Payment Card Acceptance and PCI DSS

Kevin Sisler
Director of Treasury Services
University Financial Services
University of Kentucky
(859) 257-7356

see blue.
in everything we do.
Payment Card Usage
The global brand general purpose cards—Visa, UnionPay, Mastercard, JCB, Diners Club/Discover, and American Express—generated 368.92 billion purchase transactions for goods and services in 2018, up 24.9% over 2017.

If each of the Earth’s 7.6 billion people had a credit card, they would have swiped it an average of 48 times.

At the end of 2018, global brand credit, debit, and prepaid cards in circulation reached **13.19 billion**, an increase of **10.4%** from 2017.

In 2018, the market share of debit cards of total cards in circulation was 77.46%, up from 76.89% in 2017. Credit cards accounted for a 22.54% market share, down from 23.11%.

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

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)
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

In 2018, the percentage of students surveyed that stated they used a debit/credit/prepaid card to pay for:

- Tuition and Fees – 58%
- Textbooks, school supplies, or other direct education expenses – 75%

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

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

Can you afford not to?
According to the 2019 Verizon Data Breach Investigations Report:
According to the 2019 Verizon Data Breach Investigations Report:

- Financially motivated breaches fell from 76% to 71%
- 52% of cyberattacks involve hacking
- 90% of malware arrived via email
- Continued reduction in payment card point of sale breaches
- 60% of web application attacks were on cloud-based email servers
- Misconfiguration of cloud platforms accounted for 21% of breaches caused by errors
- A third (32%) of breaches involved phishing
- Ransomware is the second biggest malware threat and accounted for 24% of malware-related breaches
Educational Institutions are Hacker Targets...

According to Verizon’s 2016 Data Breach Investigations Report (DBIR), the education sector ranked sixth overall in the US for the total number of reported “security incidents” in 2015.

“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
HOW TO PICK A CAREER IN CRIME

Global Crime Statistics in Perspective

$56B
STOLEN VEHICLE MARKET

$30B
STOLEN SMART PHONE

$85B
COCAIN MARKET

CYBERCRIME MARKET

$114B
STOLEN CREDIT CARD MARKET

$358BILLION
For what reasons are you taking credit cards on campus?

- Tuition
- Housing
- Books
- Dining Facilities
- Admissions
- Campus Payment Cards
- Meetings, Seminars, & Conference Registrations
- Gifts/Donations
- Hospital/Medical Facilities
- Registrar (i.e. Transcripts)

- Library Fees & Fines
- Campus Hotel
- Greek Recruitment
- Sale of Goods (i.e. brain probes, geological surveys)
- Services (i.e. Veterinary Diagnostics)
- Wellness Facilities
- Alumni Affairs
- Extension Services
- Theater & Concert tickets
What methods are used to process payments on campus?

- Manual Imprinters for off campus events
- Point-of-Sale (POS) Systems or Payment Applications
- Dial-up or Cellular Credit Card Swipe Terminals
- Mobile Device?
- E-commerce & Online Payment forms
Swipe Terminal Credit Card Payment

Card Swiped on a Credit Card Terminal

University’s Primary Financial Institution

Authorization & Settlement

Credit Card Processor/Acquirer (i.e. First Data)

Funds transmitted via ACH

Cardholder’s Bank (Issuer)

Authorization & Settlement

Funds moved to Your Cost Center Via JV from Treasury Services
Web-based Credit Card Payment

Your Website with a web application on a university server

Hosted Order Page
Payment Gateway (i.e. Authorize.net)

Customer enters credit card on this site and payment is processed

NOTE: No card holder data transmitted from your site

Transaction information passed (Name, Trans #, Amt)

University’s Primary Financial Institution

Credit Card Processor/Acquirer (i.e. First Data)

Funds transmitted via ACH

Treasury Services moves funds to department cost center

Cardholder’s Bank (Issuer)
UK Card Processing Environment
As of today:

215 merchant accounts

307 TID#’s (Terminal Identification Numbers – either swipe terminals or online transaction processing points)
As of today:

Number of merchant units processing by:

- Credit Card Swipe Terminals – 211
- Website – 95
- POS System or Payment Application – 1

Note: Some merchants do a combination of both a swipe terminal and Website/POS/PA
In FY 2019, UK merchant units processed:

