

PCI DSS: The Big Picture

INTRODUCTION



John Elliott

PAYMENTS, SECURITY, PRIVACY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



What is PCI DSS?



Two PCI DSS



The Standard



Banks Brands

Compliance Programs



This is really important. When someone says “PCI DSS” do they mean the standard or a compliance program?



What



Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures

Version 3.2
April 2016

1. Have firewalls
2. No defaults
3. Protect stored data
4. Encrypt transmissions
5. Use anti-virus
6. Secure apps and OSES
7. Restrict access
8. Identify and authenticate
9. Physical protection
10. Log and monitor
11. Test security
12. Have policies

https://www.pcisecuritystandards.org/document_library



What

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

22 Sub-requirements

37 Test Procedures

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

1.2.1.a Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.

1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.



Who

American
Express



Discover



JCB



Mastercard

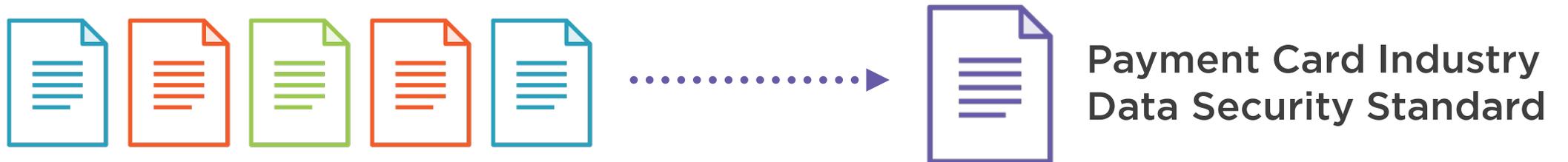


Visa



Who

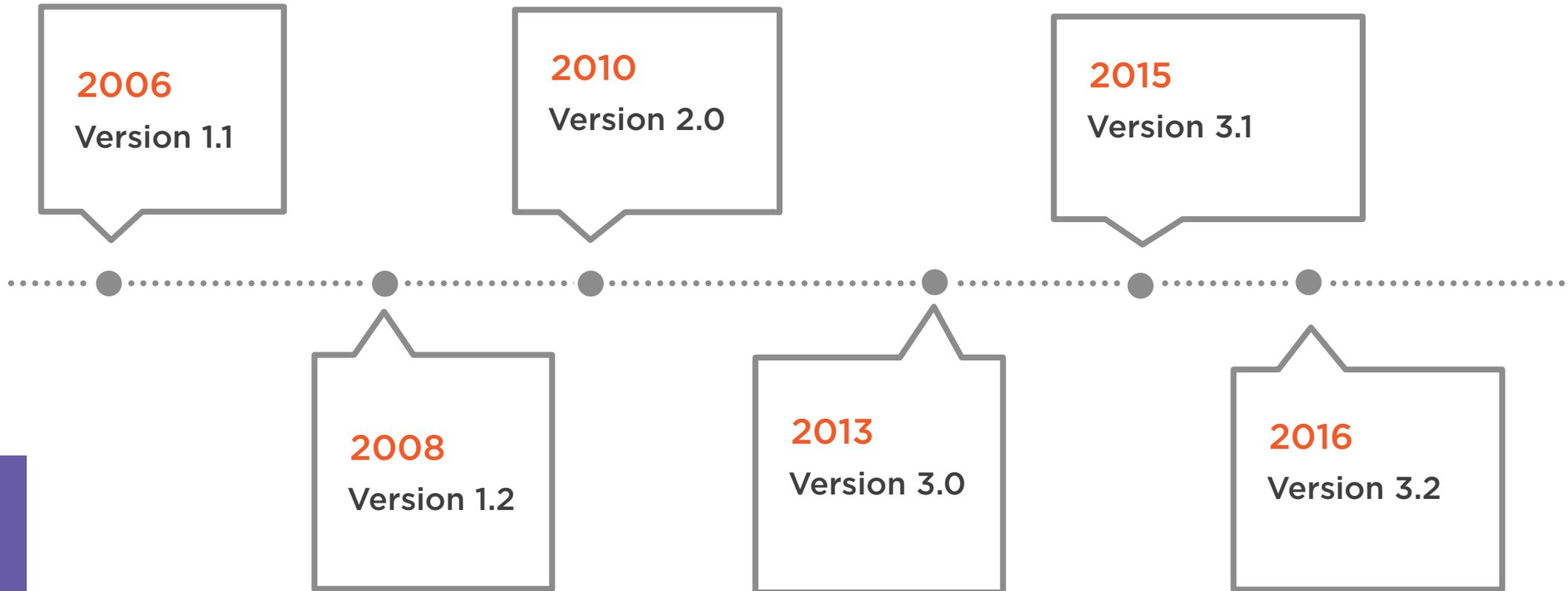
Payment Card Industry Security Standards Council (PCI SSC)



