PCI Training

- This training is to assist you in understanding the policies at Appalachian that govern credit card transactions and to meet the PCI DSS Standards for staff training to prevent identity theft.

- If your department processes credit card information, it is CRITICAL that you understand the importance of protecting this data.

PCI Training

- More than 340 million computer records containing sensitive personal information have been involved in security breaches in the U.S. since 2005. It is your top priority to protect sensitive data associated with credit card transactions.

- Breaches in data security could result in unauthorized use of personal indentifying information AND fines for your department.

Potential fallouts for Departments from a breach:

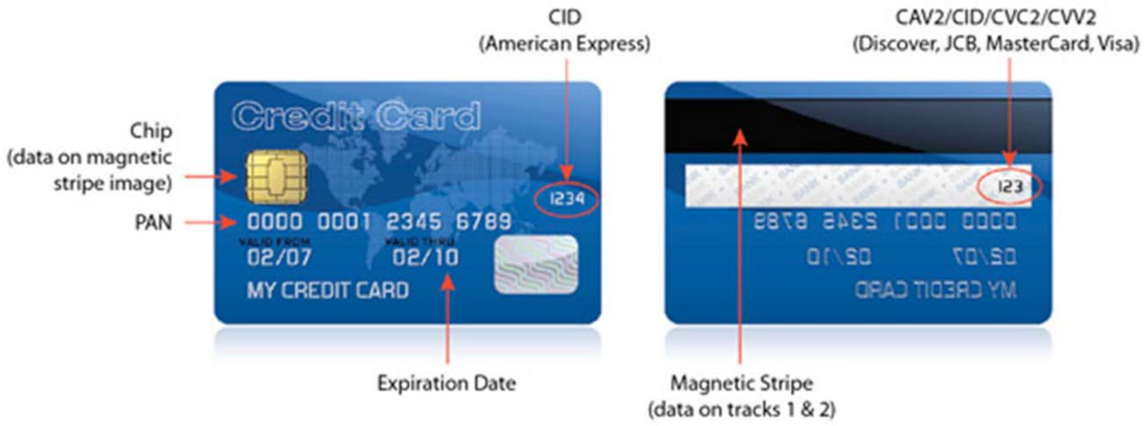
- Fines and penalties
- Termination of ability to accept payment cards
- Lost confidence, so customers go to other merchants
- Lost sales
- Cost of reissuing new payment cards
- Legal costs, settlements and judgments
- Fraud losses
- Higher subsequent costs of compliance
- Going out of business

Sensitive data

- The object of desire is cardholder data. By obtaining the Primary Account Number (PAN) and sensitive authentication data, a thief can impersonate the cardholder, use the card, and steal the cardholder’s identity.

Red arrows = Sensitive data

Types of Data on a Payment Card



Sensitive Data

- Merchants and any other service providers involved with payment card processing **must never store** sensitive authentication data.
  - This includes sensitive data that is printed on a card, or stored on a card's magnetic stripe or chip – and
  - personal identification numbers entered by the cardholder.

Sensitive data can be stolen from:

- Compromised card reader
- Papers left unprotected on office desks
- Paper stored in a filing cabinet
- Data in a payment system database
- Hidden camera recording entry of authentication data
- Secret tap into your store’s wireless or wired network

What is PCI DSS

- PCI = Payment Card Industry
- DSS= Data Security Standard
- Requirements of all Payment Brands – VISA, MasterCard, American Express, etc.
- Standards address:
  - Network Security which includes testing and monitoring requirements
  - Protection of cardholder data via policies and training
  - Storage of data & access controls
  - Requirements of annual self-assessments and attestation of compliance

PCI at Appalachian

- All departments must get approval from the PCI Compliance Committee to accept Credit cards as a payment option.
- Approval is only given to departments that meet Payment Card Industry Data Security Standards, attend training and comply with University PCI policies, NCOSC Electronic Commerce Policies and State Cash Management Law.
- Policy is located on the Controller's Webpage

State Requirements

- As a prerequisite for participating under the MSA, Appalachian State University is required to comply with all card association rules.
- This includes the rules pertaining to the PCI Data Security Standard and the completion of the annual self assessment and attestation of compliance.
- The Office of the State Controller (OSC) has oversight for the MSA (Master Service Agreement) for all state agencies,

Campus Operating Policies Highlights

- Departments:
  - Must have approval to become a credit card merchant
  - Must utilize the State's contract for credit card processing
  - Must utilize the State's approved payment gateways (internet transactions only)
  - Must be compliant with the Payment Card Industry (PCI) Data Security Standards
  - Must be responsible for all fees, fines and penalties

Processing over the web:

- A department planning to allow its customers to use credit cards over the web will be responsible for designing the departmental website. This website will serve as the "window" to the approved gateway.

