University at Buffalo
The State University of New York

Securing Credit Card Data at UB

(complying with Payment Card Industry Data Security Standards)

Carolann Lazarus
Internal Audit
PCI Compliance Initiative Co-lead
lazarus@buffalo.edu
(716) 829-6947

Tricia Canty
Financial Management
Internal Control Coordinator
tscanty@buffalo.edu
(716) 645-2639

PCI Security Standards Council™

University at Buffalo
The State University of New York

Whole Foods Hit By Hackers.

Sonic latest company to face a cybersecurity breach.

Target to Pay $18.5 Million to 47 States in Security Breach Settlement

University of Connecticut Hack Exposed Students' Credit Cards, SSNs

CYBERATTACK 101: WHY HACKERS ARE GOING AFTER UNIVERSITIES

University at Buffalo
The State University of New York

"Data Breaches Put a Dent in Colleges' Finances as Well as Reputations"

The costs of a breach can run into the millions of dollars, according to data-security professionals who work in higher education.

The list of potential expenses is long. It includes forensics consultants, call centers, websites, mailings, identity-protection and credit-check services, and litigation. Breaches can prompt major campus projects, such as risk-management reviews, campus wide encryption, and tests to determine how vulnerable networks are.

University at Buffalo
The State University of New York

- If cardholder data was stolen, would donations to the university decline?
- Would ticket sales decline if fans were concerned about purchasing tickets online?
- Would we attract quality researchers?
- Do you want to be the department that is referred to for decades as the area that allowed a breach?

University at Buffalo
The State University of New York

Agenda

- PCI DSS Overview
- Why Comply?
- Do's and Don't's
- PCI DSS Compliance at UB
- Payment Methods
- Incident Reporting
- Protecting Your Card
- UB Resources / Contacts
- Questions

University at Buffalo
The State University of New York

PCI DSS Overview

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

Started with VISA in 2001.
Incorporated into the PCI DSS in 2004 with the 6 major card brands.

Not a government regulation or law.

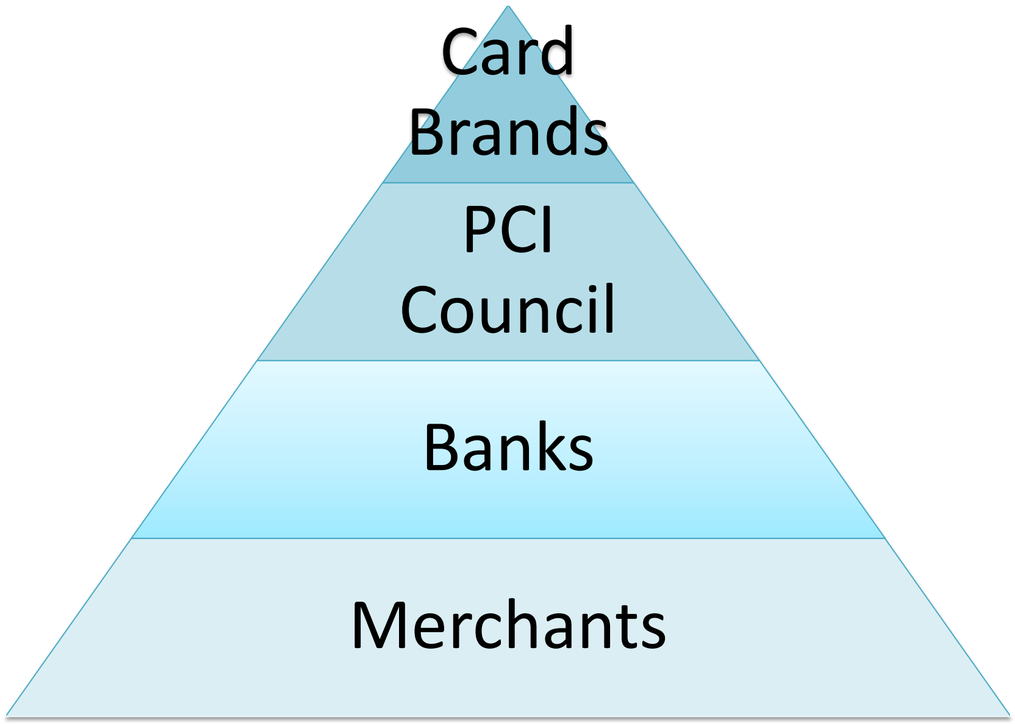
University at Buffalo
The State University of New York