**Total Transactions:** 834,817
Increase of 11.56% from FY 2018

**Total Revenue:** $129,173,625.99
Increase of 7.54% from FY 2018
### Top Ten Merchants in Total Transactions

<table>
<thead>
<tr>
<th>Merchant Name</th>
<th>Transaction Total</th>
<th>% of Total</th>
<th>Average $ per Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 UK PARKING OFFICE</td>
<td>258,505</td>
<td>39.81%</td>
<td>$20.18</td>
</tr>
<tr>
<td>2 UK ATHLETICS</td>
<td>57,412</td>
<td>8.84%</td>
<td>$763.38</td>
</tr>
<tr>
<td>3 UK STUDENT ACCOUNT SERVICES</td>
<td>46,786</td>
<td>7.21%</td>
<td>$761.87</td>
</tr>
<tr>
<td>4 UK HEALTHCARE - KC PHARMACY</td>
<td>45,421</td>
<td>7.00%</td>
<td>$32.63</td>
</tr>
<tr>
<td>5 UK DENTISTRY</td>
<td>20,821</td>
<td>3.21%</td>
<td>$159.42</td>
</tr>
<tr>
<td>6 UK CKMS</td>
<td>19,442</td>
<td>2.99%</td>
<td>$114.88</td>
</tr>
<tr>
<td>7 UK PLUS ACCOUNT OFFICE</td>
<td>18,802</td>
<td>2.90%</td>
<td>$93.76</td>
</tr>
<tr>
<td>8 UK HEALTHCARE - PATIENT ACCOUNTS</td>
<td>6,958</td>
<td>1.07%</td>
<td>$380.45</td>
</tr>
<tr>
<td>9 UK GRADUATE AND FAMILY HOUSING</td>
<td>6,405</td>
<td>0.99%</td>
<td>$527.74</td>
</tr>
<tr>
<td>10 UK HEALTHCARE - HOSPITAL #2</td>
<td>5,590</td>
<td>0.86%</td>
<td>$313.80</td>
</tr>
</tbody>
</table>

75%
### Top Ten Merchants in Total Revenue

<table>
<thead>
<tr>
<th>Merchant Name</th>
<th>Net Sales Amount</th>
<th>% of Total Net Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 UK ATHLETICS</td>
<td>$43,827,453.92</td>
<td>40.70%</td>
</tr>
<tr>
<td>2 UK STUDENT ACCOUNT SERVICES</td>
<td>$35,644,865.12</td>
<td>33.10%</td>
</tr>
<tr>
<td>3 UK PARKING</td>
<td>$5,216,246.85</td>
<td>4.84%</td>
</tr>
<tr>
<td>4 UK GRADUATE AND FAMILY HOUSING</td>
<td>$3,380,146.01</td>
<td>3.14%</td>
</tr>
<tr>
<td>5 UK DENTISTRY</td>
<td>$3,319,202.87</td>
<td>3.08%</td>
</tr>
<tr>
<td>6 UK HEALTHCARE - PATIENT ACCOUNTS</td>
<td>$2,647,162.54</td>
<td>2.46%</td>
</tr>
<tr>
<td>7 UK CKMS</td>
<td>$2,233,423.17</td>
<td>2.07%</td>
</tr>
<tr>
<td>8 UK PLUS ACCOUNT OFFICE</td>
<td>$1,762,878.16</td>
<td>1.64%</td>
</tr>
<tr>
<td>9 UK HEALTHCARE - HOSPITAL #2</td>
<td>$1,754,155.43</td>
<td>1.63%</td>
</tr>
<tr>
<td>10 UK HEALTHCARE - KC PHARMACY</td>
<td>$1,482,267.61</td>
<td>1.38%</td>
</tr>
</tbody>
</table>

94%
PCI DSS Background

Whose Crazy Idea Was This, Anyway?
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
What's in **Your** Wallet?

