



---

## PCI Compliance in Higher Education

---

California State University

Auxiliary Organizations Association

January 9, 2012

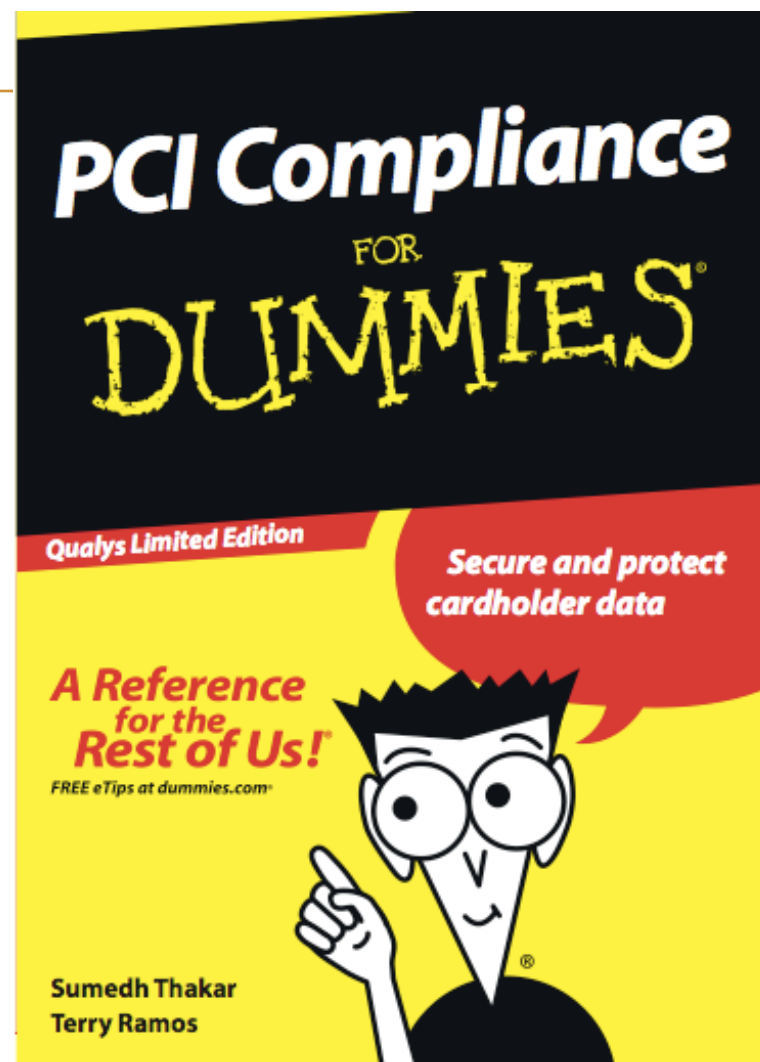
Walter Conway, QSA

403 Labs, LLC

# Agenda

---

- ❑ The PCI ecosystem
- ❑ PCI and Higher Ed
- ❑ Validating compliance:  
The SAQs
- ❑ Outsourcing: not a panacea
- ❑ Where is my silver bullet?



# Walt Conway, 403 Labs

- ❑ PCI QSA, consultant, blogger, trainer, speaker, author
  - Former Visa VP
  - Represent NACUBO at PCI Council
  - Help schools become PCI compliant
- ❑ 403 Labs: Security consulting firm
  - All things PCI: QSA, PA-QSA, ASV, PFI



Treasury Institute  
for Higher Education



# Some PCI DSS Basics

---

- ❑ Payment Card Industry Data Security Standard
- ❑ Goal is to protect Cardholder Data
  - And to keep you out of the headlines
  - PCI does not make you secure
- ❑ If you take plastic, PCI applies to you
- ❑ **PCI scope** includes
  - Any system that “**stores, processes, or transmits**” cardholder data
  - Any connected system
- ❑ PCI is a program, not a project
- ❑ Two things you need to accept about PCI
  - Your costs have gone up
  - You will change the way you do business

