




PCI Security Standards Council

Guiding open standards for global payment card security

Jeremy King, European Director
July 2012



A rowing team of men in yellow tank tops and black shorts are rowing a boat on a body of water. The focus is on the rowers in the foreground, with others visible in the background. The water is dark and rippling.

Why PCI?

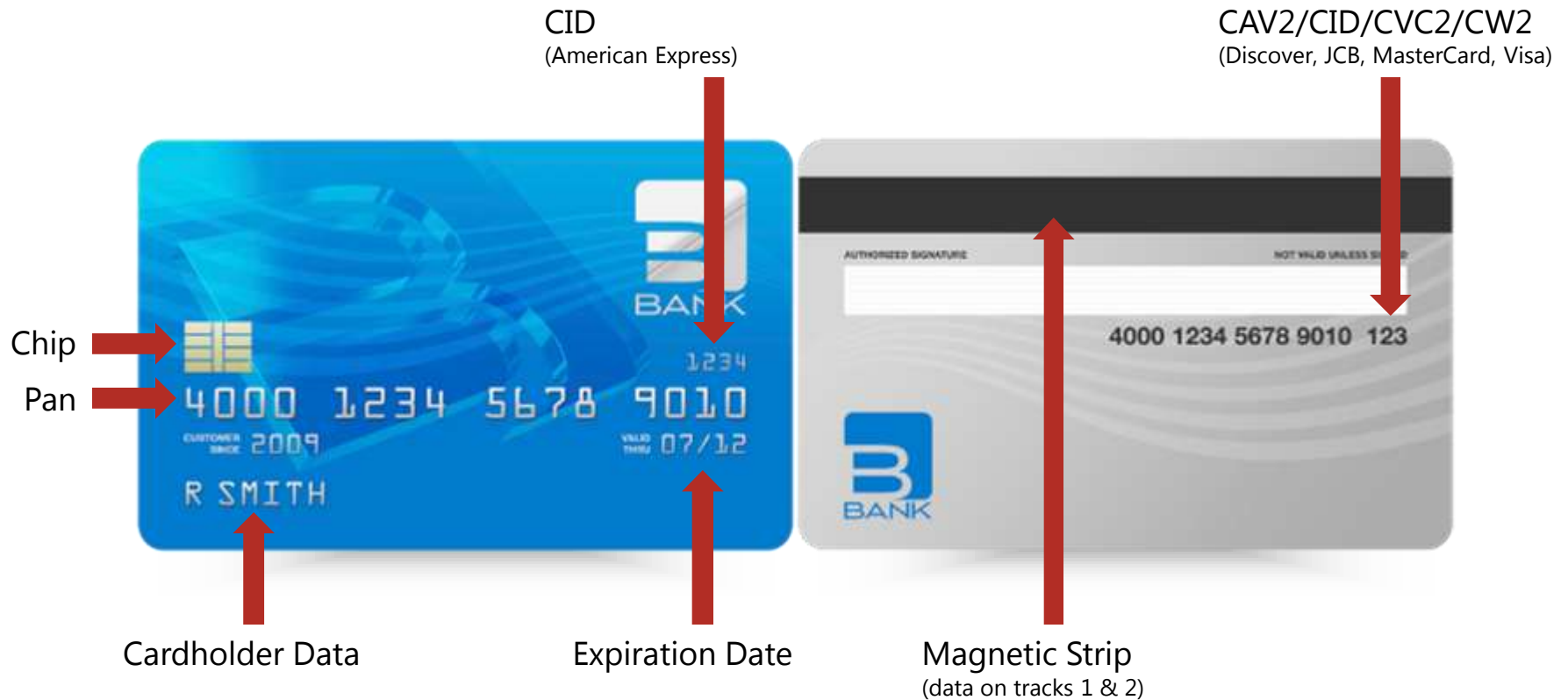
How The
Council Can
Help You

How You Can
Participate

Agenda

Your Card Data is a Gold Mine for Criminals

Types of Data on a Payment Card

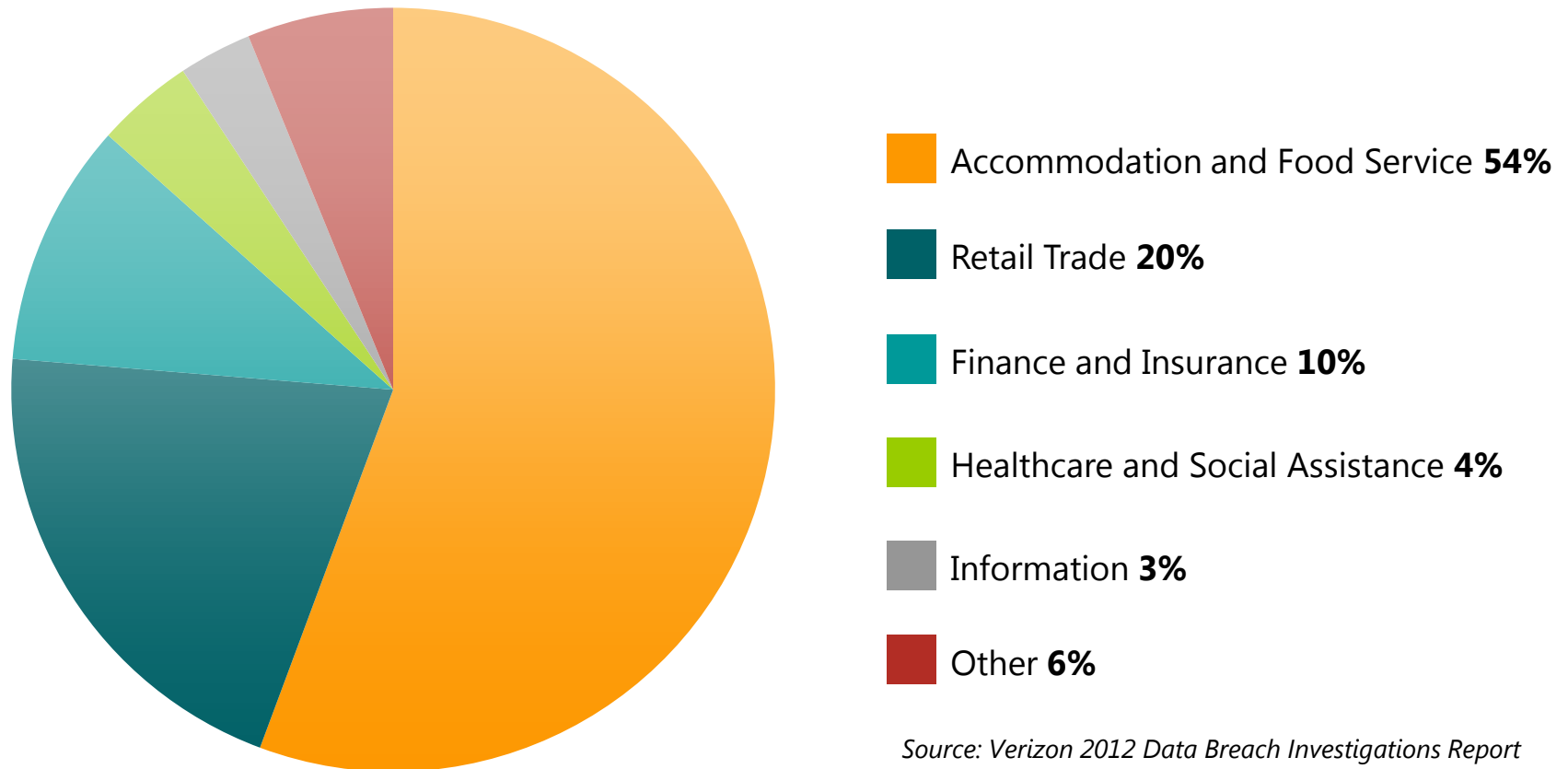


They Steal Your Data ... and They Sell It

	Country	Balance	Price
Bank of America (BOA)	USA	...	Sold
Amsouth Bank	USA	\$16,040	€700
Washington Mutual Bank (WAMU)	USA	\$14,400	€600
Washington Mutual Bank (WAMU)	USA, Multi-Currency Acct.	\$7,950 + £2,612	€500
Washington Mutual Bank (WAMU)	USA	...	Sold
MBNA America Bank	USA	\$22,003	€1,500
BANCO BRADESCO S.A.	Brazil, Dollar Account	\$13,451	€650
