A Prioritized Approach

WORKING TOWARD PCI COMPLIANCE
Action Items

- Document how your organization **stores, processes** or **transmits** credit card information
- Determine your merchant level
- Determine your validation requirements
  - Contact your merchant banks and acquirers
- Determine your SAQ validation type
- Find an ASV for compliance network vulnerability scans
  - Perform at least quarterly scans
- Annually fill out your SAQ
  - Turn in or keep on file

Gather Information

- List all Merchant Banks, Gateways and Acquirers
- List all Payment Applications
- List all PEDs used (Point of Interaction)
- List all outsourced processors, ASPs and third party processors
- List all physical locations that PAN is processed, stored or transmitted
  - Paper, Receipts, Imprints, Carbon Copies
- List all electronic storage of PAN
  - Electronic Image Files: Fax, Scan Archive, Laser Fiche or Audio Recordings: Voicemail, Customer Service Call Monitoring recordings
  - Include PAN stored on backup media
Next Steps

• List the number of all credit card transactions for all Merchant Banks and Acquirers
• Determine your merchant level
• Determine if any payment applications store credit card numbers
• Determine SAQ validation types

Document Compliance

• Determine if all PEDs are PCI compliant
• Determine if all payment applications are PCI compliant
• Determine if all 3rd party processors and 3rd parties are PCI compliant
• Obtain documentation from each
• Annually renew documentation from 3rd parties
• Annually check payment application and PED list
Action Items

• Contact the vendor, make sure payment applications are PA DSS complaint or will be.
• Contact your PIN device supplier, make sure you have compliant PIN Entry Devices.

https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html
https://www.pcisecuritystandards.org/security_standards/vpa/

Approved PIN Entry Devices

Please review the legal conditions and restrictions regarding PCI PED approval contained in the Payment Card Industry PIN Entry Device Testing and Approval Program Guide (PDF 2.23 MB).

Filter PED Vendors by Company Name:

Filter PED Entry Devices by:

Last Update: Apr 4th, 2009
41 Vendors, 271 Devices
Validation Requirements

• External Scans by an ASV, at least quarterly
• Annually fill out SAQ (even if bank has not requested one)
• If level 1 or 2 you will need an audit from a QSA

Document Data Flow

• With a network diagram document the flow of credit card information (transmission)
• Locate any places the information might be stored along the data path (storage)
PCI DSS

• Use the prioritized approach to implement the most important controls first.

<table>
<thead>
<tr>
<th>Requirement 1: Install and maintain a firewall configuration to protect cardholder data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Milestone</td>
</tr>
<tr>
<td>1.1 Establish firewall and router configuration standards that include the following:</td>
</tr>
<tr>
<td>1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations</td>
</tr>
<tr>
<td>1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks</td>
</tr>
<tr>
<td>1.1.3 Requirements for a firewall at each internal connection and between any demilitarized zone (DMZ) and the internal network zone</td>
</tr>
<tr>
<td>1.1.4 Description of groups, roles, and responsibilities for logical management of network components</td>
</tr>
<tr>
<td>1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those services, protocols, or ports considered to be important</td>
</tr>
<tr>
<td>1.1.6 Requirement to review firewall and router rule sets at least every six months</td>
</tr>
</tbody>
</table>

PCI DSS

• Start implementing the data security standard starting with policies
• Start with high level polices

  – “The City shall not store PAN (Credit Card Numbers) electronically or physically. Employees shall be trained on PCI standard annually. Background checks will be performed on all staff with access to credit card information.”
PII Policy

• If you already have a policy for handling confidential information or personally identifiable information add credit card information to confidential information or PII.

FILLING OUT THE SAQ
**SAQ A**

**Part 2b. Relationships**

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)?

- Yes
- No

Does your company have a relationship with more than one acquirer?

- Yes
- No

---

**SAQ A**

**Part 2c. Eligibility to Complete SAQ A**

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions;
- The third-party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant;
- Merchant does not store any cardholder data in electronic format; and
- If Merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically.
SAQ A

Items under section 12

- For Example
  - 12.5.1 Establish, document, and distribute security policies and procedures
  - 12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)
  - 12.8.1 Verify that the contract contains provisions requiring adherence to the PCI DSS requirements
  - 12.3.6 Acceptable network locations for the technologies
WHAT WE’VE SEEN

Common Findings

• Clients think they are compliant
  – Because they do quarterly networks scans
  – Because they filled out the SAQ
  – Because they have too few transactions

• Reality
  – Validation is not compliance
  – Compliance is an ongoing process
  – PCI DSS is required for all merchants, regardless of the number of transactions
Common Findings

- Payment card information on paper
- No network segmentation
- Logging Access
- Shared Passwords
- Verifying compliance of outsourced processing
- No one is assigned responsibility
- Not aware of PAN storage in application

PCI Pitfalls

- PCI will not make an organization’s network or data secure
- PCI DSS focuses on one type of data: payment card transactions
- The organization runs the risk of focusing on one class of data to the detriment of everything else