Payment Card Industry Compliance

May 12, 2011
Agenda

1. Common Terms
2. What is PCI?
3. How Does PCI Impact YOU?
4. Levels of PCI Compliance
5. Self-Assessment Questionnaire (SAQ)
6. PCI – High Level Overview
7. Levels 3 or 4 Merchant Compliance
8. Common Causes of Data Breaches
9. Consequences of Noncompliance
10. PCI Compliance Best Practices
11. Concluding Remarks
Common Terms

- **PCI DSS** – Payment Card Industry Data Security Standard.
- **SAQ** – Self-Assessment Questionnaire. Tool used by any entity to validate its own compliance with the PCI DSS.
- **ASV** – Approved Scanning Vendor. Company approved by the PCI Security Standards Council to conduct external vulnerability scanning services.
- **QSA** – Qualified Security Assessor. Company approved by the PCI Security Standards Council to conduct PCI DSS on-site assessments.
Common Terms

- **CDE** – Cardholder Data Environment. The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

- **CVV** – Card Verification Value, also known as Card Security Code. Refers to either magnetic-stripe data or printed security features.

- **POS** – Point of Sale. Hardware and/or software used to process payment card transactions at merchant locations.

- **Encryption** – Process of converting information into an unintelligible form except to holders of a specific cryptographic key.
What is PCI?

- **PCI DSS** is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process and/or transmit cardholder data. It presents common-sense steps that mirror best security practices.

- **PCI DSS version 2.0** became effective January 1, 2011 and is designed to provide greater clarity and flexibility to facilitate improved understanding of the requirements and eased implementation.

- The previous version of the standard (1.2.1) will be allowed until December 31, 2011. From January 1, 2012 and moving forward, all assessments must be under version 2.0 of the standard.

- Compliance with PCI standards is enforced by the founding members of the Council: MasterCard Worldwide, Visa Inc., American Express, Discover Financial Services and JCB International.
How Does PCI Impact YOU?

- If your business wishes to do credit or debit card transactions then it will be required to adhere to the PCI standards.

- If your business accepts, stores, processes or transmits credit card information, then it needs to meet the security requirements set out in the PCI DSS.

- How many credit card transactions do you accept, store, process or transmit on an annual basis?
  - There are 4 levels of PCI compliance based on volume of transactions.
  - There are fewer requirements if you process 20,000 transactions or less each year or if the card data is handled entirely by merchants or third-party service providers, such as PayPal, Chase Paymentech, etc.
  - Within each level there may be different versions of compliance based on what your company does with the credit card data and how it is acquired, stored and transmitted.
How Does PCI Impact YOU?

What is “sensitive cardholder data?”

- Everything at the end of a red arrow is sensitive cardholder data.
- Anything on the back side (CAV2, CVC2 and CVV2) and CID (Card Identification Number) must never be stored per Requirement 3.2

Source: PCI Security Standards Council
## Levels of PCI Compliance

The PCI Security Standards Council Defines 4 Merchant Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Definition</th>
<th>Type of Assessment Required</th>
</tr>
</thead>
</table>
| Level 4 | Any merchant that annually processes 20,000 transactions or less | • Annual Self Assessment Questionnaire (SAQ)  
• Quarterly network scan by Approved Scan Vendor (ASV) if applicable  
• Attestation of Compliance |
| Level 3 | Any merchant that annually processes 20,000-1 million transactions | • Annual SAQ  
• Quarterly network scan by ASV  
• Attestation of Compliance |
| Level 2 | Any merchant that annually processes 1-6 million transactions | • Annual SAQ  
• Quarterly network scan by ASV  
• Attestation of Compliance |
| Level 1 | Any merchant that annually processes 6 million or more transactions  
Any merchant who experienced a data breach | • Annual Report on Compliance by Qualified Security Assessor (QSA)  
• Quarterly network scan by ASV  
• Attestation of Compliance |

**Source:** Visa U.S.A. and MasterCard Worldwide
Self-Assessment Questionnaire Guidelines

There are 5 SAQ categories. Which one best applies to you?

SAQ A
Outsource all CHD
Card-not-present, all cardholder data (CHD) functions outsourced

SAQ B
Imprint or standalone dial-out terminals only
Imprint or standalone dial-out terminals only, no electronic CHD storage

SAQ C-VT
Virtual terminals only
Web-based virtual terminals only, no electronic CHD storage

SAQ C
Internet-connected payment application
POS or payment system connected to Internet, no electronic CHD storage

SAQ D
All other merchants and service providers
All other merchants and all service providers eligible to complete an SAQ

Is this my merchant type?

Yes

No

Is this my merchant type?

Yes

No

Is this my merchant type?

Yes

No

Navigating PCI DSS
Understanding the Intent of the Requirements

Source: https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf
SAQ A – 13 Questions

Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced:

- Your company accepts only card-not-present (e-commerce or mail/telephone order) transactions;
- Your company does not store, process or transmit any cardholder data on your systems or premises, but relies entirely on a third party(ies) to handle all these functions;
- Your company has confirmed that the third party(ies) handling storage, processing and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; and
- Your company does not store any cardholder data in electronic format.

This option would never apply to merchants with a face-to-face POS environment.

Source: https://www.pcisecuritystandards.org
SAQ B – 29 Questions

Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage:

- Your company uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers’ payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- Your company does not transmit cardholder data over a network (either an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and
- Your company does not store cardholder data in electronic format.

