

How Stores Comply with Updated PCI Version

Presenters:

Kimberly Ford

Tabitha Greiner

Dr. Branden R. Williams

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: info@conexxus.org

Presenters

Conexxus Host

Allie Russell

Conexxus

arussell@conexxus.org

Moderator

Kimberly Ford

Manager, IS

Valero Marketing & Supply

Speakers

Tabitha Greiner

CSO

Acumera, Inc

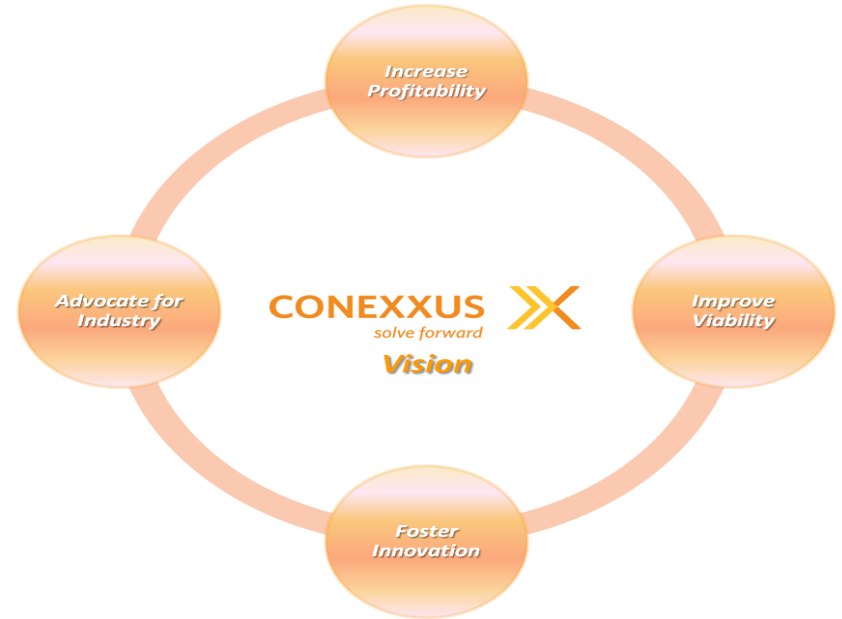
Dr. Branden R. Williams

Director, Cyber Security

Union Bank

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards...
 - Data exchange
 - Security
 - Mobile commerce
- We provide vision
 - Identify emerging tech/trends
- We advocate for our industry
 - Technology is policy



Conexxus Webinar Schedule

Month	Subject	Speaker(s)	Company
February 2017	How Stores Comply with Updated PCI Version	Tabitha Greiner Kimberly Ford Branden Williams	Acumera Valero Union Bank
March 16 2017	SIEM Presentation	Matt Bradley	EchoSat
April 2017	Internet of Things & Impact of Bring Your Own Device to the Workplace	Bradford Lowey Jeff Gibson	Wayne Fueling EchoSat
May 2017	Customer Engagement Technologies to Enhance Sales and Profitability	Ed Collupy Gray Taylor Lesley Saitta	W. Capra Conexxus Impact 21

2017 Conexxus Annual Conference

Loews Annapolis Hotel
Annapolis, Maryland

April 23 – 27, 2017



Agenda

- Fundamentals of PCI Compliance
- The realities of achieving and maintaining compliance
- Strategies and technologies to better secure CHD and ease complexities

Who does the PCI DSS apply to?

PCI DSS applies to **all** entities involved in **payment card processing**—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also **applies to all** other entities that store, process, or transmit cardholder data and/or sensitive authentication data.

Who does the PCI DSS apply to?

Service Providers (definition): Business entity that is not a payment brand, **directly involved in the processing, storage, or transmission** of cardholder data on behalf of another entity. This **also includes companies that provide services that control or could impact the security of cardholder data.**

Key Players

PCI Security Standards Council (SSC)	Payment Brands/Banks
Standards Body	Enforcement and Tracking
Education and Certifications	Penalties, Fees, and Deadlines
Documentation, Guidance, FAQs	Data Compromises

PCI DSS Key Dates

Release Date	April 2016
Retirement of 3.1	October 31, 2016
Best Practices - Requirements	January 31, 2018
SSL/Early TLS	June 30, 2018*

PCI DSS 3.2

Observations

- Incremental Updates – Expect More?
- SSL Date Updates
- Multi-factor – New Guidance Released
- Small Merchant Guide

