

# PCI "Straight Talk" 1

**Diana Kelley and Ed Moyle**

---

# Agenda

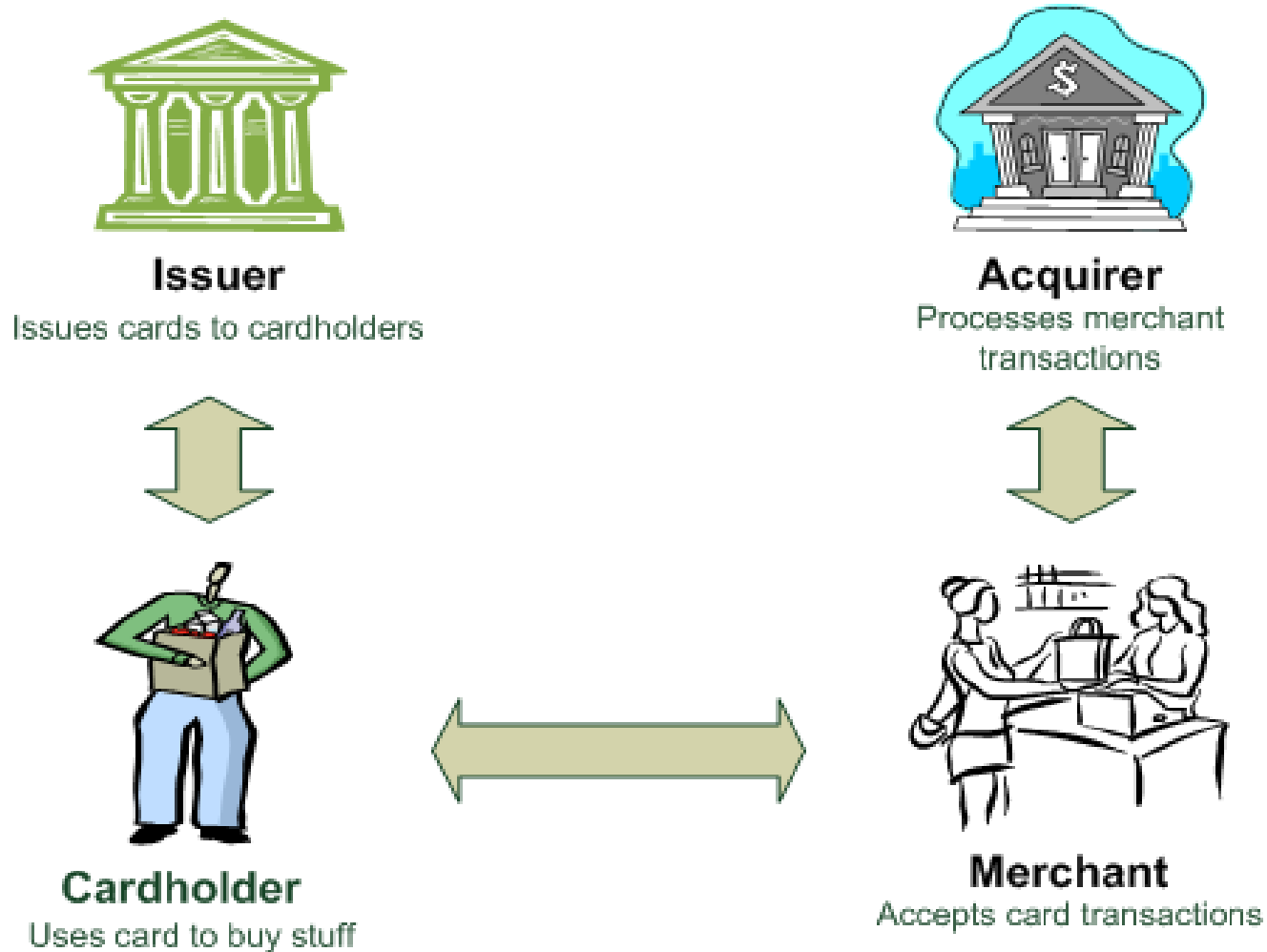
- **Quick PCI Level-set**
- **Compliance Validation**
- **Scoping the Assessment**
- **Compensating Controls**
- **Wrap up**

