Treasury Institute for Higher Education

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

PCI Compliance and Trends in Higher Education Payments

FIN 2242

James Lock, CTP
Managing Director
National Nonprofit Treasury Strategy Leader & NGO Treasury Specialist
J.P. Morgan Chase & Co

Kevin Sisler, CTP
Director of Treasury Services
University Financial Services
University of Kentucky

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS

UK Auxiliary Services

Treasury Institute for Higher Education

Mission

The mission of the Institute is to provide superior-quality, practitioner-driven content within the higher education treasury and finance community by connecting people, ideas, and solutions.

2026 Programs

- Treasury Symposium
- CBMI Treasury Track
- Senior Financial Roundtables

CBMI & TIHE Treasury Track

- Treasury Management (*FIN 2237*)
- Introduction to Capital Finance (*FIN 2232*)
- Advanced Capital Financing (*FIN 2240*)
- PCI Compliance and Trends in Higher Education Payments (*FIN 2242*)
- Fundamentals of Higher Education Investments (*FIN 2235*)
- Current Hot Topics in Risk Management (*BUS 2253*)
- Advanced Insurance & Risk Management (*BUS 2260*)
- Asset Liability Management and Long-Term Planning (*FIN 2250*)
- Advanced Endowment Management (*FIN 2251*)
- Current Issues & Trends in Strategic Treasury Management (*FIN 2248*)

Learning Objectives

Participants will gain an understanding of:

- Learn what is PCI DSS, its origin, and why it is important to comply with the standards.
- Learn about the requirements that make up PCI DSS.
- Students will be presented a “Compliance Roadmap” to help with development of their compliance program.
- Learn about technologies that will enhance the security of card data and reduce the overall scope of PCI DSS compliance.
- Introduction to the new requirements in PCI DSS version 4.0.

The Median Student Age is 26.4 years old

- Born on the cusp of Generation Z and Millennials (Incoming freshman for 2026 school year was born in 2008-2009)
- “Digital Natives” – 11 years old when the iPhone was released
- 65% of the Gen Zers said that they particularly value knowing what is going on around them and being in control[1]
- 99% of Gen Z and 98% of millennials use a mobile banking app for a wide range of tasks[2]

Median Student Age Source: Perception vs. Reality: The Typical College Student
1: True Gen: Generation Z and its implications for companies
2: Millennials and Gen Z are the most likely to use mobile banking apps

Payment expectations of a 26-year-old

- Non-Cash
- Digital (i.e. phone-based)
- Card
- Real Time
- Secure

A Campus is a "City"

1. Athletics
2. Tuition & Fees
3. Housing (Dormitories)
4. Dining (Starbucks!!!)
5. Transportation (e.g., buses)
6. Parking
7. Book Store
8. Administrative Services (e.g., Registrar, Philanthropy)
9. Hospital & Medical Clinics
10. Graduate, Family, & Faculty Housing

Campus Payment Acceptance

For what reasons are payments taken on campus?

- Tuition
- Housing
- Books
- Dining Facilities
- Admissions
- Campus Payment Cards
- Meetings, Seminars, & Conference Registrations
- Gifts/Donations
- Hospital/Medical/Dental Services
- Medical Collections (call center)
- Registrar (e.g., transcripts, diplomas)
- Library Fees & Fines
- Campus Hotel
- Greek Recruitment
- Sale of Goods/Services (i.e. brain probes, geological surveys, state regulated agricultural fee collection, veterinary diagnostic testing, soil testing, campus ID, etc.)
- Wellness Facilities
- Alumni Affairs
- Extension Services (e.g. 4-H Camps, Ag. Clinics)
- Athletic Events
- Theater & Concert tickets

Campus Payment Acceptance

How payments are received

- In-Person
- MOTO (Mail/Telephone)
- Online (eCommerce)
- Unattended Pay Stations (e.g. parking meters)
- EFT (ACH, Wire, RTP, FedNow)

What types of payments

- Cash – Coin/Currency
- Checks/Money Orders
- Credit/Debit Card
  - NFC (Apple Pay, Google Pay)
- EFT (ACH, Wire, RTP)

Digital Payment Networks

Payment	Network Size	Year Established	Receipt of Funds
ACH	All U.S. bank accounts	1974	*Same Day ACH:* Within a few hours Standard ACH: 1-2 business days
PayPal	439 million active accounts	1998	*PayPal account*: Instant *Bank account*: 30 minutes for additional fee or standard 1-3 business days
venmo	90 million active accounts	2009	*Venmo account*: Instant *Bank account*: 30 minutes for additional fee or standard 1-3 business days
RTP	1,135 financial institutions; 75%+ of U.S. DDAs enabled	2017	Within seconds
Zelle	2,300 financial institutions; 80%+ of US check/savings accounts enabled	2017	Within in minutes*
FedNow	1,700 financial institutions	2023	Within seconds

*Enrollment required. Payments may arrive in minutes but may take up to three business days.

Blockchain and Cryptocurrency on Campus

Blockchain: A digital form of record keeping. A virtual ledger (aka, Distributed Ledger). The underlying technology behind cryptocurrencies. The blockchain is decentralized.

Cryptocurrency: A type of currency that is digital and decentralized. A virtual currency. Cryptocurrency can be used as store of value, or to buy and sell things.

Potential Uses on Campus

- Donations
- Campus Payments
- NFTs
- On-chain Transcripts
- Event Ticketing

Bentley University Accepts Crypto for Tuition

https://www.bentley.edu/news/bentley-now-accepting-cryptocurrency-tuition-payments

Treasury Institute for Higher Education – PCI DSS Workshop 2022, “Crypto 101”, presented by Ruth Harpool (CampusGuard) and Preston Dubose (Texas A&M)

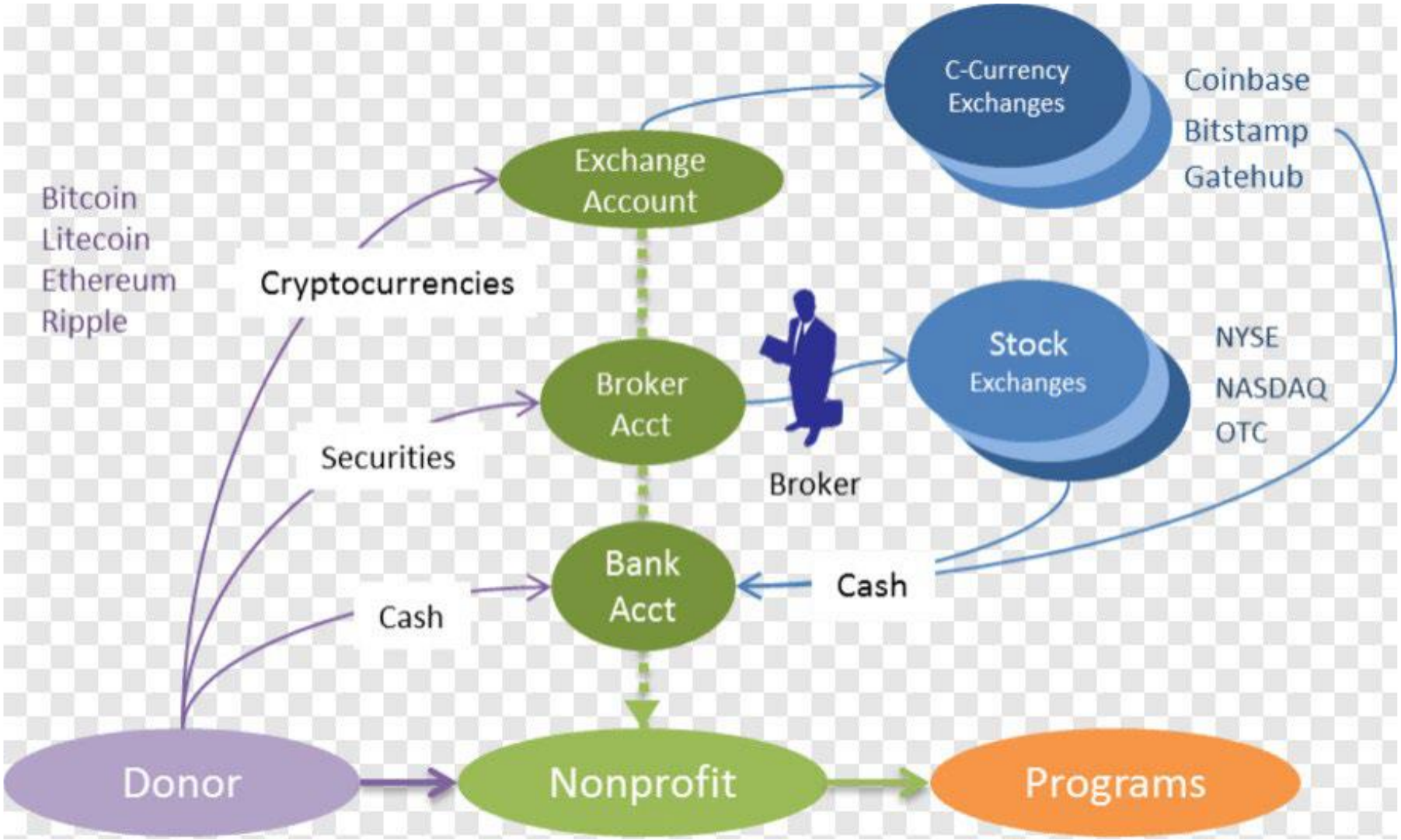
A brief list of pro-crypto U.S. schools and their foundations

Treasury Institute for Higher Education – PCI DSS Workshop 2022, “Crypto 101”, presented by Ruth Harpool (CampusGuard) and Preston Dubose (Texas A&M)

Cryptocurrency Considerations on Campus

- Is crypto a stored value or is it liquid funds?
- Are there crypto regulations?
- Is it a currency, an asset, or a commodity?
- Can the university invest in crypto under the current investment policy?
- Can the university accept cryptocurrency as a donation?
- Which cryptos should we accept?
- Can a university open an exchange account?
- What about IRS reporting and OFAC Compliance?
- Does crypto held in an exchange, does it have FDIC insurance?
- Should the university hold the crypto or immediately convert to USD?
- What if the cryptocurrency is known to be used for *nefarious activity*?
- Should we open an exchange account just in case we need to pay a crypto ransom?
  - How and when would we fund that exchange account?

Treasury Institute for Higher Education – PCI DSS Workshop 2022, "Crypto 101", presented by Ruth Harpool (CampusGuard) and Preston Dubose (Texas A&M)



Treasury Institute for Higher Education – PCI DSS Workshop 2022, "Crypto 101", presented by Ruth Harpool (CampusGuard) and Preston Dubose (Texas A&M)

Open Discussion

1) What are some payment acceptance trends happening on your campus?
    1) Digital Payments
    2) Cash vs Cashless

2) Do you currently have the ability accept cryptocurrency (e.g. Bitcoin) for payment?
    a) For what reason would you need to accept cryptocurrency?
    b) Do you have an exchange relationship already established?
    c) When receiving crypto-payments, do you exchange immediately?

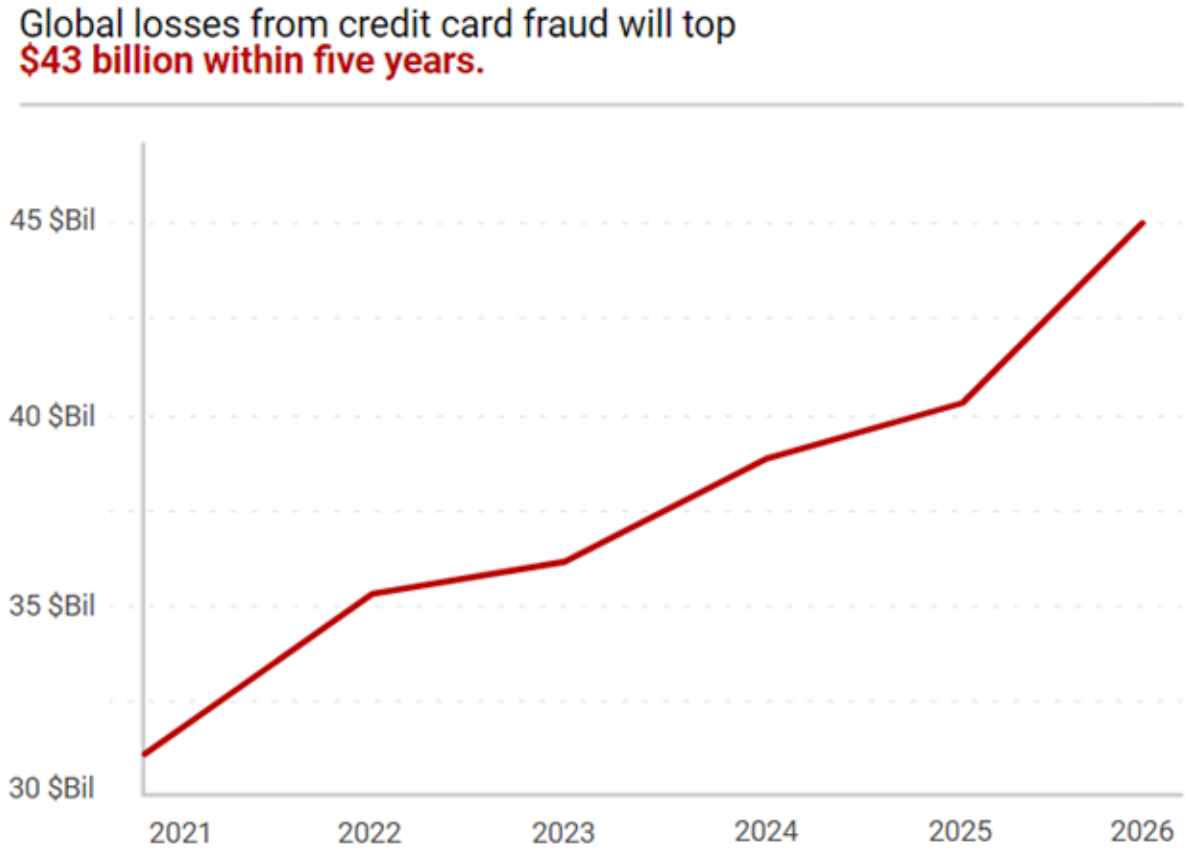
Is it a problem at YOUR school?

Payment Fraud

What is **Payment Fraud?**

Use of stolen banking or credit card information to obtain money or goods.

- Payment information can be stolen via data breaches, phishing, skimmers, lost details, and it can be purchased via the dark web
- According to security.org, 65% of credit card holders have been a victim of fraud at one point in their life
- According to Chargebacks911, leveraging the Nilson Report, credit card fraud will cost merchants and banks over $43 billion dollars from 2021 to 2026



Fraud Statistics

2.6M

fraud cases were reported in 2024

Source: Federal Trade Commission

$12.5B

lost to fraud in 2024

Source: Federal Trade Commission

25%

increase in fraud losses in 2024 over 2023.

Source: Federal Trade Commission

Data Breach Statistics

Average total cost of each data breach

$4.44M

Educational data breaches rank 6th in total cost.

Per-record cost of a data breach

$168

The average cost per record involved in a data breach was $168.

Average time to identify and contain a breach

241 days

In 2024 it took an average of 181 days to identify the breach and 60 days to contain the breach.

Source: Cost of a Data Breach Report 2025, Ponemon Institute

Ransomware Survey Results

EDSCOOP Topics Events Podcasts Videos Insig

CYBERSECURITY

All colleges hit by ransomware got data back, says survey

A global survey of 200 higher education institutions found that 100% of colleges were able to restore their data following a ransomware attack.

BY EDSCOOP STAFF • AUGUST 4, 2023

(Getty Images)

A global survey of 200 higher education institutions found that 100% of colleges were able to restore their data following a ransomware attack.

The survey, published last week by the British cybersecurity firm Sophos, reported that rates of ransomware attacks are increasing among higher education institutions, with 44% of respondents reporting attacks in 2021, 64% reporting attacks in 2022, and 79% reporting attacks this year.

