Course Audience

• This course is geared towards university staff that handle or process cardholder data and other related sensitive information. Staff can include:
  □ Individuals that manage/oversee individuals that handle credit card payments
  □ Contractors and others (including 3rd parties) that handle credit card information for your department
  □ Individuals responsible for completing annual questionnaires (SAQs) and/or tracking the results of vulnerability scans
Course Topics

• The following are topics covered by this course:
  □ Definition of PCI-DSS
  □ Importance of compliance
    • significance of PCI-DSS in higher education environments
  □ Credit Card Handling Best Practices – ways of preventing breaches and protecting cardholder data
  □ Your role in the compliance process
Course Objectives

• At the end of this course, you should be able to demonstrate an understanding of the following:
  □ Credit card security awareness
  □ Best practices required to keep sensitive information secure, and how to apply them
  □ The importance of information security as it relates to the university’s overall compliance requirements
  □ Consequences of non-compliance
What is PCI-DSS?

• PCI-DSS – Acronym for Payment Card Industry Data Security Standard
  □ Developed by the PCI-SSC (PCI Security Standards Council, launched in 2006)
  □ Multifaceted security standard*
    • Consists of 12 requirements through a combination of security management, policies, procedures, technology and other critical protective measures
  □ Latest version is PCI-DSS 2.0 effective for 3 years starting 1/2011

* Going through all 12 high level requirements is out of the scope of this presentation, but the next page lists the requirements
### PCI Data Security Standard – High Level Overview

| 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 or 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. |
Significance of PCI-DSS

- The PCI-DSS was established to help merchants proactively protect customer account data
  - Account data or cardholder data includes (but is not limited to) the Primary Account Number (PAN), cardholder name, expiration date, address
  - The data in the magnetic stripe of credit cards
  - Card security codes (CVV2/CID/CSC)
  - PINs/PIN blocks*

* May not be applicable to your merchant card location if you do not accept PIN debit transactions
PCI Compliance in Higher ED

• Very challenging environment
  □ Open and collaborative by design
  □ Highly decentralized nature affects payments:
    • Acceptance methods
    • Processing procedures
  □ Lack of uniform standards that significantly impact information security
  □ Complete visibility into campus-wide commerce is virtually impossible to sustain
PCI Requirements

• Maintain compliance at all times
  □ Apply best practices when handling cardholder data
  □ Attendance of card security awareness presentations is a requirement
  □ Managers or any staff designated to validate PCI-DSS Compliance via SAQs (Self-Assessment Questionnaires and/or Vulnerability Scans) must do so in a timely manner

"The best intrusion detection systems are neither security experts nor expensive technology, but employees. Security awareness education for employees can often be the first line of defense."

*2012 Trustwave Global Security Report

Did you know?
...There were 855 data breaches involving 174 million compromised records in 2011.

*2012 Verizon Report
PCI Requirements (continued)

• Report compliance to merchant card processor/acquiring bank through annual attestation
  □ Contingent on, but not limited to the items in the previous slide
  □ At Northwestern University, done by Treasury OPS/e-Commerce Operations via attestation to First Data Merchant Services/Citi
Credit Card Handling Best Practices

- **Protect technology/systems**
  - Each user needs own user id with strong password
  - Lock or logoff from workstations used to process credit card data when not in use
  - Prevent credit card terminals or workstations used for credit card processing from physical access by unauthorized personnel
  - Workstations must have the latest anti-virus protection software
Credit Card Handling Best Practices

• **Protect data and media**
  - Do not create spreadsheets, databases, or other documents to store credit card numbers, or otherwise store any sensitive credit card information electronically.
  - Notify supervisor ASAP if you receive full credit card numbers electronically from anyone (including the cardholder).
    - Delete the message immediately after making note of the source/sender; do not print or forward it to anyone else.
  - If your department receives credit card information via fax, the fax must be in an area not accessible by unauthorized individuals.
Credit Card Handling Best Practices

