Welcome

Campus Merchant
PCI-DSS 101
2013
Goals of this Meeting

• Introduce Team
• Terminology
• PCI Basics
• Campus Challenges
• Lessons Learned
Team Members

- FSO-Bursar Department Services staff: Mark Barton (Bursar), Theresa Couch, Eileen Gerrish, Lisa Martinez, and Robbyn Lennon
- Campus Information Security Office
- Merchant Responsible Person - Department Variable
- Internal Auditors
- Security Metrics Assessors
The Security Challenges Are:

• Keeping Technology Current
• Customer Service
• Department Procedure Consistency between different areas
• Staff Awareness
• People and Their Choices
Terminology

- **Issuer**: A Member that enters into contracts to issue cards
- **Cardholder**: One to whom a card has been issued
- **Merchant**: Person or firm that has contracted with a Member to accept cards
- **Acquirer**: A Member that enters into merchant agreements, and enters transactions into interchange
- **Processor**: An organization that provides authorization or clearing services on behalf of an Issuer of Acquirer
- **Transaction**: Data describing the sales draft, credit voucher, etc.
- **Interchange**: The exchange of transactions between Members under prescribed operating regulations
- **SAQ**: Self Assessment Questionnaire
- **PCI**: Short for PCI-DSS Payment Card Industry- Data Security Standards
- **MRP**: Merchant Responsible Person
- **PAN**: Personal Account Number (Credit Card Number)
Typical Data Breach/Fraud Cycle

Hackers search for merchants or agents with weak controls or known security vulnerabilities.

Hackers identify target and steal sensitive information by:
- Breaching the system/network
- Compromising Point of Sale (POS) Software
- Tampering with POS Devices and ATMs (PIN theft)
- Skimming

Merchant/Agent fails to comply with payment industry security standards.

Network Fraud Mitigation Activities
- Compromise investigation/forensics
- Distribution of compromised accounts
- Development of fraud fighting technologies
- Dispute resolution and loss recovery processes
- Execution of fraud and data security compliance programs

Criminals manufacture counterfeit cards for use at retail stores or at ATMs. Fraudsters may also use subsequent phishing attacks to steal additional information to conduct identity theft or CNP fraud.

Fraudulent transactions are conducted at merchant locations (Retail, CNP or ATMs). Criminals often target products that can be quickly converted to cash.

Issuer fraud mitigation activities begin.
- Issuer contacts cardholder to investigate suspicious transactions
- Or, cardholder contacts issuer to report a lost or stolen card or a suspicious transaction
- Issuer conducts a fraud investigation
- If fraud is confirmed, the issuer blocks the card and lists it on the network exception file
- Issuer sends the cardholder a new card
Inadequate Security Leads to Data Compromise Incidents

- A data compromise is an incident involving the breach of a system or network where cardholder data is processed, stored or transmitted.

- A data compromise can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

- There are the three basic types of data security breaches that can lead to a data compromise:
  - **Physical Breach** – theft of documents or equipment
  - **Electronic Breach** – electronic breach of a system or network environment
  - **Skimming** – capture of card magnetic stripe data using an external device
Common Causes of a Breach or Compromise

• Trivial and common passwords for POS systems
• Not changing the vendor supplied Password upon installation
• Outdated Antivirus software definitions
• Use of vulnerable or non compliant software
• Remote access to systems by 3rd party providers
• Having remote access turned on at all times
• People and their choices
The Costs of a Data Compromise are High

• If card account information is stolen from you, or a service provider working on your behalf, it can be used by criminals to commit fraud.

• **Financial impact:** You may be subject to significant fines and losses arising from such fraud and from not properly protecting card account information.

  Potential for significant monetary losses related to a data compromise:

  • card organization fines and assessments passed through to the merchant

  • fraud experienced on compromised cards

  • other reimbursements to issues for fraud losses passed through to the merchant:
    • Forensics, card replacement, PCI non-compliant fines etc.

