A Perfect Fit: Understanding the Interrelationship of the PCI Standards
Agenda

- Who is the Council?
- Goals and target for today’s Webinar
- Overview of the Standards and “who’s who”
  - PCI DSS
  - PA-DSS
  - PED Security Requirements
- Relationship between standards
- Facts and myths
- Q&A
Who is the Council?

• An Independent Industry Standards Body
  • Security Standards and Supporting Documents
  • Frequently Asked Questions
  • List of Approved QSAs, ASVs, PED Labs
  • Education and Outreach Programs
  • Participating Organization Membership, Community Meetings, Feedback

• One Global Voice for the Industry
Goals and Target Audience

• **Goals**
  
  – High level understanding of each of the PCI standards and what they do and who they apply to
  
  – See the interrelationship of the standards and *when combined*, how they are your best protection against a data breach
  
  – Debunk several myths surrounding PCI, the standards and compliance
Goals and Target Audience

• Target Audience
  – Merchants and service providers who are implementing the standards
  – Non technical business analysts or SMB owners who are just embarking on PCI compliance programs
  – Information security professionals wanting to get a “quick start” to understanding PCI

Please Note: This is not an in-depth technical discussion for the assessment community
The SSC understands that PCI applies to more than just merchants. As a result of industry feedback, additional standards were added to the management of the council:

- Data Security Standard (DSS)
- Payment Application Data Security Standard (PA-DSS)
- Pin-Entry Device (PED)
PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

MANUFACTURERS
PCI PED
PIN Entry Devices

SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors

MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard

PCI SECURITY STANDARDS & COMPLIANCE

Ecosystem of payment devices, applications, infrastructure and users
The Cost of Complying

Three Categories of Compliance

- Upgrading Payments Systems and Security
- Verifying Compliance (Assessment)
- Sustaining Compliance

How much does this cost your organization?

For merchants with complex or older systems, it may cost millions

The Cost of Not Complying

Same study estimated non-compliance costs significantly higher, including

- “Crisis” cost upgrades
- Repeat assessments
- Notification costs
- Brand reputation
- Shareholder and consumer lawsuits

The cost of a breach can easily be 20 times the cost of PCI Compliance

“How much does this cost your organization?”

For merchants with complex or older systems, it may cost millions

“PCI Compliance Cost Analysis: A Justified Expense.”
[This study utilized data from several sources including level 1 and level 2 merchants with 2,000 – 2,500 retail locations.]
The Five Stages of Grief

• Denial
  It doesn’t apply to me
  PCI compliance is mandatory

• Anger
  It isn’t fair
  PCI applies to all parties in the payment process

• Bargaining
  I’ll do some of it
  Compliance is “pass / fail”

• Depression
  I’ll never get there
  Many merchants already have

• Acceptance
  It’ll be OK
  PCI doesn’t introduce any new, alien concepts
# The PCI Data Security Standard

## Six Goals, Twelve Requirements

| Build and Maintain a Secure Network | 1. Install and maintain a firewall configuration to protect cardholder data  
2. Do not use vendor-supplied defaults for system passwords and other security parameters |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Protect Cardholder Data            | 3. Protect stored data  
4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software  
6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need-to-know  
8. Assign a unique ID to each person with computer access  
9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data  
11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security |
The PCI Data Security Standard

- The PCI DSS is a set of comprehensive requirements for enhancing payment account data security
- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures
- This comprehensive standard is intended to help organizations proactively protect customer payment data
Updates to PCI DSS

- October 2008:
  - PCI DSS Revision v1.2
  - Assessed and Incorporated feedback received from over 2,500 queries and suggested changes from Community Stakeholders
  - 1.2 revision address the existing six goals and twelve requirements of the DSS with future effective dates for potential new sub requirements
  - Areas of focus
    - Clarity and flexibility of requirements
    - Incorporate existing and new best practices
    - Scoping and reporting clarification
    - Eliminate overlapping sub requirements and consolidate documentation
    - Expanded FAQ and glossary
The PIN Entry Device Requirements

- These requirements are divided into the following categories:
  - Device Characteristics:
    - Physical Security Characteristics
    - Logical Security Characteristics
  - Device Management
    - Device Management During Mft.
    - Device Management Between Mft. and Initial Key Loading
  - Considers how the PED is produced, controlled, transported, stored and used throughout its life cycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.
PIN Entry Device Requirements

<table>
<thead>
<tr>
<th>Physical Attributes</th>
<th>Logical Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Attributes that deter physical Attacks</td>
<td>• Logical security characteristics include functional capabilities that preclude:</td>
</tr>
<tr>
<td>– ex penetration of device to determine key(s)</td>
<td>– Allowing device to output clear text PIN encryption key</td>
</tr>
<tr>
<td>– Planting a PIN disclosing bug within</td>
<td></td>
</tr>
</tbody>
</table>

The PED Security Requirements are designed to secure personal identification number (PIN)-based transactions globally and applies to devices (attended or unattended) that accept PIN entry for all PIN-based transactions as well as non-cardholder interface devices (hardware security modules).
PIN Entry Device Requirements

Device Types Under PED

Traditional Devices include
• Point-of-sale PED Designed for Secure PIN Entry
• Attended devices (e.g., sales clerk, cashier)

New Devices scheduled for 2008 include
• Unattended Payment Terminals (UPTs)
  – Fuel Pumps, Kiosks, Ticketing Machines
• Hardware (or Host) Security Modules (HSMs)
  – Non-cardholder interface
  – Embedded devices that are used for:
    • PIN translation, Card Personalization, Data Protection, Electronic Commerce
The Payment Application Data Security Standard

• Based on Visa USA’s PABP, PA-DSS is a comprehensive set of requirements designed for payment application software vendors to facilitate their customers’ PCI DSS compliance.

• This comprehensive standard is intended to help organizations minimize the potential for security breaches due to flawed payment applications, leading to compromise of full magnetic stripe data.

• Distinct from but aligned with PCI DSS
Fourteen Requirements...Protecting Payment Application Transactions

- Do not retain full magnetic strip, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data
- Provide secure password features
- Protect stored cardholder data
- Log Application Activity
- Develop Secure Applications
- Protect wireless transmissions
- Test Applications to address vulnerabilities
- Facilitate secure network implementation
- Cardholder data must never be stored on a server connected to the Internet
- Facilitate secure remote software updates
- Facilitate secure remote access to application
- Encrypt sensitive traffic over public networks
- Encrypt all non-console administrative access
- Maintain instructional documentation and training programs for customers, resellers, and integrators
PCI PED addresses device characteristics impacting security of PIN Entry Device (PED) during financial transactions.

PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where those applications are sold, distributed, or licensed to third parties.

PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data, and specifically to those system components included in or connected to the cardholder data environment (the part of the network with cardholder data).

PCI PED applies – PED device only

PCI PA-DSS may apply

PCI DSS applies – systems & networks
Myth:
One vendor and product will make us compliant
Myth:
Outsourcing card processing makes us compliant
Myth:
We don’t take enough credit cards to have to comply with PCI DSS
Myth: PCI is too hard.
For more Information www.pcisecuritystandards.org
Questions?
Thank You!