Payment Card Industry Data Security Standard (PCI DSS) Training Program

Center for Student Business
2022-2023

TOPICS

- Compliance
- What is PCI-DSS
- What aspects of PCI-DSS apply to my student business
- Annual self assessment
- Incident response

COMPLIANCE

Compliance with PCI DSS

- There are three things to understand about PCI DSS:
  - Standards are not optional
  - If you accept payment cards on campus, you are subject to the standards
  - There are significant financial costs to non-compliance.

- Failure to comply with PCI DSS can result in stiff contractual penalties or sanctions 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

- Additional costs could include
  - Cost of notification to affected customers
  - Cost of credit monitoring to affected customers

It only takes one incident of data compromise to put the University at risk

WHAT IS PCI-DSS

PCI Standards

- PCI DSS covers security of the environments that store, process or transmit account data
- Many other standards governing software, devices, payment processors, card issuers.

Who does PCI DSS apply to?

- Anyone who accepts credit cards
- UMASS Merchants must be PCI DSS compliant and are responsible for ensuring their compliance:
  - The program applies to all payment channels, including: in person (Point of Sale), mail / telephone order and/or e-commerce.

Why is this training important?

- This training provides knowledge and skills necessary to ensure credit card security at the university
- Everyone, not just the credit card companies, benefits from the effective application of credit card security measures
- Failure to comply with Campus policy can result in the suspension of your ability to take credit cards. This training give you the background and expectations for a merchant.

What is PCI SSC?

- PCI Security Standards Council (PCI SSC) was created in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in governance and execution of the Council's work. The PCI SSC acts as an independent standards body to provide oversight of the development and management of payment Card Industry Security Standards on a global basis
- Standards are reviewed, updated and pushed out in a three year cycle. New set of standards will be released in 2022

Merchant Levels and Compliance Validation

Level	Merchant Criteria	Validation Requirements
1	**Merchants processing over 6 million Visa transactions annually**	▪ **Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA)** ▪ **Quarterly network scan by Approved Scanning Vendor (ASV)** ▪ **Attestation of Compliance Form**
2	Merchants processing 1 million to 6 million Visa transactions annually	▪ Annual Self-Assessment Questionnaire (SAQ) ▪ Quarterly network scan by ASV ▪ Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million visa e-commerce transactions annually	▪ Annual SAQ ▪ Quarterly network scan by ASV if applicable ▪ Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually	▪ Annual SAQ recommended ▪ Quarterly network scan by ASV if applicable ▪ Compliance validation requirements set by acquirer

As one individual merchant you fall at level 4, however our bank looks at us as one entity and therefore the entire Umass system Falls under Level 1 for reporting. This includes an audit each year on each campus. Random 15 to 20 locations chosen

12 Standards

PCI DSS Requirements – High Level Overview
Build and maintain a secure network and Systems 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program 5 Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures 7 Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy 12. Maintain a policy that addresses Information security for all personnel

PCI DSS Standards Requirements – how does it apply to my business?

Requirement 3: Protect stored cardholder data

- Writing down a credit card number is NEVER allowed. If a customer's card does not work, then the customer cannot purchase anything.
- The credit card terminals should only ever print the last 4 digits of the customer credit card number. This is acceptable for receipts and reports out of the terminal.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- Your credit card terminals encrypt all credit card data when you swipe or use the chip
- Do not ever send credit card numbers via email or other messaging. If you receive a credit card number via email, immediately delete it, delete it from trash and let the business office know and email pci@admin.umass.edu.
    - Do not include the credit card number in the notification or forward the email. You may print the email and redact the cc number by blacking it out, photocopying and shredding the original.

Requirement 7: Restrict access to cardholder data by business need to know

- Only trained cashiers should handle credit cards from customers

PCI DSS Standards Requirements – how does it apply to my business?

