PCI DSS
Merchant Overview

Craig A. Henninger CISSP, QSA
Security Advisor
Introducing CampusGuard

- Full-Service QSA/ASV Firm for PCI Compliance
- Certified in US, Australia and New Zealand
- Focused Solely on Higher Education
- We Understand the PCI DSS
- We Understand Higher Education
• Quick PCI Level Set
• Common PCI Myths
• Managing Compliance
• Compliance/Validation
• Reasons to Comply
• Best Practices
• Q & A
Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS: “One Standard to Rule Them All”

Cardholder Information Security Program (CISP)

Data Security Standard (DSS)

Data Security Operating Policy

Site Data Protection (SDP)

Information and Compliance

Data Security Program
## PCI DSS: 6 Goals, 12 Requirements

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

Ecosystem of payment devices, applications, infrastructure and users
PCI Relationships

Bank
Communicates and educates merchants on PCI DSS and reports compliance status to Card Associations

CREDIT CARD SECURITY

Merchant
Responsible for enforcing and monitoring merchant compliance with the PCI DSS

Responsible for managing the PCI DSS and certifying QSAs and ASVs

Responsible for enforcing and monitoring merchant compliance with the PCI DSS

Responsible for managing the PCI DSS and certifying QSAs and ASVs
What is the PCI DSS trying to protect?
## Covered Data Elements

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>Magnetic stripe</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td>PIN/PIN block</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
</tbody>
</table>

*1st 6 / Last 4 OK*

*Only considered CHD if full PAN stored*

*“Holy Grail” for thieves*
# Merchant Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa/MC Transactions</th>
<th>MC Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&gt; 6 million</td>
<td>&gt; 2.5 million</td>
</tr>
<tr>
<td></td>
<td>Visa/MC txns/yr</td>
<td>transactions/yr</td>
</tr>
<tr>
<td>2</td>
<td>1 to 6 million</td>
<td>50,000 to 2.5</td>
</tr>
<tr>
<td></td>
<td>Visa/MC txns/yr</td>
<td>million txns/yr</td>
</tr>
<tr>
<td>3</td>
<td>20,000 to 1 million</td>
<td>All other Amex</td>
</tr>
<tr>
<td></td>
<td>Visa/MC ecommerce</td>
<td>Merchants</td>
</tr>
<tr>
<td>4</td>
<td>All other Visa/MC</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>merchants</td>
<td></td>
</tr>
</tbody>
</table>
# Merchant Levels and Validation

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa</th>
<th>MasterCard</th>
<th>Discover</th>
<th>American Express</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image" alt="Visa Logo" /> · <img src="image" alt="MasterCard Logo" /> · <img src="image" alt="Discover Logo" /> <img src="image" alt="American Express Logo" /></td>
<td><img src="image" alt="Visa Logo" /> · <img src="image" alt="MasterCard Logo" /> · <img src="image" alt="Discover Logo" /> <img src="image" alt="American Express Logo" /></td>
<td><img src="image" alt="Visa Logo" /> · <img src="image" alt="MasterCard Logo" /> · <img src="image" alt="Discover Logo" /> <img src="image" alt="American Express Logo" /></td>
<td><img src="image" alt="Visa Logo" /> · <img src="image" alt="MasterCard Logo" /> · <img src="image" alt="Discover Logo" /> <img src="image" alt="American Express Logo" /></td>
</tr>
</tbody>
</table>
|       | - Annual on-site assessment (QSA)  
- Quarterly network scan (ASV) | - Annual on-site assessment (QSA)  
- Quarterly network scan (ASV) | - Annual on-site assessment (QSA/ISA)  
- Quarterly network scan (ASV) | - Quarterly network scan (ASV) | - N/A |
| 2     | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |
|       | - Annual on-site assessment (QSA/ISA)  
- Quarterly network scan (ASV) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |
| 3     | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |
|       | - Annual Self-Assessment Questionnaire (SAQ)  
- Quarterly network scan (ASV) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |
| 4     | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |
|       | - At discretion of acquirer  
- Annual SAQ  
- Quarterly network scan (ASV) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |
|       | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) | ![Visa Logo](image) · ![MasterCard Logo](image) · ![Discover Logo](image) ![American Express Logo](image) |