# PCI DSS: 6 Goals, 12 Requirements

## PCI Data Security Standard – High Level Overview

<b>Build and Maintain a Secure Network</b>	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect cardholder data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
<b>Protect Cardholder Data</b>	<ol style="list-style-type: none"><li>3. Protect stored cardholder data</li><li>4. Encrypt transmission of cardholder data across open, public networks</li></ol>
<b>Maintain a Vulnerability Management Program</b>	<ol style="list-style-type: none"><li>5. Use and regularly update anti-virus software or programs</li><li>6. Develop and maintain secure systems and applications</li></ol>
<b>Implement Strong Access Control Measures</b>	<ol style="list-style-type: none"><li>7. Restrict access to cardholder data by business need to know</li><li>8. Assign a unique ID to each person with computer access</li><li>9. Restrict physical access to cardholder data</li></ol>
<b>Regularly Monitor and Test Networks</b>	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes.</li></ol>
<b>Maintain an Information Security Policy</b>	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security for all personnel.</li></ol>

# Campus Merchant Challenges

---

## ❑ What I learned at QSA training...

### ❑ Athletics

- Wireless (game days); ticketing; luxury boxes; links to Development and Alumni systems; call centers (voice recording); service providers; camps; email/web/fax transactions

### ❑ Development, Alumni, Foundation

- Cardholder data everywhere (PII, too); recurring payments; scanning forms; email/web/fax transactions; hosted payment apps (including home brewed); remote events; call center (voice recording)

### ❑ Medical center

- Retail spaces; food service; individual practices; patient collections including outside agencies; voice recording

# Campus Merchant Challenges

---

## ❑ Miscellaneous Auxiliaries

- Bookstore, food service: they store cardholder data
- Hotel: store cardholder data; food service; events
- Conferences: web and onsite registration
- TV/radio station: pledge drives; stored cardholder data; maintaining device security between pledge drives

## ❑ Traffic and Parking

- payment apps store cardholder data; kiosks; paper forms

## ❑ Unrelated third parties

- DVD kiosks, contractors, franchises
- Third-party **OMG!** – Are you a PCI Service Provider?

# The Self-Assessment Questionnaires (SAQs)

- Most campus merchants self-assess

SAQ Validation Type	Description	SAQ	
1	Card-not-present merchants, all cardholder data functions outsourced, no electronic cardholder data storage	A	13 Items
2	Imprint-only merchants, no electronic cardholder data storage	B	29 Items
3	Stand-alone terminal merchants, no electronic cardholder data storage	B	80 Items
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C	51 Items
"4-ish"	Merchants who process cards on isolated virtual terminals connected to the Internet	C-VT	280+ Items
5	All other merchants and service providers	D	



- "ABSD" only if no electronic cardholder data stored

# SAQ A

---

- Card-not-present merchants only
  - E-commerce, MOTO
  - Never applies in a face-to-face POS environment
- Card processing is outsourced (e.g., CASHNet)
  - No cardholder data stored, processed, or transmitted on your systems
- Third party confirms it is PCI compliant
- Only paper records, not received electronically
- You store no cardholder data electronically

# SAQ B

---

- ❑ For merchants with stand-alone dial-up terminals
  - Brick-and-mortar, MOTO, or e-commerce
- ❑ Dial-up terminals only connected to processor
  - i.e., not connected to any other systems
- ❑ Terminals not connected to Internet
- ❑ Paper records, not received electronically
- ❑ You store no cardholder data electronically



# SAQ C

---

- Payment application and Internet connection on the same device
  - Card-present or card-not-present merchants
  - Can be POS or shopping cart application
- Device is not connected to any other systems
- Store only paper records, not received electronically
- You store no cardholder data electronically
- Payment application vendor provides remote support securely



# SAQ C-VT

---

- ❑ Merchant uses a virtual terminal
  - Web browser connected to processor that hosts payment processing function
  - Enter card data manually, via a secure connection, one transaction at a time
  - Brick-and-mortar or MOTO
  
- ❑ Single payment terminal, isolated, fixed
  
- ❑ Other requirements same as SAQ C



# Everybody Else is SAQ D

The image shows a screenshot of the PCI Security Standards Council's "Attestation of Compliance, SAQ D—Service Provider Version" form. The form is titled "Attestation of Compliance, SAQ D—Service Provider Version" and includes the PCI Security Standards Council logo. Below the title, there are instructions for submission. The form is divided into several sections: Part 1. Qualified Security Assessor Company Information (if applicable), Part 2. Service Provider Organization Information, Part 2a. Services, Part 2b. Relationships, and Part 2c. Transaction Processing. Each section contains various input fields for company names, contact information, addresses, and service details.

**PCI Security Standards Council**

**Attestation of Compliance, SAQ D—Service Provider Version**

*Instructions for Submission*  
The service provider must complete the Attestation of Compliance as a declaration of the service provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and refer to the submission instructions at PCI DSS Compliance - Completion Steps in this document.