Requirement 9: Restrict physical access to cardholder data

- All credit card media are classified, secured, and logged when touched or moved. If you are adhering to #3, you should not need to classify, secure and log media. Media are paper or electronic records with credit card data on them.
- Document, and keep in a safe place, a list of all your POS terminals, the make, model number and serial number
- You must submit this list each year in the spring with your self assessment questionnaire (see slide 10)
- Secure the terminals when not in use.
- Inspect the POS terminals for tampering every day and TRAIN ALL STAFF ON HOW TO INSPECT
    - Wires sticking out of the terminal
    - New cables plugged into the device
    - Broken casings or other external markings, change in color of the terminal
    - Skimmers attached
        - Chip card should not go all the way in
        - Terminal casing looks larger than it did
    - Change in the serial number of the machine – check and verify this on a regular basis – recommend monthly as a formal process.
    - Keep a log of daily inspections – make it part of your opening routine.
        - Date, Initials of who inspected
        - If selected for the annual audit, the auditor will need to review your log
- Verify the identity of anyone claiming to be repair or maintenance – if you are not comfortable, refuse access and notify the business office and pci@admin.umass.edu
- The bank will never cold call you to tell you to do a download to repair or update your machine. If you get one of these calls, notify the business office and pci@admin.umass.edu
- Do not let anyone near the POS terminal unless you know they are a business employee and have been trained

PCI DSS Standards Requirements – how does it apply to my business?

Some skimmer examples (credit – Ingenico)

PCI DSS Standards Requirements – how does it apply to my business?

Requirement 12: Maintain a policy that addresses information security for all personnel.

- Amherst campus credit card policy http://www.umass.edu/afsystems/sites/default/files/resources/Department_CC_Policy.pdf
- Keep a list of all devices (see requirement 9) and a list of everyone who has access to them
- Training required upon hire and annually.

- **Incident response – IF YOU NEED TO REPORT SOMETHING please notify the business office and email pci@admin.umass.edu**
    - **If this is an emergency or a situation that needs to be escalated, please call 413-545-2119 and speak with Patty Roper or Jacqui Watrous.**
- Bank contact information – Banks help lines are open 24/7 and which one you call depends on your terminal.
    - Bank of America terminal (models FDxxx) 800-430-7161
    - Vantiv/WorldPay terminal (ingenico devices) 888-750-6290

Annual requirement – Self Assessment Questionnaire B submission

Each year in the spring we are required to have every merchant fill out and submit a 'self assessment questionnaire' concerning your use of credit cards. If even one merchant fails to submit this form, it puts the entire University system out of compliance so the remediation is usually to take away the ability to take credit cards. If even one merchant is out of compliance with a piece of the SAQ, it puts the entire University system out of compliance.

When you submit the SAQ form, you will be required to send a list of your POS terminals, model and serial number

Please identify who the contact person will be for the SAQ at the end of the training. This person will be the contact for a PCI messages for the academic year.

PCI DSS Standards Requirements –

Questions?

Resources:

eCommerce Manager – Patty Roper
150 Whitmore
545-2119
roper@admin.umass.edu

pci@admin.umass.edu – email address for multiple people on campus for eCommerce questions or to report issues
itprotect@umass.edu. – this email can also be contacted to report issues.

This presentation will be posted at http://www.umass.edu/afsystems/ecommerce

PCI DSS Terminology

Approved Scanning Vendor (ASV) - is a vulnerability assessment provider who provides automated software tools for scanning for vulnerabilities.

Cardholder - Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Cardholder Data - At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Internal Security Assessor (ISA) - The ISA Program provides eligible internal security audit professionals PCI DSS training and certification that will improve the organization's understanding of the PCI DSS, facilitate interactions with QSAs, enhance the quality, reliability, and consistency of PCI DSS self-assessments, and support consistent and proper application of PCI DSS measures and controls.

The Payment Application-Data Security Standard (PA-DSS) - A global security standard created by the Payment Card Industry Security Standards Council, or PCI SSC, formed by the major credit-issuing companies with the goal of delivering an effective and useful data security standard to vendors of payment application systems. The intent of this standard is to effectively prohibit secure data from being illegally accessed by unauthorized parties.

Payment processor - An organization that processes payment requests, such as credit card authorizations and settlements, to the appropriate card associations per their guidelines. Your merchant bank's processor relationship determines which payment processor you will use.

Payment gateway - An organization, such as CyberSource, that enables merchants to securely send and receive order information to and from payment processors in the appropriate format.

PCI Compliant - refers to an organization that has become compliant with the PCI DSS and has demonstrated this either through a Self Assessment Questionnaire or through formal validation (audit) by a QSA firm.

PCI DSS - Data Security Standard – a document consisting of 12 requirements and various principles all designed to provide a framework to protect payment card data and systems.

PCI SSC – Security Standards Council - the global governing body for payment card security standards. Responsible for developing, managing, education, and awareness of the PCI Security Standards including Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements.

Primary Account Number (PAN) - is essentially a payment card number (16 – 19 digit) which is generated according to the LUHNS algorithm).