• Protect data and media (continued)
  □ Old card swipe terminals must be returned to Depository Services for proper disposal
  □ If you process credit card transactions on a workstation, check with your IT staff to make sure that it is a workstation that is approved for payment processing
  □ If you notice strange behavior on your workstation, notify a supervisor or IT staff immediately
  □ If you have workstations that need to be replaced, sold, or discarded hard drives need to be “wiped” first

  • Refer to the policy on Disposal of Northwestern University Computers at: (http://www.it.northwestern.edu/policies/disposal.html)
Credit Card Handling Best Practices

- Protect paper records
  - Avoid creating paper records with card data, if at all possible
  - If your department accepts card payments via mail, or fax, never collect card security codes
  - Paper forms received with credit card information must be stored in a safe, inside a secure location inaccessible to unauthorized personnel
    - The documents must be clearly marked as containing sensitive information (i.e. folder marked “Confidential”)
    - Destroy after processing payments, using an approved shredding device or shredding service
Credit Card Handling Best Practices

- Prevent inadvertent disclosure
  - Do not send sensitive data including credit card numbers via email or instant message
  - Question anything that seems to contain unnecessary sensitive data
  - Follow guidelines for protecting data storage devices and paper records (pages 11 through 14), plus:
    - Familiarize yourself with Guidelines for Security and Confidentiality of Data Files ([http://www.it.northwestern.edu/policies/uccpolicy.html](http://www.it.northwestern.edu/policies/uccpolicy.html)) and Data Access Policy ([http://www.it.northwestern.edu/policies/dataaccess.html](http://www.it.northwestern.edu/policies/dataaccess.html))
Your role in the compliance process

• Fraud prevention
  □ Recognize refund fraud attempts; the merchant card policy requires supervisor approval to process refunds
    • Refunds can only be applied to the credit card originally charged
    • Amount of refund must be less than or equal to the original charge
    • Monitored by NU and processor
  □ Recognize unusual and suspicious credit card transactions and activity
    • Extremely large or extremely small transactions can be signs of fraud, especially in card not present transactions
    • Transactions that do not pass AVS (address verification service) and CSC (card security check) validations
Your role in the compliance process

- **Fraud prevention (continued)**
  - If you are a manager, make sure that your processes are properly documented
    - Observe proper duty segregation so that the individual processing transactions isn’t the same individual processing or approving refunds
    - Make sure that your merchant account is always properly reconciled; anomalies could be an indication of suspicious activity
- **Identify malicious insiders**
  - If someone appears to be using sensitive data inappropriately, or if sensitive data is found where it shouldn’t be, notify a supervisor or manager ASAP
Your role in the compliance process

• PCI-DSS requires employees with access to credit card data to go through a security screening
  □ New NU employees including contractors and temporary workers that will handle credit cards must go through a criminal background check
• In the event of a credit card data breach
  □ Contact us at 1-5382 (e-Commerce OPS) or 7-0422 (Treasury OPS) immediately so that we can work with the NUIT Incident Response Team and the authorities
Consequences of non-compliance

• If a NU merchant experiences a breach and was found to be non-compliant at that time, the following could occur:
  □ Assessed fines
  □ Increase processing costs
  □ Terminate card processing privileges
  □ Negative impact to reputation and brand

*All of the above won’t necessarily be contained to the department whose card operation was breached, but could impact the entire university*
What’s Next

• In the coming months, an official PCI DSS Information Security Policy will be released
  The same personnel required to review this presentation will be required to review the policy
• We will also be releasing a quiz to test your knowledge of credit card security and PCI-DSS
Acknowledge your participation

• Since participation in a credit card security awareness education program is mandatory, please click on the following link in order to acknowledge that you have reviewed this presentation:

  http://www.northwestern.edu/financial-operations/controller/treasury-operations/e-commerce-operations/pci-dss-sae.html
Resources

• Internal links

• External links