PCI DSS Security Awareness

Annual Education Module

James Madison University | University Business Office | Compliance Specialist

Training Audience

- The following training module should be completed by all University Staff that handle and/or process cardholder data.
  - Employees that process payments or issue refunds
  - Managers who have employees that have direct contact with credit card processing and data
  - Any employee that oversees, manages, or works with credit card processing software or hardware

Training Objectives

- Once you have completed this training module, you should have a comprehensive understanding of the following:
  - General background of PCI DSS
  - The twelve requirements of PCI DSS
  - Best Practices
  - Expectations and responsibilities for you as a JMU Merchant or JMU employee handling payment card information
  - Potential penalties for non-compliance
  - Overall security requirements

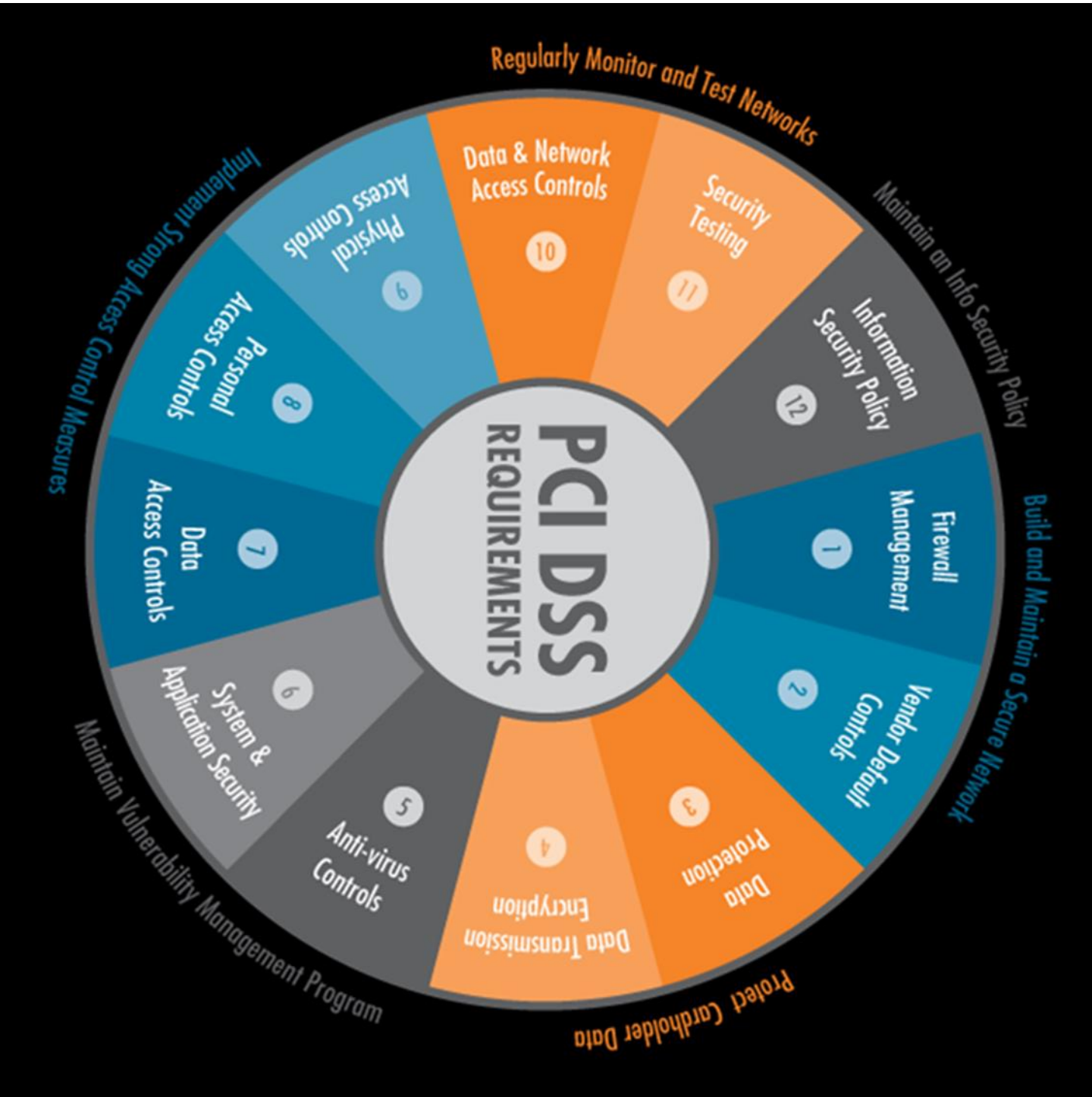
PCI DSS Background

- Purchase Card Industry Data Security Standards is most commonly referred to as PCI DSS
  - Created by the PCI Data Security Council
  - Regulations apply to anyone who stores, processes, and transmits cardholder data
  - A critical component in minimizing risk and maximizing protection
  - Applies to all forms of payment card acceptance
    - Mail, phone, fax, point-of-sale, and online
- Identifies and corrects vulnerabilities by ensuring appropriate levels of security are maintained