- Credit card information must not be stored directly on the department's webpage nor entered into the website.

- The website and its connection to the approved gateway must be reviewed by the Credit Card Compliance Committee to ensure that it meets Payment Card Industry Data Security Standards

Financial Controls

- When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited to the same credit card account from which the purchase was made.
- All transactions must be settled and recorded daily in the University's financial system via proper reporting to The Cashier's Office.

Financial Controls

□ The merchant’s copy of the receipt may or may not contain the full card number and expiration date, and should only contain the full number and expiration date if there is a business reason for doing so.

□ The merchant copy of the receipts must be kept in a secure place (i.e. locked cabinet with minimal access) for no more than 90 days.

□ At the end of 90 days, the receipts should be destroyed in a secure manner, via cross cut shearer.

Financial Controls

- Departments must assure that all university computers have installed the most recent updated versions of the University recommended antivirus, spyware detection software and other recommended security software.

- All general purpose (desktop) computers that handle credit card data must run an approved university build and be configured as a “sensitive data” workstation. Exceptions to this policy must be documented with compensating controls to replace the protections provided by the university build and “sensitive data” workstation configuration.

Reporting Requirements

- Departments must report any actual or suspected security incident in which cardholder information may have been compromised.
- The incident should be reported to Credit Card Compliance Committee and the University Controller.

Reporting Requirements

- If the incident involved the loss or suspected compromise of stored or processed electronic data, it must also be reported to the IT Security Officer.
- **THIS MUST BE DONE IMMEDIATELY. The University must report all breaches to the State Controller's Office within 24 HOURS OF DECTECTION.**

Key Data Control Items:

Under no circumstances should a department store sensitive authentication data (track data from the magnetic stripe, card-validation code CVV2 data,) after authorization (not even if encrypted).

Data Controls:

- Never send or request cardholder information to be sent via email.
- Departmental forms (web and mail order forms) should be designed so that credit card information can be easily and completely removed from the registration information.
- Departments should never request the CVV2 code on departmental forms.
- Once the credit card has been processed, this information must be destroyed immediately.
- Websites and forms should state that credit card information should never be emailed to the department.

Data Controls

- Customer records located within a department should be stored only if there is a documented business need and in a locked non-portable cabinet dedicated solely to these records.

- The Controller's Office will approve each department's business need, a proper retention schedule and method of disposing or deleting sensitive card holder information.

Data Controls

- Access to these records should be limited to only those employees who need this information to preformed approved duties.

- Under no circumstances should a department retain electronically (including Excel files, thumb drives, shadow data bases, etc.) the card numbers and expiration dates of the customer credit cards.

Data Controls

- Make sure all access to storage areas is secure and that all visitors are authorized to enter areas that cardholder data is processed or maintained.

- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

Data Controls

□ Do not use wireless PCs for processing credit card data unless approved in writing by the Credit Card Compliance Committee.

□ All personnel who have direct access to credit card information are required to attend the PCI Security Training and have access to the University Credit Card Policy.

Data Controls

- All credit card information temporarily recorded on paper should be processed immediately and then the paper document should be properly destroyed.

Data Controls

- The customer copy of the credit card receipt can only contain the last 4 digits of the credit card number. It is required that departments use double truncation which permits only the last 4 digits to be printed on both the merchant and customer receipt.

Data Controls

- Never send credit card information to the University Archives. Receipts should be destroyed via cross cut shredder immediately after the approved business need has expired.
- All general purpose (desktop) computers that handle credit card data must run an approved university build and be configured as a "sensitive data" workstation

For more information:

- www.pcisecuritystandards.org
- Appalachian State University Credit Card Policy
- Communication Policy for Security Breach for Credit Card Information and Other Identifying Information
- Appalachian Identify Theft Prevention Program Policy
- Self-Assessment Questionnaires
- Credit Card Compliance Committee x6119