Of the 200 schools reporting ransomware attacks, **100% said they got their data back**

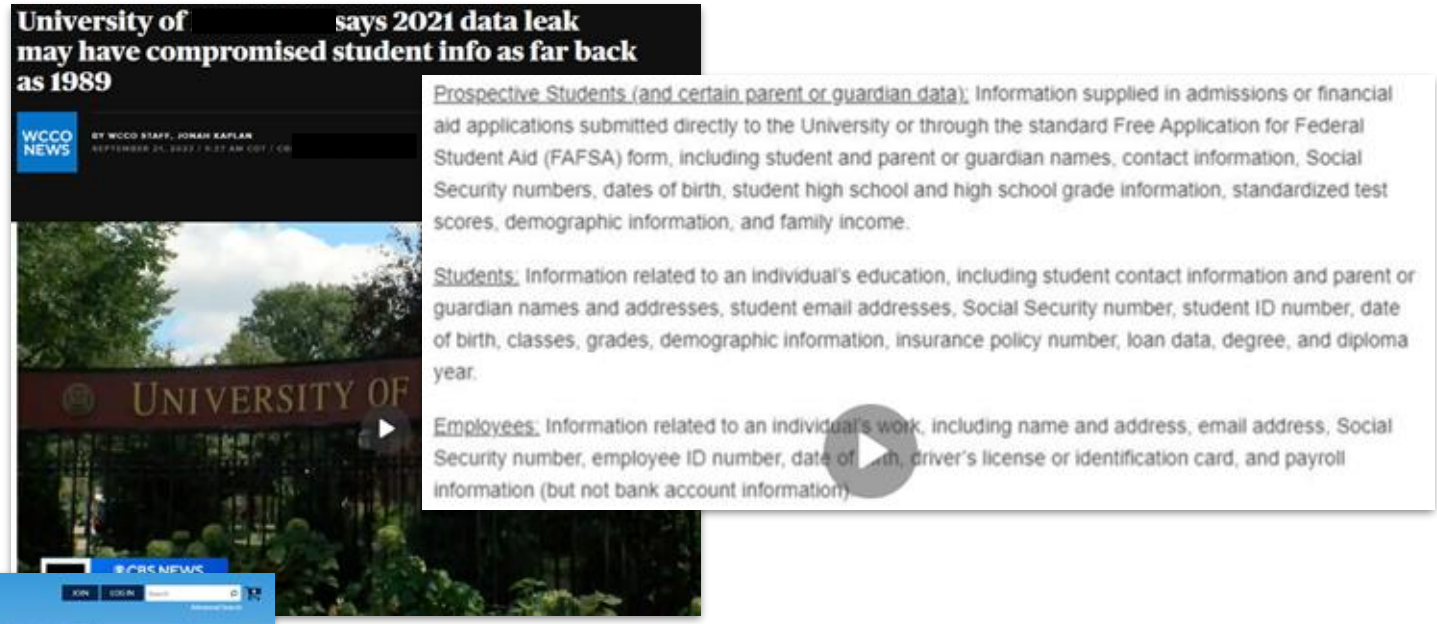
The **average cost of recovering data in 2023 was $1.06 million** among higher education institutions

The FBI recently helped bring down one of the most successful cyber gangs

https://edscoop.com/ransomware-colleges-universities-data/

Notable Recent 3rd-Party Higher Ed Breaches

MOVEit Transfer solution used by a major HE provider, 900 Schools impacted.



DOE - 800,000 Records

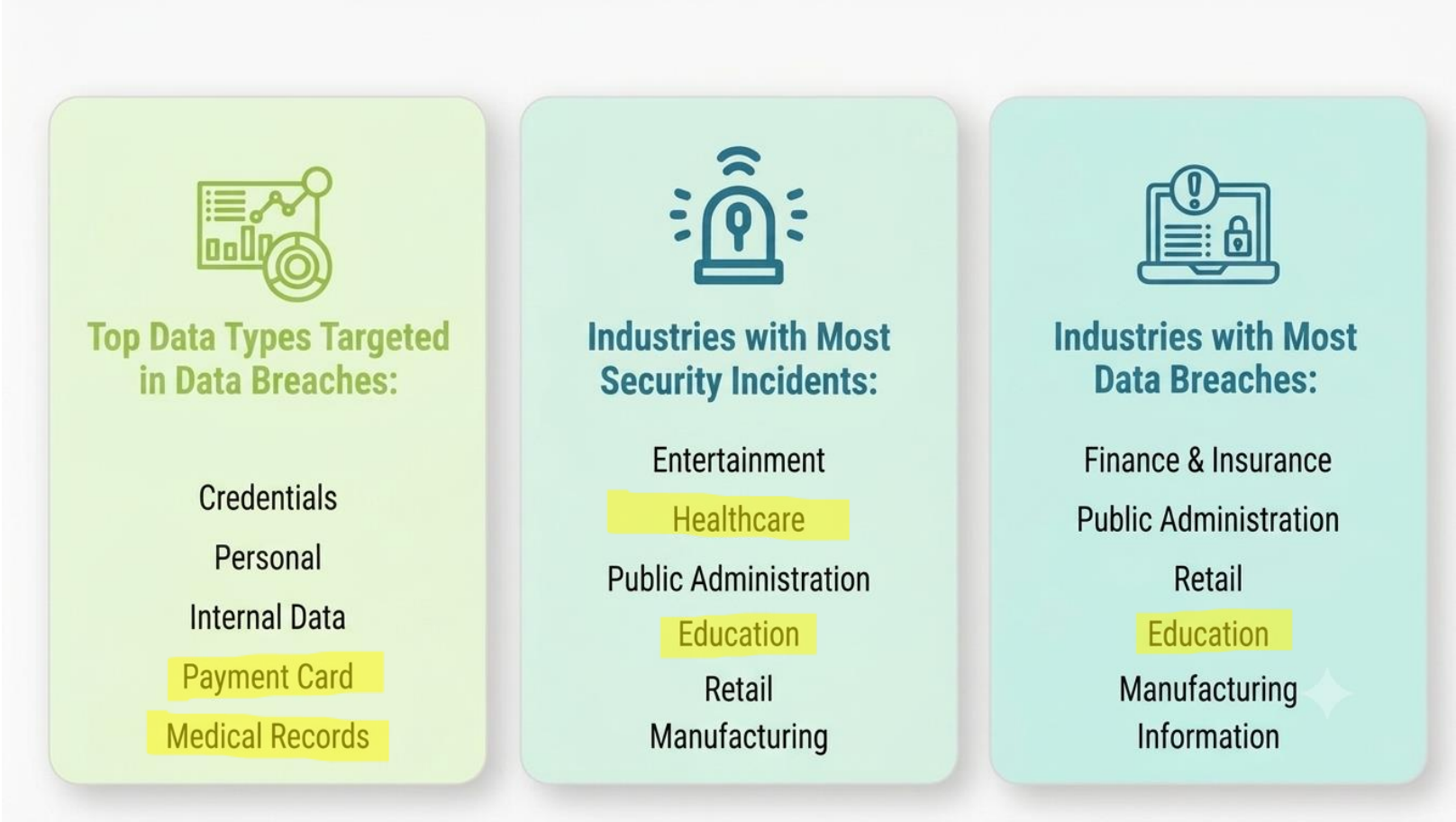
2.5 million **Loan Servicing** Records

FAFSA related - 2 million SS#, Drivers License #, Employee ID's, Student ID's, Data of Birth, Family Income, Grades, Loan Data, Emails, Parent/Guardian Data, etc.

Treasury Institute for Higher Education

Breach Data from 2025

According to the 2025 Verizon Data Breach Investigations Report:



Educational Institutions are Hacker Targets…

According to the 2024 Verizon Data Breach Investigations Report, the **higher education industry ranked 5th** in total number of data security incidents in 2023 with 1780 cases.

Bursar's Athletics Development Dining

"Why do hackers like school systems? Because the education sector, particularly at the college and university level, is a virtual buffet of valuable data." Jason Glassberg, Casaba Security

Fraud Around Campus

Common Types

- Admissions
- Academic
- Purchasing
- Financial Aid
- **Payment**

Payments

Payments coming in

Payments going out

Credit/debit cards, ACH, International Payments, Payment Alternatives

Friendly Fraud

Card Acceptance, Security, and PCI DSS

It's about **Security**, not Compliance!

Payment Card Usage

Payment Card Usage

According to the Federal Reserve, 82% of U.S. adults had a credit card in 2022. About 73% of Americans have a credit card by age 25, making credit cards the most common first credit experience for young adults.

(Source: “Credit Card Statistics And Trends 2024”, Forbes Advisor, March 2024)

Payment Card Usage

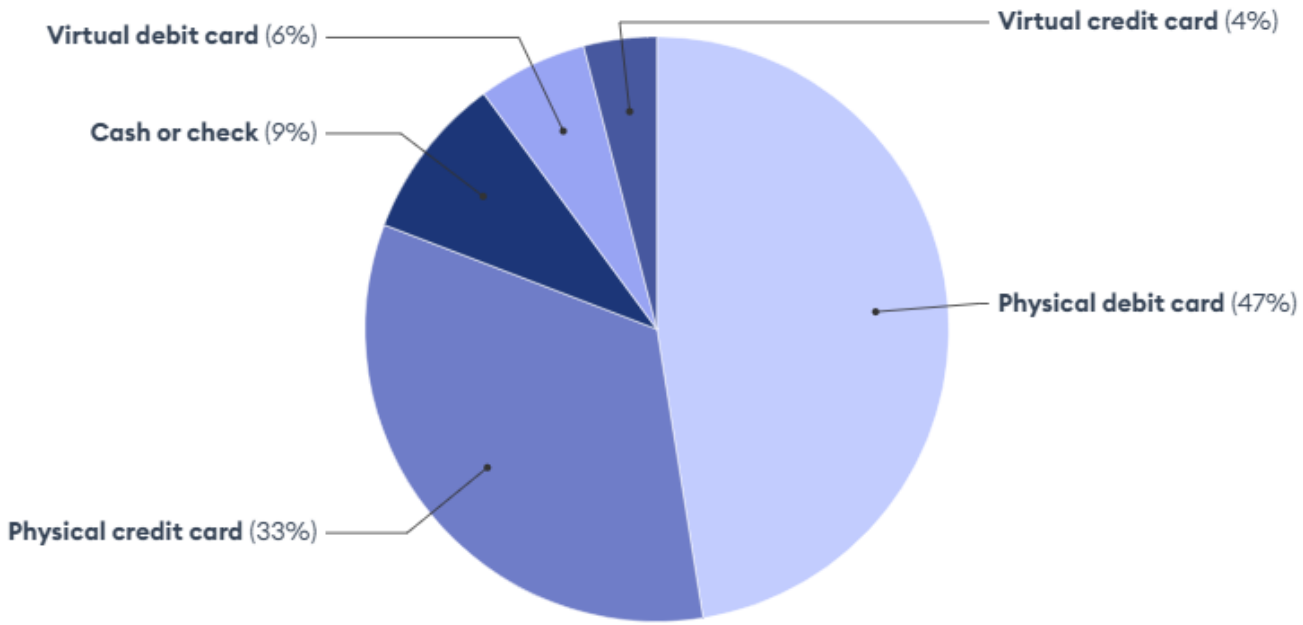
Debit cards and credit cards are the primary payment method used, with 53% of consumers using a physical or virtual debit card and 37% using a physical or virtual credit card.

(Source: Forbes Advisor OnePoll Survey: December 2023

Payment Card Usage

How Do Consumers Typically Pay for Purchases?

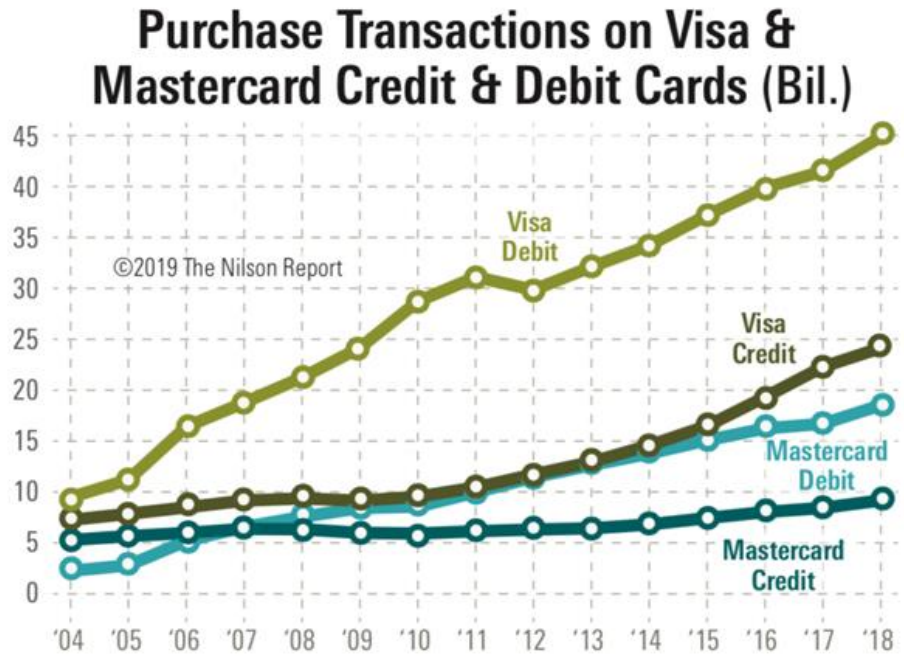
Forbes Advisor asked respondents with a bank account how they primarily pay for their purchases.



(Source: Forbes Advisor OnePoll Survey: December 2023

Payment Card Usage

In 2018, **VISA and MasterCard credit & debit cards accounted for 69.3%** of worldwide purchase transactions.

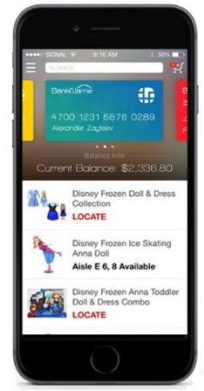


(Source: "Annual Special Report on Global Card Brands", The Nilson Report, Issue 1154, May 2019)

Payment Card Usage

When it comes to college students and “paying with plastic,” **85% of college students carry debit cards**. Additionally, **more than half (57%) hold a credit card**.

- 81% of college students still carry cash
- 85% possess debit cards
- 86% use mobile pay
- 57% have credit cards



(Source: Sallie Mae, "Majoring in Money: HOW AMERICAN COLLEGE STUDENTS AND OTHER YOUNG ADULTS MANAGE THEIR FINANCES" 2019)

Payment Card Usage

The 2019 Sallie Mae “Majoring in Money” report showed:

Among those with credit cards, students carry an average of **5.2 cards**.

Students report an **average balance of $1,183 of combined credit card debt**.

(Source: Sallie Mae, "Majoring in Money: HOW AMERICAN COLLEGE STUDENTS AND OTHER YOUNG ADULTS MANAGE THEIR FINANCES" 2019)

Payment Card Usage

Another study from US News and World indicated that **42% of college students have credit card debt**. And for 28% of that sample of 1,203 undergraduate students, **the debt exceeds $2,000**.

Almost **50%** said they use their cards for school expenses, like books and tuition, while another, nearly half, used it for living expenses.

(Source: Sallie Mae, "More Parents Are Paying Their College Kid's Credit Card Bills", Newsweek, Oct 2, 2023)

Payment Card Usage

Are you taking credit/debit card payments on your campus?

Can you afford not to?


ilovewrestlinggifs

What methods are used to process payments on campus?

Manual Imprinters for off campus events

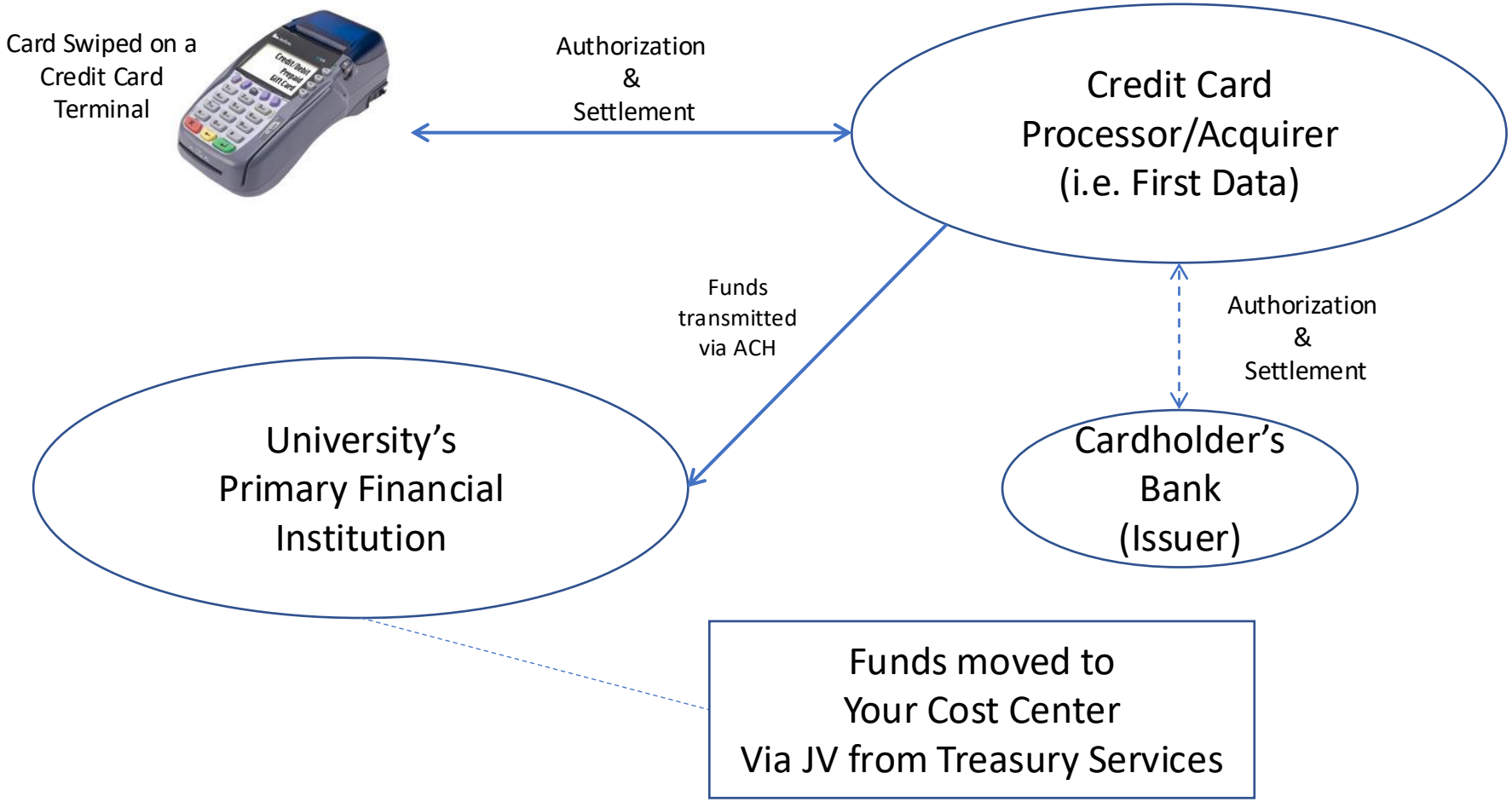
Point-of-Sale (POS) Systems or Payment Applications

Mobile Device?

