PCI DSS:
A Look Inside V3.2

11 May 2016

Janet Cookson – Director, Data Sec & Third Party Risk, Visa Inc.
Lester Chan – Director, Merchant Security, Visa Inc.

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

- PCI Security Standards Council Overview
- Why V3.2?
- V3.2 Change Drivers
- V3.2 Requirements
- Summary
- Supplemental Documents
- Key Dates
- Resources
- Questions and Answers

PCI Security Standards Council

- Global organization responsible for development, management, education, and awareness of the Payment Card Industry Security Standards

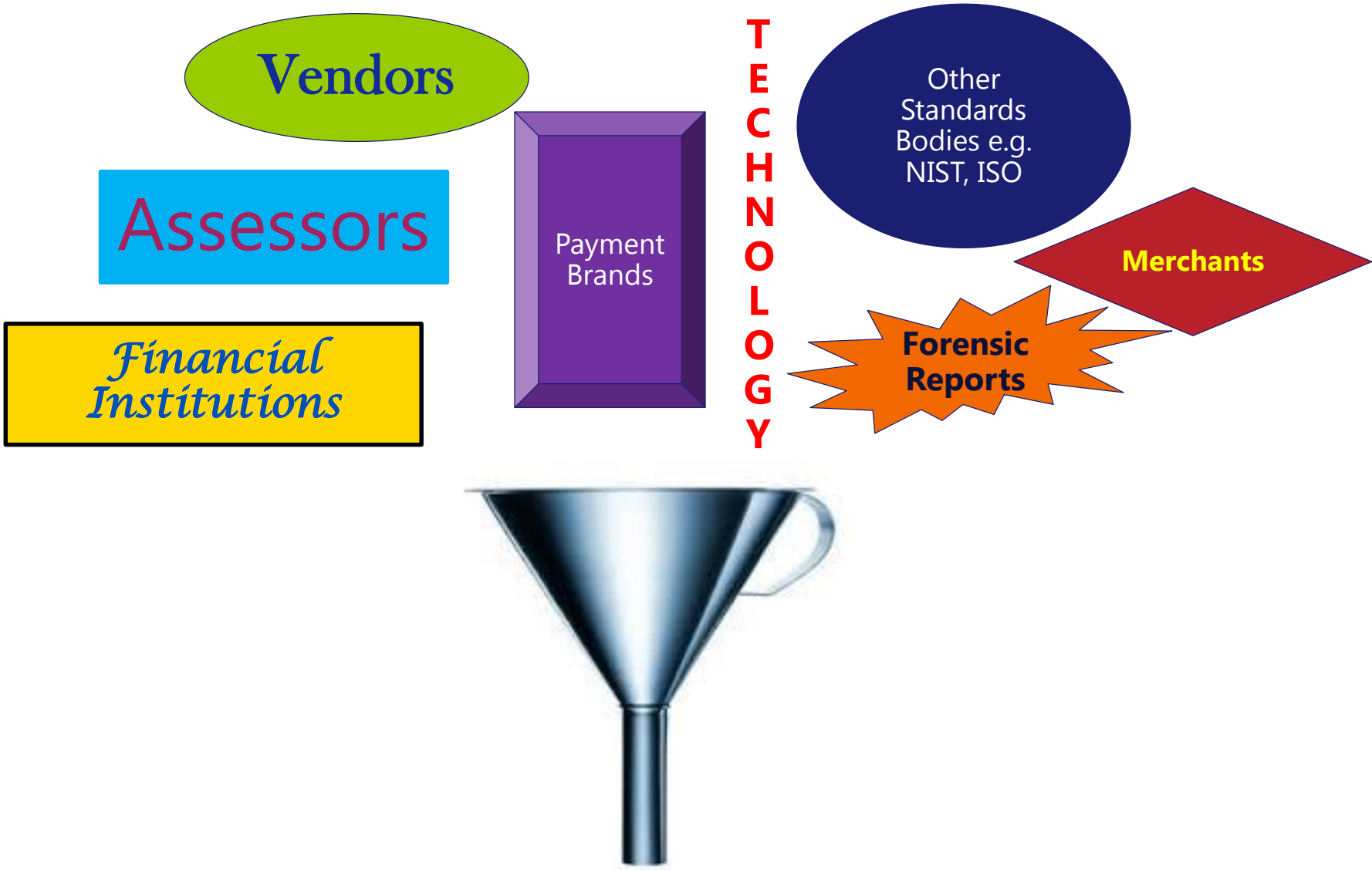
- Visa and other card brands serve as founding members and set strategic direction for the organization