What is PCI DSS trying to protect?
Increased data breaches and card fraud

Setting the Stage for Standardization

WE ALL KNOW THESE MERCHANTS

THE UNKNOWN

Breached Consumer Records: a 1-week increase of 396%

546 Breaches
18,953,433 consumer records exposed

783 DATA BREACHES IN THE U.S. 2014

85,611,528
Exposed U.S. consumer records in 2014

↑ 27.5% Over the number of Breaches Reported in 2013

As of September 16, 2014

OF SOUTHERN CALIFORNIA
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
Response From the Brands

Cardholder Information Security Program

Payment Card Industry Security Council

PCI DSS

Site Data Protection

Data Security Operating Policy

Data Security Program

Information and Compliance

seeblue. in everything we do.
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 Historical 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 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 Version 4.0 to be released in 2020.
Relationship Between the Standards

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

Manufacturers
- PCI PTS
  - PIN Entry Devices

Software Developers
- PCI PA-DSS
  - Payment Applications

Merchants & Service Providers
- PCI DSS
  - Secure Environments

PCI Security & Compliance

P2PE

Ecosystem of payment devices, applications, infrastructure and users
PCI Food Chain

PCI Security Standards Council
- PCI DSS
- PA DSS
- PIN PTS
- P2PE

Card Association
- Card Association Rules

Acquirer
- Merchant Agreement

Merchant
- Business Procedures for Credit Card Merchants (E-2-11)
- Information Security Policy
- Security Standards for PCI DSS Systems
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
<table>
<thead>
<tr>
<th>PCI DSS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network</strong></td>
</tr>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td><strong>Protect Cardholder Data</strong></td>
</tr>
<tr>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td><strong>Maintain a Vulnerability Management Program</strong></td>
</tr>
<tr>
<td>5. Use and regularly update anti-virus software</td>
</tr>
<tr>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td><strong>Implement Strong Access Control Measures</strong></td>
</tr>
<tr>
<td>7. Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td><strong>Regularly Monitor and Test Networks</strong></td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td><strong>Maintain an Information Security Policy</strong></td>
</tr>
<tr>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
## Merchant Level Classifications

<table>
<thead>
<tr>
<th>Your Level is:</th>
<th>Your business does:</th>
<th>You should:</th>
</tr>
</thead>
</table>
| 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 |
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

The cost of a breach can easily be 20 times the cost of compliance

UK PCI DSS Compliance
How do we get there?
Ahhhh!
PCI DSS Compliance Roadmap

- Merchant Classification
- Staying Compliant
- Scoping
- Gap Analysis
- SAQ Validation
- Implementation
- Scan Validation
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
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 Version 3.0

<table>
<thead>
<tr>
<th>SAQ Validation Type</th>
<th>Description</th>
<th># of Questions v3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage</td>
<td>14</td>
</tr>
<tr>
<td>A-EP</td>
<td>E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage</td>
<td>139</td>
</tr>
<tr>
<td>B</td>
<td>Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage</td>
<td>41</td>
</tr>
<tr>
<td>B-IP</td>
<td>Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage</td>
<td>83</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage</td>
<td>139</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage</td>
<td>73</td>
</tr>
<tr>
<td>D</td>
<td>All other SAQ-eligible merchants</td>
<td>326</td>
</tr>
<tr>
<td>D-SP</td>
<td>SAQ-eligible service providers</td>
<td>347</td>
</tr>
<tr>
<td>P2PE</td>
<td>Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage</td>
<td>35</td>
</tr>
</tbody>
</table>
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
UK Website Model Using a Hosted Order Page

Your Website with a web application on a UK server

Transaction information passed (Name, Trans #, Amt)

NOTE: No card holder data transmitted from your site

Hosted Order Page Payment Gateway (i.e. Skipjack)

Customer enters credit card on this site and payment is processed

Authorization & Settlement

Funds transmitted via ACH

Credit Card Processor/Acquirer (i.e. RBS WorldPay)

Funds moved to Your Cost Center Via JV from Treasury Services

University of Kentucky’s Primary Financial Institution

seeblue. in everything we do.
Merchant Classification

Outsourced Hosted Order Page

SAQ A if:
- Website hosted by a compliant 3rd party service provider
- Customers redirected 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
Merchant Classification

University Hosted Order Page

SAQ A-EP if:
- Website hosted on a university webserver
- Customers redirected 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
# Merchant Classification

