

# UNIVERSITY *of* WEST FLORIDA

## PCI DSS Compliance Training

Matthew Packard, CCEP | Internal Auditing and Compliance  
mpackard@uwf.edu | 850.857.6070

# Agenda

- ⌘ PCI DSS overview
- ⌘ The Basics
- ⌘ Your responsibilities
- ⌘ University Policies
- ⌘ Best Practices



# So...what is PCI-DSS?

## Payment Card Industry Data Security Standards

- Created by the PCI Data Security Council (Visa, MasterCard, American Express, Discover, and JCB)
- Created a common set of industry standards developed to increase the controls around cardholder data to reduce credit card fraud.
  - These standards consist of 6 goals and 12 Requirements...



# PCI DSS Standards

6 Goals

12 Requirements



Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Protect all systems against malware and regularly update anti-virus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Identify and authenticate access to system components</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel</li> </ol>

# Why am I here???

PCI Requirement 12.6.1

Educate personnel!!!

# Background Information

Over the past few decades...

- Increases in payment card usage
- Increases in e-commerce
- Increases in more “convenient” payment methods



# Background Information Continued

In our desire for convenience, we have left ourselves vulnerable

The screenshot shows a web browser window titled "The Pirate Market - Tor Browser". The address bar displays the URL "yjhzeed5osagmmr.onion/index.php?s=items&id=7899142". The page header includes "THE PIRATE MARKET" and navigation links for "PROFILE", "ACCOUNT(฿ 0.00000000)", and "MESSAGES(1)". A left sidebar lists categories such as "COUNTERFEITS(4)", "DRUGS(421)", "EBOOKS(21)", "JEWELRY(1)", "MONEY(28)", "ONLINE(34)", "TOBACCO(34)", "WEAPONS(10)", "MISCELLANEOUS(20)", "VERY POPULAR", and "NEWS". The main content area displays a product listing for "US, CA Visa/MasterCard / Amex / Discover/ x10". The product image shows logos for VISA, MasterCard, AMERICAN EXPRESS, and DISCOVER NETWORK. The price is listed as "\$70.00" and "฿0.11436414". A red box highlights the "\$70.00 USD" price. Below the price, there is an "ADD TO CART" button. The shipping and payment options are also visible.

# PCI DSS @ UWF

As a public institution we have a obligation to our students, vendors, donors, stakeholders, and the community at large to ensure that there account information is safe when processing credit card payments @ UWF



# PCI DSS—It Can Help Prevent Data Breaches!



# Non-Compliance—What's at Stake

Could result in the revocation of our ability to accept card payments

Causes damage to consumer trust and our reputation

Fines our acquiring bank \$5,000 to \$100,000 per month\*

***\$7.01 million = Average organizational cost of a data breach\*\****

\*The bank will likely pass this fine along...

