PCI Compliance 102: Small Steps to Big Gains

Wednesday, September 28, 2011
2:00 pm – 3:00 pm ET

David A. Wallace MBA, CISA/M, CISSP
GM, Data Security Standards Compliance
Chase Paymentech

This complimentary webinar is brought to you by ASAE-Endorsed Business Solutions and Chase Paymentech.

Your Presenter:

David A. Wallace
Group Manager, Security Standards Compliance

With 29 years of experience in the Information Technology (IT) industry and 14 years of Information Security management experience, David Wallace serves as Group Manager for Chase Paymentech’s Security Standards Compliance team. In his role, Wallace is responsible for managing data security compliance for Chase Paymentech’s merchant portfolio and advising merchants about the Payment Card Industry (PCI) security standards.

Prior to joining Chase Paymentech, Wallace gained invaluable experience serving in information security management roles with companies such as NationsBank, Sabre Holdings/Travelocity, Pilgrim’s Pride and Perot Systems. In addition to his professional experience, Wallace has earned several industry certifications, including Certified Information Systems Security Professional in 1999, Certified Information Security Manager in 2004, and Certified Information Systems Auditor in 2008. He is also a frequent speaker at regional, national and international information security conferences including the RSA Conference and Computer Security Institute Conference.

Wallace spent his undergraduate years attending Louisiana State University in Shreveport, La., where he studied business administration and management information systems. He earned a master’s degree in business administration from Southern Methodist University in Dallas, Texas in 2003.
Payment Card Industry Basics

Agenda

• Payment Card Industry Basics
• Am I at Risk?
• How do Compromises Happen?
• What Can I do?
• Resources and Questions
PCI Security Standards Council

- The Organization
  - Mission — Formed by five major payment brands to enhance payment account data security
  - 21 member advisory board with 500+ participating organizations
- Scope
  - Standards Management
  - Assessor accreditation

Payment Brand Data Security Programs

- Mandate compliance for entities storing, processing, or transmitting cardholder data
- Origination point for new PCI standards
- **May differ from brand to brand**
  - And in some cases from region to region
- Some more active than others
PCI Security Standards

- The PCI Data Security Standard (PCI DSS)
  - Applies to any entity that stores, processes, and/or transmits cardholder data
  - Covers technical and operational system components

- The Payment Application Data Security Standards (PA-DSS)
  - Applies to developers and integrators of applications involved in authorization or settlement.
  - Governs these applications that are sold, distributed or licensed to third parties.

- The PIN Transaction Security (PTS)
  - Applies to manufacturers of personal identification number (PIN) entry terminals used for payment card financial transactions.

**PCI Data Security Standards (PCI DSS)**

<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 the cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor supplied defaults for system password 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 network</td>
</tr>
<tr>
<td>Maintain a vulnerability management program</td>
<td>5. Use and regularly update anti-virus software</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>
## PCI Security Standards Council Accreditations

<table>
<thead>
<tr>
<th>Type</th>
<th>PCI SSC Designation</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Internal Security Assessor (ISA)</td>
<td>Merchant resource certified to validate compliance of PCI DSS</td>
</tr>
<tr>
<td></td>
<td>Qualified Security Assessor (QSA)</td>
<td>Independent third party certified to validate compliance of PCI DSS</td>
</tr>
<tr>
<td></td>
<td>Payment Application Qualified Security Assessor (PA-QSA)</td>
<td>Independent third party certified to evaluate compliance of Payment Applications to the PA-DSS</td>
</tr>
<tr>
<td>Network Scanning</td>
<td>Approved Scanning Vendor (ASV)</td>
<td>Independent third party accredited to perform network vulnerability scan</td>
</tr>
<tr>
<td>Forensics Investigation</td>
<td>PCI Forensics Investigator (PFI)</td>
<td>Independent third party accredited to perform forensics investigation in the event of suspected cardholder data breach</td>
</tr>
<tr>
<td>Laboratory</td>
<td>PCI Recognized Laboratory</td>
<td>Independent third party certified to validate compliance of PIN Transaction Security Standards</td>
</tr>
</tbody>
</table>

