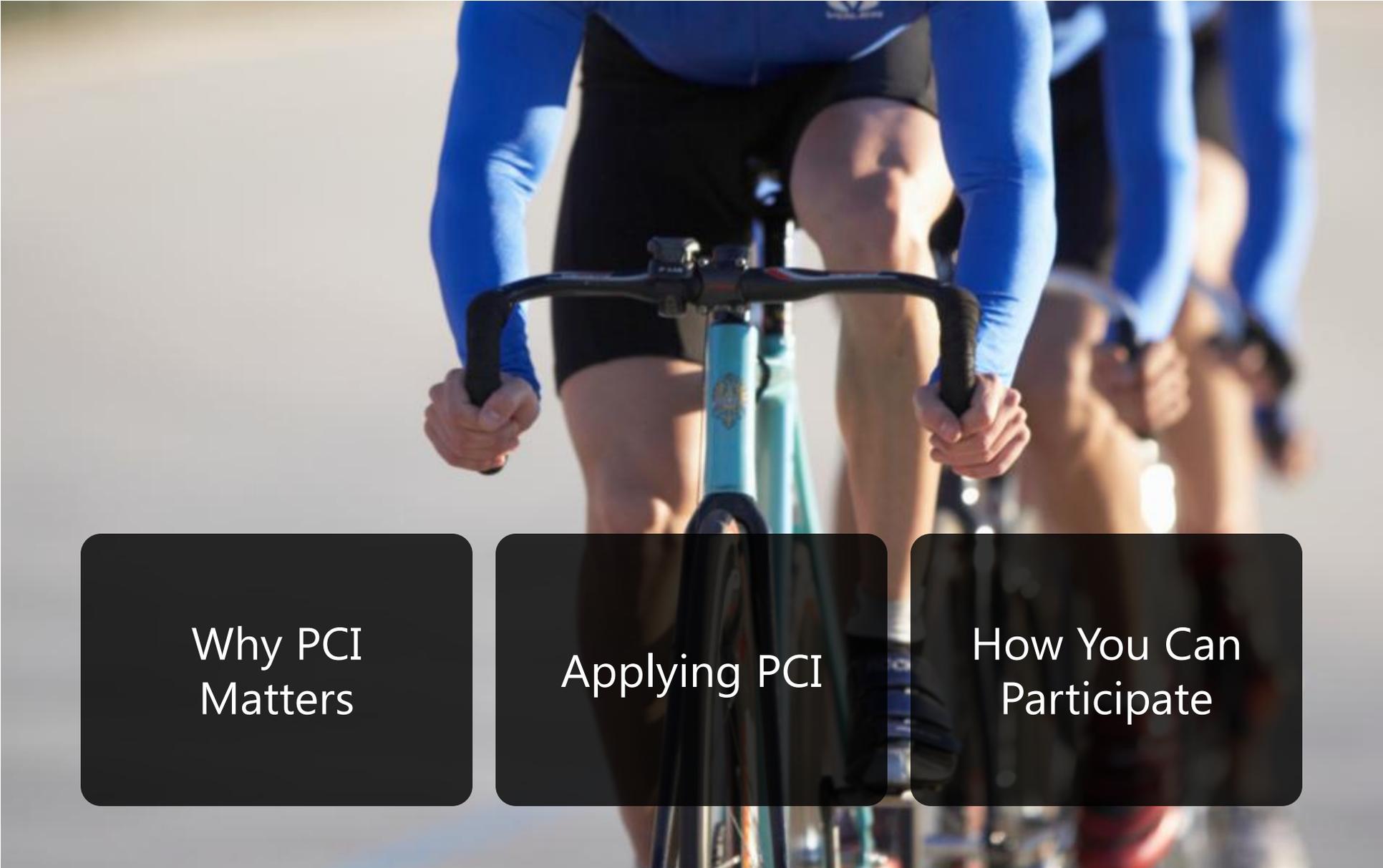


# PCI Security Standards Council

*Guiding open standards for global payment card security*

Bob Russo, General Manager  
2013





Why PCI  
Matters

Applying PCI

How You Can  
Participate

*Agenda*



Why PCI  
Matters

Applying PCI

How You Can  
Participate

*Agenda*

# About the PCI Council

## Open, global forum

*Founded 2006*

*Guiding open standards for payment card security*

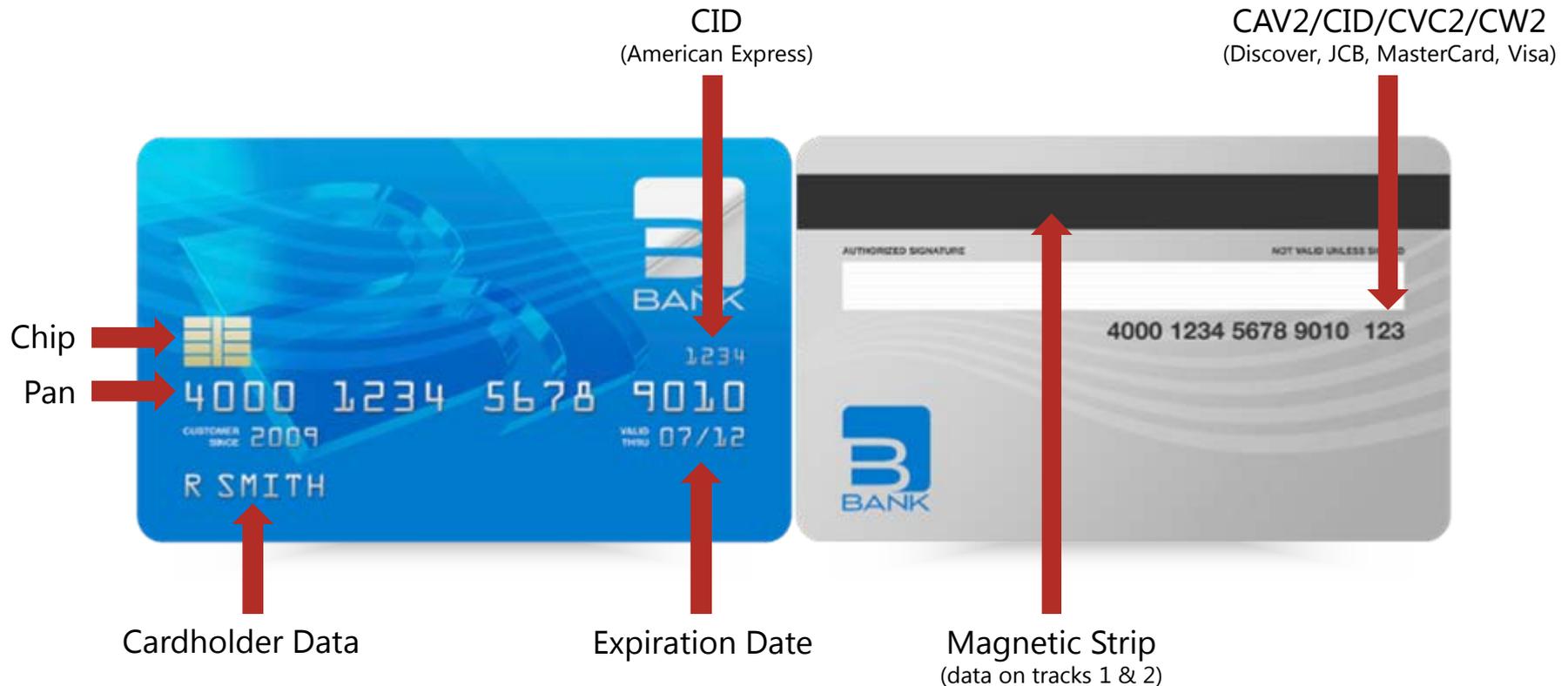
- Development
- Management
- Education
- Awareness