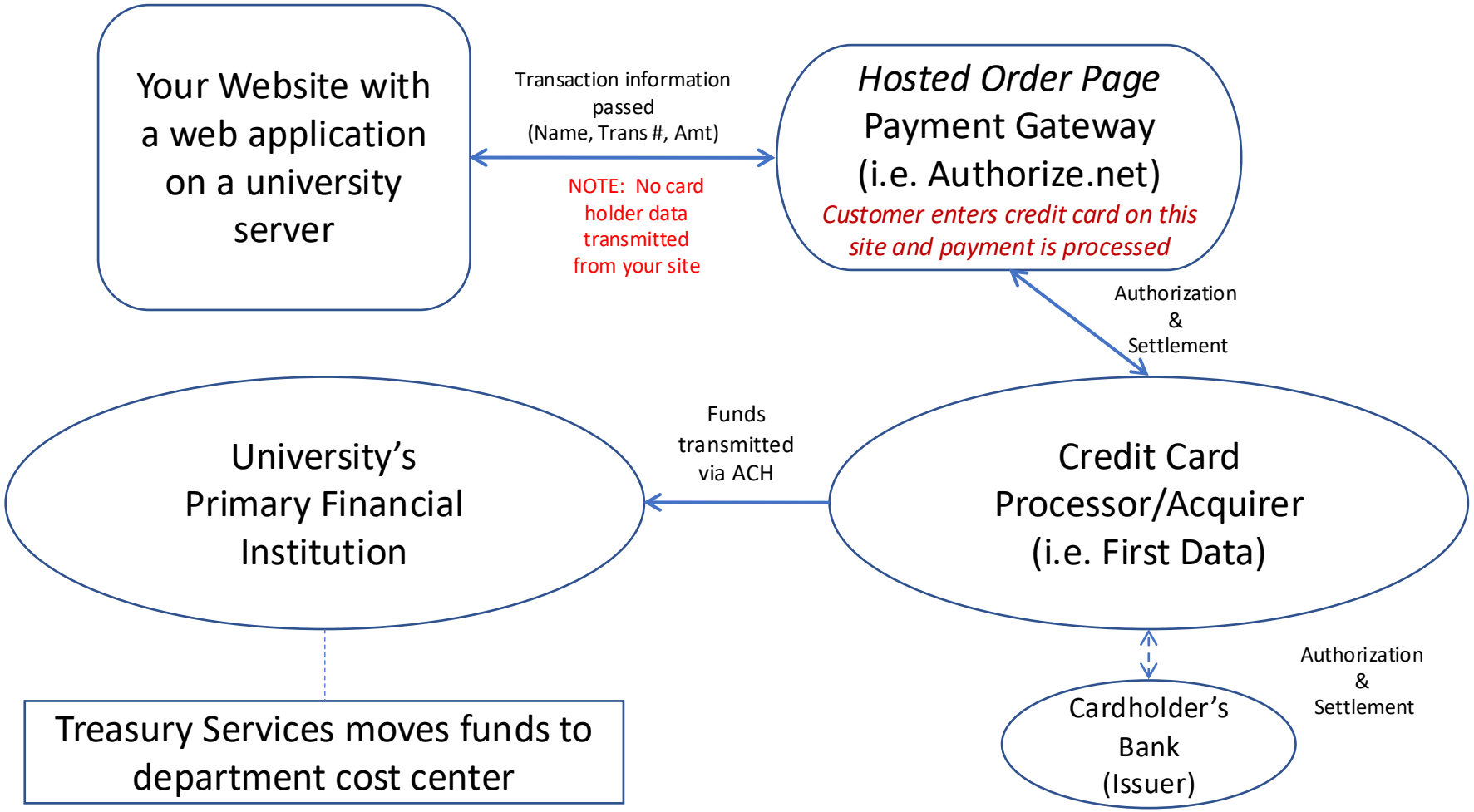
Dial-up or Cellular Credit Card Swipe Terminals

E-commerce & Online Payment forms

Swipe Terminal Credit Card Payment



Web-based Credit Card Payment



UK Card Processing Environment

UK Card Processing Environment

As of today:

198 merchant accounts

Number of merchant units processing by:

- P2PE Credit Card Terminals/Devices – 700+

- Website – ~125

- POS System or Payment Application – 10

Note: Some merchants do a combination of both a swipe terminal and Website/POS/PA

UK Card Processing Environment

For FY25, UK merchant units processed:

Total Transactions: **1,553,834**

Increase of 3.07% from FY24

Total Revenue: **$227,701,100**

Increase of 7.63% from FY24

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Top Ten Merchants in Total Dollar Volume

	Merchant Name	# of MIDs	# of Trans	Sales	Percent of Total Sales	Average Ticket
1	UK ATHLETICS	3	101,378	$74,688,876	36.68%	$736.74
2	UK HEALTHCARE	1	517,494	$51,549,895	25.32%	$99.61
3	SAS - TUITION	3	42,518	$40,911,088	20.09%	$962.21
4	UKHC PHARMACIES	11	283,558	$8,562,086	4.20%	$30.20
5	UK TRANSPORTATION SVCS (Parking)	8	329,311	$7,842,802	3.85%	$23.82
6	UK GRAD & FAMILY HOUSING	2	6,686	$4,207,917	2.07%	$629.36
7	UK DENTISTRY	9	14,779	$3,933,811	1.93%	$266.18
8	UK OFFICE OF PHILANTHROPY	3	17,221	$3,852,130	1.89%	$223.69
9	CKMS	2	13,111	$1,574,385	0.77%	$120.08
10	UK COLLEGE OF AG, FOOD, & ENV	16	7,820	$1,268,500	0.62%	$162.21

97.4%

Treasury Institute for Higher Education

UK Card Processing Environment

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Top Ten Merchants in Total Transactions

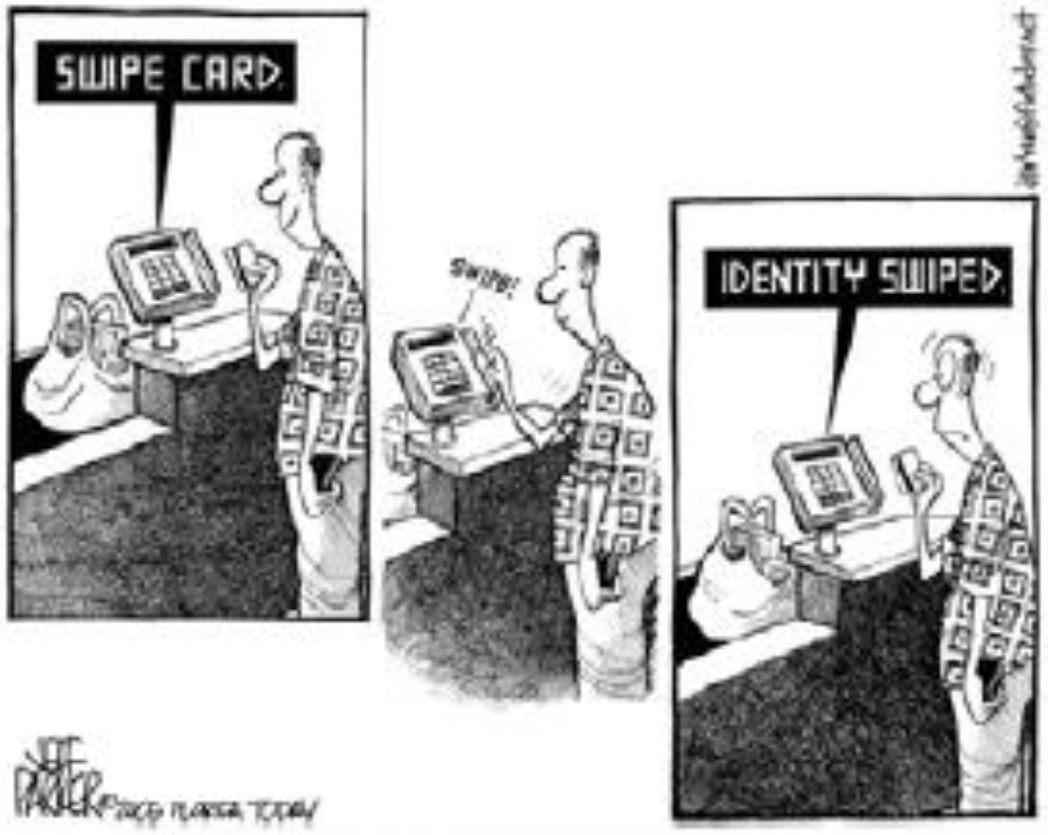
	Merchant Name	# of MIDs	Total # of Transactions	% of Total	Sales	Average $ per Transaction
1	UK HEALTHCARE	1	517,494	34.55%	$51,549,895.49	$99.61
2	UK Transportation Services	8	329,311	21.99%	$7,842,801.89	$23.82
3	UKHC PHARMACIES	11	283,558	18.93%	$8,562,086.24	$30.20
4	UK Athletics	3	101,378	6.77%	$74,688,876	$736.74
5	SAS - TUITION	3	42,518	2.84%	$40,911,088.28	$962.21
6	UK OFFICE OF PHILANTHROPY	3	17,221	1.15%	$3,852,129.56	$223.69
7	UK DENTISTRY	9	14,779	0.99%	$3,933,811.05	$266.18
8	CKMS	2	13,111	0.88%	$1,574,385.44	$120.08
9	COLLEGE OF AG, FOOD, & ENV	16	7,820	0.52%	$1,268,500.48	$162.21
10	UK GRAD & FAMILY HOUSING	2	6,686	0.45%	$4,207,916.54	$629.36

89.0%

Treasury Institute for Higher Education

PCI DSS Background

Whose Crazy Idea Was This, Anyway?



PCI DSS Background

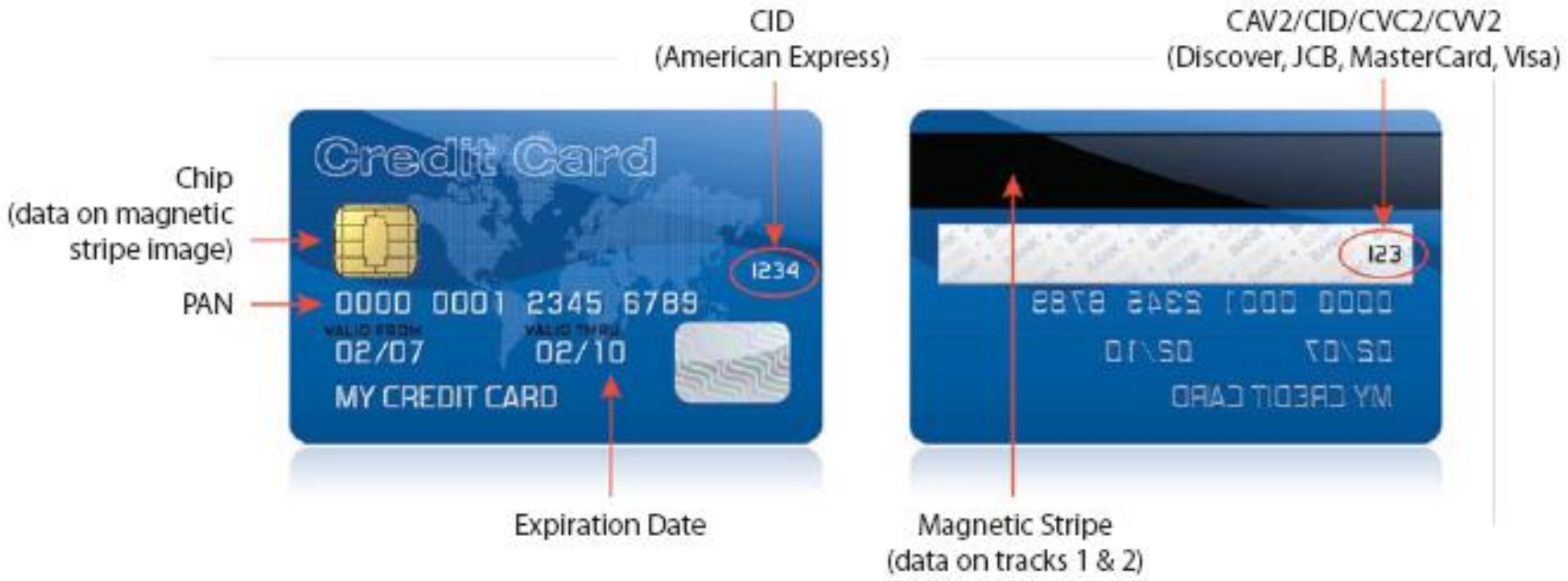
Alphabet Soup

- PCI DSS or PCI – Payment Card Industry Data Security Standard
- PA-DSS – Payment Application Data Security Standard
- QSA – Qualified Security Assessor
- SAQ – Self-Assessment Questionnaire
- ASV – Approved Scanning Vendor
- CHD – Cardholder Data
- CDE – Cardholder Data Environment
- PAN – Primary Account Number
- P2PE – Point-to-Point Encryption

PCI DSS Background

What's in *Your* Wallet?

What is PCI DSS trying to protect?




