Ball State University

PCI Data Security Awareness Training

Agenda

Ball State University

- What is PCI-DSS
- PCI-DSS Standards
- Training
- Definitions
- Compliance
- 6 Goals
- 12 Security Requirements
- Card Identification
- Basic Rules to Follow
- Myths

What is PCI-DSS?

The **Payment Card Industry Data Security Standards** (PCI-DSS) are regulations that were created to ensure safe handling of sensitive information and to protect cardholder data.

Ball State University

The PCI Council was established in 2006
by
Visa, MasterCard, Discover, and American Express

Why Have Standards

Ball State University

- To protect the credit card brands' reputation as a secure method of payment
- To protect customer cardholder data
- To establish consistency for any entity accepting credit and debit cards

Importance of Training

Ball State University

While processing credit cards you will be exposed to a lot of sensitive information that is protected by law.

This training will show you how to handle credit card information in a safe and secure manner.

Training

Ball State University

- Training is required for all campus personnel who have access to credit card information
  - As a processor of credit card transactions; or
  - Reviewers of reports that contain credit card data
- Training is required upon employment and annually

PCI-DSS Definitions

Ball State University

Cardholder	Customer to whom a card is issued or individual authorized to use the card
Cardholder Data	Full magnetic stripe or the Primary Account Number (PAN) plus any of the following • Primary Account Number • Cardholder Name • Expiration Date • Service Code
Cardholder Validation Value or Code	Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting.
Compromise	Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.
Encryption	Process of converting information into an unintelligible form except to holders of a specific key. Use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure.

PCI-DSS Definitions

Ball State University

Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks.
Information Security	Protection of information to insure confidentiality, integrity and availability
Magnetic Stripe	Data encoded in the magnetic stripe is used for authorization during transactions when the card is presented.
Merchant	Any person/business that accepts payments by debit or credit cards
Issuer	Bank or other organization issuing a payment card on behalf of a Payment Brand (e.g. MasterCard & Visa) or Payment Brand issuing a payment card directly (e.g. Amex, Discover, JCB)

PCI-DSS Definitions

Ball State University

POS	Point of Sale. Hardware and/or software is used to process payment card transactions at merchant locations
Service Code	Three or four digit number on the magnetic stripe that specifies acceptance requirements and limitations for a magnetic stripe read transaction
Vulnerability Scan	Scans used to identify vulnerabilities in operating systems, services and devices that could be used by hackers to target the university's private network
PAN	Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also referred to as the Account Number

Ball State University

Who Must Comply with PCI?

Any organization that accepts, processes, or transmits cardholder data.

This includes Ball State University

Compliance with PCI-DSS

Ball State University

- Since Ball State accepts payment cards, the university is subject to PCI-DSS standards
- Adhering to the standards is not optional
- There are significant financial costs to non-compliance
  - It only takes one incident of data compromise to put the university at risk
  - Non-compliance is not worth the risk

Compliance with PCI-DSS

Ball State University

Failure to comply with PCI-DSS can result in stiff contractual penalties or sanctions from members of the payment card industry including:

- Fines of $500,000 per data security incident
- Fines of $50,000 per day for non-compliance with published standards
- Liability for all fraud losses incurred from compromised account numbers
- Liability for the cost of re-issuing cards associated with the compromise
- Suspension of merchant accounts

Campus PCI-DSS Merchants

Ball State University

- All Ball State merchants must be PCI-DSS compliant and are responsible for ensuring their compliance
- It applies to all payments channels, including in person, mail, telephone order and e–commerce

PCI-DSS Goals

Ball State University

The 6 Goals of PCI-DSS

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI-DSS 12 Security Requirements

Ball State University

- Build and Maintain a Secure Network
  - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
  - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - *Requirement 3:* Protect stored cardholder data
  - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - *Requirement 5:* Use and regularly update anti-virus software
  - *Requirement 6:* Develop and maintain secure systems and applications