# Agenda

- **Quick PCI Level-set**
  - Players in the credit lifecycle
  - Emergence of PCI
- Compliance Validation
- Scoping the Assessment
- Compensating Controls
- Wrap up

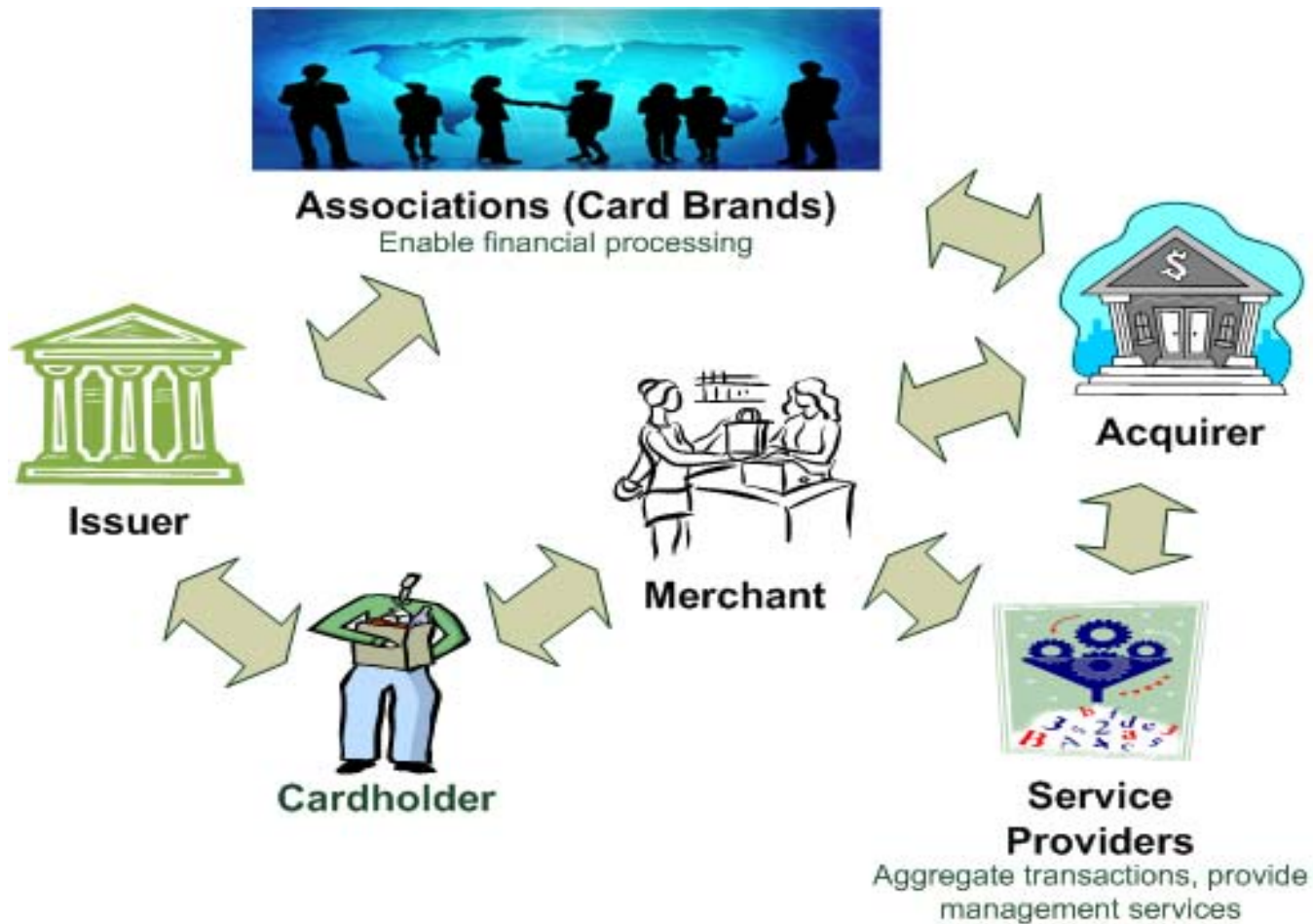
## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