Per the 2023 Verizon DBIR, there were 5,199 data breaches in 2022
Other unknown security breaches

Setting the Stage for Standardization

- Increased data breaches and card fraud
- Consumer anxiety
  - Regulatory requirements
  - Increased pressure
- Confusing payment card efforts
  - Vague implementation guides
  - Overlapping requirements and duplicated activities
  - Increased confusion on part of merchants and acquirers
  - Low adoption rates

PCI DSS Background

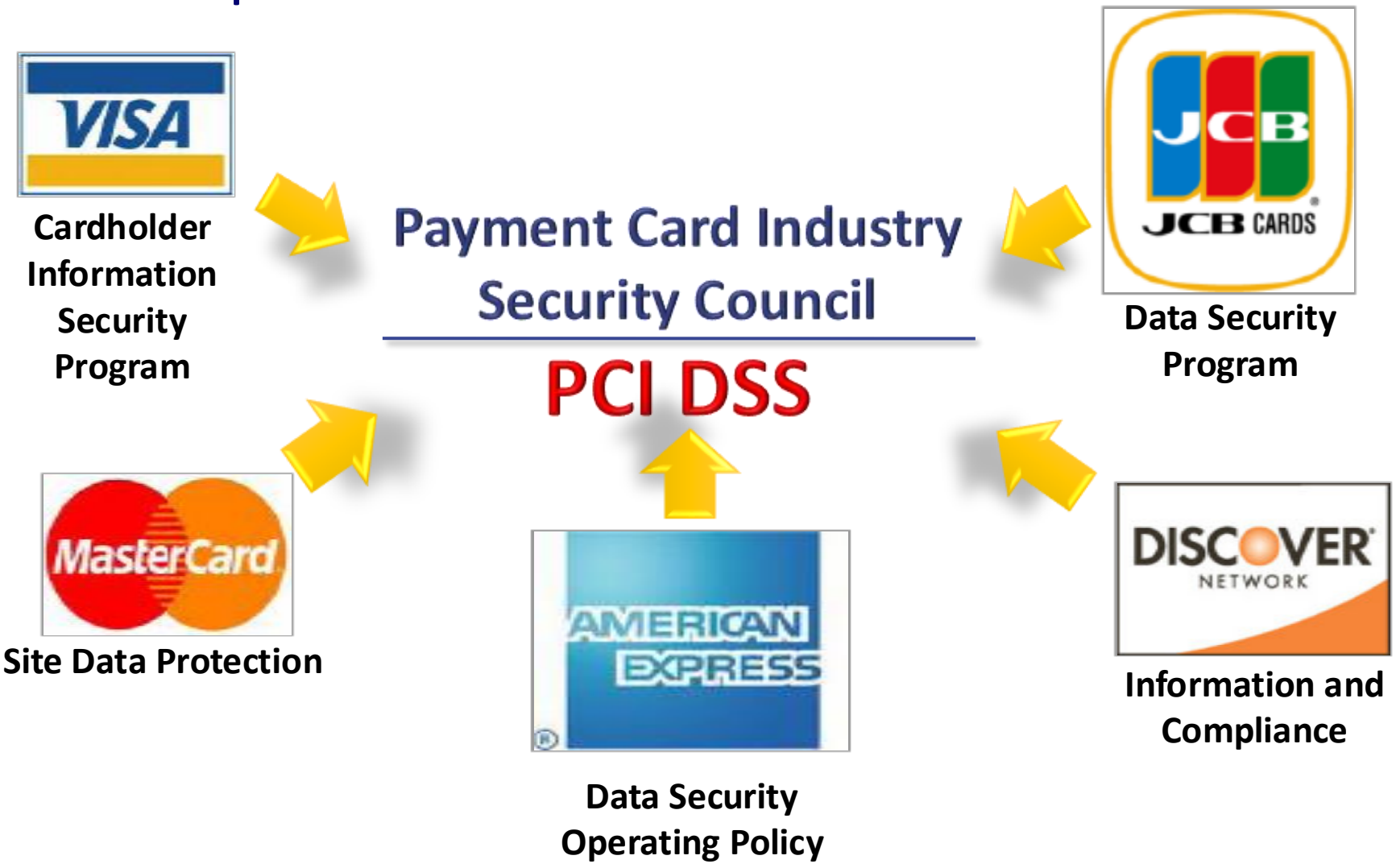
Response from the Card Brands

Payment Card Industry Security Council

PCI DSS

PCI DSS Background

Response from the Card Brands

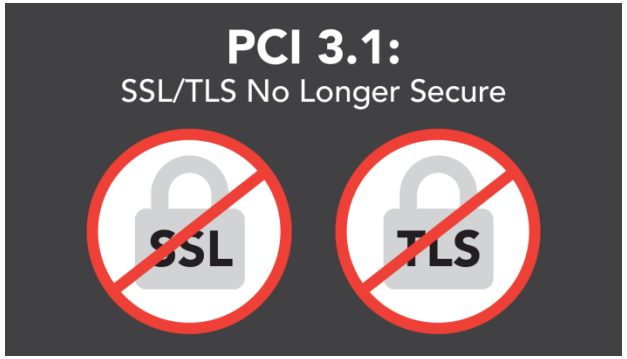


PCI DSS Background

- First version of PCI DSS (1.0) was developed by the five major card brands and released in December 2004.
- PCI Security Standards Council (PCI-SSC) was formed in September 2006, releasing PCI DSS 1.1 at that time.
- Original date that all merchants were to be PCI DSS compliance was **December 31, 2007**.

PCI DSS Background

- PCI DSS Version 2.0, released in October 2010.
- PCI DSS Version 3.0 was released in November 2013.
  - Effective date was January 1, 2015
- PCI DSS Version 3.1 was released in April 2015 and was effective upon release.
  - Requires the use of SSL and outdated TLS (versions 1.0 and 1.1) encryption to be discontinued – effective immediately.
    - Systems currently using SSL and TLS have until June 30, 2016 to discontinue use of SSL and TSL.

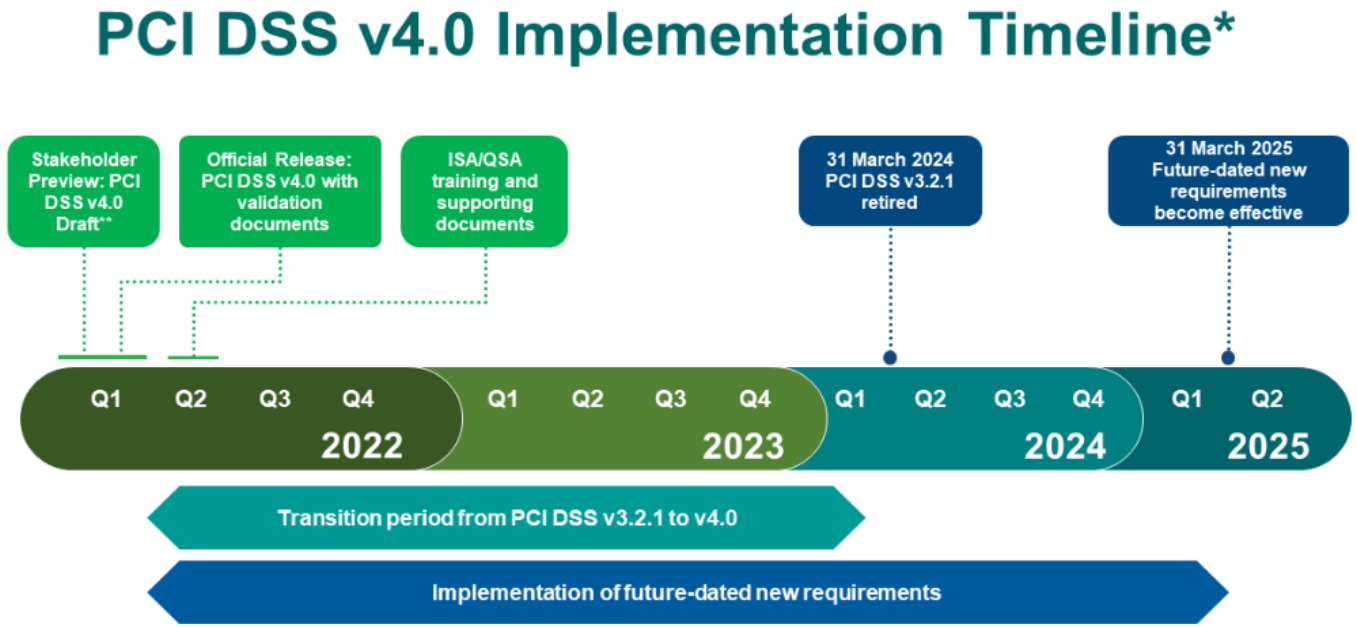


PCI DSS Background

- PCI DSS Version 3.2 was released in April 2016.
  - Becomes effective October 31, 2016, with **mandatory compliance no later than February 1, 2018**.
    - Version 3.1 expires on October 31, 2016
  - Major Changes
    - Multi-factor authentication now required for all administrative users accessing the CDE including within the internal network, not just for remote access.
    - Added requirements for service providers.
    - Extended the migration of SSL to TLS from July 1, 2016, to July 1, 2018.

PCI DSS Background

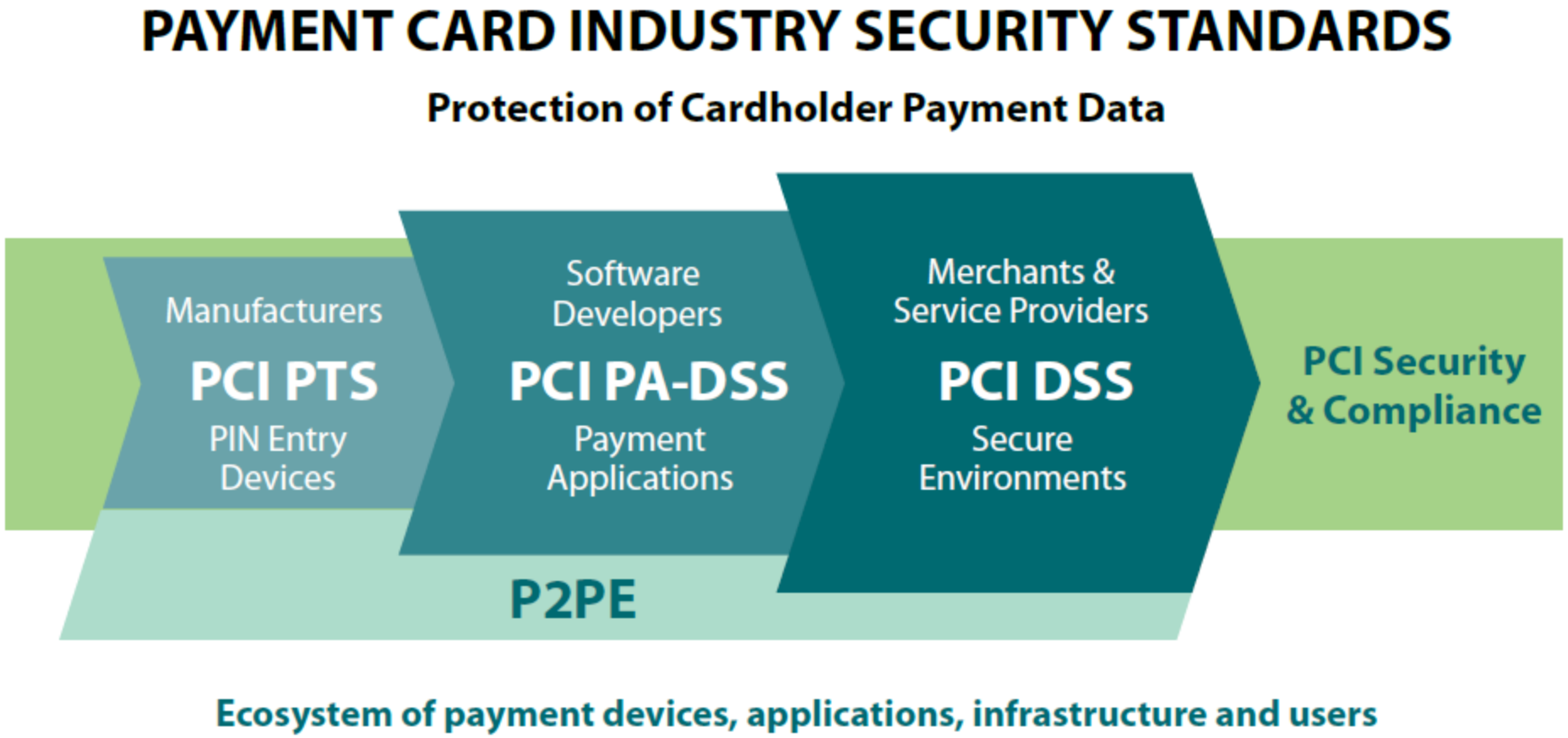
- PCI DSS Version 4.0 was released in **March 2022**
  - Becomes effective **March 31, 2025**
    - Version 3.2.1 expires on March 31, 2024



* All dates based on current projections and subject to change

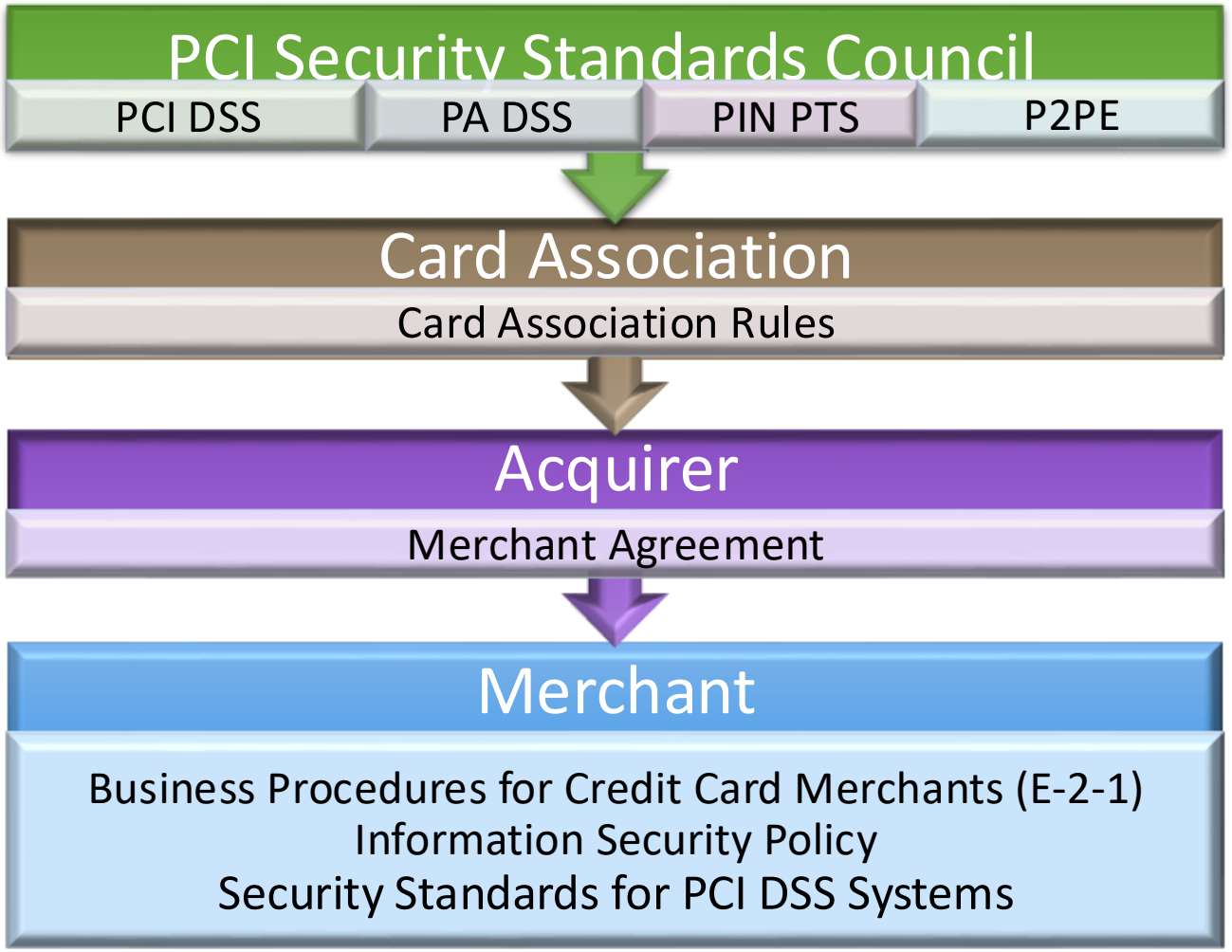
** Preview available to Participating Organizations, QSAs, and ASVs

PCI DSS Background



PCI DSS Background

PCI Food Chain



PCI DSS Background

PCI DSS Basics

- Overriding Goal: Protection of “Cardholder Data” (CHD)
  - Primary Account Number (PAN)
  - Also addresses track data, security codes (CVV, CVC, etc.), PINs – AKA Sensitive Authentication Data
- PCI applies to anyone who processes credit card payments
  - “Store, process, or transmit” cardholder data
- There are 12 requirements outlined by the PCI Security Standards Council

PCI DSS Background

PCI DSS Requirements

PCI DSS
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
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

PCI DSS Background

Merchant Level Classifications

Your Level is:	Your business does:	You should:
4	- less than 20,000 eCommerce transactions per year - less than 1 million other transactions per year	- complete an annual risk assessment using an SAQ - conduct quarterly PCI scans
3	- 20,000 - 1 million transactions per year	- complete an annual risk assessment using an SAQ - conduct quarterly PCI scans
2	- 1-6 million transactions per year	- complete an annual risk assessment using an SAQ - conduct quarterly PCI scans
1	- 6 million+ transactions per year	- conduct an annual internal audit - conduct quarterly PCI scans

PCI DSS Background

Compliance Cost

The Cost of Complying

Three Categories of Compliance

- Upgrading payment systems and security
- Verifying compliance through assessment
- Sustaining compliance