• **Reputation impact:** Potentially more damaging than the financial impacts, public trust and confidence in your organization can be negatively impacted by this type of data security breach.
<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Monthly Fine</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Level 1</td>
<td>$25,000</td>
<td>$10,000</td>
<td>$5,000</td>
<td>Months One through Three</td>
</tr>
<tr>
<td>Merchant Level 2</td>
<td>$5,000</td>
<td>$50,000</td>
<td>$25,000</td>
<td>Months Four through Six</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$50,000</td>
<td>Months Seven and Subsequent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Visa:**

**Non-Compliance**

**Storage of Track Data:**

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Assessment Amount</th>
<th>Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Level 1 and 2</td>
<td>Up to $25,000</td>
<td>First Violation</td>
</tr>
<tr>
<td></td>
<td>Up to $50,000</td>
<td>Second Violation</td>
</tr>
<tr>
<td></td>
<td>Up to $100,000</td>
<td>Third Violation</td>
</tr>
<tr>
<td></td>
<td>Up to $200,000</td>
<td>Fourth Violation</td>
</tr>
</tbody>
</table>

Merchant Level 3 – Visa does not currently have a fine structure for PCI Level 3 Merchants that are PCI Non-Compliant

**MasterCard:**

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Assessment Amount</th>
<th>Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Level 3</td>
<td>Up to $10,000</td>
<td>First Violation</td>
</tr>
<tr>
<td></td>
<td>Up to $20,000</td>
<td>Second Violation</td>
</tr>
<tr>
<td></td>
<td>Up to $40,000</td>
<td>Third Violation</td>
</tr>
<tr>
<td></td>
<td>Up to $80,000</td>
<td>Fourth Violation</td>
</tr>
</tbody>
</table>
What is PCI ????

PCI stands for the Payment Card Industry and is used to refer to:

The **PCI Security Standards Council™ (PCI SSC)**, an industry body founded by the major card brands to protect cardholder data. Founders:

![VISA](image1.png) ![MasterCard Worldwide](image2.png) ![American Express](image3.png) ![Discover](image4.png) ![JCB](image5.png)

The global **Security Standards** created and maintained by the PCI SSC to protect cardholder payment data.

**Key Learning Point:** Compliance with PCI Security Standards is **MANDATORY** for merchants and their service providers, and is enforced by the major card brands who established the **PCI SSC**
PCI History

- **2001**: Visa and MasterCard security standards
  - Visa Cardholder Information Security Program (CISP)
  - MasterCard Site Data Protection (SDP)
- **2004**: Standards combined into DSS
  - Joined by American Express, Discover, JCB
- **2006**: PCI Security Standards Council formed
- **2008**: New SAQs and PCI v1.2
- **2010**: PCI v 2.0
PCI Key Players

- Five Payment brands
  - Track compliance and enforce standards (fines, sanctions)
  - Determine event response (forensics)
  - Define merchant levels
- Acquirers (Merchant Banks) and processors
  - Set merchant level
  - Determine compliance
  - Approve compensating controls
Cardholder Data

- **PAN**
- **CID (American Express)**
- **Expiration date**
- **Magnetic stripe (data on tracks 1 & 2)**
- **CAV2/CID/CVC2/CVV2 (all other payment brands)**
# Cardholder Data

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Render Stored Account Data Unreadable per Requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Service Code</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe Data</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2/CID</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
</tbody>
</table>

- OK to store first six and/or last four digits… **ONLY!**

*Source: PCI SSC*
PCI-DSS: 6 Goals, 12 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 cardholder data
  - 4. Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program**
  - 5. Use and regularly update anti-virus software and programs
  - 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 for all personnel.
## The Self-Assessment Questionnaires (SAQs)