12 Security Requirements

Ball State University

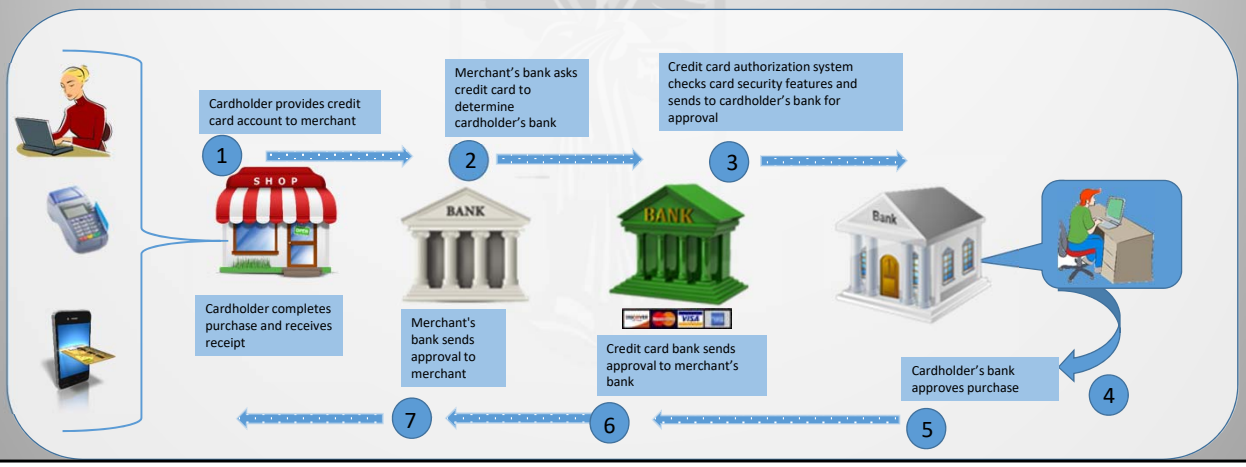
- Strong Access Control Measures
  - *Requirement 7:* Restrict access to cardholder data by business need-to-know
  - *Requirement 8:* Assign a unique ID to each person with computer access
  - *Requirement 9:* Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - *Requirement 10:* Track and monitor all access to network resources and cardholder data
  - *Requirement 11:* Regularly test security systems and processes
- Maintain an Information Security Policy
  - *Requirement 12:* Maintain a policy that addresses information security

Credit Card Processing Example

Ball State University

Card Present Transaction:
Every request receives a response that directs the acquirer or the merchant on how to proceed with the transaction (Approve or Deny)

- Seven Steps



Card Identification Features

Ball State University

All VISA account numbers start with a 4, MasterCard starts with a 5 and Discover starts with a 6. 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.

VISA card logo

VISA Holographic emblem

3 digit security code also called the CVV2 number.

Magnetic stripe containing identification, PAN and special security information.

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

Card expiration month and year. Do not accept a card after the expiration date.

Only the person whose name is embossed on a VISA is entitled to use it.

American Express ® Card Identification Features

Ball State University

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

All American Express account numbers start with a 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.

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

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.

Card expiration month and year. 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.

Importance of CVV2/CID

Ball State University

American Express
CID 4 digit number

Visa, MasterCard and
Discover 3 digit
CVV2/CID number

- The CVV2/CID number ensures the caller actually has a credit card in hand when making a purchase.
- When a customer physically hands you their card and you swipe it in a credit card terminal, you will not need to use the CVV2/CID number.
- Do you know why?
- The terminal reads and transmits data from the magnetic strip which includes the CVV2/CID security code.

Processing Computers

Ball State University

- Computers used for processing payments should only be used for processing payments
- Should never be used for non-work related processing such as e-mail should not be stored or executed on payment processing computers
- Only authorized activity should be executed
- Absolutely no personal or authentication data can be stored on the computer

Point of Sale Registers

Ball State University

- Identify any third-party claiming to be maintenance or a repair person for payment card devices before granting them access to the device
  - Review their credentials and work order
  - Call the business they are representing
- Before installing or replacing a received payment card device (or allowing a third-party to do so) receive acceptance verification from your supervisor
- Pay close attention to any suspicious behavior around a payment card device.
  - For example plugging something into the wall around or in the same room as the payment card device.
  - Opening the device
  - If you detect this report it immediately to your supervisor