The Cost of Not Complying

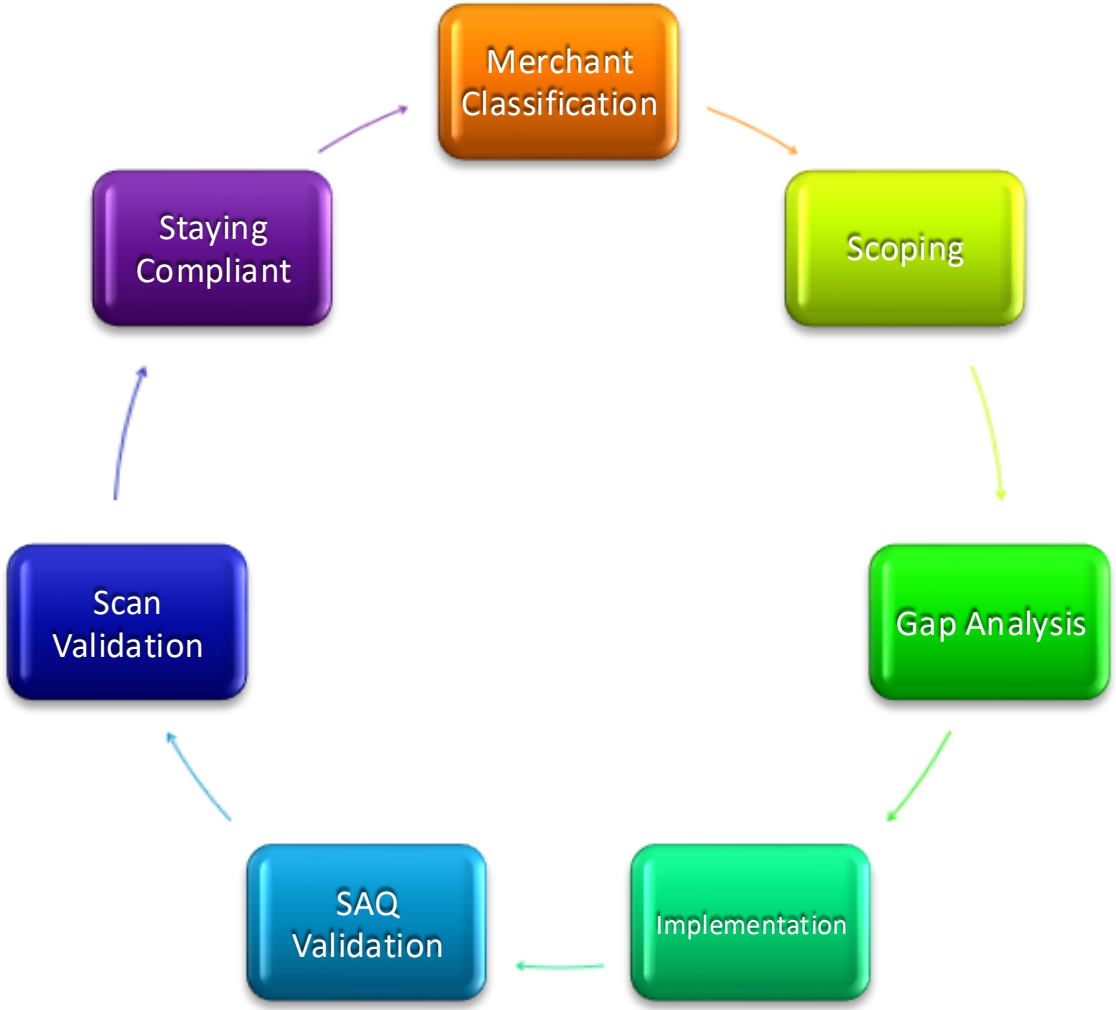
Non-compliance costs significantly higher, including—

- "Crisis" costs upgrades
- Repeat assessments (Level 1 validation)
- Notification costs
- Reputation, negative publicity
- Consumer lawsuits
- Increased processing fees
- Restrictions on card acceptance
- Prohibition on card acceptance

PCI DSS Compliance

How do we get there?

PCI DSS Compliance Roadmap



PCI DSS Compliance Roadmap

Merchant Classification

- What kind of merchant am I?
  - How do I process transactions?
    - In Person (card present)
    - Online (card not present)
    - MOTO (card not present)
  - What methods do I use to process transactions?
    - Credit Card Swipe terminal
      - Analog Telephone Line
      - Connected to the network via Ethernet (IP based)
    - Website via an Internet Payment Gateway
    - POS System or Payment Application

PCI DSS Compliance Roadmap

Merchant Classification

- What kind of merchant am I? (continued)
  - Do I store any credit card data?
    - Paper based storage only
    - Electronic storage within a Payment Application, on a Server or PC

- What Self-Assessment Questionnaire (SAQ) do I use to validate my compliance?

PCI DSS Compliance Roadmap

SAQ Validation Type	Description	# of Questions v3.2
A	Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage	14
A-EP	E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage	139
B	Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage	41
B-IP	Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage	83
C	Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage	139
C-VT	Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage	73
D	All other SAQ-eligible merchants	326
D-SP	SAQ-eligible service providers	347
P2PE	Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage	35

PCI DSS Compliance Roadmap

Merchant Classification

Point-of-Sale

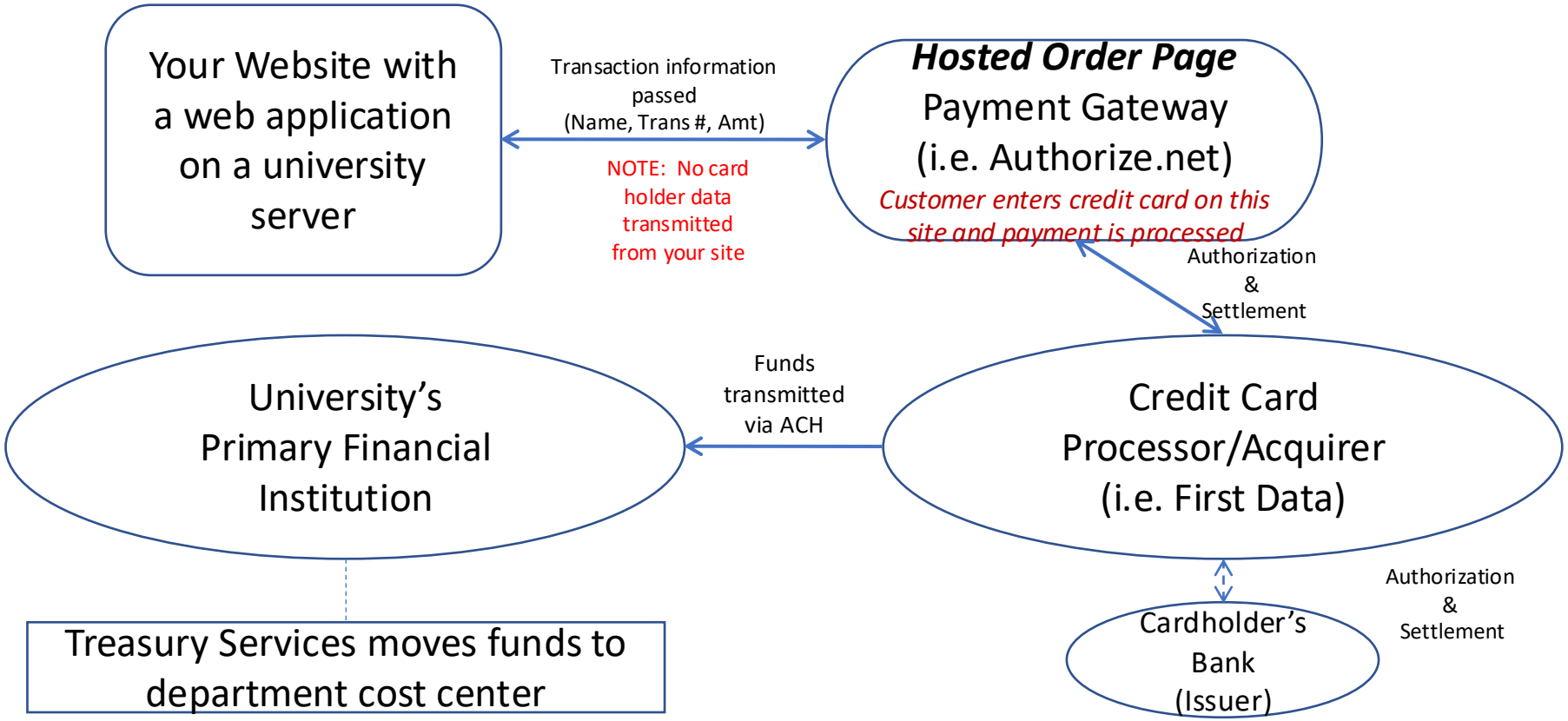
- **SAQ B** if:
  - standalone, dial-out terminal
  - not connected to other systems on your network
  - not connected to the Internet
  - not storing CHD
- **SAQ C** if:
  - on the same device as an Internet connection
  - not connected to other systems on your network
  - not storing CHD
  - vendor uses secure techniques to provide remote support
- **SAQ D** if not qualified for SAQ B or C

Photo Source: http://www.bankofamerica.com/smallbusiness/promos/jump/merchant_meetorbeat/?cm_sp=SB-Merchant-_-MerchantAcquisition-_-SB-MarketingPage_sb-bac-043_mks_merch_2.jpg

PCI DSS Compliance Roadmap

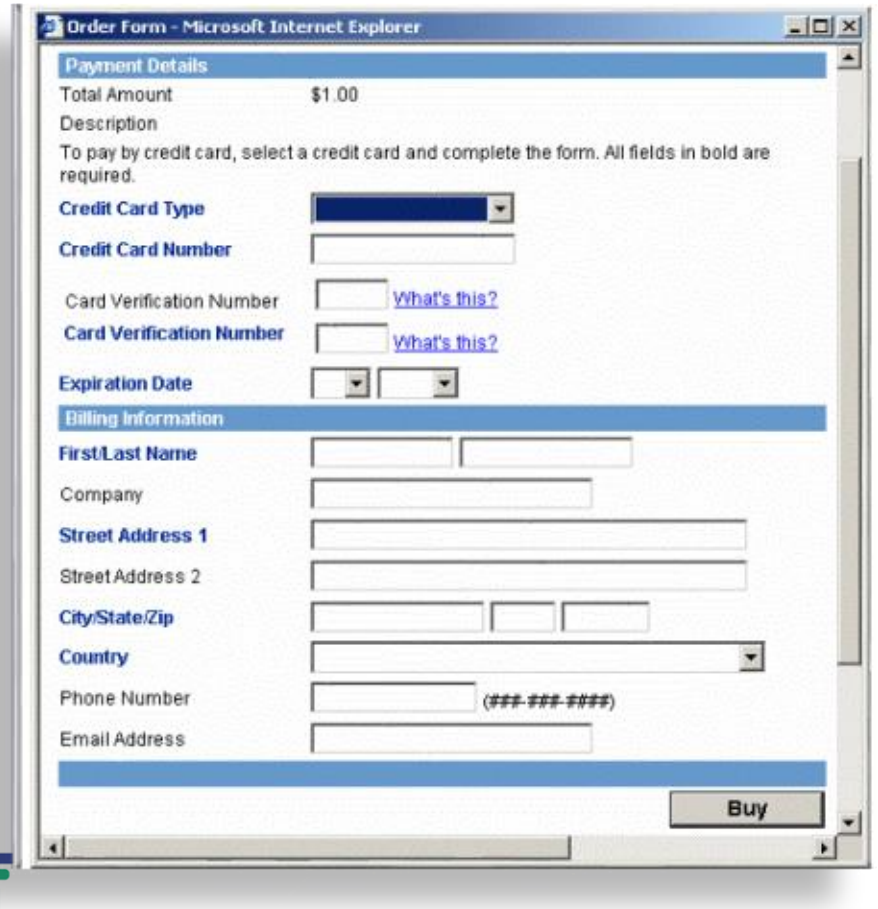
Merchant Classification

Web-based Credit Card Payment



PCI DSS Compliance Roadmap

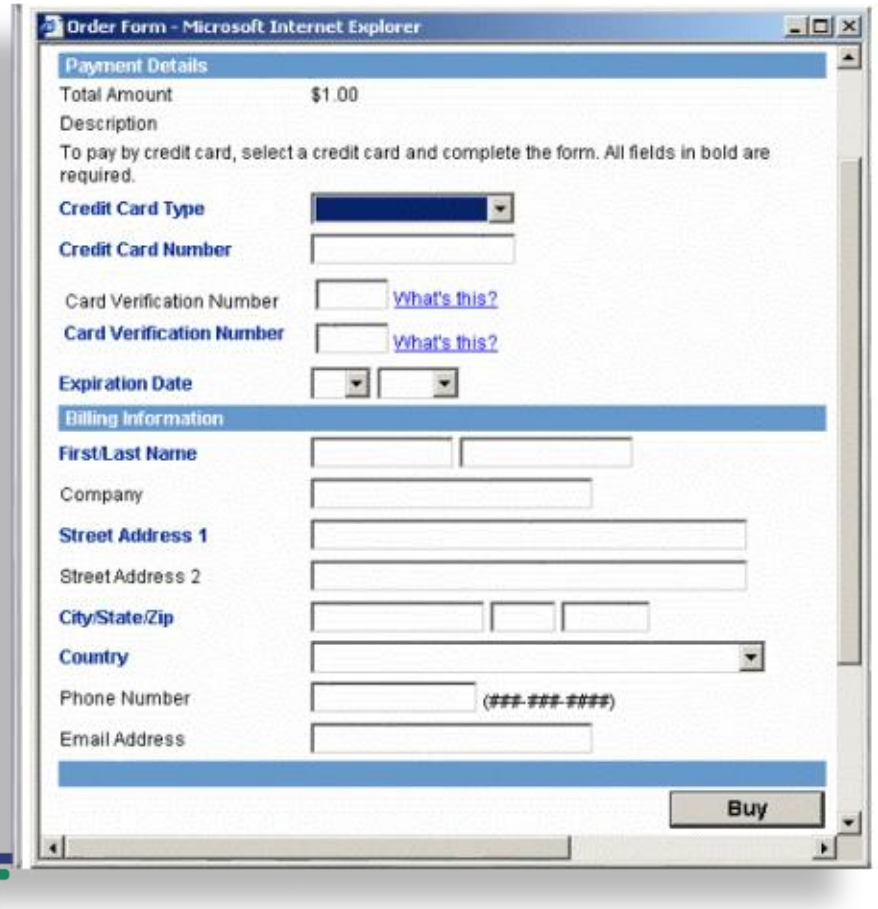
Merchant Classification
Outsourced Hosted Order Page



- **SAQ A** if:
  - Website hosted by a compliant 3rd party service provider
  - Customers redirected to a to a 3rd party service provider for all CHD storage, processing or transmission
  - 3rd party is PCI DSS compliant
  - not storing CHD
- **SAQ C** if:
  - CHD is entered from merchant's browser
  - not connected to other systems on your network
  - not storing CHD
  - vendor uses secure techniques to provide remote support
- **SAQ D** if not qualified for SAQ A or C

PCI DSS Compliance Roadmap

Merchant Classification
University Hosted Order Page



- **SAQ A-EP** if:
  - Website hosted on a university webserver
  - Customers **redirected** to a to a 3rd party service provider for all CHD storage, processing or transmission
  - 3rd party is PCI DSS compliant
  - not storing CHD
- **SAQ C** if:
  - CHD is entered from merchant's browser
  - not connected to other systems on your network
  - not storing CHD
  - vendor uses secure techniques to provide remote support
- **SAQ D** if not qualified for SAQ A-EP or C

PCI DSS Compliance Roadmap

Merchant Classification

SAQ-A versus SAQ-A-EP

	SAQ A All Cardholder Data Functions Completely Outsourced	SAQ A-EP Partially Outsourced E-commerce Payment Channel
Applies to:	**Card-not-present** merchants (e-commerce or mail/telephone-order)*	**E-commerce** merchants
Functions Outsourced	All **payment acceptance and processing** are entirely outsourced to PCI DSS validated third-party service providers	All **processing** of cardholder data is outsourced to a PCI DSS validated third-party payment processor
Control of Cardholder Data	Merchant's e-commerce website does not receive cardholder data and **has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored**	Merchant's e-commerce website does not receive cardholder data but **controls how consumers, or their cardholder data, are redirected** to a PCI DSS validated third-party payment processor
Payment Pages	The entirety of all payment pages delivered to the consumer's browser originates **directly from a PCI DSS validated third-party service provider(s)**	All elements of payment pages that are delivered to the consumer's browser originate **from either the merchant's website or a PCI DSS compliant service provider(s)**
Third-Party Compliance	Merchant confirmed that all third party(s) handling **acceptance, storage, processing, and/or transmission** of cardholder data are PCI DSS compliant	Merchant confirmed that all third party(s) handling **storage, processing, and/or transmission** of cardholder data are PCI DSS compliant
Merchant Systems	Merchant does not electronically store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party(s) to handle all these functions	
Data Retention	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically	

Source:

PCI DSS Compliance Roadmap

Merchant Classification

Virtual Terminal

Don't use Virtual Terminals on campus unless you are using an isolated, PCI DSS compliant PC installed on the segmented network!