Confidential Property of CampusGuard
# Payment Methods & Validation Requirements

<table>
<thead>
<tr>
<th>SAQ Type</th>
<th>Questions</th>
<th>Payment Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>14</td>
<td>Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced</td>
</tr>
<tr>
<td>A-EP</td>
<td>139</td>
<td>Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing</td>
</tr>
<tr>
<td>B</td>
<td>41</td>
<td>Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals – No Electronic Cardholder Data Storage</td>
</tr>
<tr>
<td>B-IP</td>
<td>83</td>
<td>Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals – No Electronic Cardholder Data Storage</td>
</tr>
<tr>
<td>C</td>
<td>139</td>
<td>Merchants with Payment Application Systems Connected to the Internet – No Electronic Cardholder Data Storage</td>
</tr>
<tr>
<td>C-VT</td>
<td>73</td>
<td>Merchants with Web-Based Virtual Payment Terminals – No Electronic Cardholder Data Storage</td>
</tr>
<tr>
<td>D</td>
<td>326</td>
<td>All other SAQ-Eligible Merchants</td>
</tr>
<tr>
<td>P2PE-HW</td>
<td>35</td>
<td>Hardware Payment Terminals in a PCI-Listed P2PE Solution Only – No Electronic Cardholder Data Storage</td>
</tr>
</tbody>
</table>
Common PCI DSS Myths

- “I can wait until the bank asks me to be compliant.”
- “Since the bank hasn’t asked me, I don’t have to be compliant.”

All merchants needed to be compliant with the PCI DSS on December 31, 2005.
Common PCI DSS Myths

- “I don’t store credit card numbers, so I have no compliance obligation with the PCI DSS.”
- “I only process a few credit card transactions per year, so I am exempt from compliance with the PCI DSS.”

The PCI DSS globally applies to all entities that store, process or transmit cardholder data.
Common PCI DSS Myths

“I only need to be *mostly compliant* with the PCI DSS.”

The PCI DSS is pass/fail. To be considered compliant, you must answer affirmatively for all requirements.
Many colleges and universities adopt the use of a 3rd party processor or payment system for tuition and other payments.

- Great idea
- Limits scope for the PCI DSS
- Designed to be hands-off at the school

Purchasing of PA-DSS compliant systems

- Can help in compliance effort
- Not a panacea
What can go wrong?

What happens when an employee enters data for the customer on their machine?

- The DSS is very definitive about transmission of CHD
  - Employees’ workstation and the network its connected to comes into scope
    - Un-needed software
    - Monitoring
    - Associated systems
    - If not segmented from the rest of the network, the rest of the school comes into scope.
Outside Payment Processing

- Using a 3rd party to process payments for the institution may alleviate some scope and PCI DSS responsibility.
  - Conference registrations, day camps, T-shirt sales etc.
  - Sites that contain a “Pay Now” button that redirects or uses embedded code to a 3rd party.
- Unless the entire site is fully hosted by a PCI Compliant Provider, compliance obligations for the Web server that hosts the site with the “Pay Now” button now fall under SAQ A-EP.
What About Mobile Payments?

Square, ProPay etc.

MasterCard and Visa both have statements for Merchants wishing to use Square and other Mobile Point Of Sale (MPOS) devices

“Due to the inherent security limitations of mobile devices, the PCI SSC is not certifying MPOS payment applications that reside on multi-purpose, consumer mobile devices (referred to by the PCI SSC as a Mobile Payment Acceptance Application Category 3) until further guidance is developed to ensure the security of cardholder data within the mobile device. Please refer to the PCI SSC Website for more information.”

(MasterCard statement on Mobile payments)
Mobile Payment Alternatives

- Purpose built cellular POS device
  - VeriFone VX520
  - FD400
  - Etc
What’s in PCI Scope?

- Card Swipe Machine?
- Office Workstations?
- Student?
- Shopping Cart?
- Computer Lab?
- Phone Transaction?
Who Must Comply?

Do you....

- Store, process or transmit cardholder data?
  - Point-of-Sale (POS)
  - Mail Order/Telephone Order (MOTO)
  - FAX
  - E-Commerce (website where customer can input their credit card information to complete a transaction)

- Use a system that processes or stores credit card data?
  - And are other systems connected to them?

IF YOU ANSWER YES TO ANY OF THE ABOVE QUESTIONS THEN PCI DSS APPLIES TO YOU!
Compliance and Validation

- While everyone must be **compliant**, most* must also **validate** compliance via assessment.
- Different levels of Merchants may require third party validation (ROC - QSA).
- Others will require the SAQ
  - Requires executive level signoff.
  - Be sure you are compliant before signing!
- May require quarterly scanning.

