - Cards without a contact chip
  - Card-not-present transactions
  - Lost-and-stolen fraud

Liability Shift

Product Type	Merchant Terminal	Liable Party
Contact Chip or Dual Interface	Magstripe Only	Liability Shifts from Issuer to Acquirer

Note: When a chip-on-chip transaction occurs, in the unlikely event there is counterfeit fraud, liability follows current *Visa International Operating Regulations*

[1]Dates and/or timelines may change