How



When



Where

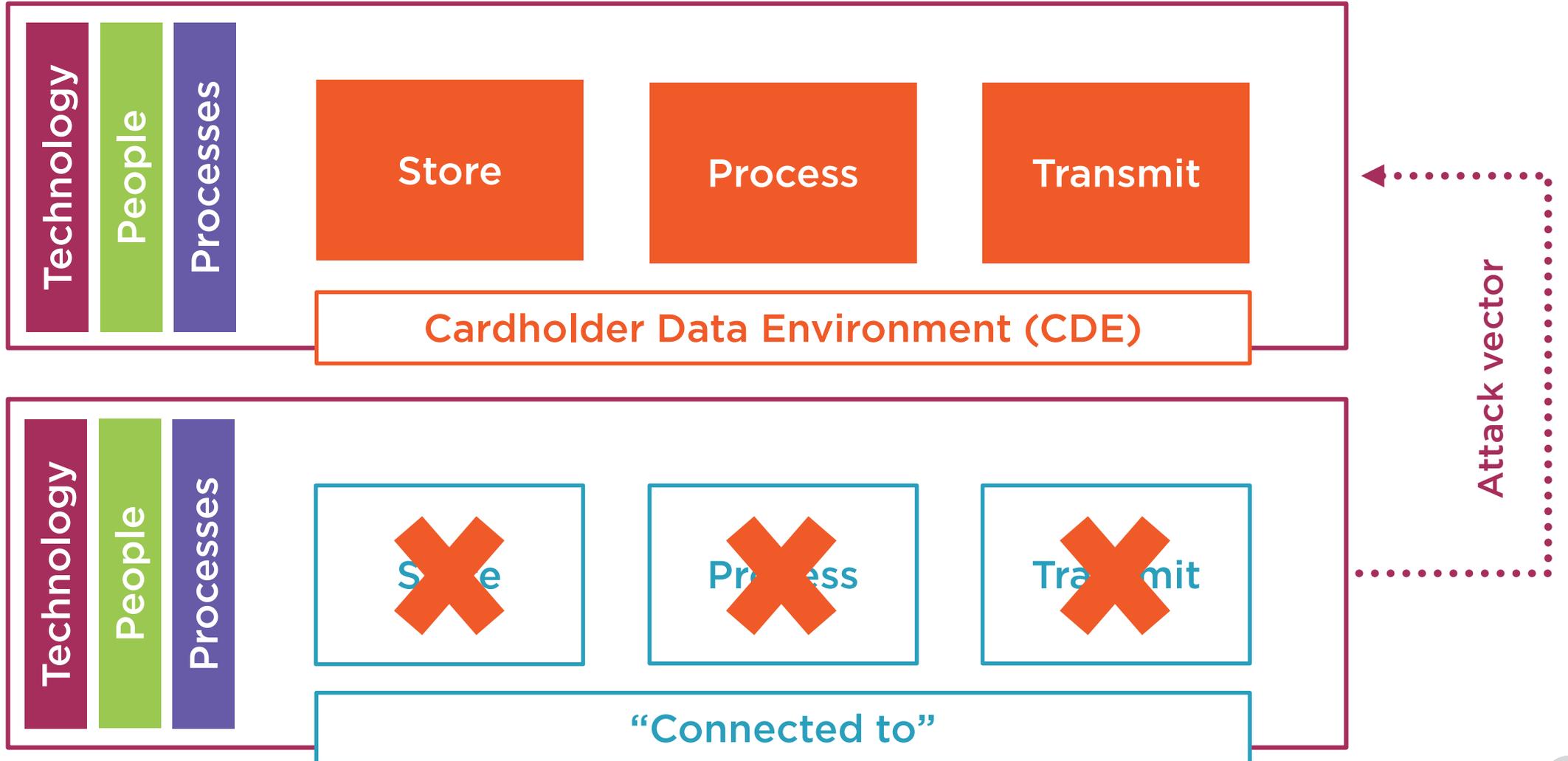
“The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment.

The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data.

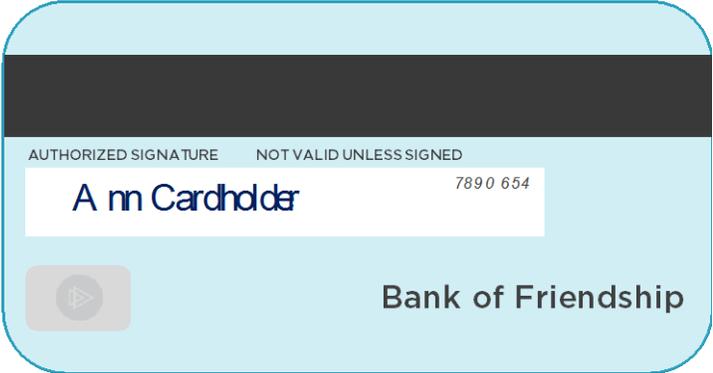
“System components” include network devices, servers, computing devices, and applications.”