- Most campus merchants self-assess

<table>
<thead>
<tr>
<th>SAQ Validation Type</th>
<th>Description</th>
<th>SAQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Card-not-present merchants, all cardholder data functions outsourced, no electronic cardholder data storage</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>Imprint-only merchants, no electronic cardholder data storage</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>Stand-alone terminal merchants, no electronic cardholder data storage</td>
<td>B</td>
</tr>
<tr>
<td>4</td>
<td>Merchants with POS systems connected to the Internet, no electronic cardholder data storage</td>
<td>C</td>
</tr>
<tr>
<td>“4-ish”</td>
<td>Merchants who process cards on isolated virtual terminals connected to the Internet</td>
<td>C-VT</td>
</tr>
<tr>
<td>5</td>
<td>All other merchants and service providers</td>
<td>D</td>
</tr>
</tbody>
</table>

- **13 Items**
- **29 Items**
- **80 Items**
- **51 Items**
- **280+ Items**
SAQ A-13 Items

• Card-not-present merchants ONLY
  – Ecommerce, use of gateways such as Cybersource, Payflow Pro, Authorize.net.

• Card Processing totally outsourced (Cashnet, Touchnet (like ASU))
  – No cardholder data is stored, processed, or transmitted on your systems

• Third party confirms it is PCI compliant
• Only paper records, not received electronically
• Store no cardholder data electronically
SAQ B- 29 Items

- For merchants with stand-alone dial-up terminals or imprinters.
  - MOTO Dial Pay
  - Face to face
- Terminals not connected to any system
- Paper records (not received electronically)
- Storing no cardholder data electronically
SAQ C- 80 Items

- Payment application and Internet connection on the same device
  - Card-present or not present merchants
  - Can be POS or shopping cart application
- Device is behind a firewall and not connected to any other systems
- Store only paper records, not received electronically
- Payment application vendor provides remote support security
- Store no cardholder data electronically
SAQ C-VT- 51 Items

- Merchant uses a virtual terminal
  - Web browser connected to processor that hosts payment processing function
  - Enter card data manually, via a secure connection, one transaction at a time
  - Brick-and-mortar or MOTO
- Single payment terminal, isolated, fixed
- Other requirements as SAQ C
Everybody Else is SAQ D

SAQ D:
- 280 questions
- All 12 PCI requirements

### Attestation of Compliance, SAQ D—Service Provider Version

**Instructions for Submission**

This form provides most complete and relevant information of this version on the requirements and compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections included in the submission instructions of PCI DSS Compliance—Completion Tag on the document.

#### Part 1: Qualified Security Assessor Company Information (if applicable)

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Contact Name</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Address</th>
<th>Country</th>
<th>ZIP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Part 2: Service Provider Organization Information

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Contact Name</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Address</th>
<th>Country</th>
<th>ZIP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Part 3a: Services

- [X] Authorization
- [X] Tokenization
- [X] PCI DSS
- [X] SCA
- [ ] EPF (E-Commerce)
- [ ] Data Migration/Upgrade Transactions
- [ ] Payment Gateway
- [ ] Chargeback Settlement
- [ ] Check/Money Orders
- [ ] Other (please specify)

List industries and businesses included in PCI DSS compliance:

#### Part 3b: Relationships

Check the box that applies:

- [ ] We have a business relationship with one or more third-party service providers, e.g., gateway, merchanting companies, data hosting, etc. We are listed on the report.

- [ ] We do not have a business relationship with any third-party service providers.

#### Part 3c: Transaction Processing

How and on what basis does your business store, process and/or transmit cardholder data?

Payment Applications in use as described as part of your service:

Payment Application Version:

[Treasury Institute for Higher Education]
SAQ A OMG!

- "Customer Service"
  - Outsource Web payments (e.g., TouchNet)
  - MOTO, fax, even walk-up orders persist
  - Staff enter transactions on their workstation (or direct student to payment kiosk)
  - Result: workstation/kiosk and every system it connects to is "in scope" for PCI

- Result: SAQ D
  - 280+ questions
  - Full PCI DSS including scans and penetration testing

Treasury Institute for Higher Education
A Word About Shortened SAQs

- Target is small merchant
- If not a perfect fit, SAQ may not be appropriate
- "You must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant"
  - Other PCI requirements may (and likely do) apply
  - Use SAQ as guide, not end of PCI compliance
Outsourcing

- Strategic question: Do you want to be in the payments business?