CITIBANK	UK, GBP Account	£10,044	€850
NatWest	UK, GBP Account	£12,000	€1000
BNP Paribas Bank	France, Euro Account	€30,792	€2200
Caja de Ahorros de Galicia	Spain, Euro Account	€23,200	€1200
Caja de Ahorros de Galicia	Spain, Euro Account	€7,846	€500
Banc Sabadell	Spain, Euro Account	€25,663	€1450



Business Sectors With the Most Breaches



Organizations Ignored PCI ... and Were Breached

96% of those breached were not PCI compliant as of their last assessment (or were never assessed/validated)

Top attack methods used to breach organizations:

- 81% of incidents involved hacking
- 69% incorporated malware
- 10% involved physical attack



2012 DATA BREACH INVESTIGATIONS REPORT
A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

Top Mistakes By Those Breached

Revealed by Forensic Audits

Weak or Blank Password for an Administrative System Account

Sensitive Information Transmitted Unencrypted on the Wire

MS-SQL Server with Weak or No Credentials for Administrative Account

Address Resolution Protocol (ARP) Cache Poisoning

Wireless Clients Probe for ESSID's from Stored Profiles When Not Connected

Continued Use of Wired Equivalent Privacy (WEP) Encryption

Client Sends LAN Manager (LM) Response for NTLM Authentication

Misconfigured Firewall Rules Permit Access to Internal Resources

Source: Trustwave 2012 Global Security Report

Guiding open standards for global payment card security

EMV Environments Also Have Risks



Lost & Stolen Card
Fraud now at its lowest
level since the industry
collation of fraud losses
began in 1991



EMV by itself does not
protect the confidentiality
of, or inappropriate access
to sensitive authentication
data and/or cardholder data

Compliance Is Good for Business

Cost of Complying

- Upgrading payment systems and security
- Verifying compliance via assessment
- Sustaining compliance
- May cost as little as \$150 to \$2,500 per IP address per year for scans for smaller merchants. Can cost millions for complex or older systems¹