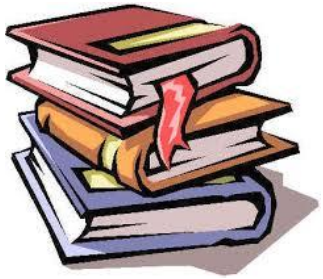
The Importance of PCI

- James Madison University has an obligation to students, vendors, alumni, and others to keep their account information safe when processing credit card payments.
- JMU must maintain compliance at all times
- A proactive step that helps JMU protect customer account information, including:
  - Magnetic stripe/track data, Primary Account Number (PAN), expiration date, card security code, pins, and other personal information

The 12 PCI DSS Requirements



Compliance in Higher Education



- JMU, like all universities, have unique challenges in maintaining PCI compliance.
  - The departments on campus are not located in a central location and vary greatly in their procedures:
    - Methods of payment card acceptance
    - Different procedures in place
    - Why they collect funds
    - Methods of fund collection
      - *In person, over the phone, online*

- The goal should be to create a cohesive and uniformed security program that protects all parties involved

PCI Regulations

- The newest version of regulations are PCI DSS 3.0 and will be in effect through 2016
  - The standards that were in place for 2.0 are still predominately the same and continue to focus on data security
- Departments should integrate PCI standards into their everyday operations and consider the regulations a normal part of daily business
- With the proper procedures, security, and vigilance in place, compliance will become the automatic standard

Policies and Requirements

- Document departmental procedures in detail, including:
  - Methods of payment card acceptance
  - Step-by-step how to guide to process payment
  - Complete list of all PCI trained employees must be maintained by each department
- Sign a new Merchant Agreement annually
- Complete Self-Assessment Questionnaire (SAQ) annually
- Complete an Equipment Inventory Audit annually
- Maintain best practices when handling payment card information

Best Practices for credit card processing

- Segregate duties when possible
  - The individuals that processes credit card transactions and refunds should not be involved in reconciling
- Do not send or accept credit card information via email
  - Notify a supervisor in the event you receive such an email
    - *Do not process a payment based on the information provided in the email; delete the email immediately; do not print or forward the email containing payment card information; notify the sender that you are unable to process the payment*
- Remember to **NEVER** store payment card data in any form for any reason, including:
  - Primary Account Number (PAN), expiration date, track data, security codes, and PIN number

Best Practices for credit card processing (Continued)

- After the transaction is complete store no more than the last four numbers of the PAN
- Store all necessary credit card documentation in a secure location
- Only allow employees who have a legitimate business need to access cardholder information
- Restrict physical access to areas where credit card information is handled and stored
- Store payment card receipts for the current fiscal year and three previous fiscal years in a secure location
- Each user needs their own user ID, coupled with a secure password that is changed regularly

Potential Security Breaches

- Secure filing cabinets being left open
- Lost or stolen keys
- Computer work station breach, infection, compromise
- New, unidentifiable equipment in point-of-sale area (skimming device)
- User ID and password stolen or given out
- Unusual/unexplained credit card transactions

According to the "2014 Data Breach Investigation Report" compiled by Verizon, there were 63,437 security incidents and 1367 confirmed security breaches last year

American Express® Card Identification Features

The letters "AMEX" and a phosphorescence in the Centurion portrait are visible under an ultraviolet light.

Pre-printed (non-embossed) Card Identification Number (CID) should always appear above the account number.

Do not accept a Card after the expiration date.

Only the person whose name is embossed on an American Express Card is entitled to use it.

All American Express account numbers start with 3. Embossing should be clear and uniform in size and spacing. The number on the front and back of the Card, plus the one printed on the sales receipt should all match.

With this statement on the Card, American Express reserves the right to "pick up" the Card at any time.

Some Cards have a hologram of the American Express image embedded into the magnetic stripe.

The signature on the back of the Card should match the customer's signature on the receipt. The signature panel is tamper-evident.

Merchant Code 10 Authorization

1-800-528-1212

if you are suspicious of a card transaction

Visa® Card Identification Features

The Dove Hologram appears on most cards, however its location on the card may vary. It can be in its traditional location on the front of the card, or a smaller hologram may be on the card back.

All Visa account numbers start with 4. The embossed account number must match the account number printed on the sales receipt.

The pre-printed Bank Identification Number (BIN) must match the first four digits of the embossed account number.

A full or partial account number is indent-printed on the tamper-evident signature panel.

A three-digit code (CVV2) must appear in the white box to the right of the signature panel or on the signature panel.

Some cards have a holographic magnetic stripe featuring doves in flight on the back of the card. These cards do not have any other hologram or magnetic stripe.