## SAQ-A versus SAQ-A-EP

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>SAQ A</th>
<th>SAQ A-EP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Card-not-present merchants</strong> (e-commerce or mail/telephone-order)*</td>
<td><strong>All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers</strong></td>
<td><strong>E-commerce merchants</strong></td>
</tr>
<tr>
<td><strong>Functions Outsourced</strong></td>
<td><strong>Control of Cardholder Data</strong></td>
<td><strong>Control of Cardholder Data</strong></td>
</tr>
<tr>
<td><strong>E-commerce merchants</strong></td>
<td><strong>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.</strong></td>
<td>**Merchant's e-commerce website does not receive cardholder data but <strong>controls how consumers, or their cardholder data, are redirected</strong> to a PCI DSS validated third-party payment processor.</td>
</tr>
<tr>
<td><strong>Payment Pages</strong></td>
<td><strong>The entirety of all payment pages delivered to the consumer's browser originates directly from a PCI DSS validated third-party service provider(s).</strong></td>
<td><strong>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).</strong></td>
</tr>
<tr>
<td><strong>Third-Party Compliance</strong></td>
<td><strong>Merchant confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant</strong></td>
<td><strong>Merchant confirmed that all third party(s) handling <strong>storage, processing, and/or transmission</strong> of cardholder data are PCI DSS compliant</strong></td>
</tr>
<tr>
<td><strong>Merchant Systems</strong></td>
<td><strong>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</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Data Retention</strong></td>
<td><strong>Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically</strong></td>
<td></td>
</tr>
</tbody>
</table>

(Source: “Understanding the SAQs for PCI DSS v3.0”, PCI SSC website, April 2015)
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
**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**
- Evidence of SAQ D and scanning
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
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 UK network must utilize the **UK PCI DSS Segmented VLAN.**
PCI DSS Compliance Roadmap

Staying Compliant

Merchant Classification

What kind of Merchant am I?

What systems, devices, networks, or records fall within my Cardholder Date Environment (CDE)?

Scoping

Gap Analysis

What are the gaps between my current processes and the PCI DSS requirements?

Implementation

SAQ Validation

Scan Validation

Complete the appropriate SAQ and ensure all requirements are met. Submit SAQ to UK Merchant Card Services (MCS).

If storing credit cards within systems or processing transactions over the network, complete quarterly ASV Scans. (Handled by UK MCS)

If CDE expands, processes change, or technologies change, perform gap analysis and implement solutions to meet the requirements.

see blue.

in everything we do.
How did University of Kentucky get there?
UK PCI DSS Compliance Process

- Formed a cross-departmental PCI DSS Oversight Committee
  - Members included:
    - Office of the Treasurer
    - Internal Audit
    - IT Security
    - Representatives from our largest transaction merchants

- Who are the merchants?
  - Surveyed all and met with many of our merchants
  - How are they processing payments?
  - Why are they processing payments?
  - Are they storing credit card data in electronic or physical format?
Hired the Director of Merchant Card Services to head MCS department and lead PCI DSS Compliance Project

Formed a PCI DSS Project Team
UK PCI DSS Project
Team Members

University Financial Services
Kevin Sisler
Dir. of Treasury Services
(859) 257-7356
Karen Lawson
MCS Administrative Support Associate
(859) 257-3969

UK HealthCare IT Security Office
Doug Fee
Chief Information Security Officer
(859) 323-1804
Bill Cotter
Cybersecurity Principal, Information Security
(859) 323-6474

UK IT Security Office
Heath Price
Associate Chief Information Officer
(859) 323-7013
George Insko
Director of Cybersecurity
(859) 257-5688
Wendell McCarty
Programmer Systems Lead
(859) 257-2200
Michael Sheron
Information Security Analyst
(859) 257-4594
Hired the Director of Merchant Card Services to head MCS department and lead PCI DSS Compliance Project

Formed a PCI DSS Project Team

Classified each merchant based on how they process credit card transactions to determine SAQ Validation type.
UK PCI DSS Compliance Process

- Determined IT infrastructure equipment and security systems necessary for PCI DSS Compliance.
  - Firewalls and network equipment
  - Internal Application Vulnerability Scanning system
  - Network Scanning System
  - Intrusion Detection and Protection system
  - File Integrity Monitoring system

- Developed a budget and official compliance plan to get approval and funding for the project.
  - We requested and received approximately $260,000 for the initial PCI DSS project
Once plan and funding was approved, IT Security led the effort to implement IT infrastructure changes to support PCI DSS segmented network.
Before PCI DSS Segmented Network

Credit Card Processing systems transmitting credit card data across UK 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
Move credit card processing systems to the UK PCI DSS Segmented Network

- 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
UK PCI DSS Compliance Process

After PCI DSS Segmented Network

UK PCI DSS Segmented Network Using MPLS Architecture
Conducted separate PCI DSS training sessions for merchants in each SAQ Validation type.