PCI DSS Overview

COMPLIANCE PLAYERS

- ✓ **Card Brands** set compliance rules and penalties
- ✓ **PCI Council** defines standards and certifies assessors
- ✓ **Banks** enforce compliance
- ✓ **Merchants (UB) and Service Providers (ePay)** must be compliant

PCI Security Standards Council™



University at Buffalo
The State University of New York

PCI DSS Overview

PCI-DSS - Six Goals and Twelve Requirements that breakdown into 200+ total specific requirements (only a subset apply to some transaction processes)

Applies to all merchants (UB) and service providers (ePay), regardless of size

Updated annually, major update every three years

All merchants must annually self-assess compliance – SAQ’s

University at Buffalo
The State University of New York

PCI DSS Overview

6 Goals and 12 Requirements of the PCI DSS

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	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. Use 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. Assign a unique ID to each person with computer access 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 employees and contractors

Depending on the method used to accept credit card payments, some of these requirements may not be applicable. For example, only a few apply to a department that uses a credit card terminal connected to an analog or cellular phone line to process credit card payments.

University at Buffalo
The State University of New York

Do's and Don'ts

If you receive an email with credit card information from a customer:

- **Reply. (delete the cardholder data)**
- **Let the customer know that policy prohibits the use of email for credit card payments because it is not secure, and that you have deleted their cardholder data.**
- **Indicate the acceptable ways to make a payment.**
- **Permanently delete the email containing the cardholder data.**

University at Buffalo
The State University of New York

Do's and Don'ts

Don't accept or send cardholder data by:

- Email
- Scan
- Copy/PDF
- Voicemail
- Fax

Do encourage online payments, but **Don't** enter cardholder data online for the customer.

Do process payments when the customer gives their credit card information. If you must send the payment information to another location to be processed, it must be stored securely and transported in locked bags.

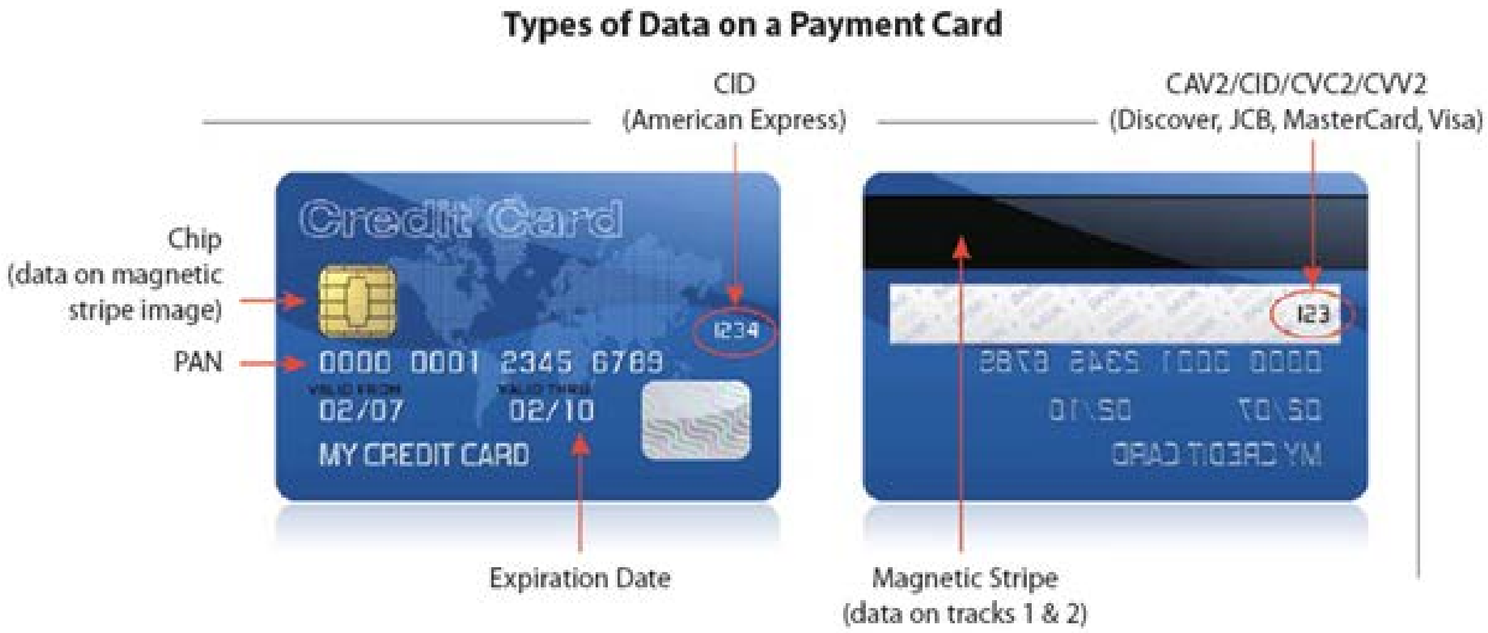
Do immediately dispose of any record with cardholder data after the payment is processed. This includes forms received through the mail. Blacking out the number is not compliant.