The Visa Brand Mark appears in the lower right corner. Visa debit cards have the word "DEBIT" printed above the Visa Brand Mark.

If you are ever suspicious about a card or a transaction, call your authorization center and request a Code 10 authorization.

MasterCard® Card Identification Features

All MasterCard account numbers start with 5. The embossing should be uniform in size and spacing, and extend into the hologram.

The three-dimensional hologram, which may appear on the front OR the back should reflect light and appear to move.

All new and re-issued consumer Debit cards must display the Debit hologram.

The pre-printed Bank Identification Number (BIN) must match the first four digits of the embossed account number.

The magnetic stripe should appear smooth, with no signs of tampering.

The valid date lists the last month in which the card is valid.

The last four digits of the account number appear on the signature panel in reverse indent printing.

Issuers have the option of placing a holographic magnetic stripe on the card back, replacing the Globe hologram or the Debit hologram.

The three-digit CVC2 appears to the right of the signature panel.

The word “MasterCard” is printed repeatedly in multicolors at an angle on a tamper-evident signature panel.

Are you suspicious about a card? Call for a Code 10 Authorization.

Discover® Network Card Identification Features

The words "DISCOVER NETWORK" will appear under an ultraviolet light.

All Discover Network account numbers start with 6. The embossing should be uniform in size and spacing, and extend into the hologram.

"Valid Thru" indicates the last month in which the card is valid.

A Business Name may be embossed below the account name.

An embossed Security Character appears as a stylized "D."

The three-dimensional hologram should reflect light and appear to move.

The magnetic stripe should appear smooth, with no signs of tampering.

The words "DISCOVER NETWORK" appear on the signature panel, and an underprint reading "VOID."

The last four digits of the account number appear on the signature panel in reverse indent printing.

The three-digit Card Identification Data (CID) appears to the right of the signature panel.

The Discover® Network Acceptance Mark appears on both sides of the card.

Merchant Code 10 Authorization

1-800-347-1111

for suspicious transactions

PCI Compliance and You

Through your continued vigilance and implementation of PCI standards, you and your department assist JMU in maintaining compliance and achieving a PCI mandate.

- You are the first line of defense against fraud at JMU
  - Recognize unusual or suspicious activity/transactions
  - If you recognize procedures/regulations not being followed contact the University Business Office immediately
  - Be ever vigilant when interacting with payment card data and credit card transactions
- As an employee, student, or volunteer who interacts with credit card data, you will have consented to a background check and completed your initial training

The Importance of Compliance

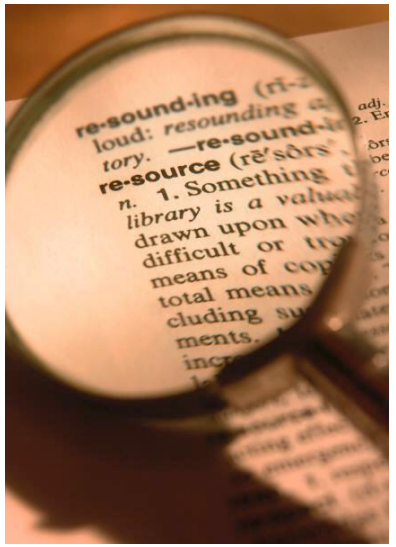
The various methods and intelligence of malicious attacks are constantly increasing and ever changing, therefore so should our due diligence with regard to compliance.

Penalties for a Breach

- Significant fines per incident
- Increased audit requirements
- Potential loss of the ability to accept payment cards
- Loss of staff time during security recovery
- Loss of business revenue due to loss of public image
- Cost of forensic investigation

Additional Resources

- UBO Data Security:
  - http://www.jmu.edu/ubo/university-departments-folder/pci.shtml
- JMU Policies:
  - 1204 – Information Security: http://www.jmu.edu/JMUpolicy/1204.shtml
  - 1205 – Data Stewardship: http://www.jmu.edu/JMUpolicy/1205.shtml
  - 1207 – Appropriate Use of IT Resources: http://www.jmu.edu/JMUpolicy/1207.shtml
  - 1210 – E-Commerce: http://www.jmu.edu/JMUpolicy/1210.shtml
- Financial Procedures Manual:
  - 4125 – Payment Cards: http://www.jmu.edu/financemanual/procedures/4125.shtml



If you have questions, comments, or concerns regarding PCI Compliance, please do not hesitate to contact me.

Wesley Howdyshell

University Business Office | Compliance Specialist

howdysjw@jmu.edu | 540.568.4674 | jmu.edu/ubo

Congratulations!

- You have completed your annual PCI Security Awareness Training module
  - This training is good for one calendar year after you pass the quiz

- REMEMBER, the training is not official until you complete the quiz with a grade of 80 percent or better.
  - Quiz is accessed via the same webpage you accessed this module
  - Once complete, fill out the certificate of completion and return to the UBO at MSC 3516