PCI DSS 3.2 – New Requirements

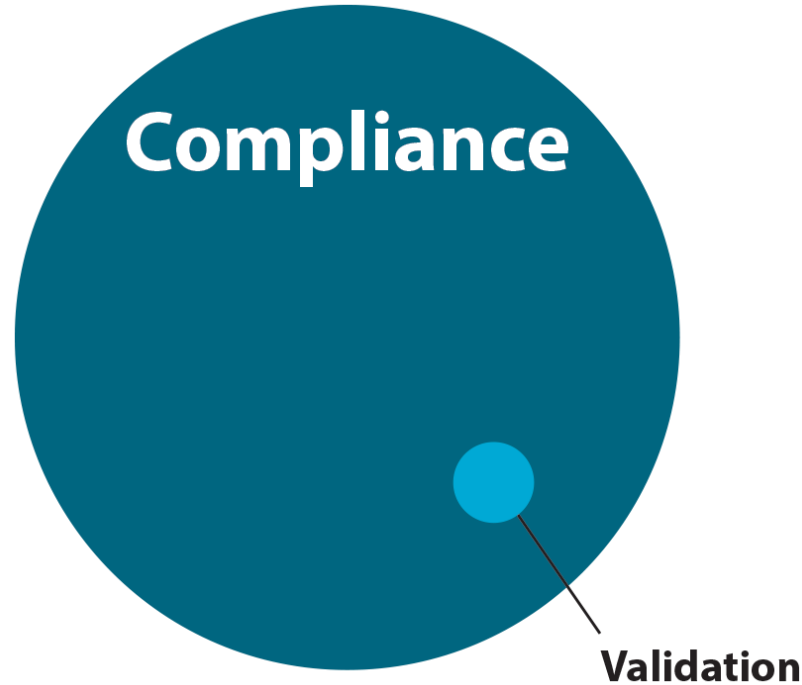
ALL

- 6.4.6 Ensuring continuous compliance
- 8.3.1 Multi-factor for admin

Service Providers

- 3.5.1, 10.8, 10.8.1, 11.3.4.1, 12.4.1, 12.11, 12.11.1

Compliance vs. Validation



Compliance vs. Validation - Breaches



Brand Relationships

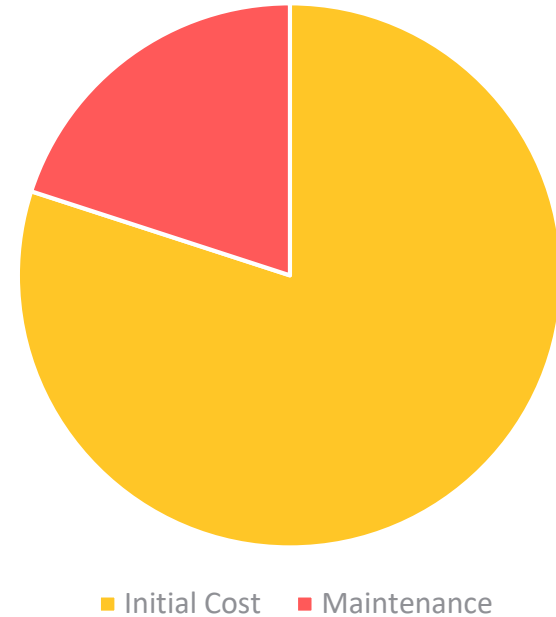
If you have a relationship with an oil brand:

- Make sure you understand your contractual requirements in regards to PCI Compliance
- Ask them if they have any PCI related programs or recommendations
- Some oil brands have recommended vendors, some have required vendors, some directly resell

Realities – Achieving Compliance

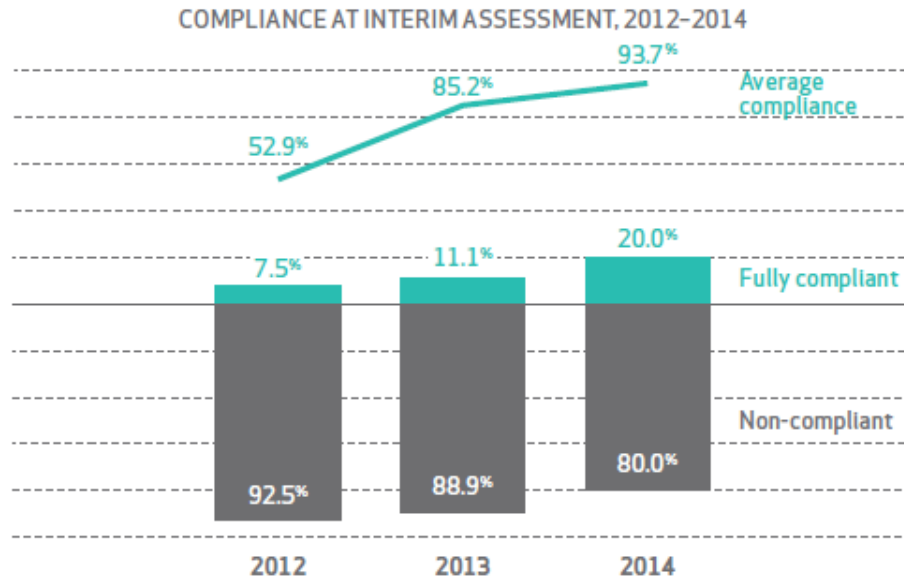
Efforts to Comply

- \$\$\$ for hardware, software, services
- Human capital
- On-going costs/Continuous compliance



Realities – Maintaining Compliance

Maintaining compliance is even harder



Verizon 2015 PCI
Compliance Report

Memorable Quote

“We are but one change control away from non-compliance.”