\*\*2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute

# Agenda

---

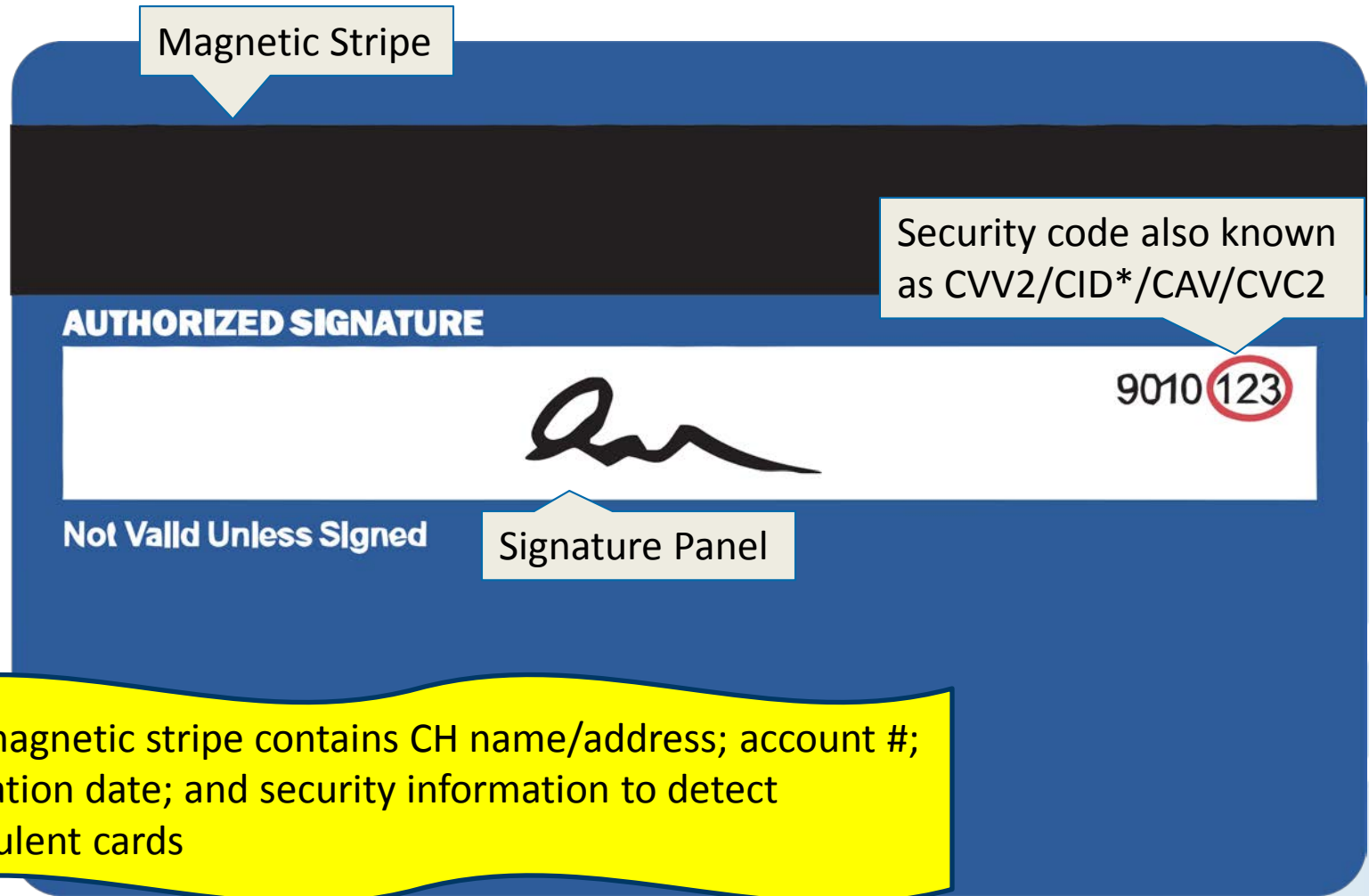
- PCI DSS overview
- **The Basics**
- **Your responsibilities**
- **University Policies**
- **Best Practices**



# The Basics: Credit Card Anatomy (Front)



# The Basics: Credit Card Anatomy (Back)



The magnetic stripe contains CH name/address; account #; expiration date; and security information to detect fraudulent cards

\*American Express refers to this code as the CID and it is located on the front of the card

# What is Cardholder Data (CHD)? ...technically

Primary Account Number (PAN): Consists of the full credit/debit card number

CHD consists of the PAN plus any one of the following:

Cardholder name

Expiration date

Security Code

# The Last 4 Digits

Storage of the *last four digits* of a credit card number is allowed & does not constitute CHD

Customer receipts should not show more than the *last four digits* of the credit card number

Computer systems and software used to process credit card transactions should not display more than the *last four digits* of the credit card number

# Cardholder Data Procedures: *Magnetic Stripe/PIN/Code*

The University does not permit the storage of the codes found on the magnetic stripe, PIN/PIN block data, or the card validation code.



# Cardholder Data Procedures: *Access Control*

All employees that have access to CHD must keep this information in the strictest confidence, and protect it from unauthorized access or disclosure.

Access to this information should be on a need-to-know basis only.

# Cardholder Data Procedures: *Electronic Records*

CHD should NEVER be stored in electronic format\*

CHD should NEVER be included in email or other electronic messages

*\*Entering CHD into e-market portals (Lumens/HigherOne/CashNet/etc.) does not qualify. As this data is not being stored on our campus network.*

# Cardholder Data Procedures: *Paper Records Procedures*

Paper documents must be protected, stored securely, and disposed of securely.

Avoid the use of paper documents whenever possible.

*If unavoidable, please refer to the [paper document standards/procedures](#) provided on the UWF Financial Services PCI Compliance webpage.*

# Agenda

- PCI DSS overview
- The Basics
- **Your responsibilities**
- **University Policies**
- **Best Practices**



# Workstation Responsibilities

Each workstation ***must be a dedicated, PCI compliant, ITS approved*** payment machine

Each user is required to have a ***unique login*** for operating POS device

Keep login ***credentials confidential*** and do not share with others

***Secure the credit card environment*** from non cashier personnel

# Workstation Responsibilities

## Continued

**Log off** whenever stepping away from machine

Log off another cashier and **login with your own credentials** when processing transaction

**Turn off POS device** at night and secure area

**Keep your workstation clear** of any sensitive materials

# Agenda

---

- PCI DSS overview
- The Basics
- Your responsibilities
- **University Policies**
- **Best Practices**