Do use an approved disposal method such as a cross-cut shredder or a locked destruction bin.

Don't store the full cardholder account number, either electronically or hardcopy. (only the 1st six or last 4 digits)

University at Buffalo
The State University of New York

Do’s and Don’ts



What is cardholder data?

- Primary Account Number (PAN)
- Cardholder name
- Expiration date

.

What is sensitive authentication data?

- Magnetic stripe
- CAV2/CID/CVC2/CVV2
- PIN

Sensitive authentication data can never be stored for any reason.

University at Buffalo
The State University of New York

Do's and Don'ts

Storage of 1st 6 digits/ last 4 digits is permitted

	Data Element	Storage Permitted	Protection Required
Cardholder Data	PAN	Yes	Yes
	Cardholder name	Yes	No
	Service code	Yes	No
	Expiration date	Yes	No
Sesitive Authentication Data	Magnetic stripe	No	No storage permitted
	CVC2/CVV2/CID	No	No storage permitted
	PIN/PIN block	No	No storage permitted

Only considered CHD if full PAN stored

PAN – Primary account number

If the full PAN is stored, your department is categorized as the riskiest type of merchant and must meet over 200 PCI compliance requirements, including the fact that the PAN must be unreadable.

University at Buffalo
The State University of New York

Compliance at UB

PCI Compliance Initiative

- January 2017 – this is a re-boot
- Co-Sponsored by the Controller and the Director of Internal Audit
- Goal – to improve UB's compliance now and going forward.

Financial Management

- Work with department/units to determine the most appropriate method to accept payment for goods, services, donations.
- Manage completion of required annual PCI self-assessments (SAQ's)
- Develop and Coordinate training

University at Buffalo
The State University of New York

Compliance at UB

Departments

- Complete the required annual PCI Training through Financial Management
- Complete the course – “Information Security: Everyone’s Responsibility”
- Consult with Financial Management prior to accepting payment cards as a form of payment for goods and services.
- Review and comply with the following university policies:
  - ✓ Credit/Debit Card Merchant Requirements Policy
  - ✓ Safeguarding Cash and Cash Equivalents
  - ✓ Password Protection Policy
  - ✓ Protection of Regulated Private Data
- Develop and maintain procedures for accepting credit cards

University at Buffalo
The State University of New York

Compliance at UB

UB Information Technology (UBIT)

- Maintain security standards as required by PCI DSS
- Keep current with PCI DSS regulations and make changes to systems and processes as appropriate
- Consult on technical PCI DSS issues
- Assist when there are incidents and data breaches
- Assist with mandatory annual training sessions

University at Buffalo
The State University of New York

Compliance at UB

WHY?

- Failure to certify compliance can result in fines, penalties, forensic costs, card replacement costs, customer notification costs, and loss of privilege to accept credit cards.
- A breach of credit card information damages UB's reputation and brand.
- PCI Standards apply to all types of payments including in-person, telephone, and web transactions.
- PCI compliance is mandatory if you accept credit card payments.

