• How did we get here?

• PCI DSS 2.0

• PA-DSS 2.0

• PCI SSC Education & Resources

• Q&A
How Did We Get Here?
How Did We Get Here?

- Revision or version is effective immediately
- Phase in new requirements
- Provide guidance for those in middle of assessment process
- Keep organizations in compliance

Month 24
New Version Release

- Issue new version or revision
- Provide stakeholders summary of changes
- Ensure any new requirements have lead time

Months 0-9
New Version Released / Quiet Period
- Communications, implementation and dissemination of release
- Prepare for the formal feedback period
- Evaluate immediate feedback as needed

Months 21-24
New Release Final review

Months 10-12
Feedback Period
- Open formal feedback process
- Feedback forms compiled

Months 13-20
Feedback Review and Decision
- Communicate compiled feedback
- Analyze trends and concern areas
- Impact analysis
- Propose changes
- Determine action plan
- Issue preliminary version or revision for final review
Feedback

PCi Data Security Standard

- Propositions from Associations
- Compromise Trends
- Questions Posed to the Council
- SIG Input
- Advisory Board
- Community Meeting
- Proactive feedback from QSAs, ASVs and POs
- Webinars and PCI SSC Presentations
- Direct Feedback from Payment Brands
New Three-Year Lifecycle

1. Market Implementation (10/1/08 – 6/30/09)
   - Discuss New Version / Revision (9/30/10)
   - Feedback Begins (7/1/09 – 10/31/09)

2. Feedback Review and Decision (11/1/09 – 4/30/10)

3. Feedback Review and Decision (11/1/09 – 4/30/10)

4. Old Standards Retired (December 31)

5. Final Review (October)

6. Draft Revisions (November – April)

7. Feedback Begins (April – August)

8. Market Implementation (All Year)

YEAR 1: Evaluate
YEAR 2: Provide
YEAR 3: Evolve

Evolving Technology
DSS & PA-DSS
Community Meeting

PCI Security Standards Council
PCI DSS 2.0 Lifecycle

- Version 2.0 published October 28, 2010
- Effective January 1, 2011
- Feedback begins November, 2011
- Version 1.2.1 retired December 31, 2011
- Community Meetings September / October 2011
Drivers for Change

- Provide greater clarity on PCI DSS & PA-DSS requirements
- Improve flexibility
- Help manage evolving risks / threats
- Align with changes in industry best practices
- Clarify scoping and reporting
- Eliminate redundant sub-requirements
Changes to the PCI DSS & PA-DSS

- Clarifications
- Additional guidance
- Evolving requirements

Your feedback has made the standard more mature and will help secure payment card data well into the future!
At a Glance – Key Updates

- Scoping
- Logging
- Risk-based approach
- Alignment between PA-DSS & PCI-DSS
- Recognition of small merchant environments
- New website and updated supporting documentation
• PCI DSS applicability

• Clarify boundaries between the Internet and the CDE (1.3)

• Issuers and sensitive authentication data (3.2)

• Rendering PAN unreadable (3.4)

• Additional sources for secure coding for non-web based applications (6.5)

• Time synchronization services (10.4)
Other PCI DSS v2.0 clarifications include:

- Updates to Report on Compliance (ROC) template
- Key management procedures (Requirements 3.6.4 – 3.6.6)
- Anti-virus logs (Requirement 5.2)
- Requirement 8
  - Align authentication for cashiers with PA-DSS
  - Clarifying authentication factors
- Identify target areas for intrusion detection (11.4)
- More flexible policy for remote access to CHD (12.3.10)

AOCs:
- Reformatted for better information flow

SAQs:
- Align with new PCI DSS requirements
• Relationship between PCI DSS and PA-DSS

• Scoping the cardholder data environment (CDE)