Where



Why



Who: The PCI SSC

What: A prescriptive security standard with about 280 requirements

When: Since 2006

Why: Because criminals steal card data

Where: All systems that store, process or transmit cardholder data or are “connected to”



**Payment Card Industry (PCI)
Data Security Standard**

Requirements and Security Assessment Procedures

Version 3.2
April 2016



Why

Why does an organization need to comply with PCI DSS?





**Because someone
asked them to!**

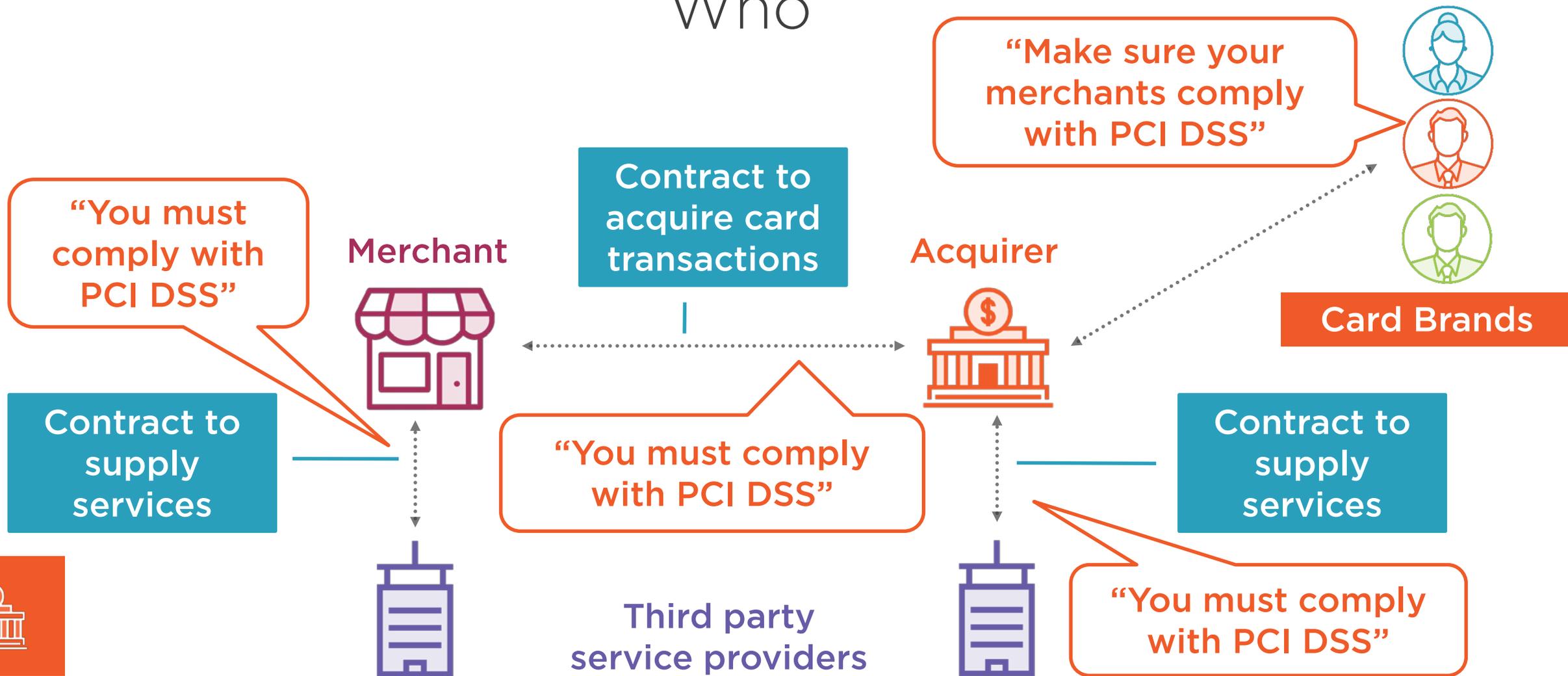
Compliance with the PCI
standards is (generally) not a
legal requirement



**So why do organizations
have to comply?**



Who



When



Normally organizations are asked to validate they are compliant with PCI DSS once a year.

(but being compliant is a year-round, day-to day process)



What

Report on Compliance (RoC)



Independent assessment of requirements by Qualified Security Assessor (QSA)

Self Assessment Questionnaire (SAQ)



Perform self assessment of requirements:
Complete paper form

Self Assessment Questionnaire (SAQ)



Perform self assessment of requirements:
Complete web form provided by acquiring bank



How



Who? Compliance programs
come from card schemes
via the acquirer

Why: It is contractual

When: Validation is annual

How: By SAQ or RoC



Summary



There are two PCI DSSes

1. The standard

- Next module

2. Compliance programs

- How you demonstrate compliance, to who, and why

Ten PCI DSS myths

- That you're bound to hear ...