### Players in the Payment Lifecycle (simple view)



# Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

## Players in the Payment Lifecycle\* (complex view)



\*Four-Party Network Pictured

# Setting the Stage for the PCI DSS

## ● The “Card Not Present” (CNP) model

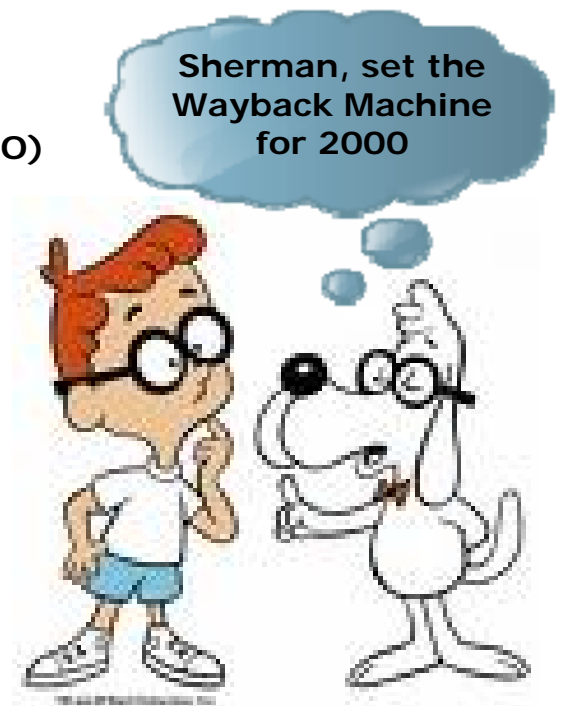
- Same model used for Mail Order/Telephone Orders (MOTO)
- Merchants responsible for fraud

## ● Huge consumer anxiety

- Reluctance for consumers to use cards online

## ● Low adoption for technical initiatives

- SET
- SPA/UCAF
- Verified by Visa



## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

# Response from Brands: Security Programs



Cardholder  
Information  
Security Program  
(CISP)

In response, card brands developed security initiatives to help secure transactions, appease vendors, and bolster consumer confidence



Data Security  
Operating Policy



Site Data Protection  
(SDP)



