Office of Treasury Operations

Payment Card Industry Data Security Standards (PCI DSS) Training
Overview

- Payment Card Anatomy
- Authorization Process
- PCI DSS – Defined
- PCI DSS – Requirements
- PCI DSS – Mandatory
- PCI DSS – Summary
- Resources
Cardholder Data vs. Sensitive Authentication Data

Cardholder Data (Front of Card):

- PAN (Primary Account Number)
- Expiration Date
- Cardholder Name
Other important features to distinguish real vs. fraudulent card:

- **Hologram**
  - Sometimes on back of card, different for each card brand, and AMEX does not have one

- **Card Brand Logo**

- **Issuing Bank Logo**

- **Debit Identifier** (informs you that the card is tied to a checking/savings bank account)
Cardholder Data vs. Sensitive Authentication Data

**Sensitive Authentication Data** (Back of Card):
- **CVC or CVV (Card Verification Code)**
  - 3 or 4 digit code used in card-not-present transactions
- **Full Magnetic Stripe**
  - Data encoded in the magnetic stripe used for authorization during card-present transactions
Authorization Process

1) Cardholder (customer) presents card to merchant (or enters information into secured web payment application)

2) Merchant sends data to acquiring bank (processor)

3) Acquiring bank sends data to issuing bank for approval

4) Once transaction is approved, data is sent back to merchant

Purdue is required to take appropriate measures to ensure the data transmitted remains secure along the way.
PCI DSS – Defined

Set of requirements to ensure cardholder data remains secure

- Primary goal is to protect cardholder data

- Compliance is mandatory per the payment brands (example: Visa, MasterCard, American Express, and Discover) in order for us to maintain our privileges to accept payment cards

- Helps protect against fraud
PCI DSS – Defined

- PCI standards apply to all merchants and processors that store, process, or transmit cardholder data

Note:
- Applies to ALL payment channels (i.e. point of sale systems, web, or swipe terminal)
- Compliance standards are set forth by payment brands
- Security is a layered approach that is ongoing
# PCI DSS – Requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain Secure Network</td>
<td>• Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>• Do not use vendor–supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>• Protect stored cardholder data*</td>
</tr>
<tr>
<td></td>
<td>• Encrypt transmission of cardholder data across open, public records*</td>
</tr>
<tr>
<td>Maintain Vulnerability Management Program</td>
<td>• Use and regularly update anti–virus software</td>
</tr>
<tr>
<td></td>
<td>• Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>• Restrict access to cardholder data by business need–to–know*</td>
</tr>
<tr>
<td></td>
<td>• Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>• Restrict physical access to cardholder data*</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>• Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>• Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>• Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>

*We will focus on these requirements*
Requirements:

- **Protect stored cardholder data**
  
  - Place transactions immediately and directly into point-of-sale system or swipe terminal
  
  - If information is received in a written format, be sure to keep it secured or locked up until the transaction can be processed then shred or confidentially recycle
Requirements:

- Encrypt transmission of cardholder data across open, public networks*

  ➢ Under no circumstances should cardholder data be emailed or sent via any other unencrypted communication tool
PCI DSS – Requirements

Requirements:

- **Restrict access to cardholder data to a business only need-to-know basis** *
  
  - If you do not have a direct business need for the information, you should not have access to it
  
  - Make sure each individual has their own unique logon ID for any system
PCI DSS – Requirements

Requirements:

- **Restrict physical access to cardholder data**
  - Keep all written cardholder data secured or locked up until you are able to run the transaction
  - Destroy the written data via cross-cut shredding or confidential recycling once transaction is run
PCI Compliance is Mandatory

Risks of Non-Compliance:

- Large monetary fines assessed to Purdue/your department
- Loss of merchant’s ability to accept payment cards
- Reputational risk for Purdue University brand name

Benefits of Compliance:

- Helps protect against fraud
- Allows you to continue accepting payment cards
- Keeps your department and Purdue out of the headlines
Proactively protect cardholder data by maintaining the following guidelines:

- Keep data secure and confidential
- Process transactions immediately
- Do not email payment card information
- Restrict/limit access to cardholder data
PCI DSS – Summary

- Easiest way to comply:

**DON’T KEEP CARDHOLDER DATA!!**

- Find and eliminate prohibited data
- Do not keep data that you do not need
- Frequently review your processes for compliance
For additional information or further detail on any aspect of PCI DSS, review the following resources:

- [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)


You may also contact us via email at [treasury@purdue.edu](mailto:treasury@purdue.edu)