PCI-DSS Compliance

Elahe Russell

February 12, 2019

What is PCI-DSS?

THE **PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)** IS AN INFORMATION SECURITY STANDARD INTENDED TO OPTIMIZE THE SECURITY OF CREDIT, DEBIT AND CASH CARD TRANSACTIONS AND PROTECT CARDHOLDERS AGAINST MISUSE OF THEIR PERSONAL INFORMATION.

PCI Readiness Review

- LSU engaged CampusGuard as a Qualified Security Assessor (QSA)
- Met with PCI Team and Information Technology (IT)/Security teams
- Conducted PCI training sessions for merchants and IT
- Provided preliminary results to Executive Leadership
- Participated in 14 onsite merchant interviews

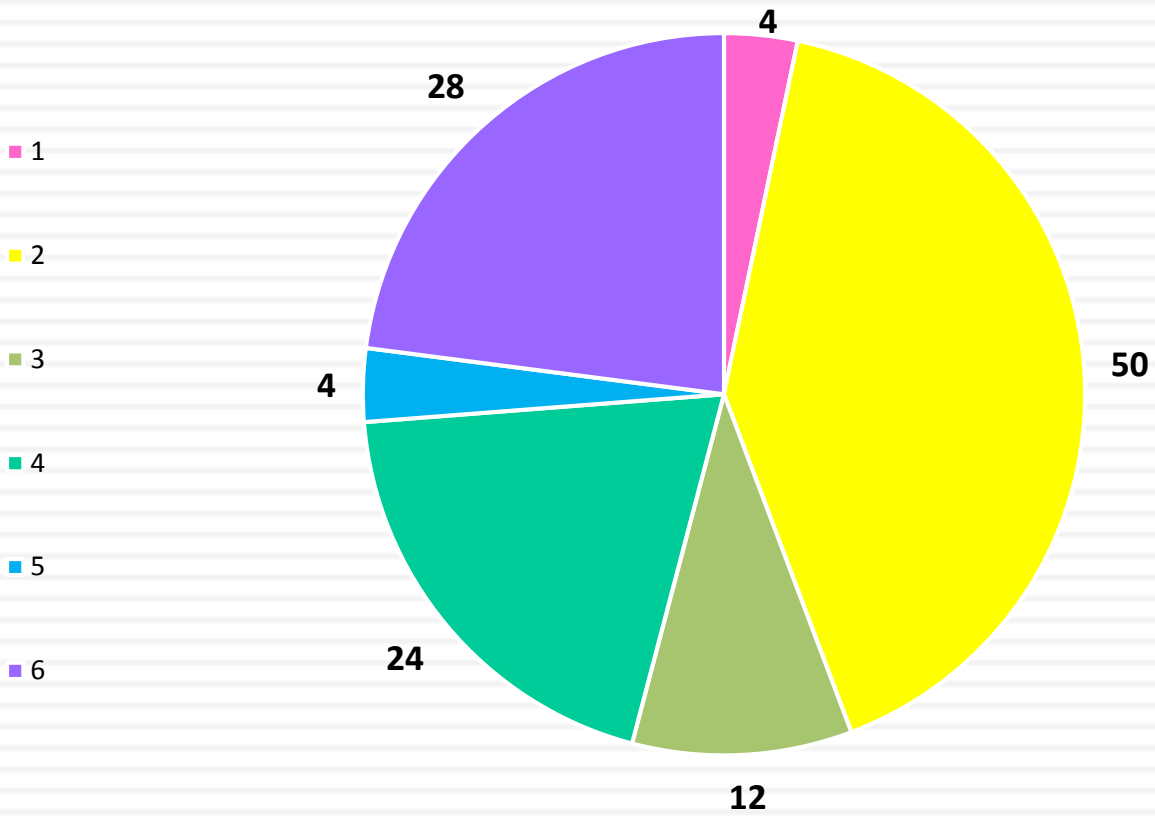
Merchant Interviews

Athletics Ticket Office	Pennington Biomedical Research Center
Auxiliary Services – Event Management	Residential Life
Auxiliary Services – Union Theater	Rural Life Museum
Bursar Operations	Student Health Center
Center for Computation and Technology	University Laboratory School
LSU Golf Course	University Recreation
Parking, Traffic & Transportation	Veterinary Medicine

PCI-DSS Milestones

Milestone	Goal
1	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it!
2	**Protect systems and networks, and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises, and the processes for responding.
3	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.
6	**Finalize remaining compliance efforts, and ensure all controls are in place.** The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