Qualified Security Assessor (QSA) – is a Information Security and PCI expert who works for a QSA firm and who has been certified by the PCI SSC to be fit and proper to validate whether a company / environment is PCI compliance

Report on Compliance (ROC) - the report on compliance refers to a report that shows that an environment has been validated by a QSA in accordance with the PCI DSS. The outcome of the validation assessment may result in a Report of Compliance opinion of Compliant or Not Compliant depending the evidence provided to support the compliance assertions provided by the merchant or service provider to the QSA

Self-Assessment Questionnaire (SAQ) – A validation tool for merchants and service providers that are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures. The purpose of the SAQ is to assist organizations in self-evaluating compliance with the PCI DSS, and you may be required to share it with your acquiring bank. There are multiple versions of the PCI DSS SAQ to meet various business scenarios.

Service Provider - An entity that stores, processes or transmits cardholder data on behalf of merchants. Examples of service providers include hosting and payment services for merchants. Such providers do not have direct service provider contractual relationships with acquiring institutions, other than for their own merchant activities, but nonetheless still fall into scope for the PCI DSS where they store, process or transmit payment cards on behalf of merchants. It is the merchant responsibility to ensure the service providers operate in a way that is complaint with the PCI DSS.

Validation / Audit - refers to the final stage of PCI compliance whereby a Qualified Security Assessor (QSA) will validate and attest the compliance status of the environment under assessment for compliance with the PCI DSS.

Vulnerability Assessment – is a technical security audit that uses automated tools to test for security flaws, mis-configurations and weaknesses in infrastructure and applications (to a relatively limited extent).

Useful PCI DSS References

PCI Security Standards Council https://www.pcisecuritystandards.org/

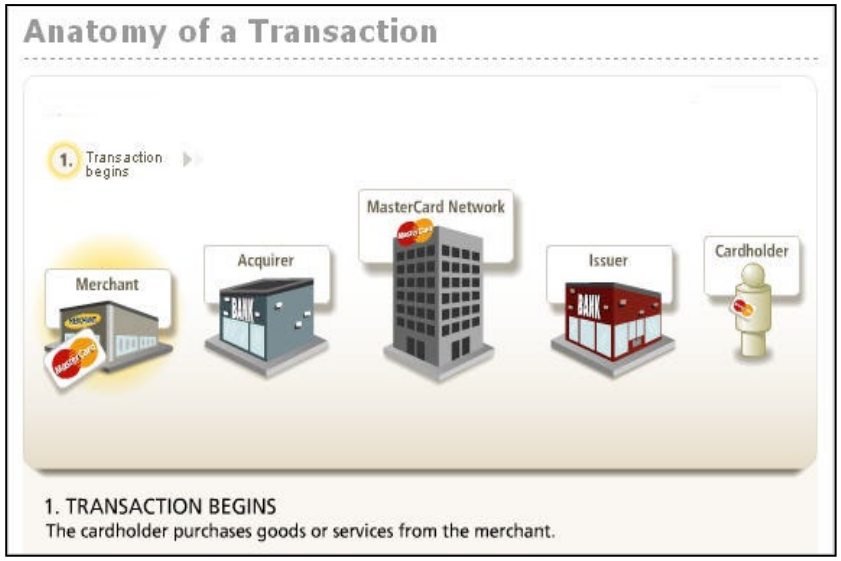
PCI Security Standards Council educational resources https://www.pcisecuritystandards.org/pci_security/educational_resources

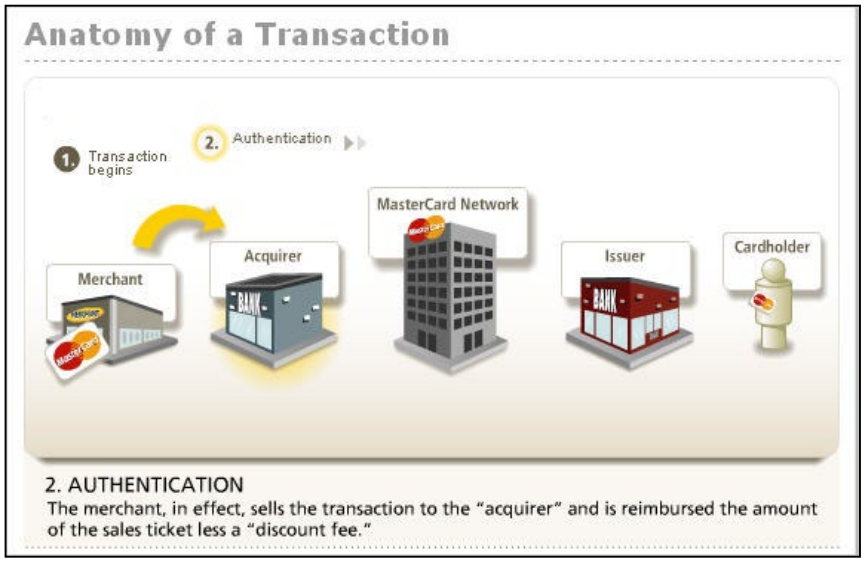
Skimming resource guide https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Skimming%20Resource%20Guide-v05.pdf