- Outsourcing some or all processing can simplify your path to PCI compliance
  - Service Providers – You use their systems, services
  - Software Application Vendors – You buy a software package, and host it on your own system
Outsourcing: Service Providers

- Service Providers store, process, or transmit cardholder data for you (e.g., TouchNet)
- Merchant is still responsible
  - Ensure service providers are PCI compliant
  - Validate, and include PCI compliance in contract
  - Control third-party connections
- Visa and MasterCard websites list Level 1 PCI-compliant service providers
Outsourcing: Applications

- Payment Application Data Security Standard (PA-DSS)
  - Compliant third-party payment applications
  - Validated applications listed on PCI Council website
- PA-DSS is for third-party payment application software used in authorization or settlement
- Visa and MasterCard mandate PA-DSS applications
- PA-DSS is not a silver bullet
Campus Merchant Challenges

- **Athletics**
  - Wireless (game days); ticketing; luxury boxes; links to Development and Alumni systems; call centers (voice recording); service providers; camps; email/web/fax transactions

- **Development, Alumni, Foundation**
  - Cardholder data everywhere (PII, too); recurring payments; scanning forms; email/web/fax transactions; hosted payment apps (including home brewed); remote events; call center (voice recording)
Campus Merchant Challenges

- Medical center
  - Retail spaces; food service; individual practices; patient collections including outside agencies; voice recording
- Auxiliaries
  - Bookstore, food service: they store cardholder data
  - Hotel: store cardholder data; food service; events
  - Conferences: web and onsite registration
  - TV/radio station: pledge drives; stored cardholder data; device security between pledge drives
Campus Merchant Challenges

- Traffic and Parking
  - Payment apps store cardholder data; kiosks; paper forms
- Unrelated third parties
  - DVD kiosks, contractors, franchises
  - Third-party OMG! – Are you a PCI Service Provider?
PCI Gap Analysis – An Approach

- Meet with every campus merchant
  - How they take payment cards
  - What data they store (paper, electronic)
  - How they process refunds, chargebacks
  - What happens when things go wrong
- Identify PCI compliance gaps
- Identify remediation options
- Ground rule: “No harm, no foul”
- PCI “Requirement 0”
How Schools Address PCI

- 72% said Finance leads PCI, rest shared with IT
- 54% fund PCI compliance centrally (declining)
- Between 1 and 1.5 FTE dedicated to PCI
- 70% had key policies in place
- 70% compliant or expected to be within 6 months
- Schools generally not satisfied with acquirer support
- A number experienced a data breach/fined
How Schools Address PCI

- Secure top management commitment
  - PCI is a business not a security issue
  - Budget adequately: PCI is a program not a project
- Build a dedicated, multidisciplinary team
- Inventory data, processes, vendors
  - Ask, interpret, verify where stuff is, where it goes
- Engage stakeholders, communicate
  - Hold users accountable
Where's My Silver Bullet?

- Minimize PCI scope (aka, PCI “Requirement 0”)
  - Store no cardholder data (even paper)
  - Segment your network
  - Change business processes and procedures
  - Perform a PCI Gap Analysis
- Emerging technologies
  - Tokenization
  - Point-to-point encryption
Conclusions

- PCI compliance is a business issue
- PCI compliance is pass/fail
- You are one system change from being noncompliant
- Use the right SAQ
- You can outsource processing, but not your responsibility
- You do not want to be a service provider
- Take advantage of all your resources
Lessons Learned

• Legacy Procedures
• New Staff
• Fax Machines
• Policy
• Contractual third party processing verification
• Scoping
• Ignoring compliance issues
• Failed Vulnerability scans
Wrap Up

• Resources:
  – Higher Education PCI Blog (Treasury Institute) treasuryinstitutepcidss.blogspot.com
  – Treasury Institute for PCI Workshop:
    • www.treasuryinstitute.org