Ball State Procedures

Ball State University

- Contact the Controller's Office when considering any changes to your credit card system
- PCI Questionnaire and Scans
- Daily Batch Settlements (covering and cross training in case of absences)
- Daily Transmittals and Reconciliations
- Retention policy
- Incident response
- Background checks

Basic Credit Card Security Rules

Ball State University

- Keep the card in the customer's line of sight at all times.
- Match signatures on the signed receipt to the back of the card.
- Accept only the 4 major credit cards, or those identified by your department.
- Write cardholder information only on designated forms.
- Obtain the security code on the back of the card for all telephone sales.
- Store all documents containing cardholder data in a secure locked area.
- Process refunds to the card used for the original purchase.
- Never share cardholder information outside your work environment.
- Never send or receive card data through e-messaging. (ie. Email, e-mail attachments, texting or chat rooms.)

Note: Some of the rules may not apply to your department since each department may have different business processes. Always check with supervisor when you are not sure.

Basic Credit Card Security Rules

Ball State University

Keep the Card in the Customer's Line of Sight at All Times

DO's

- Place the card on the counter as you log into the POS terminal.
- Hold the card up in front of you or keep it on the counter if you need to use both hands.

DO NOT's

- Place the card below the counter
- Walk away with the customer's card or leave it sitting on the counter
- Place the card in a drawer
- Lastly, do not place the card behind anything that would block the customer's view of seeing their card

Basic Credit Card Security Rules

Ball State University

Match signatures on the signed receipt to the back of the card

- Verify a signature appears on the card
- Verify the signatures on the card and the receipt look a like.
- Verify the signature area on the card is intact and not voided.
- Verify the color markings on the signature stripe are there.
- If you have any concerns or the signatures do not match contact your supervisor.

Basic Credit Card Security Rules

Ball State University

Obtain the Security Code on the Back of the Card for all Telephone Sales

- When you ask for the security code you are validating the card is in the physical possession of the cardholder.
- If the CVV2/CID number does not match the issuing bank's file, the transaction will be declined.
- The CVV2/CID number should never be written down on a paper document.
- The CVV2/CID number can only be entered through a terminal.

Basic Credit Card Security Rules

Ball State University

Write Cardholder Data Only on Designated Forms

- If Mail/Phone order transactions are permitted in your department. Then record:
  - Customer's name
  - Phone number
  - Credit card number
- Once the order has been placed or recorded all paper documents should be securely shredded in cross shedder or securely stored if the department's Mail/Phone procedure permits

Credit Card Security Rules

Ball State University

Store All Documents Containing Card Holder Data in a Secure Locked Area

- To secure cash and credit card receipts:
  - Organize credit card receipts into a stack
  - Place the receipts inside a cash bag
  - Deliver the bag to the safe or cash room
- Order forms should only remain in a restricted area under lock and key until the forms can be destroyed by a designated individual.

Credit Card Security Rules

Ball State University

Process Refunds to the Card Used for the Original Transaction

- If the original order was an internet transaction the cardholder's information and card number will be linked to the order. A refund will be automatically issued based on the information recorded.
- Do NOT enter a customer's card information over the phone to issue a refund for an internet transaction.
- If a customer does not have their original card when requesting a refund inform them a check will be issued for the refund amount.

Credit Card Security Rules

Ball State University

Do Not Discuss Cardholder Information Outside of Your Work Area

- Do not discuss a customer and their credit card anywhere outside of the designated work area
  - This includes the break room, hallway or at lunch
- Do not discuss or send any card data through e-messaging
  - This includes e-mails, e-mail attachments, texting, chat rooms or any social media

PCI DSS Myths?

Ball State University

Myth 1 – One vendor and product will make us compliant
- No single vendor or product fully addresses all 12 requirements of PCI-DSS

Myth 2 – Outsourcing card processing makes us compliant
- Outsourcing simplifies but does not provide automatic compliance
- We must ensure providers comply with PCI standards
- Request a certificate of compliance annually from providers

Myth 3 – PCI compliance is an IT project
- The IT staff implements technical and operational aspects
- PCI compliance is an ongoing process of assessment, remediation, reporting

PCI DSS Myths?