Data Security Program



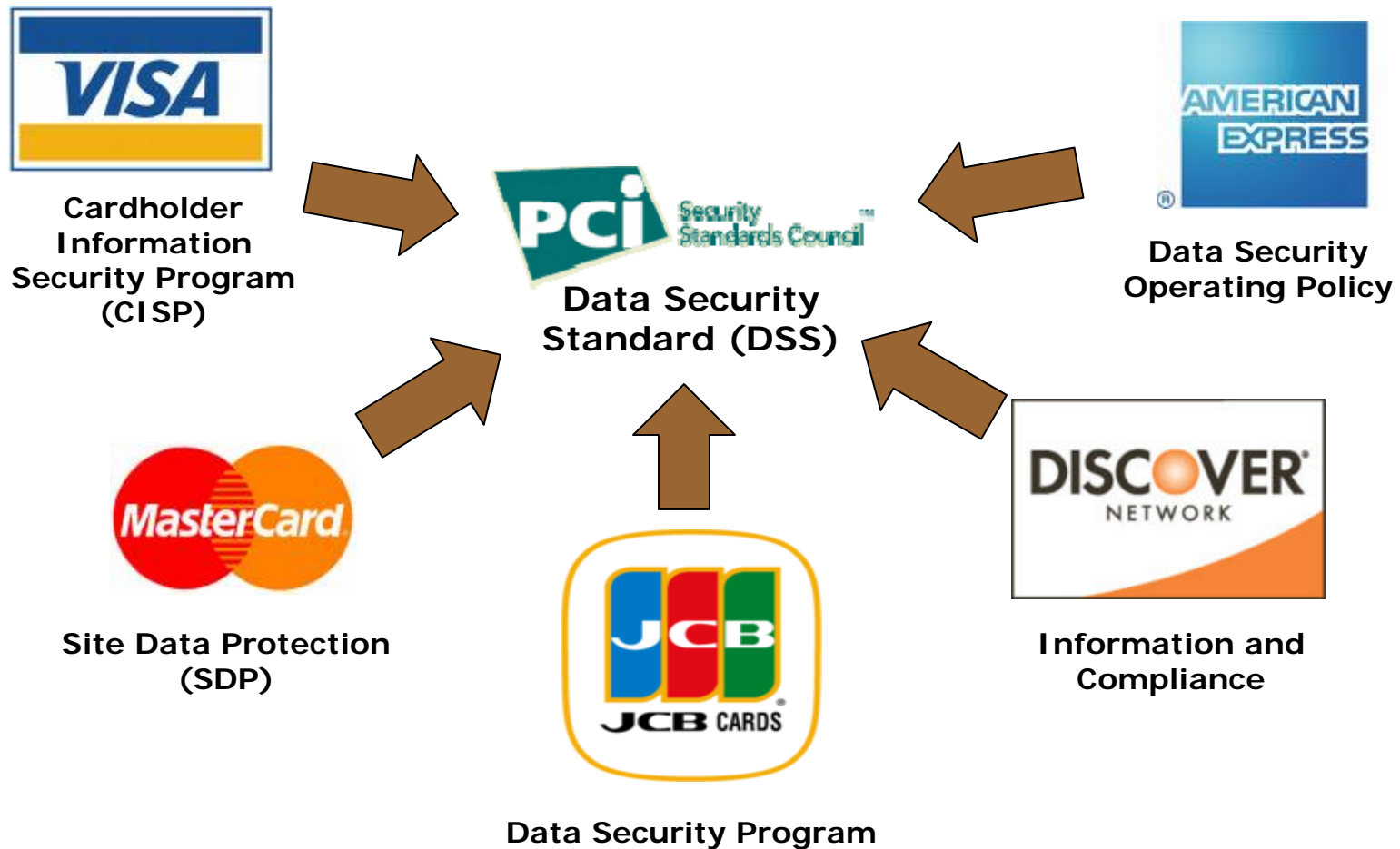
Information and  
Compliance

## Too Many Programs?

- **How many merchants accept *just one* card brand?**
  - Each merchant had (usually) three or more compliance programs to address
- **Pressure from merchants (and acquirers) to standardize**
  - Merchants put pressure on acquirers to standardize into one program
  - Acquirers feel the pressure from merchants and advocate as well

# Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

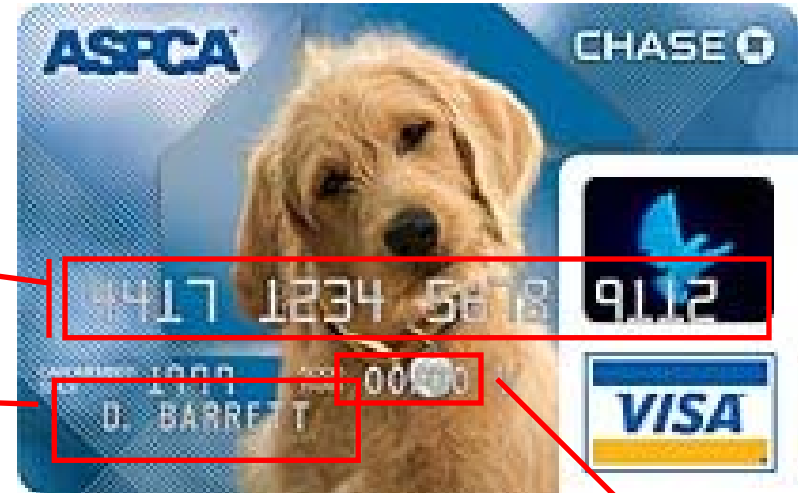
## PCI DSS: "One Standard to Rule Them All"



# Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

## What's in your wallet?

Image Source: <http://www.firstusa.com/>



Primary Account Number (PAN)

Cardholder Name

Expiration Date





Magnetic Stripe

Card Verification Value (CVV)

Image Source: <http://www.sti.nasa.gov/cvv.html>

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

*Covered Data Elements (Data Source: PCI DSS Version 1.2, October 2008)*

	Data element	Storage permitted	Protection Required	PCI DSS Requirement 3.4*
<b>Cardholder data</b> 	PAN	Yes	Yes	Yes
	Cardholder name	Yes	Yes**	No
	Service code	Yes	Yes**	No
	Expiration data	Yes	Yes**	No
<b>Sensitive authentication data (SAD)</b> 	Magnetic stripe	No	No storage permitted	No storage permitted
	CVC2/CVV2/CID	No	No storage permitted	No storage permitted
	PIN/PIN block	No	No storage permitted	No storage permitted