Source: https://www.pcisecuritystandards.org
SAQ C-VT – 51 Questions

Merchants using only web-based virtual terminals, no electronic cardholder data storage.

- Your company’s only payment processing is done via a virtual terminal accessed by an Internet-connected web browser;
- Your company’s virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company accesses the PCI DSS compliant virtual terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);
- Your company’s computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
- Your company’s computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
- Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts; and
- Your company does not store cardholder data in electronic format.

This option would never apply to e-commerce merchants.

Source: https://www.pcisecuritystandards.org
SAQ C – 80 Questions

Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.

- Your company has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
- The payment application system/Internet device is not connected to any other systems within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
- Your company store is not connected to other store locations, and any LAN is for a single store only;
- Your company retains only paper reports or paper copies of receipts;
- Your company does not store cardholder data in electronic format; and
- Your company’s payment application software vendor uses secure techniques to provide remote support to your payment application system.

Source: https://www.pcisecuritystandards.org
SAQ D – 288 Questions

SAQ D has been developed for all service providers defined by a payment brand as eligible to complete an SAQ, as well as SAQ-eligible merchants who do not meet the descriptions of SAQ types A through C, above.

Source: https://www.pcisecuritystandards.org
The Goals and General Requirements of the 12 PCI Data Security Standards

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and maintain a secure network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect cardholder data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a vulnerability management program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement strong access control measures</td>
<td>7. Restrict access to cardholder data by business need-to-know</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>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>Maintain an information security policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>

Source: PCI Security Standards Council
Level 3 or 4 Merchant Compliance

- Annual completion of Self-Assessment Questionnaire (SAQ)
- Quarterly network scan, if applicable
- Attestation of Compliance – Level 3 only
Common Causes of Data Breaches

- People
  - Employees – not just IT professionals

- The 2010 Annual Study: U.S. Cost of a Data Breach reveals:
  - The most common threat is negligence, at 41% of all breaches.
  - 31% of all breaches fall under the fastest-growing category, malice or crime.

However, most corporate data breaches are not publicized to avoid alarming customers.
Consequences of Noncompliance

- A merchant’s failure to comply with PCI DSS is a breach of contract.
- Several consequences will result in the event of a breach of contract:
  - Card Provider Fines (range from $5K to $500K)
  - Government Fines (range from $5M - $20M)
  - Loss of the privilege to accept payment cards
  - Potential lawsuit
  - Poor corporate governance
  - Loss of reputation with customers
  - Loss of investor confidence
Consequences of Noncompliance

Threats from Sensitive Data Exposure May Lead to Serious Business Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Losses from fraud</td>
<td>Banks and repayment processors may reclaim losses they sustain as a result of a merchant's data breach</td>
</tr>
<tr>
<td>Expenses for credit monitoring</td>
<td>Customers whose data is stolen may be entitled to credit monitoring for at least a year</td>
</tr>
<tr>
<td>Fines by card brands</td>
<td>Card companies may issues fines for PCI DSS noncompliance and prohibited data storage practices</td>
</tr>
<tr>
<td>Remediation costs</td>
<td>Capital expenditures may be necessary to replace or upgrade compromised hardware, software, applications and communications</td>
</tr>
<tr>
<td>Brand damage</td>
<td>Public reporting of breach often is required by law, making it impossible to escape widespread bad publicity and loss of confidence in the merchant’s brand</td>
</tr>
<tr>
<td>Expense of forensic examination and in-depth PCI audit</td>
<td>Depending on the extent of a breach, a forensic investigation could take months with very high costs</td>
</tr>
<tr>
<td>Ability to service or acquire customers</td>
<td>Business processes could be sufficiently interrupted to make it difficult or impossible to conduct “business as usual”</td>
</tr>
<tr>
<td>Potential lawsuits</td>
<td>Merchants who have experienced a breach have faced lawsuits from customers, financial institutions, ISOs, payment processors, card brands, state attorneys general and more</td>
</tr>
<tr>
<td>Drop in market capitalization</td>
<td>When financial damages reach a high enough point, a merchant’s stock value and overall market capitalization can drop</td>
</tr>
</tbody>
</table>

Source: Itpolicycompliance.com
PCI Compliance “Best Practices”

- Educate yourself
  - Knowledge of how and where card data is being accessed, transmitted and stored
  - Understand how the credit card data flows from transaction to billing in your organization
  - Know what is in your merchant agreement
- Whenever possible, eliminate cardholder data instead of securing it
  - Mask all characters except the last 4 digits
  - NEVER display or store the security code
  - Encrypt using the AES encryption functions
- Use third parties to process transactions
  - Understand the contract you sign with your credit card processor
Concluding Remarks

Benefits of Compliance

- Lower likelihood of a breach and faster recovery if there is a breach
- Reduced risk of financial loss through fines, lost business, lawsuits, etc.
- Mitigate risk
Contact Us:

Jeff Ziplow, Partner
Phone: (860) 561-6815
Email: jziplow@blumshapiro.com

Dominic Barone, Manager
Phone: (860) 570-6374
Email: dbarone@blumshapiro.com

Linda Piazzaroli, Supervisor
Phone: (860) 570-6405
Email: lpiazzaroli@blumshapiro.com