Guiding open standards for global payment card security

# Your Card Data is a Gold Mine for Criminals

## Types of Data on a Payment Card



# Overview: *The Five Stages of Grief*



Denial

Anger

Bargaining

Depression

Acceptance

After the 5 stages of grief. . .

... setting open standards for global payment card security

# The 5 Stages of Breach



**Disbelief**



**Bargaining**



**Lawyer**



**Anger**

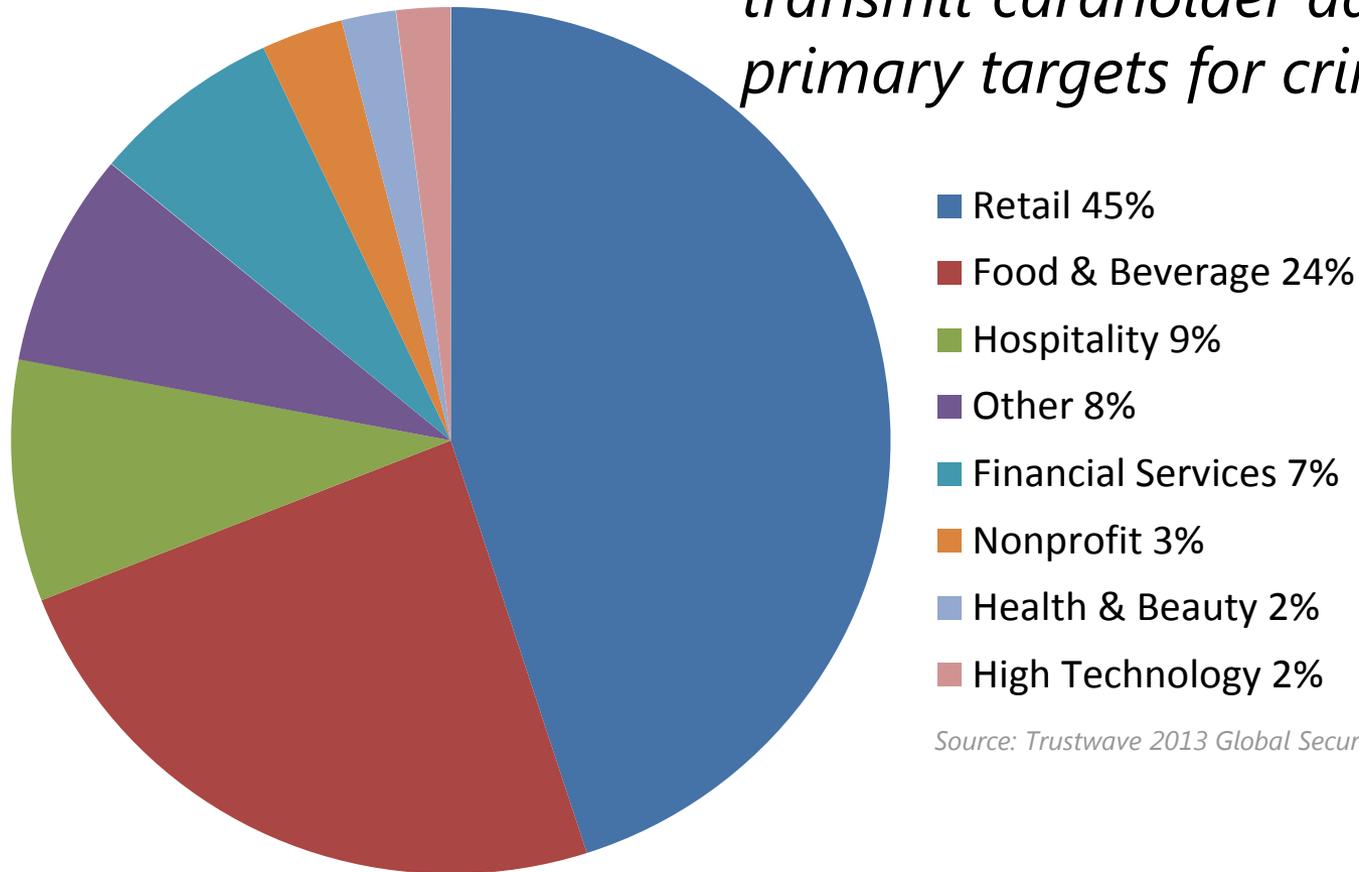


**Resignation**

Guiding open standards for global payment card security

# Business Sectors With the Most Breaches

*Systems that store, process or transmit cardholder data remain primary targets for criminals*