\* 3.4 –Encrypt, one-way hash, truncate, or use compensating controls (alternately, don't store at all)

\*\* Applies when stored with the PAN

# Agenda

- Quick PCI Level-set
- **Compliance Validation**
  - Compliance vs. validation
  - Who does what
- Scoping the Assessment
- Compensating Controls
- Wrap up

# Compliance Validation

- **Everyone** involved in the payment lifecycle **must** *be* compliant with the standard
  - If you *store, process, or transmit* cardholder data
  - This applies to most organizations
- Certain parties must also **validate** compliance
  - Validation to be performed by an approved party
  - Compliance status regularly reported in a standardized document called a "ROC" (Report on Compliance)

# Validation: Who Has to Validate

## ● Merchants

- Merchants exceeding a *card brand specified* threshold for volume (think millions)\*
- Merchants who have been told to validate by their acquirer

## ● Service Providers (Processors and Gateways)

- Exceeding a *card brand specified* threshold for volume\*

## ● When required to support business relationships

## Validation: Approved Options

### ● Option 1: Qualified Security Assessors (QSAs)

- Have gone through Visa background investigation
- Working for an approved firm (QSAC, Qualified Security Assessment Company)

### ● Option 2: Certify Yourself\*

- Verify strict rules about who can do this
- *Level 1 merchants only* (no service providers)
- Must follow the audit procedures
- Must have acquirer agreement
- An approved officer (think CEO or CFO) attests to the results and signs on the "dotted line"

\*In practice, this is rarely done

## Validation: Scanning vs. Assessment

- **Two different types of approved vendors**
- **Assessment provided by QSAs**
  - Certified to provide assessment services
  - Deliverable is a completed ROC
- **Scanning services provided by ASVs  
(Approved Scanning Vendors)**
  - Approved to conduct the (quarterly) scanning activity on your behalf
  - Deliverable is an external technical scan report

# Agenda

- Quick PCI Level-set
- Compliance Validation
- **Scoping the Assessment**
  - Setting appropriate scope
  - Enforcing scope
- Compensating Controls
- Wrap up

## About Scope

- **Detailed in the requirement itself**
  - Pages 5 through 7 of PCI DSS 1.2
  - Flow chart on scoping/sampling in Appendix F
- **The scope of the assessment *must include* the entirety of the cardholder data environment (CDE)**
- **Cardholder data environment is:**
  - Any system that stores, processes, or transmits credit card information
  - Any machine(s) not separated from those machines
- **This means, unless you strategize, *the whole network could be in scope***