Strategies

- Outsourcing
- Devalue Data
- Simplification



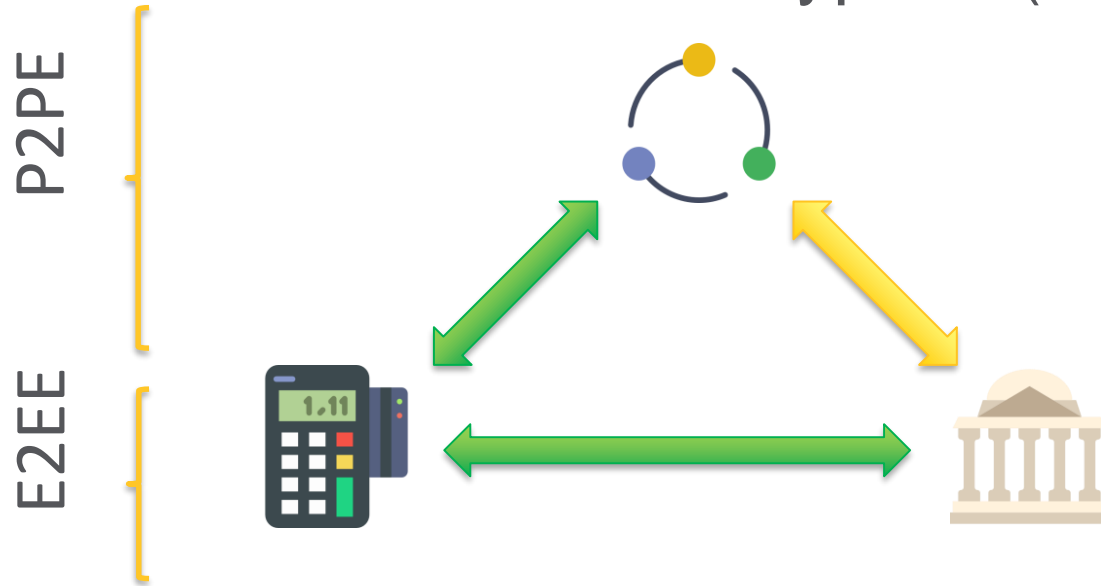
Technologies - Tokenization

Use Tokens instead of PAN

- Scope, architect, and implement properly
- Remove PAN data
- All ops done on token
- Scope reduced to Terminal

Technologies - Encryption

Point to Point Encryption (P2PE) Defined



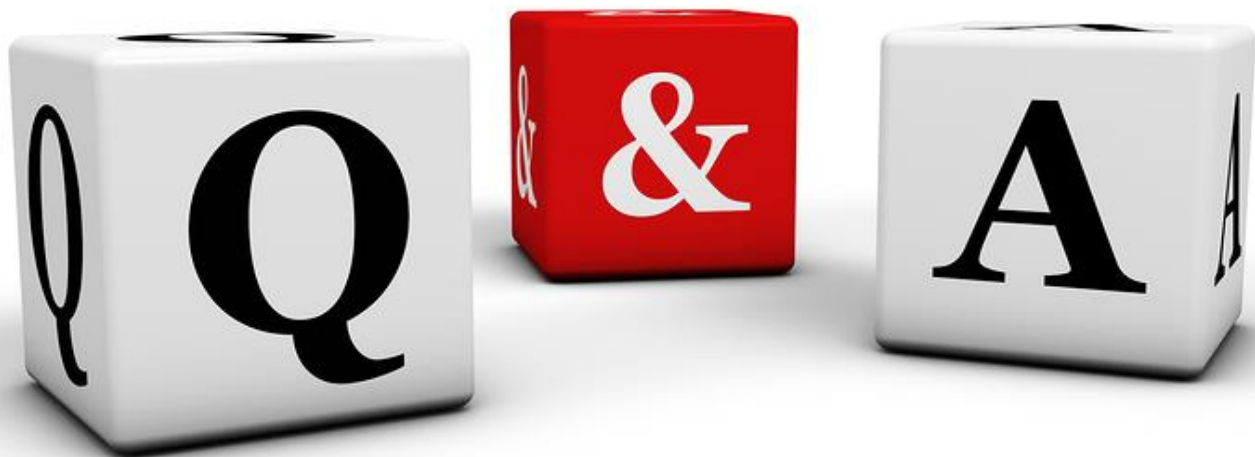
Technologies - Mobile

ApplePay, SamsungPay, AndroidPay

- Similar to EMV, but possibly cheaper interchange!
- Requires equipment upgrade

Conexus Mobile Standard

- Mobile Application on Consumer Device
- Service Provider handles CHD



- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Group: [Conexxus Online](#)
- Follow us on Twitter: [@Conexxusonline](#)

March 16, 2017 @ 12:00PM Eastern:

SIEM Presentation