Source: Trustwave 2013 Global Security Report

# Top Mistakes Revealed by Forensic Audits

*Weak or default passwords*

\*\*\*\*\*



*Lack of employee education*

*Security deficiencies introduced by third parties*



*Slow self-detection*

# Low-hanging fruit

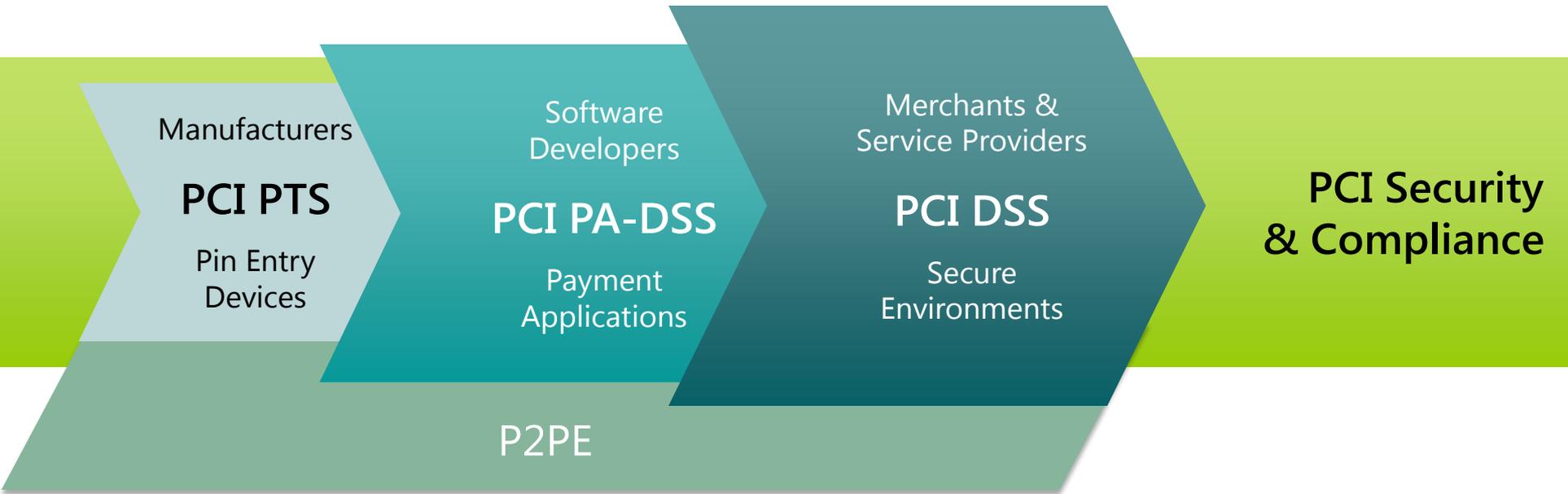
- 92% of breaches were from an external attack
- **76% exploited weak security or credentials**
- 55% were undertaken by organized criminal gangs
- **78% of the attack potentials were rated as Low or Very low**
- 84% of attacks took only hours to perpetrate
- 62% of attacks took months to discover
- **69% were discovered by an external party**



Source: 2013 Verizon Data Breach Investigations Report

# PCI Security Standards Suite

Protection of Cardholder Payment Data

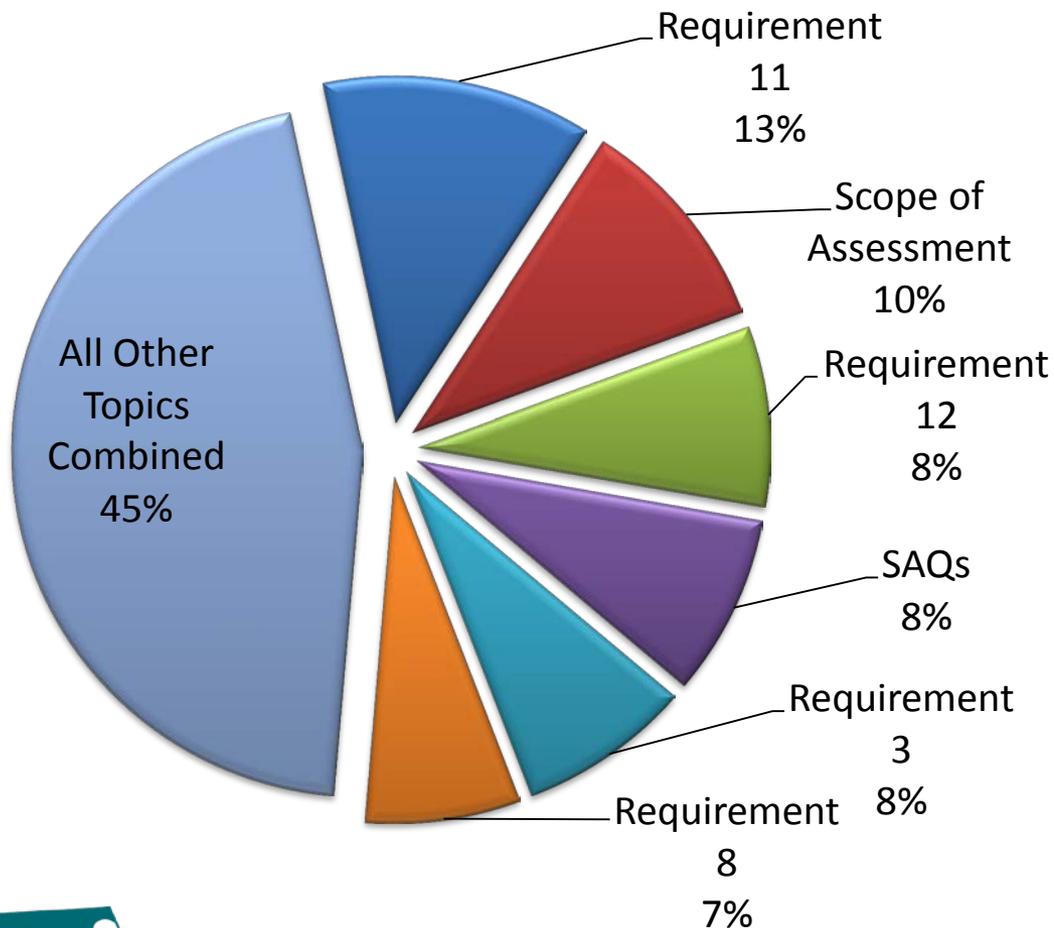


*Ecosystem of payment devices, applications, infrastructure and users*

Guiding open standards for global payment card security

# Standards Updates: Key Feedback Areas & Timeline

## Top 6 Feedback Topics



### End of Aug.

- Summary of changes highlights document & webinar

### Early Sept.

- Draft versions shared with PCI community

### Community Meetings

- Drafts discussed

### 7 Nov

- Standards published

# *For Device vendors - PTS POI 4.0 Just Released!*

## **Key Changes**

**Security policy**

**Device  
implementation  
documentation**

**Restructure open  
protocols module**

**Enhanced  
interface testing**

**Added source  
code reviews**

**Open source code  
reviews**

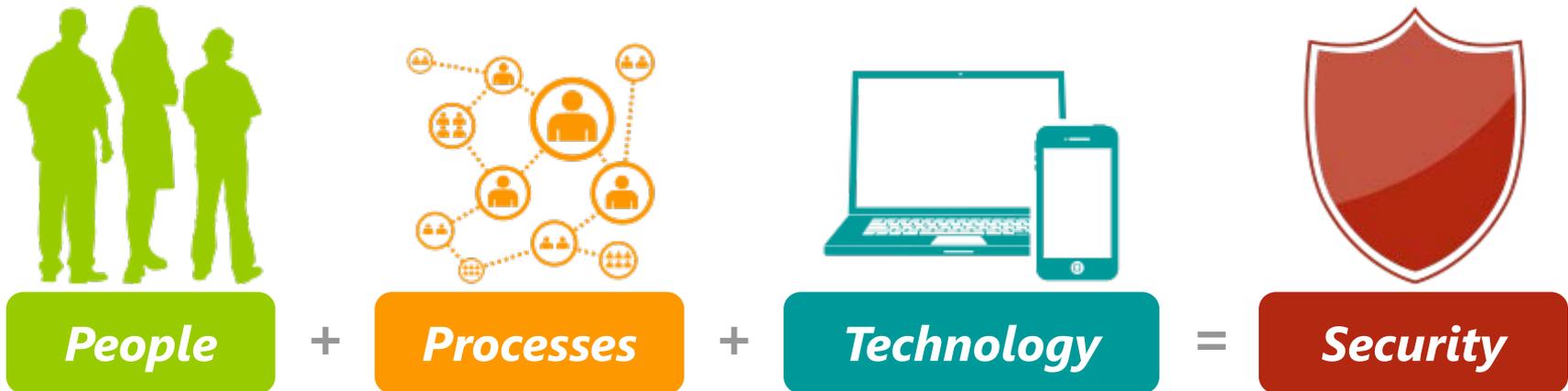
# Point-to-Point Encryption



## Point-to-Point Encryption

- Available to all members of the payment chain
- Also called "P2PE"
- Optional standard for decreasing scope
- PCI 2PE hardware /hardware requirements available
- PCI P2PE "Hybrid" requirements available