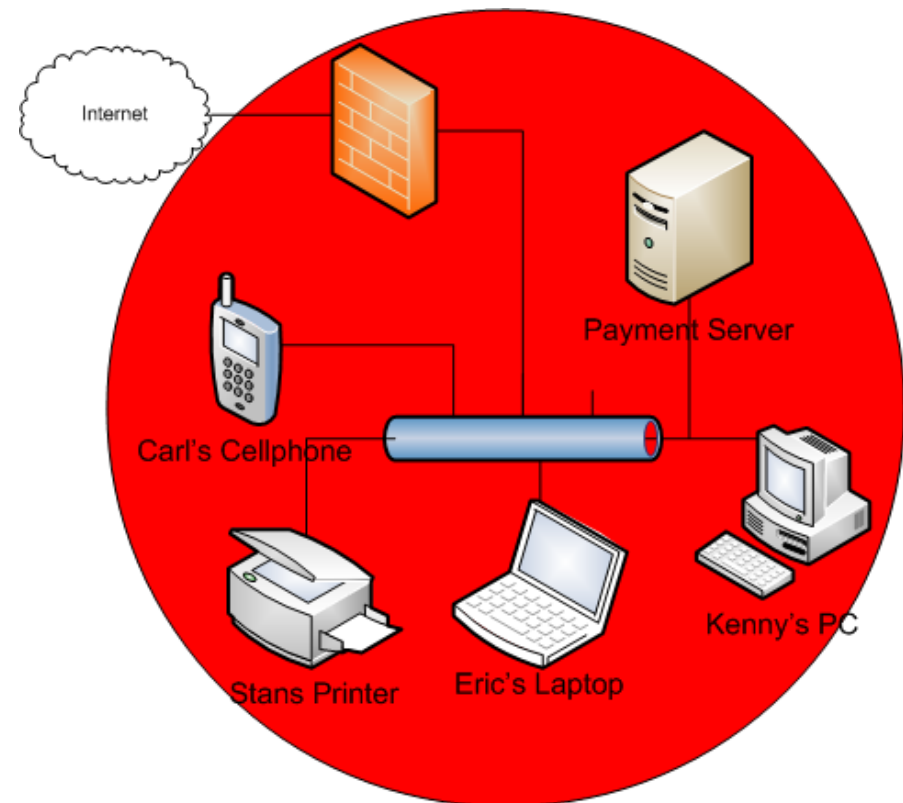
## The Importance of Scope

- **The larger the scope, the worse off you are**
  - Increased cost
  - More impactful to operations
  - Greater likelihood of finding non-conformities with the standard
- **Your most important goal**
  - reduce the scope of the assessment through zoning
  - Isolate payment systems away from problem areas

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

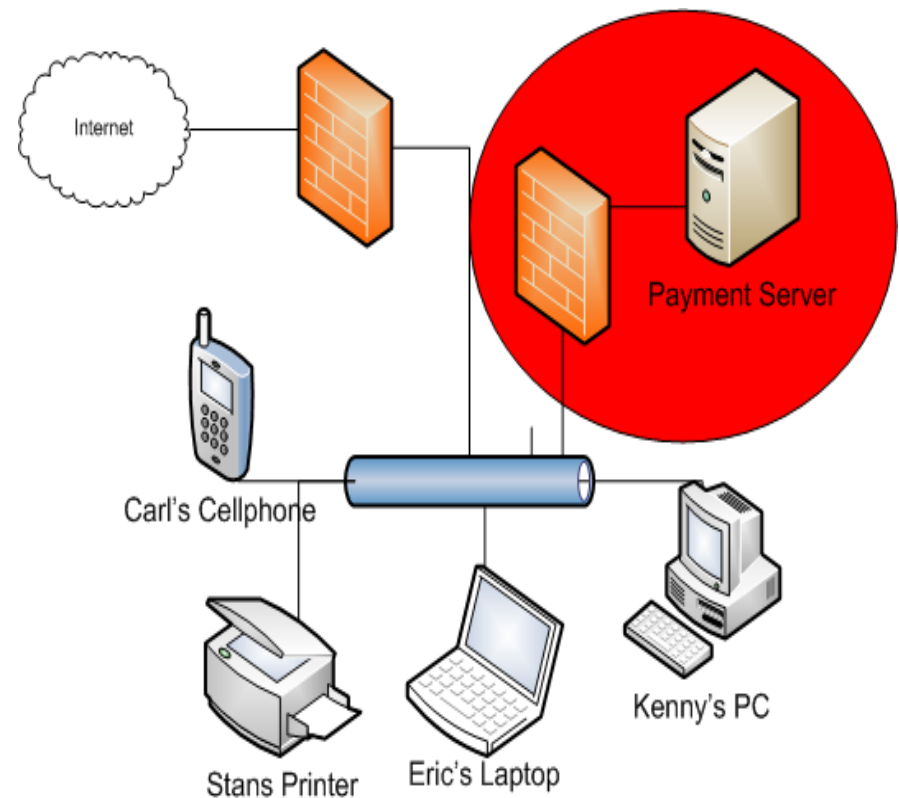
# No Segregation: The "Worst Case Scenario"

- **No segregation – where most firms start out**
- **Therefore, the entire network is in scope**
  - Includes problematic areas like mobile devices
  - Includes equipment unrelated to card processing like workstations and printers
- **You don't want this**
  - Incredibly expensive to assess
  - A recipe for "less-than-stellar" outcome on the ROC



# Let's Try That Again

- **Strategic Scope**
- **Only payment systems are in scope**
  - Includes payment systems and applicable network equipment
- **Better all around**
  - Costs less to assess
  - Assessment doesn't impact other areas of the business
  - Much more likely to "pass"
  - Higher degree of confidence in the ROC contents