## Merchant Validation Levels and Requirements

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Volume</th>
<th>Requirements</th>
<th>Compliance Validation Target</th>
</tr>
</thead>
</table>
| 4              | Less than 20,000 ecommerce or less than 1 million transactions with one card brand | • Self-Assessment Questionnaire  
• Quarterly network scans | 12/31/2006 |
| 3              | Between 20,000 and 1 million Visa or MC ecommerce transactions in a 12 month period | • Self-Assessment Questionnaire  
• Quarterly network scans | 12 months from date of notification |
| 2              | Between 1 and 6 million Visa or MC transactions in a 12 month period | • Self-Assessment Questionnaire  
• Quarterly network scans | Dec 31st of year following notification¹ |
| 1              | Greater than 6 million Visa or MC transactions in a 12 month period | • Onsite Assessment ¹  
• Quarterly network scans | Sept. 30th of year following notification² |

¹ MasterCard now requires Level 1 and Level 2 merchant assessments to be performed by an assessor – QSA or ISA  
² MasterCard requires all Level 1 and Level 2 merchants to validate compliance by June 30, 2011
Payment Brand Enforcement

- Prohibited data storage fines: up to $480,000/year
- PCI Non-Compliance fines: up to $675,000/year
- Compromise fines:
  - Vary based on incident severity
  - Assessed in addition to non-compliance fines

Self Assessment Questionnaire Types

<table>
<thead>
<tr>
<th>SAQ Validation Type</th>
<th>Description</th>
<th>SAQ Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>outsourced. This would never apply to face-to-face merchants.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Imprint-only merchants with no electronic cardholder data storage</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>Stand-alone dial terminal merchants, no electronic cardholder data storage</td>
<td>B</td>
</tr>
<tr>
<td>4</td>
<td>Merchants with IP terminals, or POS systems connected to the Internet, no electronic cardholder</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>data storage, no networked devices</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Payment processing done via Virtual Terminal accessed via browser on Internet (No Ecommerce)</td>
<td>C-VT</td>
</tr>
<tr>
<td></td>
<td>All other merchants (not included in Types 1-4 above) and all service providers defined by a</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>payment brand as eligible to complete an SAQ.</td>
<td></td>
</tr>
</tbody>
</table>
The Prioritized Approach – Simply

• Six Milestones:
  1. If you don’t need it, don’t store it
  2. Secure the perimeter
  3. Secure applications
  4. Monitor and control access to your systems
  5. Protect stored cardholder data
  6. Finalize remaining compliance efforts, and ensure all controls are in place

• Tools and guidance on the PCI SSC Web site

Is Your Association at Risk?
In the News . . .

Hackers steal PINs from ATMs at 7-Eleven stores

Skimming Devices Target Debit-Card Readers

The OTHER Retailers

... The Reality

... The Reality

... The Reality

©2011, Chase Paymentech Solutions, LLC. All rights reserved.
What Do Hackers Want?

Payment Card Data is a target for criminals looking to turn data into cash quickly.

Source: Trustwave Global Security Report 2011

What Could a Compromise Cost My Association?

<table>
<thead>
<tr>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
<th>Example 4</th>
<th>Example 5</th>
<th>Example 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Merchant</td>
<td>Retailer</td>
<td>Restaurant</td>
<td>Retail / Ent.</td>
<td>Restaurant</td>
<td>Service Provider</td>
</tr>
<tr>
<td>PCI Level</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Number of Account at risk</td>
<td>45,760,000</td>
<td>22,000</td>
<td>156,000</td>
<td>33,330</td>
<td>69,000</td>
</tr>
<tr>
<td>Data at risk</td>
<td>Magnetic Stripe</td>
<td>Magnetic Stripe</td>
<td>Magnetic Stripe</td>
<td>Magnetic Stripe</td>
<td>Account Numbers</td>
</tr>
<tr>
<td>Visa Fine</td>
<td>40.9 M</td>
<td>$15,000</td>
<td>$10,000</td>
<td>$15,000</td>
<td>$17,500</td>
</tr>
<tr>
<td>MasterCard Fine</td>
<td>24 M</td>
<td>$10,000</td>
<td>$90,000</td>
<td>$14,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>Visa ADOR Fine</td>
<td>N/A</td>
<td>$420,000</td>
<td>$ -</td>
<td>$60,000</td>
<td>$ -</td>
</tr>
<tr>
<td>Compliance Cases</td>
<td>$ -</td>
<td>$390,000</td>
<td>$3,000</td>
<td>$ $</td>
<td>$ -</td>
</tr>
<tr>
<td>Forensic Investigation</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Cost of Upgrades</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Merchant Brand Damage</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>TOTAL</td>
<td>&gt; $64.9 M</td>
<td>&gt; $454,000</td>
<td>&gt; $490,000</td>
<td>&gt; $101,600</td>
<td>&gt; $117,500</td>
</tr>
</tbody>
</table>
While many POS vendors have patched their systems to support security controls, many companies are still running very old software.