Met with some merchants and helped change the way they process in order to minimize their risk.
  - Use of hosted order pages.
  - Move from POS systems to swipe terminals.
  - Discontinue use of Virtual Terminals.
UK PCI DSS Compliance Process

- Coordinated and assisted merchants with their own PCI Compliance program and SAQ submission.
  - Developed policy templates for each merchant category.
  - Developed FAQ to assist merchants in filling out SAQ’s.

- Met with our higher risk SAQ C & D merchants individually and guided them through moving their systems to the segmented network and completing their SAQ’s.
UK PCI DSS Compliance Process

- Annually submitting our Self-Assessment Questionnaire to our transaction processor/acquirer to validate University’s overall PCI DSS compliance.

- Running the required quarterly Approved Scan Vendor (ASV) Vulnerability scans for a SAQ C & D merchants and submitting scans to transaction processor/acquirer.

- Conduct annual Penetration Testing to ensure networks and systems are secure and compliant with PCI DSS.
  
  Requirement 11.3.
UK PCI DSS Compliance
Major Objectives
Obj. #1: Minimize the amount of credit card data that is collected, stored, and transmitted by University servers via the UK network.

- Web-based merchant units should utilize a Hosted Order Page provided by a PCI Compliant 3rd Party Internet Processing Gateway service provider (i.e. Skipjack).

- 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.
If you don’t need it, DON’T KEEP IT!
UK PCI Compliance Plan

Goals

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
UK PCI Compliance Plan

Goals

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

- 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

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

* Eliminate, encrypt, one-way hash, truncate or use compensating controls.

**Protect if stored with PAN.
If you don’t need it, DON’T KEEP IT!

(especially keep it off your computers, servers, and network)
## Data Storage Basics

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

Goals

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

- Records containing credit card numbers should be physically secured and access controlled.

- Physical records containing credit card data should be destroyed or made unreadable **3 years** after a transaction is processed.

* According to Record Series U0239 of the State University Records Retention Schedule for Kentucky
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.
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.
Merchant Unit Responsibilities (continued)

- Attendance to an annual PCI DSS Compliance Training seminar conducted by the UK Merchant Card Services Department.

- 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.
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.
Office of the Treasurer 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.
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
Project 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.
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
According to PCI DSS version 2.0, you must verify the scope of your Cardholder Data Environment (CDE).

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?
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 DSS Compliant

- Additional merchant duties under Requirement 12.8
- Written agreement
- Due diligence
- Evidence of PCI compliance
  - Report of 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
- 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 – Our 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)
PCI DSS Compliance
Points of Emphasis

- External/Outsourced Vendors (e.g. Follett, Morrison’s Cafeteria, Sodexho at Commonwealth, KMSF) – Our 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.
Mobile Payments via cell phone apps (i.e. Square)

- Very few, if any, certified PCI DSS compliant solutions
- Most solutions claim to encrypt CHD at the time of swipe
  - What about key-entered transactions when a card won’t swipe
  - Probably SAQ-D if key-entered transactions are allowed
- PCI SSC released best practices for mobile payment acceptance in August 2014
  - Mobile Payment Acceptance Security Guidelines for Merchants as End-Users v1.1*

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.
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.
EMV

- Also known as “Chip and Pin”
- Vastly reduces card-present fraud
- Makes counterfeiting cards infeasible
- Introduces a dynamic, cryptographic element
- Will take 3-5 years for adoption
- Increase in CNP fraud
- Cards still have mag stripe for now
- Liability Shift to merchants in October 2015
PCI DSS Compliance

Emerging Technologies

A Holistic Approach to Security is Required

P2PE
Encrypts/Devalues card data at the point of entry

Tokenization
Replaces/Devalues card data at rest

EMV
Reduces fraud from counterfeit cards at point-of-sale

Point of Sale
Important Links

- **PCI Security Standards Council** – https://www.pcisecuritystandards.org


- **Prioritized Approach to PCI DSS Compliance** – https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

- **PCI DSS SAQ’s** – https://www.pcisecuritystandards.org/document_library?category=saqs#results

- **The Treasury Institute for Higher Education** – http://www.treasuryinstitute.org/pcidssworkshop/
PCI DSS Workshop
April 26-29th, 2020
Hyatt Regency Savannah
Savannah, Georgia

http://www.treasuryinstitute.org
Any questions?

Thank you for attending!

Kevin Sisler
Director of Treasury Services
University Financial Services
University of Kentucky
Phone - (859) 257-7356
Email – Kevin.Sisler@uky.edu