PCI SSC Releases Update

Payment Card Industry Security Standards Council Releases PCI Data Security Standard Version 3.2
— Data Breach Trends Drive Modifications to Global Standard for Payment Security

WAKEFIELD, Mass., 28 April 2016 — Today the PCI Security Standards Council (PCI SSC) published a new version of its data security standard, which businesses around the world use to safeguard payment data before, during and after a purchase is made. PCI Data Security Standard (PCI DSS) version 3.2 replaces version 3.1 to address growing threats to customer payment information. Companies that accept, process or receive payments should adopt it as soon as possible to prevent, detect and respond to cyberattacks that can lead to breaches.

Why V3.2?



PCI DSS V3.2

V3.2 Change Drivers

Industry Feedback on SSL Dates

Administrative Access and Change Control

Service Providers

Clarification and Guidance

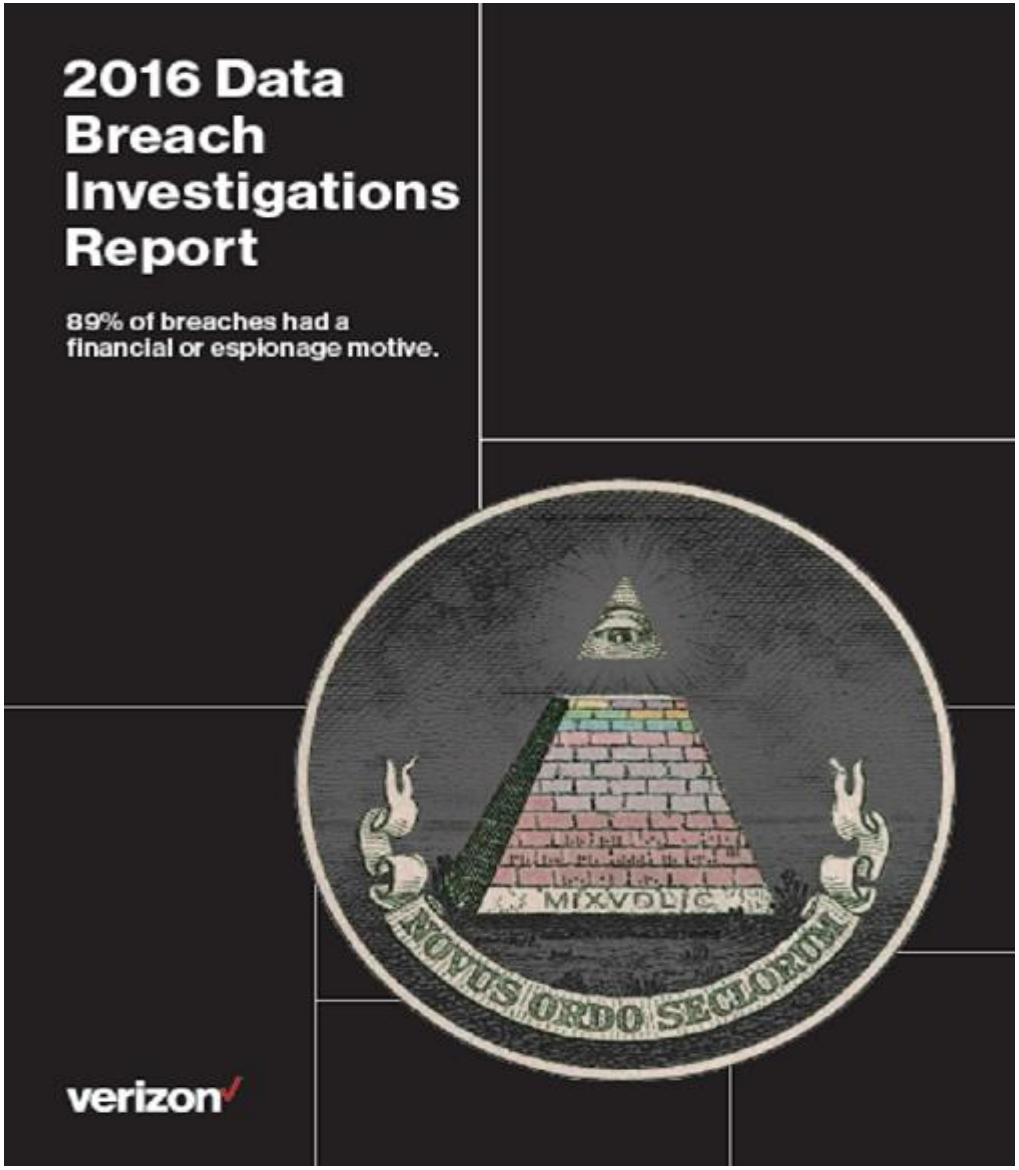
Industry Feedback on SSL Dates

Migration deadlines extended to 30 June, 2018

- New implementations must not use SSL/early TLS
- Service Providers must have secure service offering by 30 June, 2016
- All entities must cut over to secure versions of TLS by 30 June, 2018
- Prior to June 30, 2018, existing implementations must have a formal Risk Mitigation and Migration Plan in place
- POIs verified as not susceptible to known SSL vulnerabilities may use SSL/early TLS after 30 June, 2018

Note: If SSL/early TLS is used, Appendix A2 applies

Administrative Access



Administrative Access

New Requirement

8.3.1 - Incorporate multi-factor authentication for all personnel with administrative access into the cardholder data environment.

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

Change Control

New Requirement

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

Service Providers

New Requirements

- **3.5.1** - Documentation of cryptographic architecture
- **10.8** - Detect/report on failures of critical security control systems
- **11.3.4.1** - Penetration testing on segmentation controls every six months
- **12.4.1** - Establish responsibility for PCI DSS
- **12.11** -Confirm personnel are following security policies and operational procedures at least quarterly

Note: These requirements are a best practice until January 31, 2018, after which they become requirements.

Clarification and Guidance

- Display of PAN greater than first six/last four requires business need
