PCI COMPLIANCE 2016

PRESENTATION BY: Dawn MacAdams-Mull
Director, PCI Compliance and Merchant Card Programs
Contact Info: 215-746-6369
dawnmac@upenn.edu
PCI DSS
I’d love to talk about PCI … no really.
Purpose of PCI Compliance

• The Payment Card Industry has established important and stringent security requirements to protect credit card data. These are called PCI Data Security Standards or “PCI-DSS”.
  – Protects against:
    • Identity theft
    • Fraudulent activity

• The PCI-DSS policy defines the way in which credit card merchant accounts must protect cardholder data and achieve PCI compliance based on the method that credit cards are processed.
  – Various processing methods include:
    • Phone processing
    • POS SwipeTerminals
    • E-Commerce
Risk of Non-Compliance

• Without adherence to the PCI-DSS standards, your Company would be in a position of unnecessary reputational risk and financial liability.
• Merchant account holders who fail to comply are subject to:
  – Any fines imposed by the payment card industry.
  – Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees.
  – Suspension of the merchant accounts.
  – Companies who are found to fail PCI compliance will be held liable and any fees or fines will be imposed against them.
  – BAD PUBLICITY FOR BUSINESS
The PCI DSS Process

• Compliance with PCI DSS is a continuous process that begins with an assessment of the environment.
• Remediation is the process of fixing vulnerabilities.
• Regular reports are required for PCI DSS compliance.
Some Common Terms

- **PCI:** Payment Card Industry
- **DSS:** Data Security Standards
- **CDE:** Card Data Environment
- **PAN:** Primary Account Number
- **SAD:** Sensitive Authentication Data
- **QSA:** Qualified Security Assessor
- **ISA:** Internal Security Assessor
- **SAQ:** Self Assessment Questionnaire
- **AOC:** Attestation of Compliance
- **ROC:** Report on Compliance
- **ASV:** Approved Scanning Vendor
- **PTS:** Pin Transaction Security
- **POI:** Point of Interaction
- **POS:** Point of Sale
- **P2PE:** Point to Point Encryption
- **CVV:** Card Verification Value
PCI DSS Applicability

• If you take payments via credit/debit card, PCI applies to you.
• “The primary account number is the defining factor in the applicability of PCI DSS requirements: PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.”
PCI DSS Applicability
PCI DSS Applicability

• Cardholder Data (CHD)
  – Primary Account Number (PAN)
    • Truncated PAN: up to first 6 and last 4

• Cardholder Name (when kept with PAN)

• Expiration Date (when kept with PAN)

• Generally, on the front of the card
  – Nothing in PCI DSS forbids CHD storage
PCI DSS Applicability

• Sensitive Authentication Data (SAD)
  – Full magnetic stripe data or equivalent on a chip
  – CAV2/CVC2/CVV2/CID
  – PIN/PIN block
• Generally, on the back of the card
• NEVER STORE SAD after authorization
<table>
<thead>
<tr>
<th>SAQ Validation Type</th>
<th>Description</th>
<th># of Questions v3.0</th>
<th>ASV Scan Required v3.0</th>
<th>Penetration Test Required v3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card not present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage.</td>
<td>14</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>A-EP</td>
<td>E-Commerce merchants redirecting to a third party website for payment processing, no electronic cardholder data storage.</td>
<td>139</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>B</td>
<td>Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage.</td>
<td>41</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>B-IP</td>
<td>Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage.</td>
<td>83</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the internet: No e-commerce or electronic cardholder data storage.</td>
<td>139</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage.</td>
<td>73</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>D-MER</td>
<td>All other SAQ-eligible merchants.</td>
<td>326</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
## PCI DSS: 6 Goals, 12 Requirements

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Build and maintain a secure network</td>
<td>1. Install and maintain a firewall configuration to protect data</td>
</tr>
<tr>
<td></td>
<td>2. Change vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>2. Protect cardholder data</td>
<td>3. Protect stored data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks</td>
</tr>
<tr>
<td>3. Maintain a vulnerability management program</td>
<td>5. Use and regularly update antivirus software</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>4. Implement strong access control measures</td>
<td>7. Restrict access to data to a need-to-know basis</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>5. Regularly monitor and test networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>6. Maintain an information security policy</td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
SCOPE
What is Scope?

What is in My PCI Scope?

– All locations and all flows of cardholder data (CHD)
– The Cardholder Data Environment (CDE): All people, processes and technology that store, process or transmit CHD
– ALL SYSTEMS connected to the above
– All systems which can affect the security of the CDE
Scoping is the First Step

• “The first step of a PCI DSS assessment is to accurately determine the scope of the review.”
  – This should be done at least annually
  – Prior to the annual assessment
  – All Card Holder Data locations, and all card data flows must be included

  Even places where it’s not supposed to be!
Assessing your Scope – Steps

• Scope assessment is a process of Defining and Documenting what’s in scope
• Your end product will be the set of documents which define what you need to assess for PCI compliance
• Save your documentation for next year
Scoping Tasks

• Identify and document all data
  – Data discovery tools may be needed
• Verify that NO Card Holder Data exists outside of the Card Data Environment
• Verify that the scope is appropriate
  – Create diagrams and/or inventories
• All CHD outside your CDE expands the CDE, unless deleted or moved into CDE
• Document your assessment procedure and retain the data
Before You Start – Educate Yourself

• Read the PCI DSS, all of it at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
  – Read all the Intro, not just the requirements
  – Business Managers are responsible for knowing it
  – Reading just the SAQ is insufficient

• If you don’t understand it all, that’s OK!
  – Read the **Guidance** column
  – The PCI DSS/PA-DSS Glossary of Terms is very helpful
  – Ask your campus IT/Security partners to explain the technology

• Know your related business policies
  – Purchasing, security, merchant services, wireless, banking, service providers, breach reporting, etc.
Next Steps

• Start by Re-examining your scope
  – Can it be reduced or limited?
  – You may need to change business processes
  – Ask your QSA to assist

• Reorganize scope in larger organizations?
  – Will you do a single assessment or separate it into multiple reporting areas for SAQs?
  – Decide who approves reporting decisions
The Next Steps

• Decide how to organize and store your documentation and evidence
  – Keep SAQs and evidence for three years
  – Control access – need-to-know

• Select appropriate SAQ(s)
  – Acquirer approval may be needed

• Working with the SAQ
  – It’s all about the documentation
  – Answers must be verifiable; do you have evidence?
  – All continuous processes must be documented over time
    • Do you have records showing that daily tasks have been done daily? Yearly tasks annually?

• Personnel lists must be kept up-to-date
Remediation and Reporting

• Where did you answer “No”?  
  – Compliance gap  
  – Determine remediation steps  
    • Changes to people, process, technology  
    • Assign tasks and set due dates

• If it’s not Yes, it’s probably No  
  – “Usually”, “Maybe”, “We will” don’t count

• All No answers must be addressed  
• N/A documented

• Final Report  
  – Send your SAQ/AOC to your acquirer  
  – Make sure the AOC (Attestation of Compliance) has the proper signatures  
  – Keep a copy with your supporting evidence
You can hire a QSA company to assist.
If you have not worked with PCI DSS before, it is a good idea to get a QSA for the education alone.
A QSA can:
- Validate your scope of compliance
- Prepare gap assessments
- Perform a full PCI assessment
  - And prepare the Report on Compliance (ROC)
  - Assist with the Attestation of Compliance (AOC)
  - Speak with your team and with business leaders
PCI Compliance is a 24/7 requirement, NOT a yearly requirement. Scope can change quickly, there is no final step, and there is no finish line.
Questions