# *The Bottom Line*



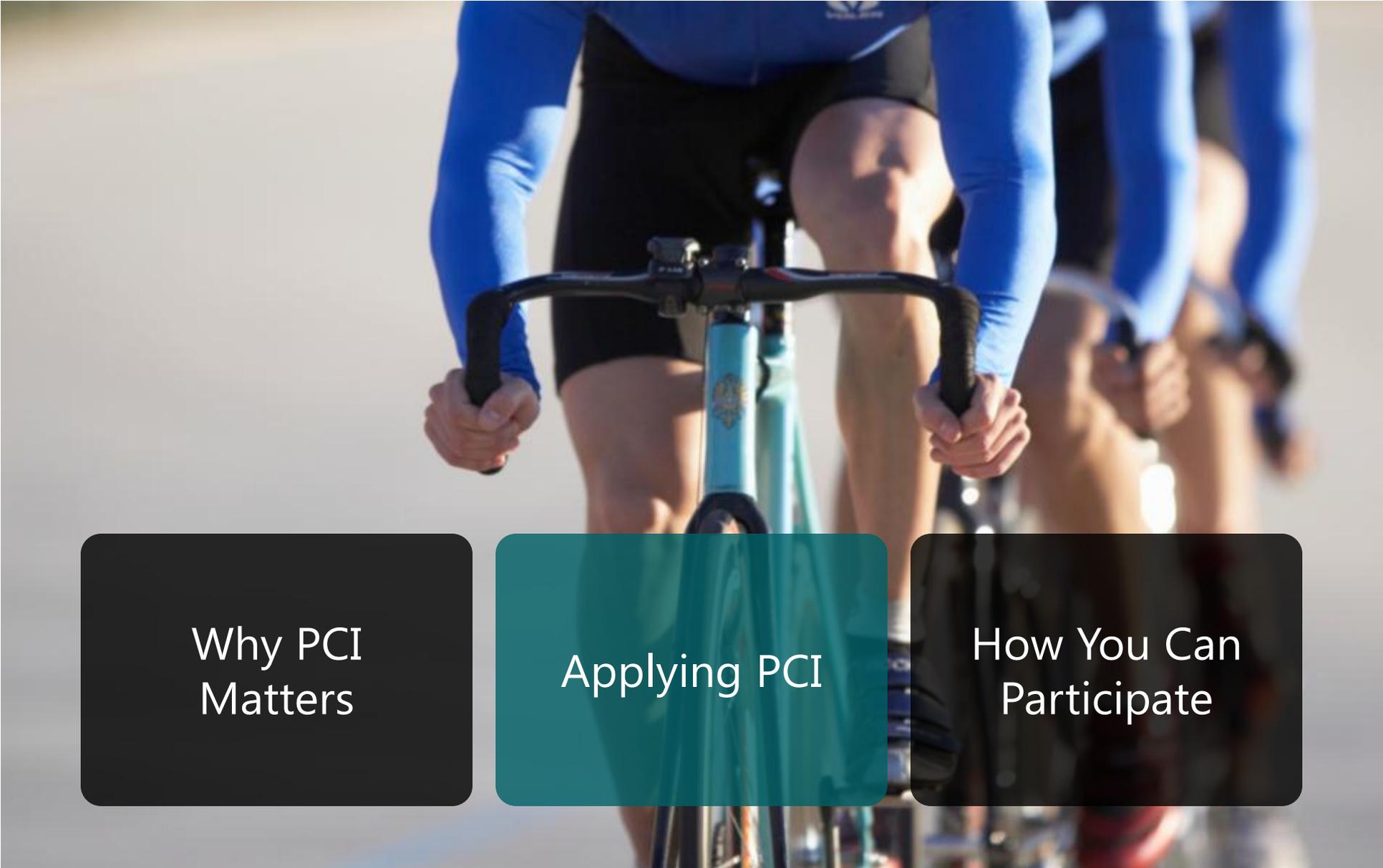
***Compliance Doesn't Equal Security***

# "Compliance" Versus "Security"



# *"Compliance" Versus "Security"*





Why PCI  
Matters

Applying PCI

How You Can  
Participate

*Applying PCI*

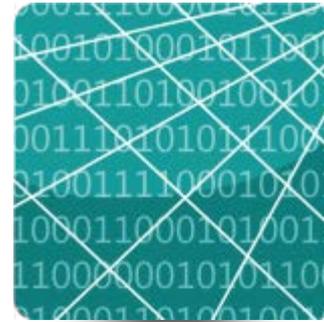
# Applying PCI in Your Environment



Mobile



P2PE



Virtualization



ATM



Tokenization



Cloud



EMV

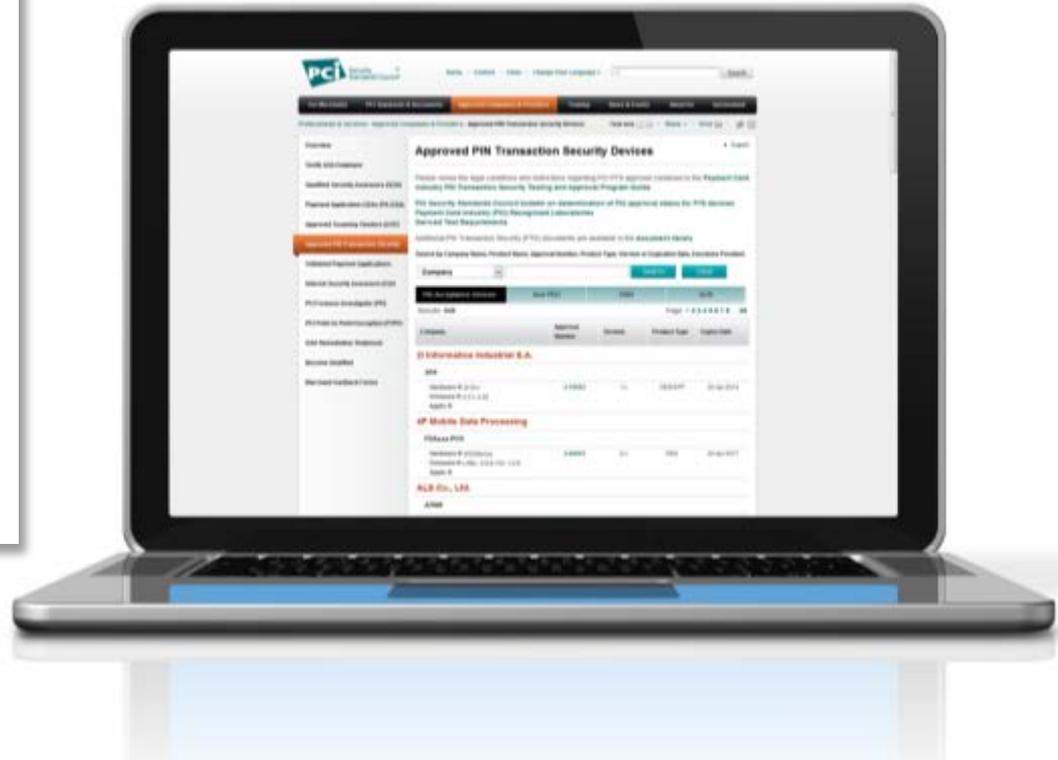
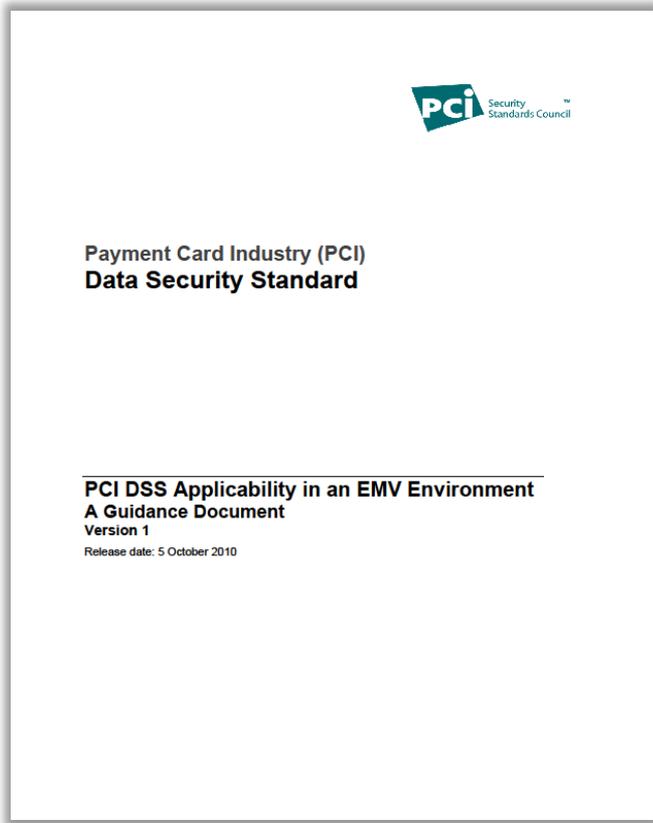
Guiding open standards for global payment card security

# *Even EMV Chip Needs PCI*



EMV chip by itself does not protect the confidentiality of, or inappropriate access to sensitive authentication data and/or cardholder data in card-not-present or Internet transactions

# Even EMV Chip Security Needs PCI



Guiding open standards for global payment card security

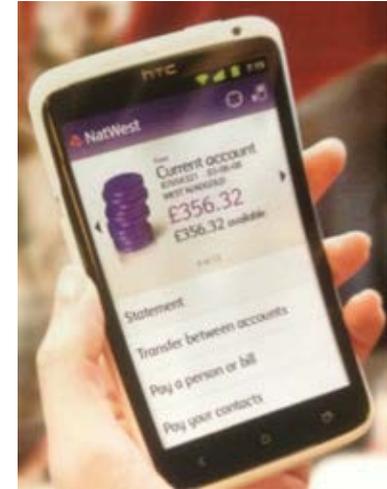
# *New Technology – New Challenges*



Making Payments



Accepting Payments



Applications

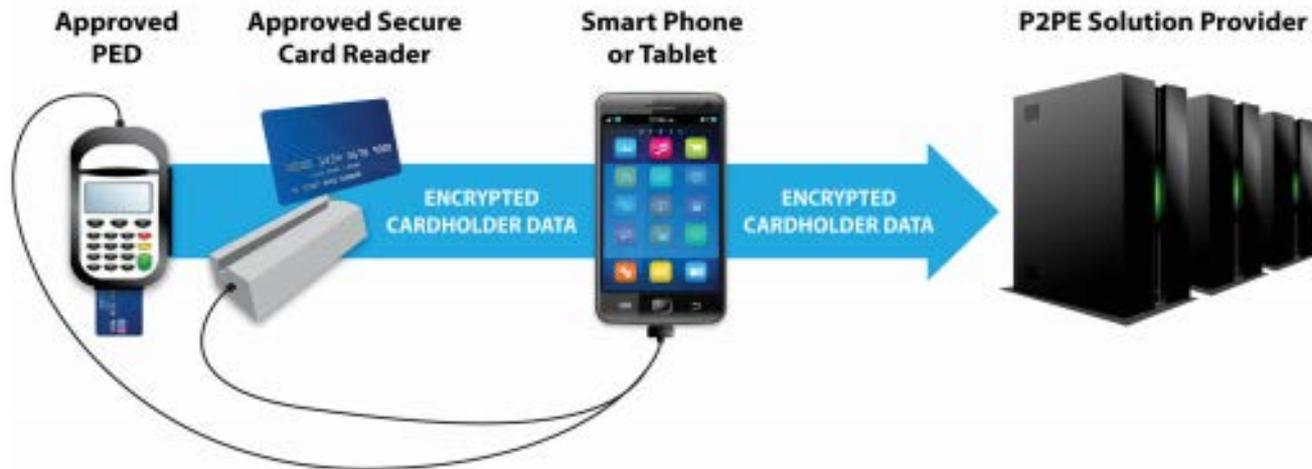
# Mobile Payments and the PCI Council

Identified mobile applications that can be validated to PA-DSS

Published merchant guidance for 'mobile' solutions leveraging P2PE

Developed best practices for developers

New merchant guidance



Guiding open standards for global payment card security

# Areas of Focus for Mobile

**“MOBILE”**

```
graph TD; MOBILE["MOBILE"] --> Devices; MOBILE --> Applications; MOBILE --> ServiceProviders["Service Providers"];
```

## **Devices**

Tamper-responsive,  
PTS Devices (e.g.  
SCR) using P2PE

## **Applications**

Requirements and/or  
Best Practices for  
authorization and  
settlement

## **Service Providers**

Service provider  
protection of  
cardholder data and  
validation

# Guidance on Mobile Payment Acceptance Security

**PCI** Security Standards Council AT A GLANCE  
MOBILE PAYMENT ACCEPTANCE SECURITY

## Accepting Mobile Payments with a Smartphone or Tablet

Many merchants seek innovative ways to engage customers and improve the shopping experience. The ever-expanding capabilities of mobile devices such as smart phones or tablets now includes payment acceptance. Along with the increased convenience at the Point of Sale, mobile payment acceptance can also bring new risks to the security of cardholder data. Securing account data at the point of capture is one way that you can actively help in controlling these risks. In 2012, validated Point-to-Point Encryption (P2PE) solutions will be listed on the PCI Council (PCI SSC) website. If you choose to accept mobile payments, these solutions may help you in your responsibilities under PCI DSS.