- Move all examples from the requirements and place into guidance

- Update wording to requirements, testing procedures and guidance to improve understanding and intent
- Two new appendices
  - Address SSL/early TLS
  - Move DESV requirements into PCI DSS

Summary

- **Dates to remove SSL have been extended to June 30, 2018**
- **Service Providers must offer a secure TLS offering by June 30 2016**

- **Administrative access to the CDE requires MFA**
- **Change control procedures must include checks to ensure PCI DSS controls are applied**

- **5 new requirements for Service Providers**
  - Document cryptographic environment,
  - Detect/report on critical control failures,
  - More frequent pen testing on segmentation controls,
  - PCI DSS governance,
  - Self checks to support BAU

- **Display of PAN can support longer BINs**
- **Two new appendices to support SSL and DESV**

Supplemental Documents

Now available –

https://www.pcisecuritystandards.org/document_library

- Summary of Changes
- Glossary
- SSL/TLS Info Supplement
- SAQs
- ROC template and AOCs
- Prioritized Approach
- FAQs, etc.

V3.2 Key Dates

Apr 2016

Publication of PCI DSS V3.2

Assessments can be performed to V3.1 or V32

Oct 2016

V3.1 Retires

Organizations should be adhering to V3.2

All assessments use V3.2

Jan 2017

Visa stops accepting V3.1 reports

Feb 2018

New requirements are no longer best practice and compliance is required

Reminder SSL/early TLS Dates

June 30, 2016	Service Provider must have secure service offering
June 30, 2018	All entities must cut over to secure version of TLS
Prior to June 30, 2018	Existing SSL/ early TLS implementations must have Risk Mitigation and Migration Plan

Additional Resources

- PCI SSC Document Library: https://www.pcisecuritystandards.org/documents_library
  - PCI DSS 3.2
  - Summary of Changes
- PCI SSC blog: http://blog.pcisecuritystandards.org
  - Preparing for PCI DSS 3.2
  - Working with ASVs on Failed Scans
  - Reporting new SSL/TLS dates for PCI DSS v3.1
- SSL/Early TLS Information Supplement
  - https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information_Supplement_v1.pdf
- Bulletin on updated migration dates (Dec 2015)
  - https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_and_Early_TLS_-v12.pdf
- Visa Data Security Website – www.visa.com/cisp
  - Alerts, Bulletins
  - Best Practices, White Papers
  - Past Webinars

Q & A