- **SAQ C** if:
  - on the same device as an Internet connection
  - not connected to other systems on your network
  - not storing CHD
  - vendor uses secure techniques to provide remote support
- **SAQ D** if not qualified for SAQ C

PCI DSS Compliance Roadmap

Merchant Classification

Service Providers

- Additional merchant duties under Requirement 12.8
- Written agreement
- Due diligence
- Evidence of PCI compliance
  - Report on Compliance
  - **VISA List of PCI DSS Compliant Service Providers** (http://usa.visa.com/merchants/risk_management/cisp_service_providers.html)

    MasterCard also has a similar list (http://www.mastercard.com/us/sdp/serviceproviders/compliant_serviceprovider.html)
  - Evidence of SAQ D and scanning

PCI DSS Compliance Roadmap

Merchant Classification

POS System

- **SAQ C** if:
  - on the same device as an Internet connection
  - not connected to other systems on your network
  - POS software is PA-DSS compliant
  - not storing CHD
  - vendor uses secure techniques to provide remote support
- **SAQ D** if not qualified for SAQ C

PCI DSS Compliance Roadmap

Merchant Classification

Payment Applications

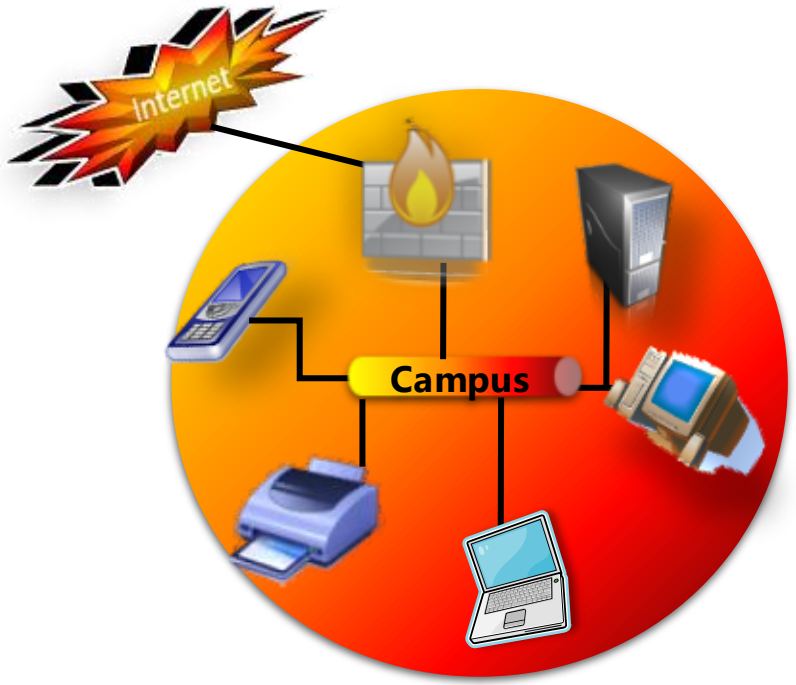
- Vendor-supplied: PA DSS
  - Payment application should be listed in the **PCI SSC List of Validated Payment Applications** (https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php)
- In-house developed by merchant: PCI DSS
- In-house developed by service provider: PCI DSS

- Any systems used to process transactions via the internet over the network must utilize a Segmented, Secured Network.

Before PCI DSS Segmented Network

Credit Card Processing systems transmitting credit card data across open campus network

- No segregation
- Entire network is in scope
  - Including mobile devices
  - Including unrelated equipment
- Disadvantages
  - Costly to scan
  - Likely scan failure
  - Operational impact of scanning



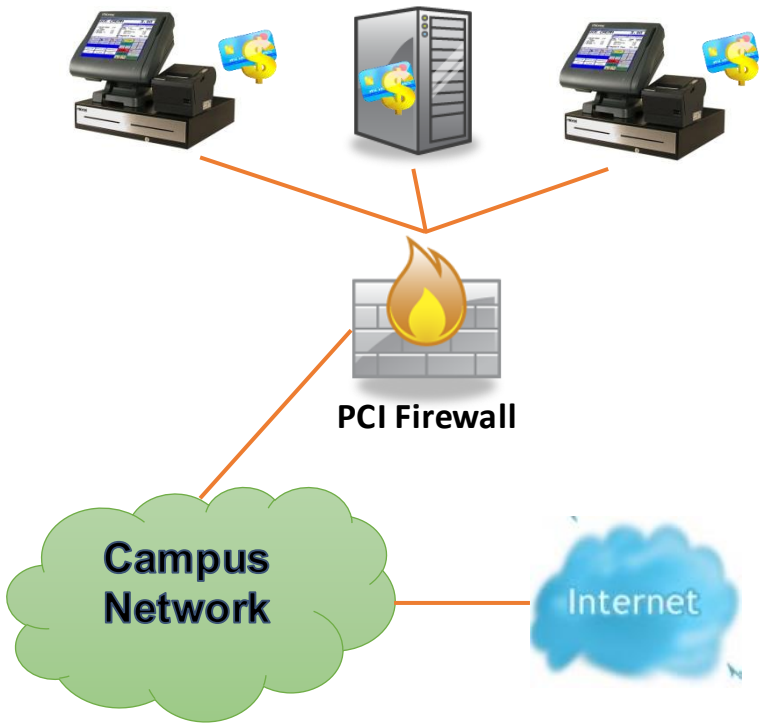
PCI DSS Segmented Network Implementation

- Move credit card processing systems to the **PCI DSS Segmented Network**
  - UK used MPLS architecture to create a private, virtual network
  - Installed a firewall between PCI network and campus network
    - Firewall rules block all inbound traffic
    - Firewall rules block all outbound traffic except specific locations required by payment processing devices inside the network
  - Limits cardholder data environment scope to those devices behind the PCI firewall

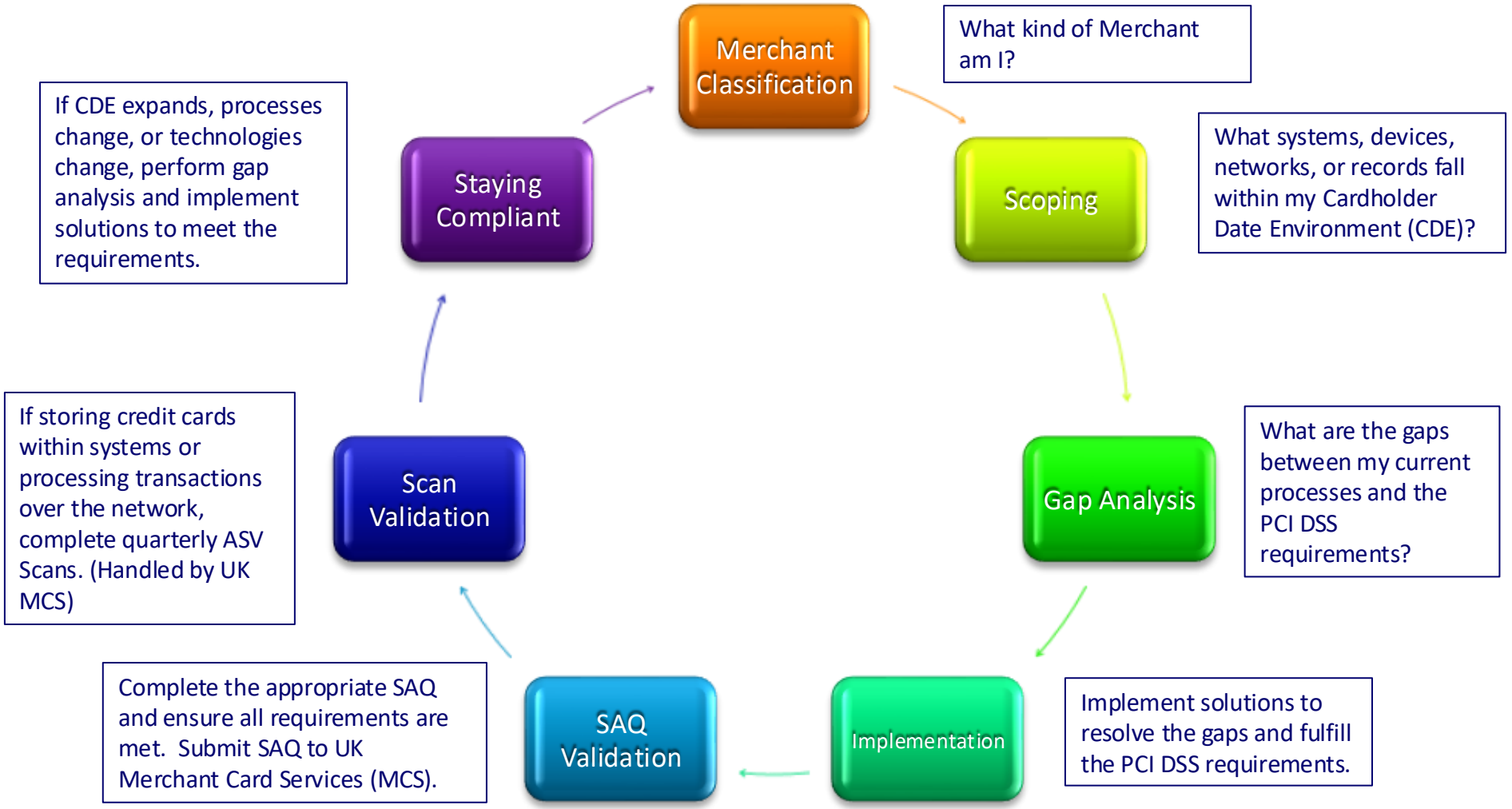
PCI DSS Compliance Roadmap

After PCI DSS Segmented Network

PCI DSS
Segmented Network
Using MPLS Architecture



PCI DSS Compliance Roadmap



UK PCI DSS Compliance Major Objectives

PCI DSS Compliance Objectives

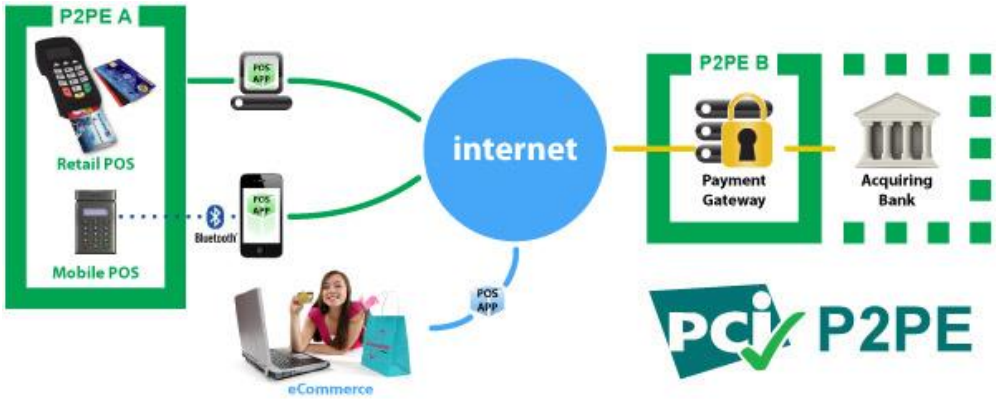
Obj. #1: Minimize the amount of credit card data that is collected, stored, and transmitted by University servers via the UK network.

- Utilize **Point-to-Point Encryption (P2PE)** and **Tokenization** solutions to keep card data off the network and out of systems

PCI DSS Compliance Objectives

Emerging Technologies

Point-to-Point (P2PE) Encryption



- P2PE is a “game changer”
- Encrypts CHD at the point of swipe, removing network and systems from scope for PCI DSS compliance.
- Major difference from E2EE solutions is that the merchant has no access to the encryption keys.
- More companies are bringing PCI P2PE compliant solutions to the market.

Bluefin Payment Systems FREEDOMPAY element payment services

PCI DSS Compliance Objectives

Emerging Technologies

Tokenization

- Great solution for systems needing the ability to store payment data for recurring transactions without storing CHD.
  - After credit card transaction is processed and authorized, the merchant is provided a token to store that is tied to that credit card being processed.
  - Replaces/Devalues Card Data at rest.
- The method of processing the transaction is still in scope.
- Ultimate solution would be to combine tokenization solution with P2PE solution.

PCI DSS Compliance Objectives

Emerging Technologies

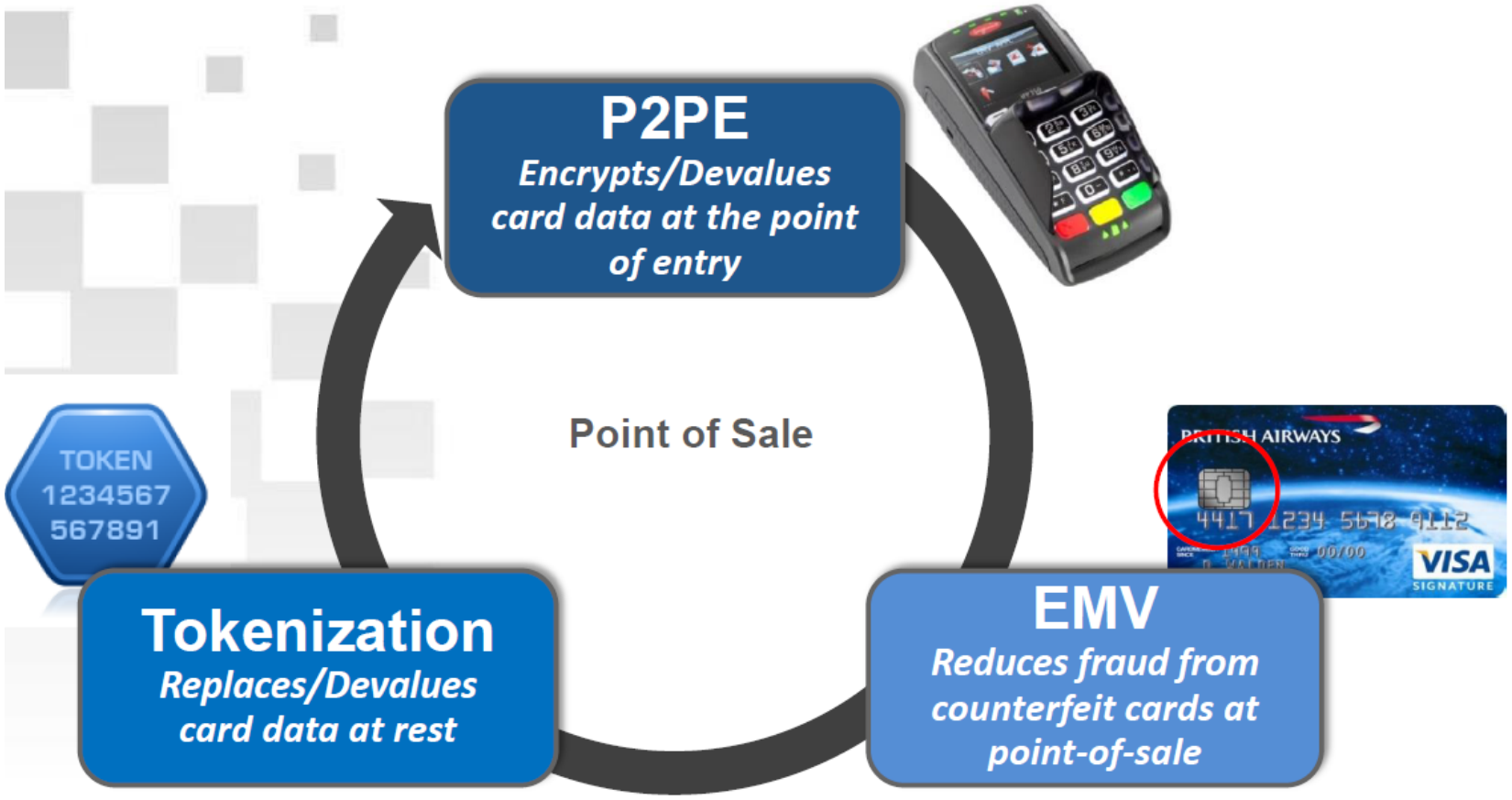
EMV

- Also known as “Chip and Pin”
- Vastly reduces card-present fraud
- Makes counterfeiting cards infeasible
- Introduces a dynamic, cryptographic element
- Increase in CNP fraud
- Cards still have mag stripe for now
- Liability Shift to merchants in October 2015

PCI DSS Compliance Objectives

Emerging Technologies

A Holistic Approach to Security is Required



PCI DSS Compliance Objectives

Obj. #1: **Minimize the amount of credit card data that is collected, stored, and transmitted by University servers via the UK network.**

- Utilize **Point-to-Point-Encryption (P2PE)** and **Tokenization** solutions to keep card data off the network and out of systems
- Web-based merchant units should utilize a Hosted Order Page provided by a PCI Compliant 3rd Party Internet Processing Gateway service provider (i.e. Authorize.net)
- Merchant units should discontinue using web-based Virtual Point of Sale Terminals
  - Card data keyed into a personal workstation via a web browser to process a credit card transaction

Credit Card Data Storage Motto

If you don't need it, DON'T KEEP IT!