This At a Glance provides an example of a P2PE solution that leverages a mobile device's display and communication functions to secure mobile payments. Central to the example is the use of an approved hardware accessory in conjunction with a validated P2PE solution. Combining a validated P2PE solution with mobile devices such as phones or tablets helps to maintain data security throughout the payment lifecycle.

The diagram illustrates the data flow for mobile payment acceptance. It starts with an 'Approved PED' (Peripheral Device) and an 'Approved Secure Card Reader' connected to a 'Smart Phone or Tablet'. A blue arrow labeled 'Encrypted Cardholder Data' points from the mobile device to a server rack labeled 'P2PE Solution Provider'.

**PROTECT CARDHOLDER DATA**  
The PCI Data Security Standard (PCI DSS) requires merchants to protect cardholder data. You must protect any payment card information, whether it is printed, processed, transmitted or stored.

**For merchants interested in utilizing an off-the-shelf mobile payment acceptance solution:**

**Partner with a Provider of a Validated Solution**  
Validated P2PE solutions ensure that cardholder data is encrypted before it enters a mobile device. Using a validated and properly implemented P2PE solution greatly reduces the risk that a malicious person could intercept and use cardholder data. Solution providers will often provide you with a card reader that works with your mobile device. Validated solution providers will have a list of approved card readers (also called Point of Interaction or POI) that have been tested to work securely with their solution. The solution provider is responsible for ensuring that any POI used with their solution has been validated as compliant with the appropriate PCI SSC security requirements, including the Secure Reading and Exchange of Data (SREX).  
Your solution provider will also tell you how to safeguard your mobile payment acceptance system. This guidance is contained in a P2PE Instruction Manual (PIM). Your acquirer or payment brand may ask you to complete a P2PE Self-assessment Questionnaire as part of your annual PCI DSS validation – including confirming that you are following the solution provider's PIM. You should coordinate with your acquirer or payment brand.

**PCI** Security Standards Council

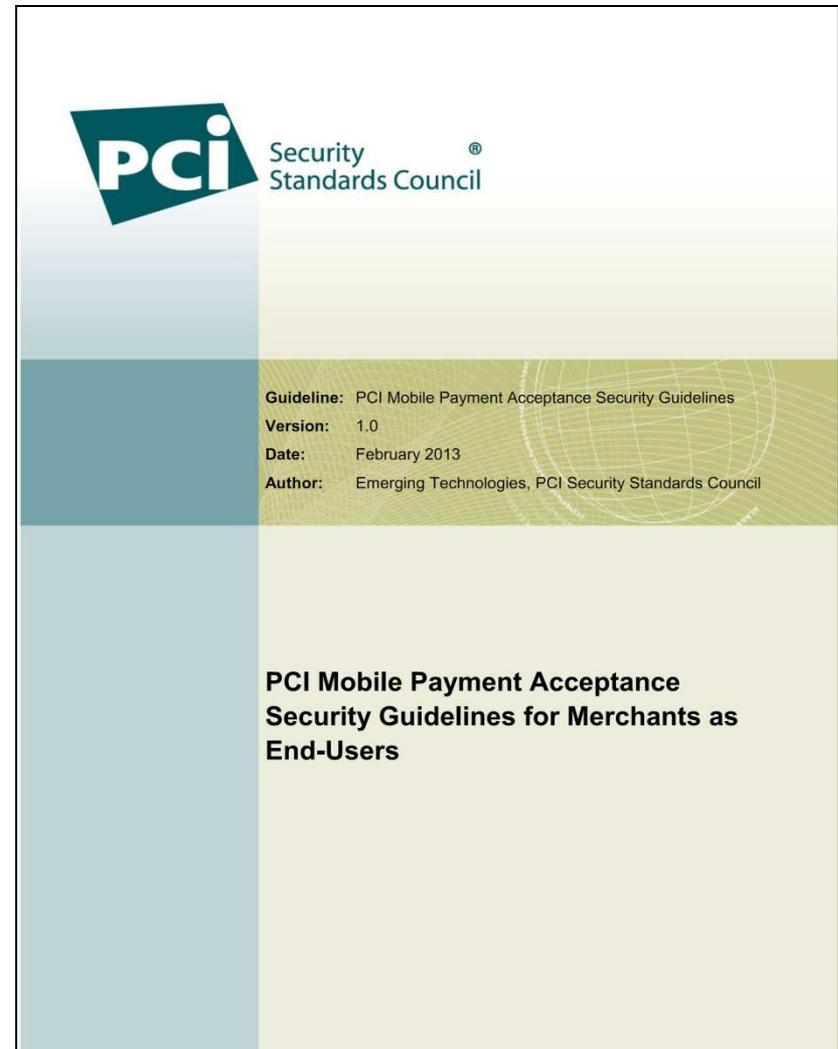
**Guideline:** PCI Mobile Payment Acceptance Security Guidelines  
**Version:** 1.0  
**Date:** September 2012  
**Author:** Emerging Technologies, PCI Security Standards Council

## PCI Mobile Payment Acceptance Security Guidelines for Developers

# New Mobile Guidance for Merchants

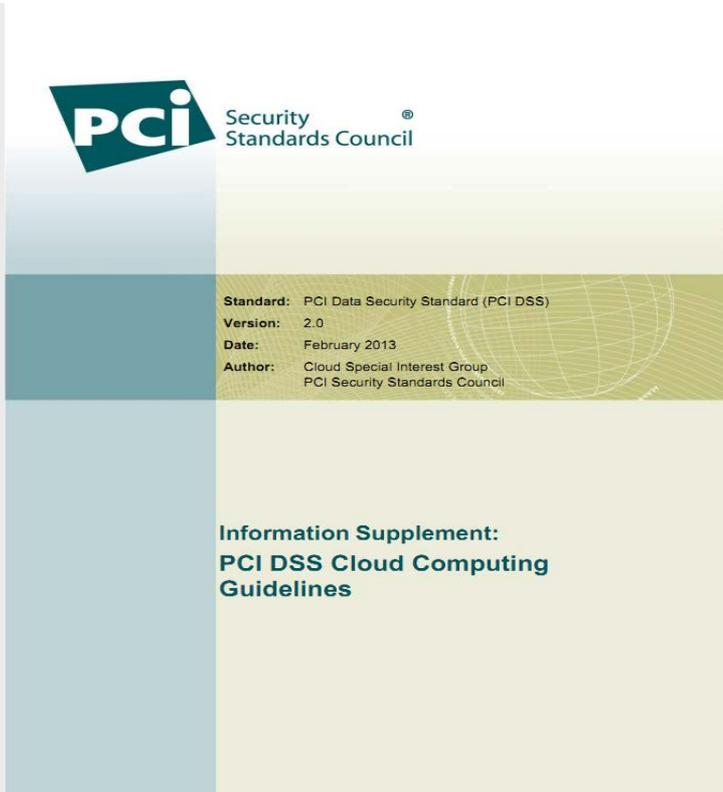
For Merchants as End-Users

- Objectives and guidance for the security of a payment transaction
- Guidelines for securing the mobile device
- Guidelines for securing the payment acceptance solution