Ball State University

Myth 4 – PCI will make us secure
- Successful completion of a scan or assessment is ONLY a snapshot in time
- Security exploits are NON-STOP and get stronger every day
- PCI compliance efforts are a continuous process of assessment and remediation to ensure safety of cardholder data

Myth 5 – PCI is unreasonable; it requires too much
- Most aspects of PCI-DSS are a common best practice for security

Myth 6 – PCI requires us to hire a Qualified Security Assessor
- PCI-DSS provides the option of doing an internal assessment with an officer sign-off if acquirer and/or merchant bank agree

PCI DSS Myths?

Ball State University

Myth 7 – We don't take enough credit cards to be compliant

- PCI compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one

Myth 8 – We completed a SAQ so we're compliant

- Technically, this is true for merchants who are not required to do on-site assessments for PCI-DSS compliance. True security of cardholder data requires non-stop assessment and remediation to ensure the likelihood of a breach is kept as low as possible.

Myth 9 – PCI makes us store cardholder data

- Both PCI-DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors

PCI DSS Myths?

Ball State University

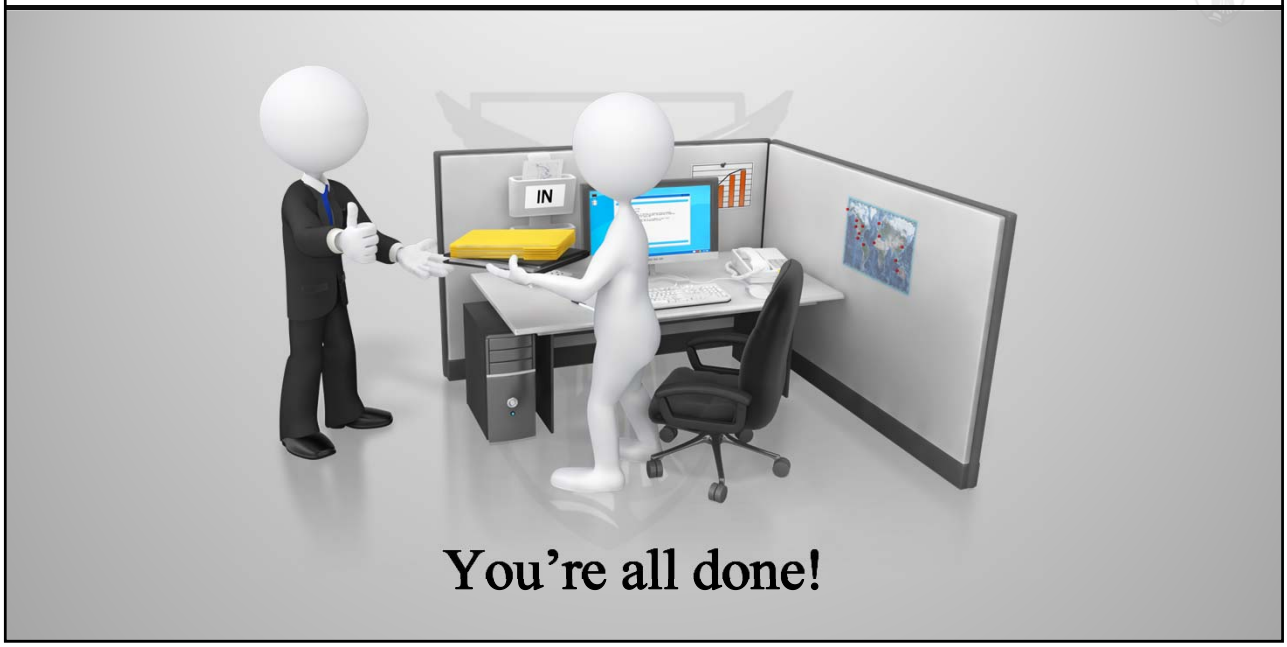
Lastly….

Myth 10 – PCI is too hard

- Understanding PCI-DSS can seem daunting, especially for merchants without security or a large IT department
- However, PCI-DSS mostly calls for good, basic security

Great Job!

Ball State University



You're all done!