## Scope and the Point of Sale

- **Does the scope include the POS? (yes, it does)**
  - However, what the size of that scope is at each retail location can vary greatly
  - Could just be the POS device itself (e.g. dialback terminal)
- **Factors influencing scope at the POS**
  - Connectivity to other systems
  - Type of POS (Internet/VPN, Terminal/PC, or Dial-back)

## How to Scope: Creating Zones

- **Define logical “zones” that segregate the cardholder environment**
- **Enforce those zones using a physical or technical control**
  - Technical boundaries (firewalls, routers)
  - Physical boundaries (“air gap” networks, different facilities)
- **Document how the control enforces the zone**

# Are Your Zones “Strong Enough”?

- **They’ve upped the ante on zoning in 1.2**
  - **For networks:** *“... segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access...”*
  - **For third parties:** *“merchants and service providers must manage and monitor the PCI DSS compliance of all associated third parties with access to cardholder data”*
- **QSA still has to agree with you**
  - Document your analysis and justification
  - A QSA is more likely to agree if you have documentation
- **You need to have policy/procedure**
  - Having a zone implies management and governance
  - Make sure that your policy/procedure reflects how you enforce the zone

## Key Points: Scope and Zones

- **Before you dive into the assessment process, the most important thing you can do is set scope**
  - Limit scope to reduce number of systems (and therefore the number of problem areas)
  - Smaller scope means less cost to you – both in the amount paid to assessors and the impact to your daily operations
  - Failure to appropriately scope is the #1 reason for failing an assessment – don't succumb to the "include it all" mentality

# Agenda

- Quick PCI Level-set
- Compliance Validation
- Scoping the Assessment
- **Compensating Controls**
  - When to use compensating controls
  - Picking the “right” control
- Wrap up

## When You Can't Meet a Control...

- **Most firms (all?) have requirements they can't meet**
- **Ideally, you'll know about them prior to the assessment**
  - A "success strategy" is to have compensating controls already documented prior to the audit taking place
- **Compensating controls are a *temporary* measure you can use while you put an action plan in place**
  - Keep in mind that compensating controls have a "shelf life"
  - The goal is to facilitate compliance, not obviate it

# Compensating Controls

- Meets the intent and rigor of the requirement
  - *Rigor*: provides as much assurance (effectiveness) as the control in the standard
  - *Intent*: fulfills the same goal as the control in the standard
- A stopgap – not intended for long-term use
  - The goal is to provide time to migrate, not as a way to avoid ever complying
- Requires concurrence
  - Your assessor needs to agree with it, so document accordingly
  - Document *how* and *why* you think it meets intent and rigor

## Drill-Down: Compensating Controls

### ● You can't:

- Use compliance with other PCI requirements as a compensating control (if that control is already required)

### ● You can:

- Use compliance with other PCI requirements as a compensating control (if that control is not already required) \*
- Deploy new/additional controls over and above what's required

\* Be careful, also has to meet original intent/rigor

# Agenda

- Quick PCI Level-set
- Compliance Validation
- Scoping the Assessment
- Compensating Controls
- **Wrap up**

# Wrap Up – PCI Introduction

## ● The PCI DSS is:

- A set of minimum baseline security requirements for entities in the payment process
- A unified standard agreed to by all card brands to ease the compliance burden for merchants
- Required – everyone involved in payments must comply
- Managed and administered by the PCI Standards Council

# Wrap Up – Compliance Validation

## ● Compliance validation:

- Is required for firms meeting the criteria set by the card brands (high volume merchants and service providers)
- Must be performed by an approved party according to the defined procedures (QSAs or internal resources at some merchants)
- Is different from scanning, but the requirements for who provides service are similar (QSAs provide assessment, ASVs provide scanning)

## Wrap Up: Scope

- **Set scope as aggressively as you can**
- **Make sure that your QSA agrees with you**
- **Document what you are using as a “zone” to enforce scope boundaries**
- **Don’t be afraid to increase scope if you find out something new about your environment**
- **Remember that the POS counts so be sure to include it**

## Wrap-up: Compensating Controls

- **If you absolutely, positively can't meet a requirement, use a compensating control**
  - Sometimes, you'll already have one in place
- **Document, document, document**
  - A QSA is very likely to agree with compensating controls that have a risk analysis and an action plan attached
  - Unlikely to agree with a compensating control that's informal or undocumented

Questions? Comments

**Thank you!**