WHY?

University at Buffalo
The State University of New York

Compliance at UB

The University needs your help in limiting potential losses, fines & penalties.

Knowledgeable staff are our best defense.

We want everyone to treat customer data as they would treat their own.

University at Buffalo
The State University of New York

Payment Methods

CUSTOMER

Web-based “shopping cart”

↓

Payment Gateway -

Nelnet (ePay)/Authorize.net

↓

Acquiring Bank

KeyBank

Web-based is the preferred method to accept credit cards at UB

University at Buffalo
The State University of New York

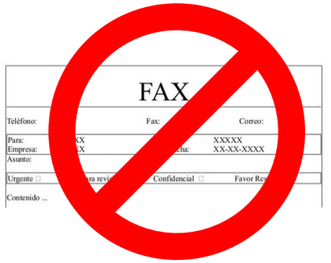
Payment Methods

CARD_IN_HAND

PHONE

eMAIL

MAIL



FAX

Acquiring Bank

KeyBank

University at Buffalo
The State University of New York

Payment Methods

Credit Card Alternative – Campus Cash

- No PCI requirements – standard best practices for security
- Campus Cash (students) and Flexibull Bucks (faculty/staff)
- All members of the University Community have these available “on” their card
- Add funds via web or app (iOS and Android) using a credit card.
- “Stored Value & Credit (SVC)” accounts
- EZ Pay web application available to accept SVC payments

University at Buffalo
The State University of New York

Incident Reporting

Any suspected or confirmed exposure of regulated private data, which includes credit card data, or security breach of a system containing such protected data must be reported immediately to the Information Security Officer sec-office@buffalo.edu

Suspicious transaction?? Don’t put yourself at risk. If the card is denied, request they use a different card. If the transaction seems irregular, let your supervisor know. Do not attempt to confiscate the card.

University at Buffalo
The State University of New York

Protecting Your Card

Card Safety Tips:

- If you have a pin associated with your card, do not store it in the same place.
- Never answer an email or text that asks for your account number or personal information.
- Don’t give your card information over the phone unless you initiated the call and you’re talking to a trusted bank or merchant.
- If there is a line for tips or gratuities on your receipt, draw a line through it so additional amounts can’t be added.
- Check your account often. It’s not “if” but “when”.
- Don’t give your social security number to your healthcare providers.

University at Buffalo
The State University of New York

Resources

Policies & Procedures

UB Credit/Debit Card Merchant Requirements

http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/credit-debit-card-merchant-reqs.html This policy also lists UB related links, including Data Protection, and external links, including PCI and VISA Security.

Safeguarding Cash and Cash Equivalents

http://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/safeguarding-cash1.html

Future:

PCI Compliance Policy – in process, anticipated midyear 2018

Credit Card Processing Procedures – Department template, anticipated late 2018

University at Buffalo
The State University of New York

Contacts

Contact Information

Financial Management
Phone: 716-645-2660
http://buffalo.edu/finances
Tricia Canty Email: tscanty@buffalo.edu

Information Security Office
Phone: 716-645-7979
Email: sec-office@buffalo.edu
Jeff Murphy Email: jcmurphy@buffalo.edu

University at Buffalo Foundation
Phone: 716-645-3013
Chris Decker Email: cdecker@buffalo.edu

UB Card
Phone: 716-645-5172
Martha McILroy Email: mn1@buffalo.edu

PCI Compliance Initiative
Carolann Lazarus
Email: lazarus@buffalo.edu
Phone: 716-829-6947

Keith Curtachio
Email: knc@buffalo.edu
Phone: 716-645-0366

University at Buffalo
The State University of New York

Recap

- ✓PCI-DSS has lots of detailed specifics under a common-sense set of categories
- ✓UB is updating it’s PCI compliance program
- ✓Accepting card payments means accepting the responsibilities of addressing security
- ✓UB staff are needed to support compliance
- ✓UB has resources to ease compliance
- ✓PCI incidents need to be reported

University at Buffalo
The State University of New York

Questions