Source: Trustwave Global Security Report 2011

How Do Compromises Happen?
Top 5 Reasons Breaches Happen:

• #5 - Device Tampering
• #4 – Default Passwords
• #3 – No Anti-Virus protection
• #2 – Known vulnerabilities not patched
• #1 – No Firewall

Skimming Attack – Hardware Modification
Skimming Attack – Secondary MSR

Skimming Attack – PIN Capture Membrane
Skimming Attack – Bluetooth Module

Put them all together…

- Remote (Internet) attack
  - Attacker finds a system, directly connected to the Internet
  - Exploits an un-patched vulnerability to take control of the system
  - Downloads cardholder data from the payment application
  - Installs malware on the system to steal future transactions

- Point-of-Sale terminal theft and/or swap
  - Attacker steals a terminal
  - Extracts existing cardholder data
  - Installs a skimmer
  - Swaps compromised terminal with new terminal at another location and repeats
What can I do?

Use PA-DSS Validated Payment Applications

- Validated payment applications:
  - Do not store prohibited data or cardholder data past authorization and settlement
  - Versions available for most applications
  - Configured to update and patch automatically
  - Listed on the PCI Security Standards Council Web Site

- Cost: Varies by application
#5 - Payment Hardware Best Practices

- Securely mount terminals to deter theft
- Use PCI PTS validated terminals
  - Support strong keys (Triple DES aka ‘TDES’)
  - Tamper resistant if stolen
    - Memory is deleted if device is opened
    - PIN encryption key is deleted if device is opened
    - Cannot be used in skimmer/replacement attack
  - Required by July 1, 2010 for merchants accepting PIN Debit
  - Listed on the PCI Council web site
- Cost: Varies by terminal

#4 - Use Strong Passwords

- Change the default password on a new system
- Choose a good password
  - Easy to remember
  - Hard to guess
  - Mixed Case, Alpha-Numeric, Special characters
    - Pink Floyd
    - Pink Floyd!
    - P1nk F10yd!
    - F10yd!P1nk
    - FP11!0nykd
- Cost FREE
#3 - Install and Use Anti-Virus Software

- Anti-Virus software
  - Usually includes anti-virus, anti-spyware and a personal firewall
  - Checks the hard drive and memory for existing infections
  - Monitors communications for infected files and web pages
  - Updates automatically via the Internet

- **Cost:** Often FREE from Internet Service Provider

#2 – Apply Patches

- Update software patches:
  - Address newly identified vulnerabilities
  - Released
    - Regularly (Microsoft “Patch Tuesdays”)
    - As needed when critical vulnerabilities appear
  - Can be downloaded and installed automatically

- **Cost:** Free
#1 – Install a Firewall

- Consumer-grade firewalls:
  - Available since the late 1990s
  - Require little or no configuration
  - Available from most large retailers
  - **Cost:** Less than $100
Additional Resources

Chase Paymentech
Cardholder Data Security
http://www.chasepaymentech.com
http://www.chasepaymentech.com/datasecurity

PCI Security Standards Council
Validated Payment Applications
PTS Certified devices
Self-Assessment Questionnaires
Prioritized Approach
https://www.pcisecuritystandards.org/
https://www.pcisecuritystandards.org/security_standards/vpa/
https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallis\nl.html
https://www.pcisecuritystandards.org/saq/index.shtml
https://www.pcisecuritystandards.org/education/prioritized.shtml

Visa Cardholder Info Security Program
Visa/BBB Data Security Microsite
Visa Alert Page
http://usa.visa.com/merchants/risk_management/cisp.html
http://www.bbb.org/data-security/
http://usa.visa.com/merchants/risk_management/cisp_alerts.html

MasterCard Site Data Protection Program
https://sdp.mastercardintl.com/

Trustwave
Portal: Level 4 Merchant Portal
Free Risk Profile
http://www.trustwave.com
http://www.trustwave.com/level4poi/
http://chasepaymentech.riskprofiler.net referral code: WELCOMECHASEPAY

Questions?

David A. Wallace
Group Manager, Security Standards Compliance
Chase Paymentechn

david.wallace@chasepaymentech.com
www.chasepaymentech.com/asae