• Sampling of business facilities and system components

• Virtualization

• Detection of rogue wireless access points
PCI DSS 2.0 - Evolving Requirements

- Risk based approach for addressing vulnerabilities
  - Assign risk ranking to vulnerabilities (Requirement 6.2)
  - Also impacts Requirements 6.5.6 and 11.2
  - Sunrise date July 1, 2012
• **Virtual Terminals**
  – Only payment processing is done via a virtual terminal (VT)
  – VT access is via merchant’s PC and browser
  – Merchant PC is not connected to other locations or systems
  – PCI DSS compliant third party service provider
  – No special software or hardware installed on the PC (for card swipe or data collection)
  – No electronic storage of cardholder data

• **SAQ C review**
  – Payment application and Internet connection on same device or same local area network (LAN)
  – Payment application/Internet device segmented from all other systems, in a single store environment
Other Activities

- Feedback is still being considered
- Navigating guide
- Training
- Additional information supplements
  - Issuer guidance
  - Virtualization
  - Bluetooth
  - Scoping
  - Emerging technologies
PA-DSS 2.0 - Additional Guidance

• PA-DSS applicability to payment applications on hardware terminals
  – PTS validated POI device
  – Required dependency
  – PCI DSS compliant settings must be enabled by default
• Facilitate centralized logging (4.4)
  – Payment application to facilitate a merchant’s ability to assimilate logs into their centralized log server
  – Implementation Guide to include instructions and procedures for incorporating payment application logs into a centralized logging environment.

• Risk based approach for addressing vulnerabilities (7.1)
  – Risk ranking
  – Also impacts 5.2.6
• Implementation guide to include instructions for configuring underlying systems (such as OS) to prevent inadvertent capture or retention of cardholder data (2.1)
  – For example, system backup or restore points
• Cryptographic key material stored by previous versions to be rendered irretrievable (2.7)
  – Secure deletion or deletion of KEK
• Merge requirements 10 and 11
• AOVs:
  – Reformatted for better information flow
PA-DSS 2.0 - Clarifications (cont’d)

• **General**
  – Applicability information aligned with PCI DSS
  – Relationship between PA-DSS and PCI DSS
  – Bulleted test procedures have now been separated
  – Imported PCI DSS requirements and testing procedures

• **Clarified testing guidance to PA-QSAs**
  – PA-QSA must have access to the testing laboratory and validate the clean installation of the lab environment
  – Only test card numbers used for the simulation/testing

• **Clarification that “N/A” findings must be explained in RoV**
PA-DSS 2.0 Lifecycle

- Version 2.0 published 28 October, 2010
- Effective January 1, 2011
- Feedback begins November, 2011
- Version 1.2.1 retired December 31, 2011
- Community Meetings September / October 2011
Ongoing Evaluation

1. Standards Published
   - October

2. Standards Effective
   - January 1

3. Market Implementation
   - All Year

4. Feedback Begins
   - November

5. Old Standards Retired
   - December 31

6. Feedback Review
   - April–August

7. Draft Revisions
   - November–April

8. Final Review
   - May–July

YEAR 1
- Provide
- Evaluate
- Evolving Technology
- Guiding Recommendations

YEAR 2
- Provide
- Evaluate
- Evolving Technology
- Guiding Recommendations

YEAR 3
- Provide
- Evaluate
- Evolving Technology
- Guiding Recommendations

COMMUNITY MEETINGS
- September–October
PCI DSS and PA-DSS 2.0 Resources

- Security standards and supporting documents
- Quick reference guide
- Searchable frequently asked questions
- List of approved PED labs, QSAs, ASVs, PA-QSAs,
- Education and outreach - e.g., fact sheets, webinars
- Participating membership, meetings, collaboration
- A global voice for the industry
New Website

https://www.pcisecuritystandards.org
• Feedback from numerous sources have been incorporated into PCI DSS 2.0 and PA-DSS 2.0

• 2.0 versions do not introduce any new major requirements

• PCI Security Standards provide a solid foundation for a security strategy

• We will continue to look at evolving threats and technologies

• Even though you have more time, move toward adopting 2.0 ASAP
Q&A