Guiding open standards for global payment card security

# New SIG Guidance – Cloud

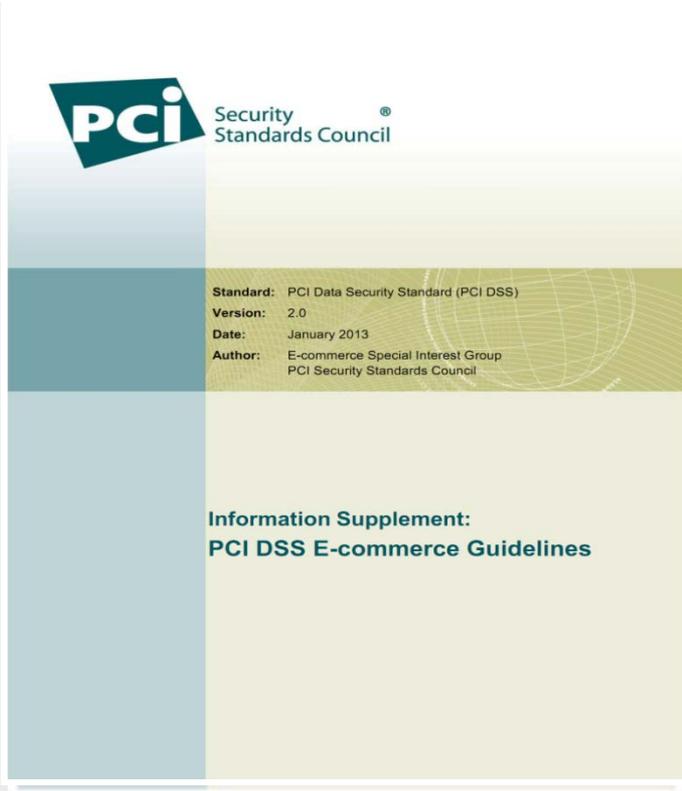


Cloud

Guidance on the use of cloud technologies and considerations for maintaining PCI DSS controls in cloud environment

**Go to our website today to download these new guidelines!**  
**<https://www.pcisecuritystandards.org/index.php>**

# New SIG Guidance – eCommerce



eCommerce

Guidance on the use of e-commerce technologies in accordance with the PCI DSS

**Go to our website today to download these new guidelines!**  
**<https://www.pcisecuritystandards.org/index.php>**

# New SIG Guidance – PCI DSS Risk Assessment



## Risk Assessment

Guidance for choosing the risk assessment approach that works best for your business to secure your card data

**Go to our website today to download these new guidelines!**  
**<https://www.pcisecuritystandards.org/index.php>**



Why PCI  
Matters

Applying PCI

How You Can  
Participate

*How You Can Participate*

# 2013 Training Highlights



*Online Internal Security Assessor (ISA) Training*

*P2PE Assessor Training*

*Corporate PCI Awareness – Let Us Come To You!*

*Online Awareness Training in Four Hours*

*Qualified Integrators and Resellers (QIR)<sup>™</sup> Program*

*PCI Professional Program (PCIP)<sup>™</sup>*

**To learn more, visit:**  
*[www.pcisecuritystandards.org/training/index.php](http://www.pcisecuritystandards.org/training/index.php)*



# *Qualified Integrators and Resellers (QIR)<sup>™</sup>*

# QIR Addresses Common Misconceptions

*I'm using a PA-DSS validated application, so I must be OK.*

*I'm using a "reputable" 3<sup>rd</sup> party, so they must be doing a secure installation.*

*This applies only to brick and mortar establishments.*





*People, Process & Technology*

# *Importance of Small Business Participation: Passwords*



# Payment Card Industry Professional (PCIP)<sup>™</sup>



**Support your  
organization**



**Professional  
credibility**



**Competitive  
advantage**



**Global  
directory**

***Now Available***

# Internal Security Assessor (ISA) Program

*A comprehensive PCI DSS training and qualification program for eligible internal audit security professionals that you asked for!*



- Improves your understanding of PCI DSS and compliance procedures
- Helps your organization build internal expertise
- Teaches processes that can reduce the cost of compliance

# *PCI Awareness Training*

**Team  
Building**

**Convenience**

**Cost**

**We come to you!**

# 2013 Training Dates

## May

3-4	ISA	New Orleans, LA
3-4	QSA	New Orleans, LA
20-21	ISA	Denver, CO
22-23	QSA	Denver, CO

## June

10-11	ISA	Orlando, FL
12-13	QSA	Orlando, FL
14-15	PA-QSA	Orlando, FL
24-26	P2PE	London, UK
25	Awareness	Sao Paulo, Brazil
26-27	ISA	Sao Paulo, Brazil
27	PCIP	London, UK

## July

14-15	ISA	Toronto, Canada
16-17	QSA	Toronto, Canada
18-20	P2PE	Toronto, Canada

## August

19-20	ISA	Boston, MA
21-22	QSA	Boston, MA

## September

19-21	P2PE	Las Vegas, NV
20-21	QSA	Las Vegas, NV
22-23	ISA	Las Vegas, NV
22-23	PA-QSA	Las Vegas, NV

## October

24-26	P2PE	Nice France
25-26	QSA	Nice, France
27-28	PA-QSA	Nice , France
27-28	ISA	Nice, France

## November

15-16	ISA	Kuala Lumpur, Malaysia
17-18	QSA	Kuala Lumpur, Malaysia
19	Awareness	Kuala Lumpur, Malaysia