**Part 1. Qualified Security Assessor Company Information (if applicable)**

Company Name:		Title:	
Lead QSA Contact Name:		E-mail:	
Telephone:		Country:	
Business Address:			
State/Province:		ZIP:	
URL:			

**Part 2. Service Provider Organization Information**

Company Name:		Title:	
Contact Name:		E-mail:	
Telephone:		Country:	
Business Address:			
State/Province:		ZIP:	
URL:			

**Part 2a. Services**

Services Provided (check all that apply):

<input type="checkbox"/> Authorization	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> 2-D Secure Access Control Service
<input type="checkbox"/> Switching	<input type="checkbox"/> PSP (E-commerce)	<input type="checkbox"/> Process Magnetic-Stripe Transactions
<input type="checkbox"/> Payment Gateway	<input type="checkbox"/> Clearing & Settlement	<input type="checkbox"/> Process MOTO Transactions
<input type="checkbox"/> Hosting	<input type="checkbox"/> Billing Processing	<input type="checkbox"/> Other (please specify):

Let facilities and locations included in PCI DSS (level):

**Part 2b. Relationships**

Does your company have a relationship with one or more third-party service providers (e.g. gateway, web-hosting companies, airline booking agents, loyalty program agents, etc)?  Yes  No

**Part 2c. Transaction Processing**

How and in what capacity does your business store, process and transmit cardholder data?

Payment Applications in use or provided as part of your service: Payment Application Version:

- SAQ D:
  - 280 questions
- All 12 PCI requirements

# SAQ A OMG!

---

## ❑ “Customer Service”

- Outsource Web payments (e.g., CASHNet)
- MOTO, fax, even walk-up orders persist
- Staff enter transactions on their workstation (or direct student to payment kiosk)
- Result: workstation and every system it connects to is “in scope” for PCI

## ❑ Result: SAQ D

- 280+ questions
- Full PCI DSS including scans and penetration testing

# A Word About Shortened SAQs

---

- ❑ Target is small merchant
- ❑ If not a perfect fit, SAQ may not be appropriate
- ❑ *“You must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant”*
  - Other PCI requirements may (and likely do) apply
  - Use SAQ as guide, not end of PCI compliance

# Outsourcing

---

- ❑ Strategic question:  
Do you want to be in the payments business?
- ❑ Outsourcing some or all processing can simplify your path to PCI compliance
  - Service Providers – You use their systems, services
  - Software Application Vendors – You buy a software package, and host it on your own system

# Outsourcing: Service Providers

---

- ❑ They store, transmit, or process cardholder data on your behalf
- ❑ You are still responsible
  - Ensure service providers are PCI compliant
  - Validate, and include PCI compliance in contract
  - Control third-party connections
- ❑ Visa and MasterCard websites lists PCI-compliant service providers

# Outsourcing: Applications

---

- ❑ Payment Application Data Security Standard (PA-DSS)
  - Compliant third-party applications for merchants, processors
  - Validated applications listed on PCI Council website
- ❑ PA-DSS is for third-party payment application software used in authorization or settlement
  - Not for internally-developed or customized applications
  - Not for back-office or database applications
  - PA-DSS does not address functionality
- ❑ Visa and MasterCard mandate PA-DSS applications

# Where's My Silver Bullet?

---

- ❑ Minimize PCI scope (aka, PCI “Requirement 0”)
  - Store no cardholder data (even paper)
  - Segment your network
  - Change processes and procedures
  - Map your cardholder data flow
  - Perform a PCI Gap Analysis to identify non-compliant processes and systems

- ❑ Get trained:
  - PCI Council training
  - Treasury Institute PCI Workshop (April 23-5, 2012)

# Conclusions

---

- ❑ PCI compliance is a business issue
- ❑ PCI compliance is pass/fail
- ❑ You are one system change from being noncompliant
- ❑ Use the right SAQ
- ❑ You can outsource processing, but not your responsibility
- ❑ You do not want to be a service provider
- ❑ Take advantage of all your resources

# Thank You

---

☐ Your comments? Questions? Thoughts?

email: [wconway@403labs.com](mailto:wconway@403labs.com)

☐ Follow my PCI column at  
[storefrontbacktalk.com](http://storefrontbacktalk.com)

☐ Higher Education PCI blog (Treasury Institute)  
[treasuryinstitutepecidss.blogspot.com](http://treasuryinstitutepecidss.blogspot.com)