# UWF PCI DSS Policies



## INTERNAL AUDITING & COMPLIANCE

- Services
- Resources
  - Auditing Resources
  - Compliance Resources
  - Important PCard Information
  - Other Links of Interest
  - PCard Reference Guide
- PCI Compliance**
  - Professional Organizations
  - State of Florida Colleges and Universities
  - Top 10 Findings or Questions Related to the PCard
  - UWF Policies & Procedures
- About Us

**Additional Information**  
Silent Witness  
White Collar Crime Presentation  
Official PCI Security Standards Council Site

**Internal Auditing & Compliance**  
Bldg. 20W / Rm. 157  
11000 University Pkwy.

## Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Council has established Data Security Standards that must be complied with by all entities that accept credit card transactions. These standards include controls for handling and restricting credit card information, and related computer and Internet security. UWF is dedicated to full compliance with PCI DSS.

### Introduction

The University of West Florida accepts on-line credit card payments as a convenience to our customers. Students may make payments on-line through their MYUWF account for current charges. UWF accepts Visa, MasterCard or American Express credit card transactions.

Due to the nature of their activities, several departments have been authorized to accept credit card transactions for their specific programs. These departments must follow strict procedures to protect the customers' credit card information.

### Authorization

Departments must be authorized by the University Controller in order to collect funds. To begin this process, the department should discuss the proposed activity with the University Controller, who can be reached at (850) 474-2120. The Cashiers may be able to accommodate the department through existing systems, or may recommend that the Department submit a Departmental Request for Authorization (pdf) form along with supporting documentation clearly describing the scope of the proposed activity.

Departmental Request for Authorization (pdf) forms will be reviewed and evaluated by the University Controller and ITS for security issues related to the protection of customer Cardholder Data. The Departmental Request for Authorization (pdf) proposal must assure the protection of Cardholder Data and compliance with PCI DSS.

## Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Council has established Data Security Standards that must be complied with by all entities that accept credit card transactions. These standards include controls for handling and restricting credit card information, and related computer and Internet security. UWF is dedicated to full compliance with PCI DSS.

### Contacts

The following personnel may be contacted for questions or further information:

**Linda Howard** Cashiers 474-2120

### Procedures, Forms, and Links

The following procedures forms and links are related to credit card transactions:

- Employee Credit Card Security Training (docx)
- Dept Request for Authorization (pdf)
- Credit Card Security Awareness Training Program (docx)
- PCI DSS Overview of Standards and Requirements (pdf)
- Cardholder Data (docx)
- Cr Card-Eliminating Credit Card Numbers from Paper Doc (pdf)
- Paper Document Procedure (pdf)
- Cr Card-Service Providers with Access to Cardholder Data (docx)
- Credit Card Telephone Log (xlsx)
- Credit Card Receipt Document (docx)
- Credit Card Document Inventory (xls)
- Dept Self Assessment Questionnaire (pdf)
- PCI DSS Web Site
- PCI DSS Security Policies (pdf)
- Skimming Prevention At-a-Glance (pdf)
- Skimming Prevention for Merchants (pdf)

We strive to provide accurate and useful information in a manner that helps you find what you are looking for. We would like to have your feedback related to the utility of this information, additional information you would like to see on this site, or any other suggestions for improvement. Please email us at [lhoward@uwf.edu](mailto:lhoward@uwf.edu) or call 474-2120 with your feedback.



# PCI DSS Security Policy

Technologies **NOT** allowed to access the cardholder environment



Open or public WIFI (non VPN)



Removable electronic media  
(USBs, etc.)



Laptops



Tablets



Smartphones

# PCI DSS Security Policy

Activities **NOT** allowed while accessing and/or connected to the cardholder environment



Checking email



Visiting any website not directly associated and pertinent to the actions being performed



Make internet or intranet connections that are not explicitly necessary

# Agenda

- PCI DSS overview
- The Basics
- Your responsibilities
- University Policies
- **Best Practices**



# Best Practices

Maintain strong passwords and update regularly

- [Password Dos and Don'ts](#)

Be on the lookout for skimming devices

- [Familiarize yourself with the point-of-sale equipment and check regularly for modifications](#)

Be sure your station is physically secured at all times

# Best Practices Continued

Destroy CHD immediately\* (cross-cut shredder)

Notify the Compliance Officer or Financial Services immediately if there is a change in personnel

Never send CHD via electronic messages/email

Never share your login credentials

Be on the lookout for phishing/social engineering attempts to steal your credentials

- [Avoiding phishing and social engineering attacks](#)

*\*Only write down CHD when absolutely necessary... it usually is not.*

# UNIVERSITY *of* WEST FLORIDA

Questions?

[mpackard@uwf.edu](mailto:mpackard@uwf.edu) | 850.857.6070