# Be Involved – Contribute Your Expertise!



Chief Security Officers

Information Security Professionals

Compliance Officers

Forensic Investigators

Technologists

**Join! Become a Participating Organization today**

IT Managers

Risk Managers

Chief Information Officers

Legal Experts

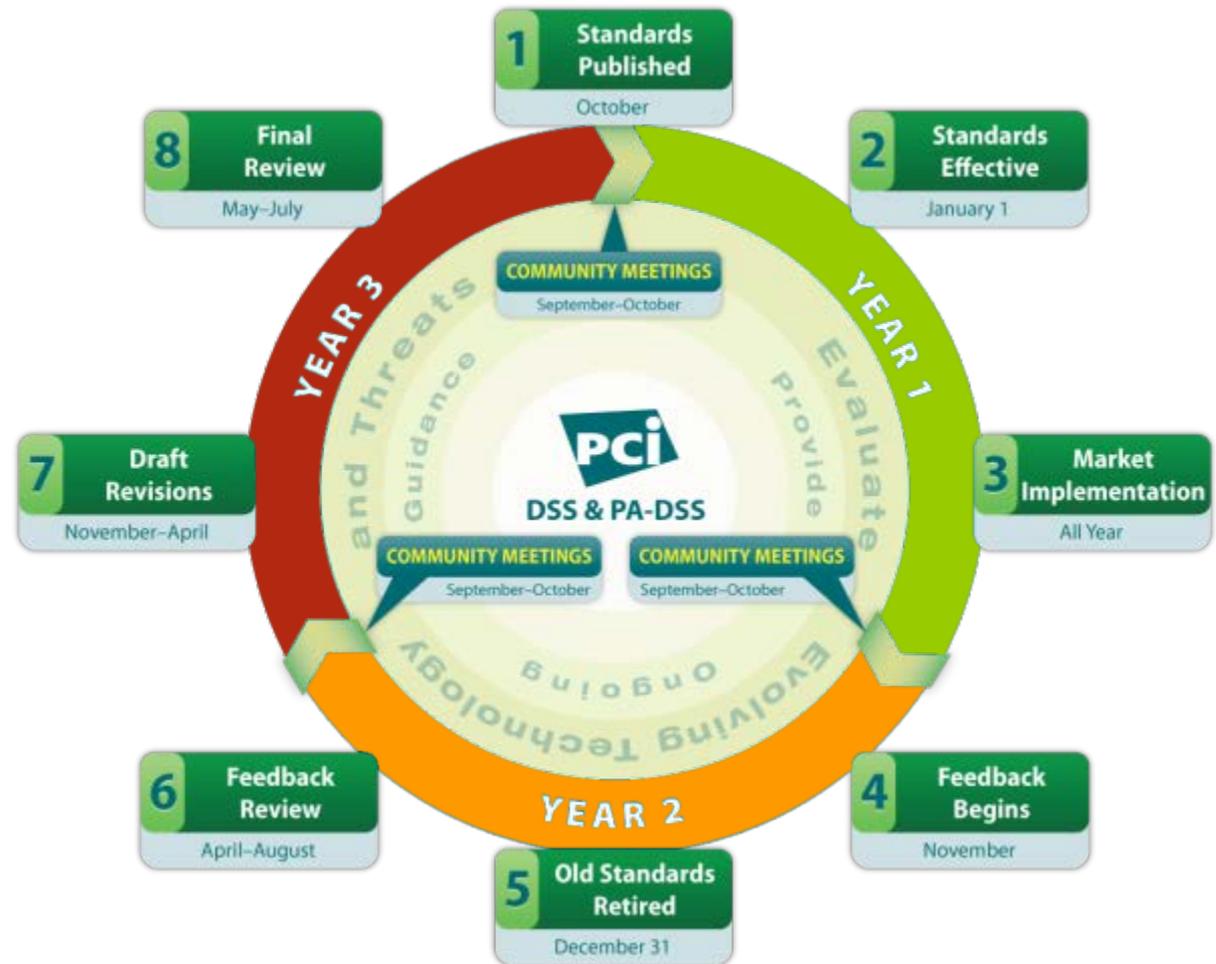
Data Security Experts

# Help Participate in Standards Development

Implementation  
Feedback

Formal  
Feedback

Draft Revisions  
Feedback



Guiding open standards for global payment card security

# 2013 Special Interest Groups- Join us!



**Best Practices for  
Maintaining PCI  
Compliance**



**Third Party  
Security  
Assurance**

***Visit PCI SSC website to sign up***

# 2014 SIG Proposal & Election Timeline

**1 June 2013**

**Proposal  
Period Open**

**25 July 2013**

**Proposal  
Period Close**

- Select SIG proposals chosen (***mid-August 2013***)
- Selected SIG proposals presented at the North American & European Community Meetings (***September & October 2013***)
- Electronic election by POs only (***November 2013***)

SAVE THE DATES!

# 2013 COMMUNITY MEETINGS



● LAS VEGAS

## NORTH AMERICAN COMMUNITY MEETING

24–26 September 2013

Mandalay Bay Convention Center  
Las Vegas, Nevada



● NICE

## EUROPEAN COMMUNITY MEETING

29–31 October 2013

Nice Acropolis  
Nice, France



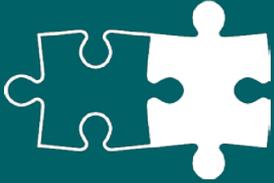
● KUALA LUMPUR

## ASIA-PACIFIC COMMUNITY MEETING

20 November 2013

Shangri-La Hotel  
Kuala Lumpur, Malaysia

# *Get Involved – We Need Your Input*



***Join***



***Learn***



***Input***



***Network***



***Nominate***



***Vote***

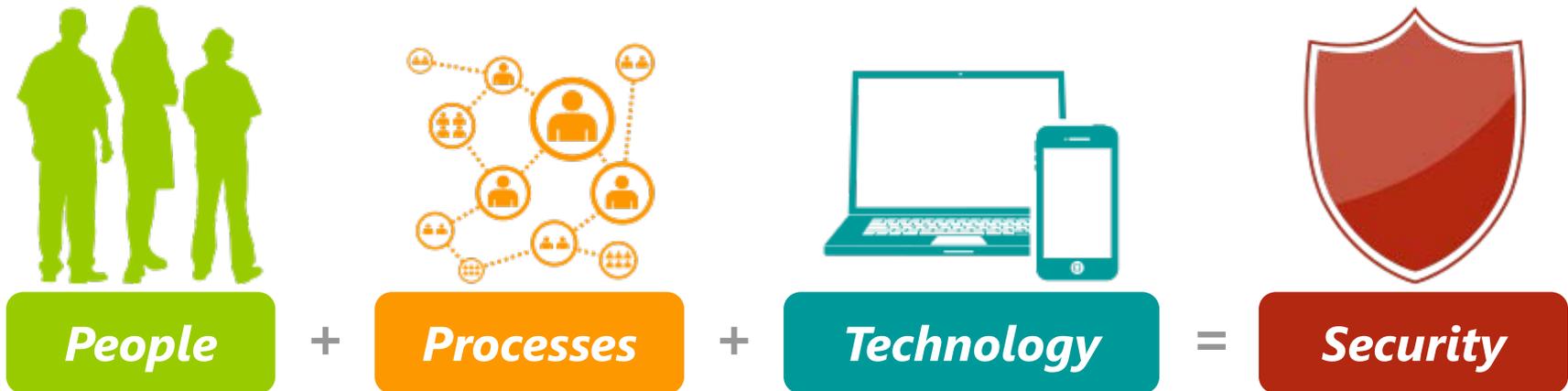


***Share***



***Influence***

# The Formula for PCI Success



# *Security vs. Compliance*



*Questions?*



Please visit our website at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)