UNIVERSITY of MARYLAND BALTIMORE

UMB Policy and Procedure on Payment Card Industry Data Security Standards (PCI DSS)

Presenter:
Cindy Lyons, Deputy Controller

Panelists:
Jordan Nixon, Assistant Controller-Bursar
Alexandra Zouras-Wieneke, Director – Change Management Advisory Services
Carol Nelson, Assistant Director – CITS Quality Assurance

April 13, 2021

UNIVERSITY of MARYLAND BALTIMORE

Agenda

1. Introduction
2. Define PCI-DSS
3. UMB Policy
4. UMB Procedure
5. Questions and Discussion

UNIVERSITY of MARYLAND BALTIMORE

1. Introduction

PCI Webpage:
https://www.umaryland.edu/financialservices/payment-card-industry-pci-compliance/

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS?

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a mandated set of security requirements agreed upon by major credit card companies. These requirements apply to all payment card transactions and to the merchants/organizations that accept these cards as forms of payment.

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS (cont'd)?

- These standards were established by the major credit card companies (e.g. VISA, MasterCard, etc.)
- These companies formed the PCI Security Standards Council to manage compliance with PCI-DSS

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS (cont'd)?

Purpose for PCI-DSS:

To ensure that companies accepting payment cards as a form of payment for goods and services maintain a secure environment to:

- Prevent unauthorized access to personal data
- Prevent fraudulent transactions
- Minimize financial loss

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS (cont'd)?

What could happen if UMB is not compliant?

- Significant penalties and fines imposed by the credit card company
- Revocation - Credit card company can revoke the merchant account to prevent UMB from accepting payment cards
- Damage to reputation
- Litigation
- Additional oversight from government agencies

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS (cont'd)?

How is UMB achieving compliance?

- Established the UMB PCI Compliance Committee – a team of CITS, Finance, and Change Management Advisory Services staff that oversee department compliance

- Engaged CampusGuard, a cybersecurity and compliance organization, to guide UMB in navigating the requirements, oversee implementation, and to periodically assess and attest that UMB is in compliance

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS (cont'd)?

How is UMB achieving compliance?

- UMB Policy VIII-99.08(A) on Payment Card Industry Data Security Standards
- Accompanying Procedure: Payment Card Industry (PCI) Data Security Standards (DSS) Compliance and Payment Card Transactions
- Incorporated PCI Policy and Procedure into the Procedure on Establishing and Accounting for Payment Card Accounts

UNIVERSITY of MARYLAND BALTIMORE

2. What is PCI-DSS (cont'd)?

How is UMB achieving compliance?

- PCI Webpage
  - Navigation - About UMB>Administration and Finance>Financial Services>PCI Compliance (on the left navigation panel)
- Annual PCI training required (LMS)
- Annual SAQs
- Documented department procedures (template provided) and department training
- Periodic department reviews for compliance

UNIVERSITY of MARYLAND BALTIMORE

3. UMB Policy VIII-99.08(A): Payment Card Industry Data Security Standards

UNIVERSITY of MARYLAND BALTIMORE

3. Policy

Applies to:

All UMB Employees and Authorized Affiliate Employees

Key Terms:

- Cardholder Data (CHD)
  Those elements of payment card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code, and Sensitive Authentication Data. The Service Code permits where the card is used and the purpose of its use.

- Sensitive Authentication Data
  Additional elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.

UNIVERSITY of MARYLAND BALTIMORE

3. Policy

Purpose:

- Prevent financial loss
- Protect confidentiality of personal information when processing payments
- Establish internal controls
- Reduce risk of fraud and breach
- Comply with PCI-DSS and other regulatory organizations

UNIVERSITY of MARYLAND BALTIMORE

3. Policy

Statement:

- PCI Compliance is mandatory
- Disciplinary action for failure to comply
- Payment card types and processing equipment must be approved by the UMB Controller or designee
- Internal controls and procedures are required and documented at the Operational Unit level
- Properly dispose CHD as described in the accompanying Procedure

UNIVERSITY of MARYLAND BALTIMORE

3. Policy

Statement (cont'd):

- Prohibit Operational Units from entering online payments on behalf of customers
- Describe unacceptable methods of communicating CHD
- Prohibit saving, storing, or retaining sensitive authentication data
- Restrict payment methods (e.g. UMB does not accept PayPal payments)

UNIVERSITY of MARYLAND BALTIMORE

3. Policy

Assigns responsibilities:

- Office of the Controller (OOTC) authorized to create the Procedure
- All personnel with responsibilities in payment card transactions, including reconciliations, information technology, systems, data, and so forth are required to comply with PCI DSS, UMB Policy, and Procedure

UNIVERSITY of MARYLAND BALTIMORE

4. UMB Procedure on Payment Card Industry Data Security Standards Compliance and Payment Card Transactions

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

Applies to all Operational Units and individuals with responsibilities related to processing, managing systems, data, and accounting for transactions

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Operational Units develop written procedures as described in the Procedure under General Guidelines
    - A sample template is available to assist Operational Units

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Key points:
  - Payment methods (e.g. online) are limited
  - A unit PCI Coordinator is required
  - Payments may only be processed by UMB or Authorized Affiliate Employees
    - Students cannot process payments unless they are employees

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Key points:
  - Bank-issued equipment must be used for payments that are not processed online
  - Payments through unauthorized electronic methods such as UMB computers, Square, etc. are prohibited

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Mail and phone payments should be processed within one business day
- Destroy CHD by the close of business, but no later than 24 hours

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- CHD Destruction:

The preferred method for destruction is micro cross-cut shredding. Alternatives may be used as long as the CHD is unreadable and destroyed. Examples include punching holes through the card number, expiration date, and security code for CHD that is documented on a form. Writing over the CHD with a black marker is NOT an acceptable method for destroying CHD.