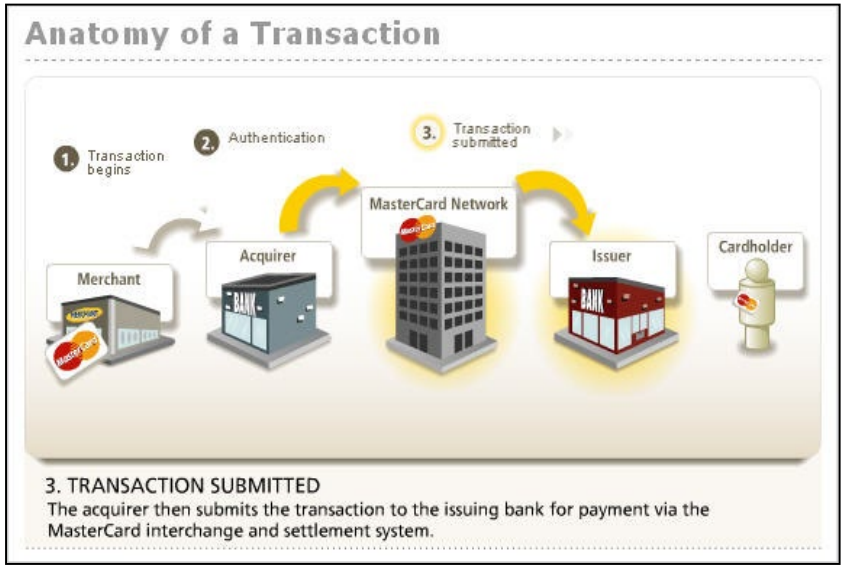
Amherst Campus credit card resources http://www.umass.edu/afsystems/ecommerce

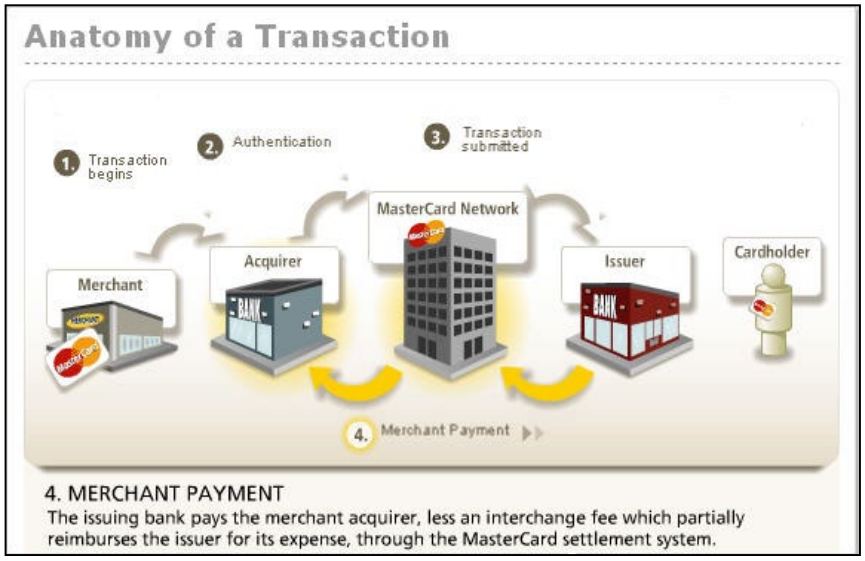
Amherst campus credit card policy http://www.umass.edu/afsystems/sites/default/files/resources/Department_CC_Policy.pdf

How Payment Processing Works (Technical Process)









Source: MasterCard.com