(especially keep it off your computers, servers, and network)

PCI DSS Compliance Objectives

Obj. #2: **Protect any credit card data that must be collected, stored, or transmitted by University servers via the UK network.**

- Creation of a secure network isolated from the UK public network to be used for processing card transactions
- Installation of Firewalls: Network and Application
- Physically securing web-servers and network equipment

PCI DSS Compliance Objectives

Obj. #2: **Protect any credit card data that must be collected, stored, or transmitted by University servers via the UK network.** (continued)

- POS and Payment Applications will be PA-DSS Compliant
  - Stored card numbers are masked
  - Card data is encrypted for transmission
  - Provide secure authentication features
  - System logging
  - Secure Remote Access features

PCI DSS Compliance Objectives

Obj. #2: **Protect any credit card data that must be collected, stored, or transmitted by University servers via the UK network.** (continued)

- Antivirus Protection installed on servers/workstations processing credit card transactions
- Secure access controls
- System Logging
- Server and Application scanning
- External vulnerability scanning and penetration testing
- Many more

Guidelines for Cardholder Data Elements

Type of Data	Data Element	Storage Permitted	Protection Required	Rendered Unreadable*
Cardholder Data	Primary Account number (PAN)	Yes	Yes	Yes
	Cardholder Name**	Yes	Yes**	No
	Service Code	Yes	Yes**	No
	Expiration Date	Yes	Yes**	No
Sensitive Authentication Data (SAD) 	Full Magnetic Stripe Data2	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

* Eliminate, encrypt, one-way hash, truncate or use compensating controls.
**Protect if stored with PAN.

Data Storage Basics

Do's	Don'ts
Do understand where payment card data flows for the entire transaction process	Do not store cardholder data unless it's absolutely necessary
Do verify that terminals comply with the PIN entry device security requirements	Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe after authorization
Do verify that your payment applications comply with PA-DSS	Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked
Do retain cardholder data only if authorized, and ensure it's protected	Do not store any payment card data in payment card terminals or other unprotected PCs, laptops or smart phones
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies	Do not locate servers or other payment card system storage devices outside of a locked, fully secured and access- controlled room
Do ensure that any third-party card processor complies with PCI DSS, PED and/or PA-DSS as applicable	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones

Credit Card Data Storage Motto

If you don't need it, DON'T KEEP IT!

(especially keep it off your computers, servers, and network)

PCI DSS Compliance Objectives

Obj. #3: **Minimize, eliminate, and/or secure any <u>physically</u> stored card data.**

- Records containing credit card numbers should be physically secured and access controlled
- Physical records containing credit card data should be destroyed **3 years*** after a transaction is processed

* According to Record Series U0239 of the State University Records Retention Schedule for Kentucky

PCI DSS Compliance Objectives

Obj. #4: **Assure all University merchants maintain PCI DSS compliance.**

- Annual submission by merchants of Self-Assessment Questionnaires (SAQ) and any other documentation requested to prove compliance.
- Develop a program with Internal Audit to conduct PCI DSS Compliance functional audits of merchant units.

PCI DSS Compliance Responsibilities

Merchant Unit Responsibilities

- Each merchant unit is responsible for their own PCI DSS Compliance.
  - Failure to comply PCI DSS Compliance can result in the loss of the privilege to accept credit card payments.
- Development of a departmental credit card data information security policy, procedures or plan.
- Implementation of all data security controls necessary to comply with PCI DSS requirements.

PCI DSS Compliance Responsibilities

Merchant Unit Responsibilities (continued)

- Attendance to an annual PCI DSS Compliance Training seminar conducted by the UK Merchant Card Services Department.
  - Ensure all department employees handling credit cards are trained on basic PCI DSS compliance and department policies/procedures.
- Units in SAQ Validation Types 4 and 5, are required to complete **quarterly vulnerability scans** with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of the passing scans from the ASV.

PCI DSS Compliance Responsibilities

Merchant Unit Responsibilities (continued)

- Annual submission of:
  - Completed SAQ and associated Attestation of Compliance
  - PCI DSS Compliance Certificates from any 3rd party service providers
  - Evidence where the unit's 3rd Party payment application (software) is included on the PCI SSC List of PA-DSS Validated Payment Applications
  - Any other documentation requirements deemed necessary by the Merchant Card Services Department to validate the merchant's PCI DSS compliance.

PCI DSS Compliance Responsibilities

Treasury and Merchant Card Services

- Provide guidance and support to the merchant units' PCI DSS Compliance efforts.
- Make recommendations on how to lower a merchant unit's risk of exposure to breaches, thus moving them into a lower level SAQ Validation Type.
- Coordinate and assist in the completion and submission of SAQ's by all merchant units.
- Serve as Liaison between merchant unit and the Credit Card Processing Acquirer (WorldPay)
- Assist merchants in responding to a possible breach and coordinate breach investigation.

PCI DSS Compliance Responsibilities

UK IT Security Office

- Provide guidance and support to the merchant units' PCI DSS Compliance efforts from a technical perspective.
- Make recommendations on how to implement Compensating Controls that will meet particular PCI DSS requirements.
- Work with UK IT to help implement any network infrastructure changes to be utilized in the University's PCI DSS Compliance efforts.
- Assist merchants in getting their systems onto the PCI DSS (MPLS) network.
- Oversee rule changes on PCI DSS firewall.
- Provide Application and Website Vulnerability Scanning.
- Assist merchants in responding to a possible breach and coordinate breach investigation.

PCI DSS Compliance Challenges and Issues

PCI DSS Compliance Challenges

- Is this an IT or a Finance/Treasury project?
  - Both - must get IT and upper management “buy-in”

- Merchant “buy-in” and acceptance.
  - High risk merchants reluctant due to departmental funding requirements for PCI DSS, as well as limited technical resources within their department.

PCI DSS Compliance Challenges

- Funding
  - Major IT purchases
    - Firewalls and network equipment
    - Internal Application Vulnerability Scanning system
    - Network Scanning System
    - Intrusion Detection and Protection system
    - File Integrity Monitoring system
    - Training for each of these systems
    - Additional IT Security Personnel
  - We requested and received approximately $260,000 for the initial PCI DSS project
    - Also received $40,000 recurring for necessary PCI DSS equipment/system upgrades

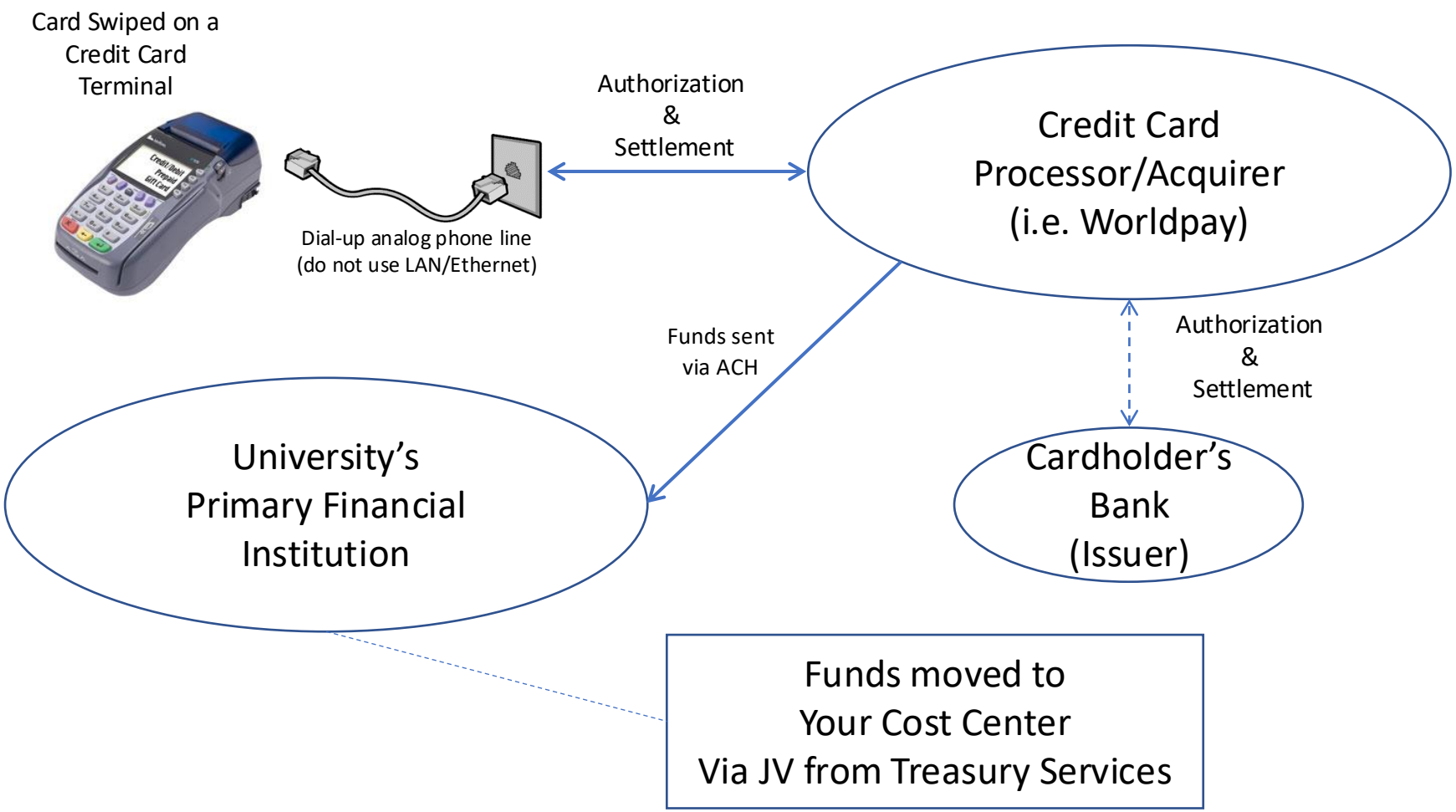
PCI DSS Compliance Current Issues

- PCI DSS requires documentation of the scope of your Cardholder Data Environment (CDE)
  - Can be accomplished with dataflow and payment flow diagrams

EXAMPLES

Example: CDE Transaction Flow Diagram

Swipe Terminal Credit Card Payment

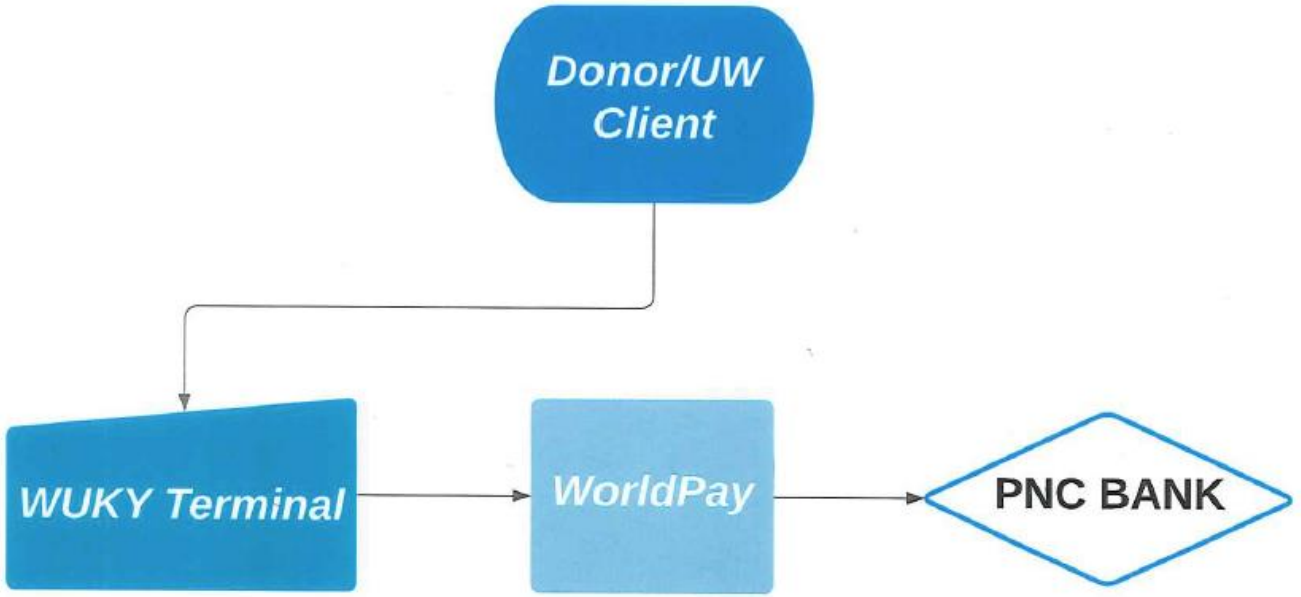


Example: CDE Transaction Flow Diagram

NPR ROCKS @ 91.3 | WUKY.ORG

WUKY

VERIFONE
VX 520 Terminal

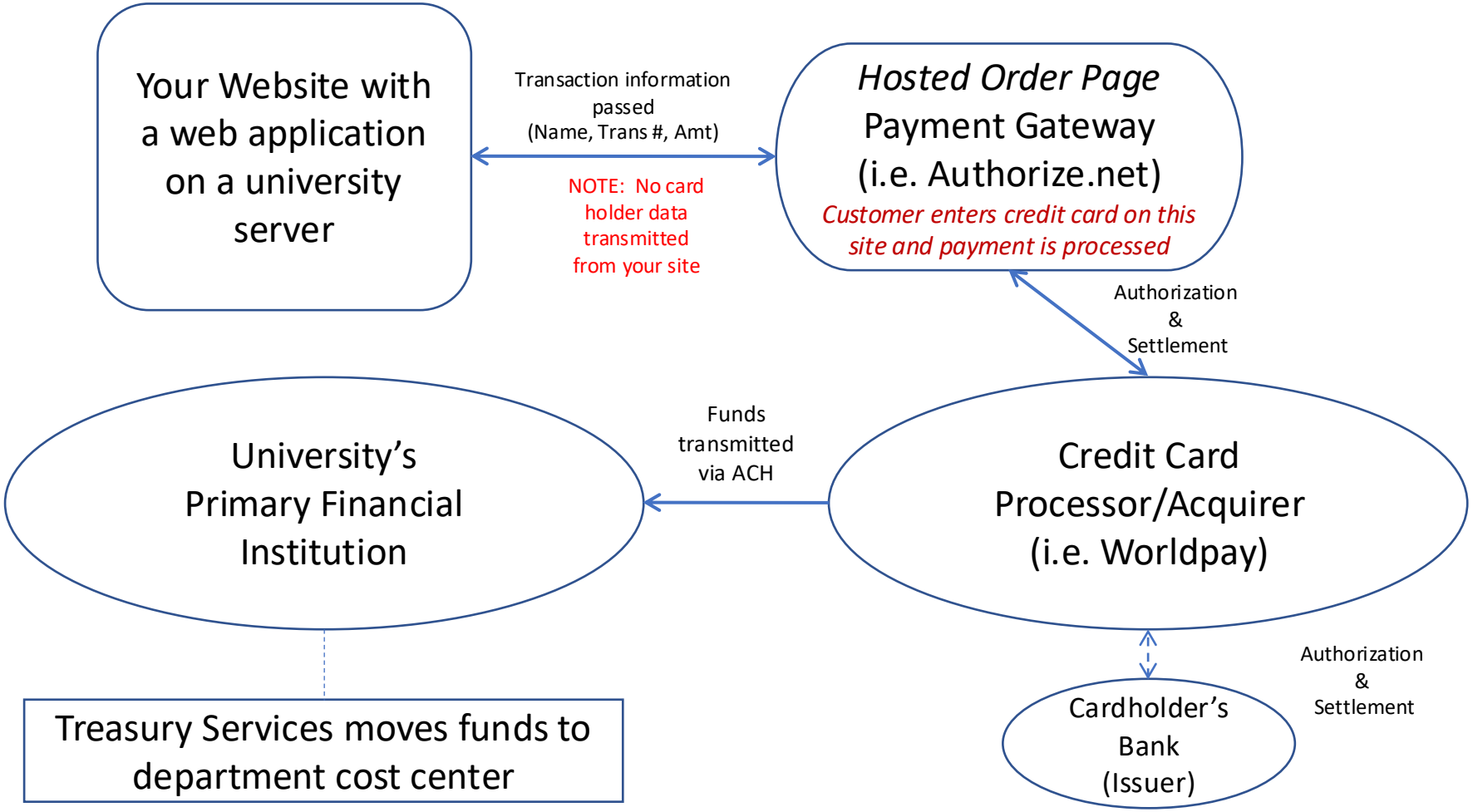


Treasury Institute for Higher Education

Example: CDE Transaction Flow Diagram

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Web-based Credit Card Payment