* Validation for level 4 merchants is at the discretion of the acquiring bank
Verizon Data Breach Investigative Report
Verizon Data Breach Investigative Report

- 2013 may be remembered as the “year of the retailer breach,” but a comprehensive assessment suggests it was a year of transition from geopolitical attacks to large-scale attacks on payment card systems.

- 2013 – 1367 confirmed breaches
  - Actual data or financial loss
- 2013 – 63,437 Incidents
  - Systems were compromised
- 95 Countries Represented

![Number of breaches per threat action category over time](image)
Verizon Data Breach Investigative Report

Attacks by type:
A Campus Is A “City"

Challenges for PCI Compliance:
- Open networks and systems
- Scope creep
- Overloaded staff
- Fiscal constraints
PCI Non-Compliance

In the event of a data breach, the card brands can:

- Assess fines
  - Up to $500,000 per brand per breach
- Require that you notify victims
- Require that you pay card replacement costs
- Require that you reimburse fraudulent transactions
- Require forensic investigations be performed by a PCI approved firm
- Require that you validate as a Level 1 merchant (QSA)
News Travels Fast: Do you want to be in it?

Ohio University suffers yet another data breach incident

What's the matter with Ohio University? It was just announced that hackers gained access to 60,000 student medical records from the campus health center. Along with health information, these records included Social Security numbers and addresses.

This is just the latest data theft incident in a long series of issues at Ohio University. Over the last two months, they have also experienced the theft of 300,000 alumni and donor records including 137,000 Social Security numbers. Before that, the university's intellectual property files, emails and
Consequences

Direct Costs
- Discovery / Forensics
- Notification costs
- Identity monitoring costs
- Additional security measures
- Lawsuits
- Fines

Indirect Costs
- Loss of customer confidence
- Loss of productivity
- Distraction from core business
- Become a level 1 merchant

10,000 accounts X ~$200 / account = $2 Million

Reputation – Priceless!
Some Best Practices

- NEVER e-mail credit card information
- NEVER store credit card numbers in any database or spreadsheet
- Mask all but last 4 digits of cc number
- Keep credit card documentation locked in a safe or SECURE filing cabinet
- Permit only those employees who have a legitimate “need-to-know” access to cardholder info
- Don’t allow unauthorized persons access to areas where credit card data is stored
Some Best Practices

- Destroy documentation containing credit card information when no longer needed for business or legal reasons
- Document departmental desktop procedures
- Update cash handling procedures
- Segregate duties – the individual performing reconciliation should not be involved in processing credit card sales or refunds
Some Gotcha’s

- Credit card numbers kept for “recurring” payments (spreadsheets, paper in drawers, etc)
- Credit card info received and stored via email
- Credit card info stored in other “non-processing” applications
- Credit Card info stored in paper/forms in departments
- A campus department processing credit cards for Foundation (may place it as “Service Provider” role)
- No in-office procedures
PCI DSS is a Process

- Payments Analysis
- Merchant Discovery
- Documentation
- Preliminary Scanning
- Gap Analysis
Assessment

- Where does credit card processing take place?
  - IT involved?
- Who controls it?
- What policy and controls are currently in place?
PCI DSS is a Process

Discovery and Assessment → Remediation

- Payments Analysis
- Merchant Discovery
- Documentation
- Preliminary Scanning
- Gap Analysis

- Correct Problems
- Compensating Controls
Remediation

- Who should control the process?
- Define resources required
- How does the PCI DSS affect this process?
- Implementation
PCI DSS is a Process

Discovery and Assessment
- Payments Analysis
- Merchant Discovery
- Documentation
- Preliminary Scanning
- Gap Analysis

Remediation
- Correct Problems
- Compensating Controls

Validation
- ROC or SAQ Submission
- Quarterly Scanning
- Penetration Testing
Validation

- Completing SAQs
  - Vulnerability scans
  - Penetration tests
  - Policies and procedures
PCI DSS is a Process

Discovery and Assessment
- Payments Analysis
- Merchant Discovery
- Documentation
- Preliminary Scanning
- Gap Analysis

Remediation
- Correct Problems
- Compensating Controls

Validation
- ROC or SAQ Submission
- Quarterly Scanning
- Penetration Testing

Re-Validate every 12 months
Resources

- PCI Security Standards Council
  - www.pcisecuritystandards.org/

- Card Associations
  - www.visa.com/cisp
  - www.mastercard.com/sdp

- Privacy Rights Clearinghouse
  - http://www.privacyrights.org/

- Ponemon Institute
  - http://www.ponemon.org/

- CampusGuard
  - www.campusguard.com/
Questions