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Online Payment Processors (aka Gateway, Marketplace):
  - Gateway and application vendors approved by the Office of the Controller (OOTC) and Strategic Sourcing and Acquisition Services (SSAS)
  - See the Procedure on Establishing and Accounting for Payment Card Accounts.

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Third-party contractors (e.g. bookstore, parking, vending):
  - Contractors approved by SSAS
  - Contact the PCI Compliance Committee (PCC) for assistance in obtaining the necessary attestation of PCI compliance from the contractor

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

General Guidelines:

- Annual PCI Compliance Survey and PCI Self-Assessment Questionnaire (SAQ) are required
- The UMB PCI Compliance Committee (PCC) will coordinate distribution of the survey and questionnaire with Operational Units

UNIVERSITY of MARYLAND BALTIMORE

4. Questions?

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

This section is discussion of the PCI Procedure. Refer to the procedure document.

The best practice is to have the cardholder retain possession of the card and initiate the payment.

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

Links to additional resources:

- Establishing and Accounting for Payment Card Accounts
- UMB Policy X-99.08(A)on Disposal of Media Containing Data
- UMB Procedure on Disposal of Media Containing Data

UNIVERSITY of MARYLAND BALTIMORE

4. PCI Procedure

Links to additional resources:

- Merchant Account Request Form
- Swipe Terminal Inventory Sheet
- Telephone/Mail Payment Card Processing Form
- Reconciliation Template
- Department Procedure Template
- UMB IT Incident Response Policy

UNIVERSITY of MARYLAND BALTIMORE

4. Reconciliations

UNIVERSITY of MARYLAND BALTIMORE

4. Reconciliations

- Reconciliation and daily batch processes must be documented
- Reconciliations should be performed by someone who is not directly involved in processing transactions
- Three reconciliations to perform:
  1. Sales reconciled with payments processed. Compare sales report with daily batch report.

Example: If ten people pay $50 to reserve a seat in a class, then the sales should show 10 seats @$50 each and the batch report from the sales terminal should show $500 processed for the day.

UNIVERSITY of MARYLAND BALTIMORE

4. Reconciliations

- Three reconciliations to perform (cont'd):

  2. Batch reconciles with the amount funded. Compare batch report with merchant bank activity.

  Example: Using the previous example, the $500 on the batch report from the terminal should match the amount reported by the merchant bank. The amount reported by the merchant bank is available online. The amount for this day should be $500.

UNIVERSITY of MARYLAND BALTIMORE

4. Reconciliations

- Three reconciliations to perform (cont'd):

    3. Merchant bank activity reconciles with the amount posted in Quantum Analytics. Compare the merchant bank activity with the Analytics detail report.

    Example: Using the previous example, the $500 reported by the merchant bank should match the amount posted in Quantum. Look in Quantum Analytics to compare the amounts.

UNIVERSITY of MARYLAND BALTIMORE

4. Reconciliations

- Templates are available here to assist with reconciliations
- Reconciliations are required to be performed at least once per calendar month
- Reconciliations must be documented, reviewed, signed, and dated by the preparer and the department administrator (or designee)

UNIVERSITY of MARYLAND BALTIMORE

4. Reconciliations

- Differences must be investigated immediately.
- Any unresolved differences must be reported in writing to the Operational Unit head, University Controller, and Change Management Advisory Services (CMAS)
- Email CMAS if assistance is needed with establishing reconciliation procedures

UNIVERSITY of MARYLAND BALTIMORE

4. Payment Device Inspections

UNIVERSITY of MARYLAND BALTIMORE

4. Payment Device Inspections

- Inspect public-access devices (e.g. kiosk, terminal) daily
  - Secure shared devices in a locked area when not in use or after hours when possible

- Examine the equipment for tampering evidence:
  - Damaged tamper sticker (tamper stickers are available from the Cashier's Office)
  - Unusual markings or damage to the device

- If tampering is suspected
  - Discontinue use of the device
  - Contact BB&T/Truist to obtain a new device
  - Report the information to the supervisor, unit PCI Coordinator
  - The PCI Coordinator reports the tampering to the PCI Committee

UNIVERSITY of MARYLAND BALTIMORE

4. Suspected Security Breach or Fraud

- A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

- Fraud is a willful or deliberate act, expression, omission or concealment with the intent of obtaining an unauthorized benefit, such as money or property, by deception or other unethical means.

If a security breach or fraud is suspected, immediately contact the employee's supervisor and the unit PCI Coordinator. The PCI Coordinator is responsible for contacting the PCI Committee and Change Management Advisory Services.

If the suspected activity involves computers (hacking, unauthorized access, etc.), also contact the Operational Unit's IT support team and immediately notify the Center of Information Technology Services (CITS)

UNIVERSITY of MARYLAND BALTIMORE

4. Questions?

UNIVERSITY of MARYLAND BALTIMORE

4. UMB Procedure on Establishing and Accounting for Payment Card Accounts

UNIVERSITY of MARYLAND BALTIMORE

4. Procedure on Establishing and Accounting for Payment Card Accounts

- Merchant accounts must be established in accordance with the Procedure.
- In addition to providing the steps for setting up a merchant bank account, this procedure includes information on recording revenues and expenses (i.e. bank fees)
- Merchant Account Request Form
  - Includes listing of unit personnel engaged in payment card transactions
  - Personnel changes going forward must be emailed to DL-CITSPCICompliance@umaryland.edu

UNIVERSITY of MARYLAND BALTIMORE

5. Questions?

Email: DL-CITSPCICompliance@umaryland.edu