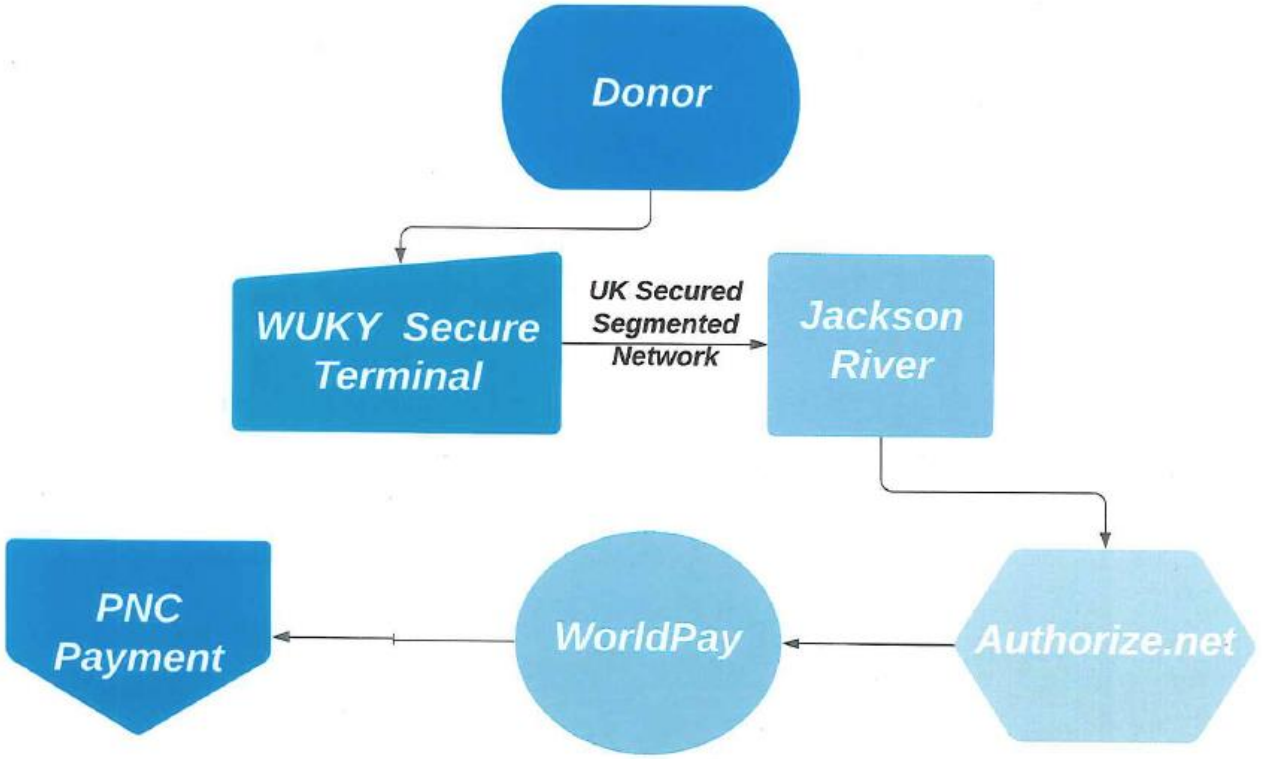
Treasury Institute for Higher Education

$

Example: CDE Transaction Flow Diagram

NPR ROCKS @ 91.3 | WUKY.ORG
WUKY

Virtual Terminal



PCI DSS Compliance Current Issues

- How do you handle the following when it comes to PCI DSS:
  - Voice over IP (VoIP) telephone systems
  - Multi-use networked printers, copiers, fax machines
  - Networked printers or fax machines that store data on a hard drive
  - Campus backup systems (Tivoli)
  - Voicemail and fax systems integrated with email systems
  - Email system – can you prevent credit cards from being emailed?
    - BPM E-2-1 states “Under no circumstance will credit card information be obtained or transmitted via email.”

PCI DSS Compliance Current Issues

- SAQ collection, organization via a SAQ Console solution.
- Training – purchase online training modules or develop/conduct your own training?
- QSA Review?
- Centralized payment solution for all merchants trying to process payments via their website?
- Training for IT, Purchasing, and Legal personnel.
- Making sure PCI DSS language is included in contracts for any systems, services, etc. that will be processing credit card payments.

PCI DSS Compliance Current Issues

- Make sure PCI DSS language is included in contracts for any systems, services, etc. that will be processing credit card payments. (SERVICE PROVIDERS)

Service Providers must be PCI Compliant

- Additional merchant duties under Requirement 12.8
- Written agreement
- Due diligence
- Evidence of PCI compliance
  - Report of Compliance from a QSA
  - **VISA List of PCI DSS Compliant Service Providers** (http://usa.visa.com/merchants/risk_management/cisp_service_providers.html)

    MasterCard also has a similar list (http://www.mastercard.com/us/sdp/serviceproviders/compliant_serviceprovider.html)
  - Evidence of SAQ D and scanning

PCI DSS Compliance Current Issues

- Wireless (Wi-Fi)
  - Use it only for non-sensitive data transmission, if possible (not for cardholder data)
  - Enable WPA2 (WiFi Protected Access) if capable
  - Refer to wireless-specific PCI requirements in all Requirements except 5 and 7.
- Wireless – UK's policy has been that we do not allow the transmission of credit card data for processing across the university wireless network. (Cellular swipe terminals are OK)
  - This policy changed as we rolled out P2PE credit card terminals

PCI DSS Compliance Objectives

Points of Emphasis

- External/Outsourced Vendors (e.g., B&N, Morrison's Cafeteria, Sodexho at Football Stadium, Aramark Dining Services) – UK policy is that these vendors are NOT allowed to use the university network to transmit credit card data for processing. They must provide their own internet connection and network equipment.
- Virtual Terminal Solutions - We encourage our campus merchants to not use Virtual Terminal Solutions. If necessary, these systems must be on the PCI DSS network and are classified as an SAQ-C.

PCI DSS Compliance Objectives

Points of Emphasis

- PCI DSS and Security awareness training must occur upon hire and at least annually for all personnel with credit card handling/processing responsibilities.
  - Requires documentation of employee acknowledgement of the PCI DSS and Security policies
    - Train your employees:
      - University PCI DSS and IT Security Policies
      - Department Policies & Procedures for Credit Card Processing and PCI DSS Compliance
      - Campus wide PCI DSS training within campus training system – (e.g. SANS - “The Payment Card Industry Data Security Standard”)

PCI DSS Compliance Objectives

Points of Emphasis

- Inspection of terminal devices for tampering
  - Should be inspected on a regular basis (daily or weekly)
  - Each inspection must be logged

PCI DSS Compliance Objectives

Points of Emphasis

Tamper Inspection Log

University of Kentucky

This document is to be used by departments that use terminals or similar devices to process in-person payments.

Department Name:	
Device Location:	
Device ID/Model # - Device 1	
Device ID/Model # - Device 2	
Device ID/Model # - Device 3	
Device ID/Model # - Device 4	
Device ID/Model # - Device 5	
Device ID/Model # - Device 6	

Name of Reviewer	Date of Review	Device Number	*Indicate that each area was reviewed with a Y or N*					
			Serial Number match?	Model number match?	Tamper Evident Stickers intact?	Foreign Object Attached to device?	Pry Marks or Bent, Broken, or Stressed Seams?	Anything unusual?
Sam Smith	*5/22/2018*	*3*	*Y*	*Y*	*Y*	*N*	*N*	*N*

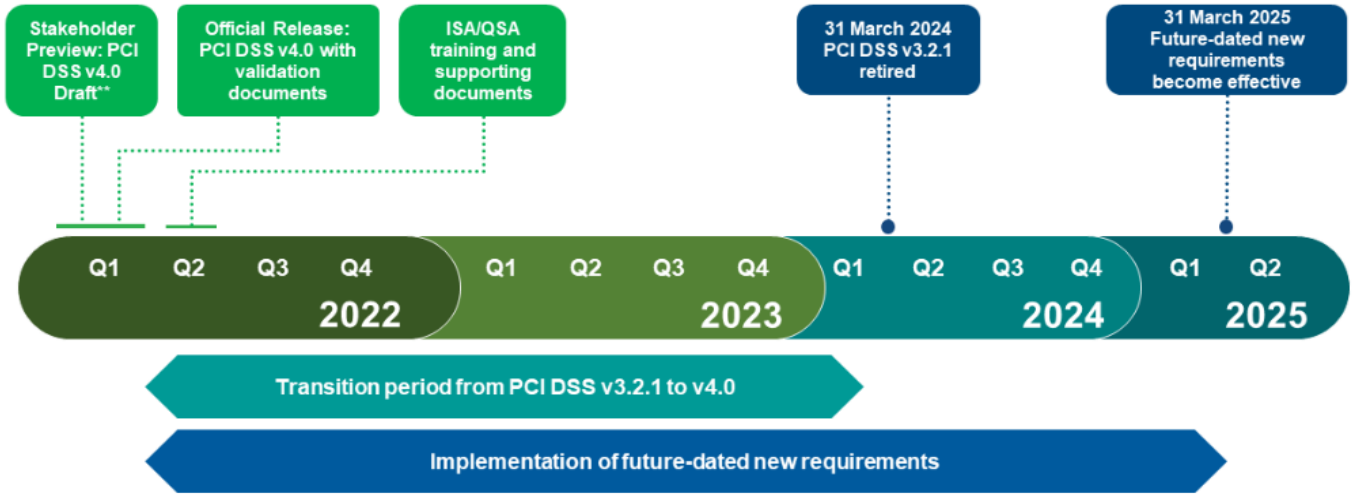
Treasury Institute for Higher Education

PCI DSS
Version 4.0

PCI DSS Version 4.0

- PCI DSS Version 4.0 was released in **March 2022**
  - Becomes effective **March 31, 2025**
    - Version 3.2.1 expires on March 31, 2024

PCI DSS v4.0 Implementation Timeline*



* All dates based on current projections and subject to change

** Preview available to Participating Organizations, QSAs, and ASVs

PCI DSS Version 4.0

- PCI SSC Key Goals for Version 4.0
  - Ensure standards meet security needs for the payments industry
  - Add flexibility and support additional methodologies for security
  - Promote security as a continuous process
  - Enhance validation methods and related procedures
- Introduces 64 new requirements that were not present in version 3.2.1
- Two approaches to validation: Defined and Customized
- Provides definitions for Timeframes
  - Every three months – 90-92 days
  - Immediately – Must be acted upon without delay
  - Promptly – Must be acted upon in a reasonable timeframe

PCI DSS Version 4.0

PCI DSS v4.0, key take-aways:

1. **Access Management** - The new version of the PCI DSS contains revisions to the authentication requirements to reflect the latest industry best practices for password and multi-factor authentication (MFA).
   a) MFA to be used for all accounts accessing CHD, not just Admins
   b) Passwords must be changed at minimum every 12 months
   c) Use of strong passwords at least 15 characters in length
   d) Access privileges reviewed every six months

2. **Risk Assessment** - The risk assessment requirement was modified to ensure that the risk assessment is not being treated as a "checkbox exercise" by organizations. PCI DSS 4.0 provides greater clarity and guidance for organizations on the risk management process.

(Source: https://ermprotect.com/blog/pci-dss-v4-0-what-you-need-to-know-now/

PCI DSS Version 4.0

3. **Flexibility: Customized Implementation to Meet the Intent of Security Controls** – This "Customized Approach" will allow organizations to design their own controls and implement them based on the intent of the requirements. This allows companies more flexibility to adopt new technologies or security solutions and not have to wait for the standard to catch up.

4. **Scoping** - The accuracy of PCI DSS scope is documented and confirmed at least once every 12 months and upon significant changes to the in-scope environment. For service providers, the scope must be reviewed every 3 months and upon significant changes to the in-scope environment.

(Source: https://ermprotect.com/blog/pci-dss-v4-0-what-you-need-to-know-now/

PCI DSS Version 4.0

5. **Security Awareness Training –** The requirements for training of end-users are enhanced to include more information regarding current threats and vulnerabilities that could impact the security of the cardholder data environment, including Phishing and Social Engineering. Must be reviewed/updated every 12 months.

6. **Encryption** - Card encryption requirements have been expanded to include all transmissions of cardholder data.

7. **Service Providers -** Mandates that service providers "support their customers' requests for information to meet Requirements, including providing AOCs (or other acceptable documentation) and some form of 12.8.5 responsibility matrix.

(Source: https://ermprotect.com/blog/pci-dss-v4-0-what-you-need-to-know-now/

PCI DSS Version 4.0

Highlighted SAQ changes

SAQ	Immediately	31 March, 2025
A-EP	6.2.1 Secure software development for bespoke and custom software and prevent common coding vulnerabilities 12.10.3 Personnel available for 24*7 incident response	6.3.2 Inventory of bespoke and custom software, and third-party software components 6.4.2 Deploy an automated technical solution for public-facing web applications to detect and prevent web-based attacks. [manual or automated review option removed] 6.4.3 Manage payment page scripts 8.4.2 MFA for all access into the CDE. 8.4.3 Ensure MFA not susceptible to replay attacks and cannot be bypassed by users 11.6.1 Change- and tamper-detection for payment page headers/content
B-IP	6.3.1 Identify and risk rank security vulnerabilities (applies to merchant firewall/router devices)	None
P2PE	9.4.1.1 Secure storage of offline media backups with cardholder data	3.2.1 Data retention and disposal policies and procedures to cover any Sensitive Authentication Data stored pre-authorization
C-VT	8.2.4 Documented authorization for user ID lifecycle changes	5.4.1 Automated detection and protection against phishing attacks 8.3.6 Minimum 12-character alphanumeric passwords / passphrases
C	6.2.1, 6.2.4 Secure software development for bespoke and custom software and prevent common coding vulnerabilities 12.10.3 Personnel available for 24*7 incident response	5.4.1 Automated detection and protection against phishing attacks 8.4.2 MFA for all access into the CDE. 8.4.3 Ensure MFA not susceptible to replay attacks and cannot be bypassed by users 8.6.1, 8.6.2, 8.6.3 Multiple controls to manage application and system accounts

- **Analyse the changes before committing to v4.0; many new SAQ Requirements are not future-dated**

(Source: Worldpay/VikingCloud "Insights, Impact and Implementation of PCI DSS Version 4.0" Webinar, June 28, 2022)

PCI DSS 4.0 – SAQ A Changes

New Requirements:

- Apply security patches/updates for known vulnerabilities
- Strengthened authentication requirements
- Quarterly ASV scanning
- Maintain an inventory of all scripts
- Verify the authenticity of headers and redirections
- Change detection for sites hosting vendor iFrames

PCI DSS 4.0 – SAQ A Changes

6.4.3 – Payment page scripts (iFrames) are inventoried, authorized, and integrity checked (4/1/25) – ON HOLD
- e.g., Content Security Policy (CSP), Sub-resource Integrity (SRI)

8.3.6 – Passwords required to have a minimum of 12 characters with both letters and numbers (4/1/25)

8.3.9 – If MFA is not used, then passwords much change every 90 days (or use zero trust / real-time analysis)

11.3.2 – Quarterly passing third-party ASV scans are required(4/1/25)

11.3.2.1 – ASV scans are also required after any significant change

11.6.1 – Change and tamper detection mechanisms for payment pages (4/1/25) – ON HOLD
- Review headers and payment pages at least every seven days

PCI DSS Version 4.0

Highlighted SAQ changes – SAQ A

Req.	Description of Change	Implementation Timeframe
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.	Immediately
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary	31 March, 2025
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Immediately
11.3.2.1	External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists	Immediately
11.6.1	A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	31 March, 2025

(Source: Worldpay/VikingCloud "Insights, Impact and Implementation of PCI DSS Version 4.0" Webinar, June 28, 2022)

PCI DSS Version 4.0

- PCI DSS 4.0 Implementation Recommendations
  - 2022-23 – Read and fully understand the new requirements
    - Attend training sessions, webinars, etc.
  - 2023 – Perform a GAP Analysis using 4.0 requirements
  - 2023-24 – Implement controls to fill GAPS identified in order to meet PCI DSS 4.0 requirements
  - By **March 31st, 2025** – Validate and Attest using PCI DSS 4.0

PCI DSS Compliance Resources

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

THE PAYMENTS ACADEMY
Education, Collaboration, Leadership

www.thepmtsacademy.org

TPA Annual Conference

May 2nd - 5th, 2027
Hyatt Regency St. Louis
St. Louis, MO

Treasury Institute for Higher Education

PCI DSS Compliance Resources

Treasury Institute for Higher Education

www.treasuryinstitute.org

Treasury Symposium 2027

Las Vegas, NV
January 10-13, 2027

PCI DSS Compliance Resources

Important Links

- **PCI Security Standards Council** – https://www.pcisecuritystandards.org
- **PCI DSS Quick Reference Guide** – https://www.pcisecuritystandards.org/document_library/?document=pci_ssc_quick_reference_guide
- **Prioritized Approach to PCI DSS Compliance** – https://www.pcisecuritystandards.org/document_library/?document=Prioritized_Approach_PCI_DSS_4_0
- **PCI DSS SAQ's** – https://www.pcisecuritystandards.org/document_library?category=saqs#results
- **The Treasury Institute for Higher Education –** http://www.treasuryinstitute.org
- **The Payments Academy –** https://www.thepmtsacademy.org/

cbmi
COLLEGE BUSINESS MANAGEMENT INSTITUTE

Any questions?

Thank you for attending!

Auxiliary Services

Treasury Institute for Higher Education

SACUBO
SOUTHERN ASSOCIATION OF COLLEGE AND UNIVERSITY BUSINESS OFFICERS