Findings by Milestone



Recommendations

DO NOT	DO
× Process or transmit cardholder data (CHD) on general use computers	✓ Discontinue using workstations as a method to enter payment card information
× Accept CHD via email	✓ Provide PCI-listed P2PE solutions or stand alone terminals to eliminate the need to enter CHD on employee workstations
× Use campus wi-fi for payment processing	✓ Destroy CHD in a PCI compliant manner
× Accept CHD faxed to network or multi-function printers	✓ Use cross-cut shredders to destroy any CHD
× Retain or store paper including CHD	✓ Regularly check hardware for skimming devices

Action Items

- Formalize PCI Team and charter
- Review all merchants and related payment processes
- Verify equipment and media inventory
- Eliminate storage of CHD/secure information disposal
- Cease email and unsecured fax acceptance of payment card information
- Update Incident Response Plan
- Revise and update institutional policy

- Create departmental procedures for merchants
- Formalize training of departmental merchants
- Implement procedures for inspecting devices
- Complete Self-Assessment Questionnaires (SAQs)
- Review service provider compliance
- Implement third-party service provider management program

PCI Team

Elahe Russell	erussell@lsu.edu	Accounting Services
Beth Nettles	studbr@lsu.edu	Bursar Operations
Anthony Gonce	agonce1@lsu.edu	Internal Audit
Sumit Jain	sjain@lsu.edu	IT Security and Policy
Daniel Butcher	dbutch1@lsu.edu	Bursar Operations
Sean Robbins	sean@lsu.edu	Network Engineering
Jeff Deveer	jeff@lsu.edu	Athletics
Tyler French	tfrench1@lsu.edu	Bursar Operations
Sam Abboud	sabbou2@lsu.edu	College of Human Sciences and Education
Jan Bernath	jbernath@agcenter.lsu.edu	LSU Agricultural Center
Monica Mougeot	monica.mougeot@pbrc.edu	Pennington Biomedical Research Center

CashNet Project Update

Daniel Butcher

February 12, 2019

Background & Timeline

- Merchant Services
  - Payment Card Industry Data Security Standards (PCI-DSS)
- Cashiering Solution
  - Workday Student Design Partner Group

CashNet Modules

- eBill
- ePayment
- SmartPay
- Payment Plans
- Cashiering
- eMarket
- eRefund

Project Phases

Phase I

- eMarket
  - Storefront
  - Checkout
- SmartPay

Phase II

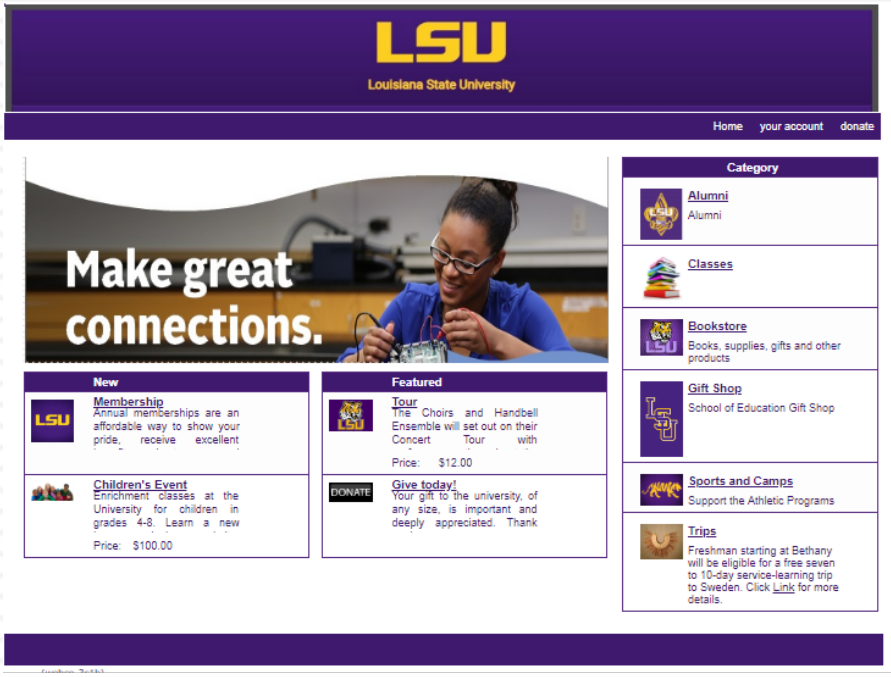
- Cashiering
  - Bursar Operations
  - Merchants

Phase III

- eBill
- ePayment
- Payment Plans
- eRefund

CashNet Advantages

- Merchant ID owned by CashNet
  - Significant reduction of PCI scope
- Automated departmental deposits
- P2PE solutions for cashiering
- Customizable storefronts



Challenges

- Real-time G/L validation with Workday
- G/L segment limitation
- Student Modernization Program timeline
- Merchant adoption (eMarket)
- Third-party vendor contacts (eMarket)

Questions

Daniel Butcher
Assistant Director
Bursar Operations
dbutch1@lsu.edu