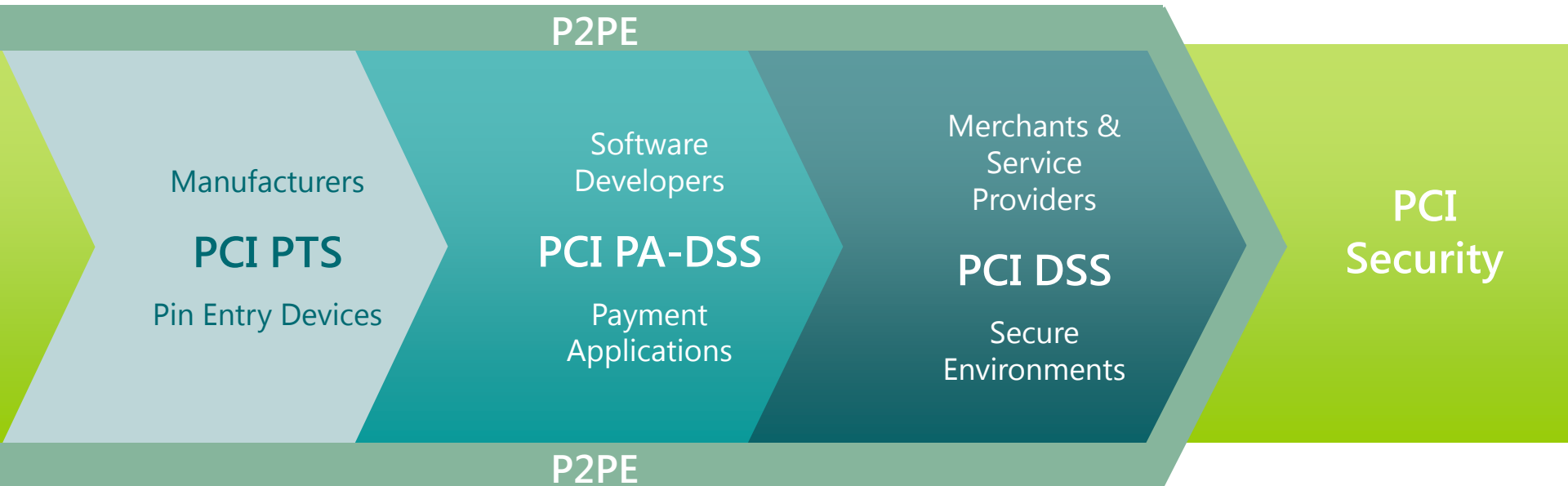
Cost of a Breach

- Average cost per compromised record is \$214
- Average cost of a breach event is \$7.2 million
- Non-compliance cost is an average of 2.65 times the cost of compliance
- Also: business disruption, reduced productivity, fees, penalties, other legal and non-legal settlement costs²

Sources: (1) PCI Compliance Cost Analysis: A Justified Expense.” A joint analysis conducted by Solidcore Systems, Emagined Security and Fortrex. (2) Ponemon Institute.

PCI Security Standards

Help You Protect Cardholder Data



Ecosystem of payment devices, applications, infrastructure and users

Guiding open standards for global payment card security

About the PCI Council

Open, global forum

Founded 2006

Guiding open standards for payment card security

- Develop
- Manage process
- Educate
- Foster Awareness



Guiding open standards for global payment card security

Global Representation, 600+ Members

- PayPal
- RSA, The Security Division of EMC
- Starbucks
- TSYS
- VeriFone Systems, Inc.
- Wal-Mart Stores, Inc.

- Barclaycard
- British Airways
- Cartes Bancaires
- European Payments Council
- IATA
- Ingenico
- Tesco Stores Limited

- Cisco
- Citi
- First Data Corporation
- Heartland Payment Systems
- JPMorgan Chase&Co.
- McDonald's Corporation

• Cielo

• Woolworths Limited

* *Board of Advisors*

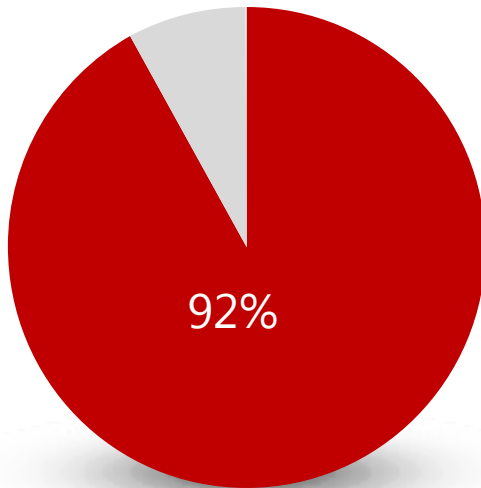
Guiding open standards for global payment card security

The PCI Data Security Standard

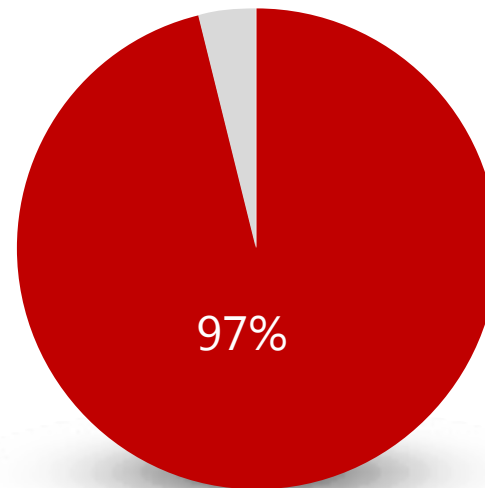
Six Goals	Twelve Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors

PCI Standards Help Secure Your Data

92% of compromises were simple



97% were avoidable through simple or intermediate controls



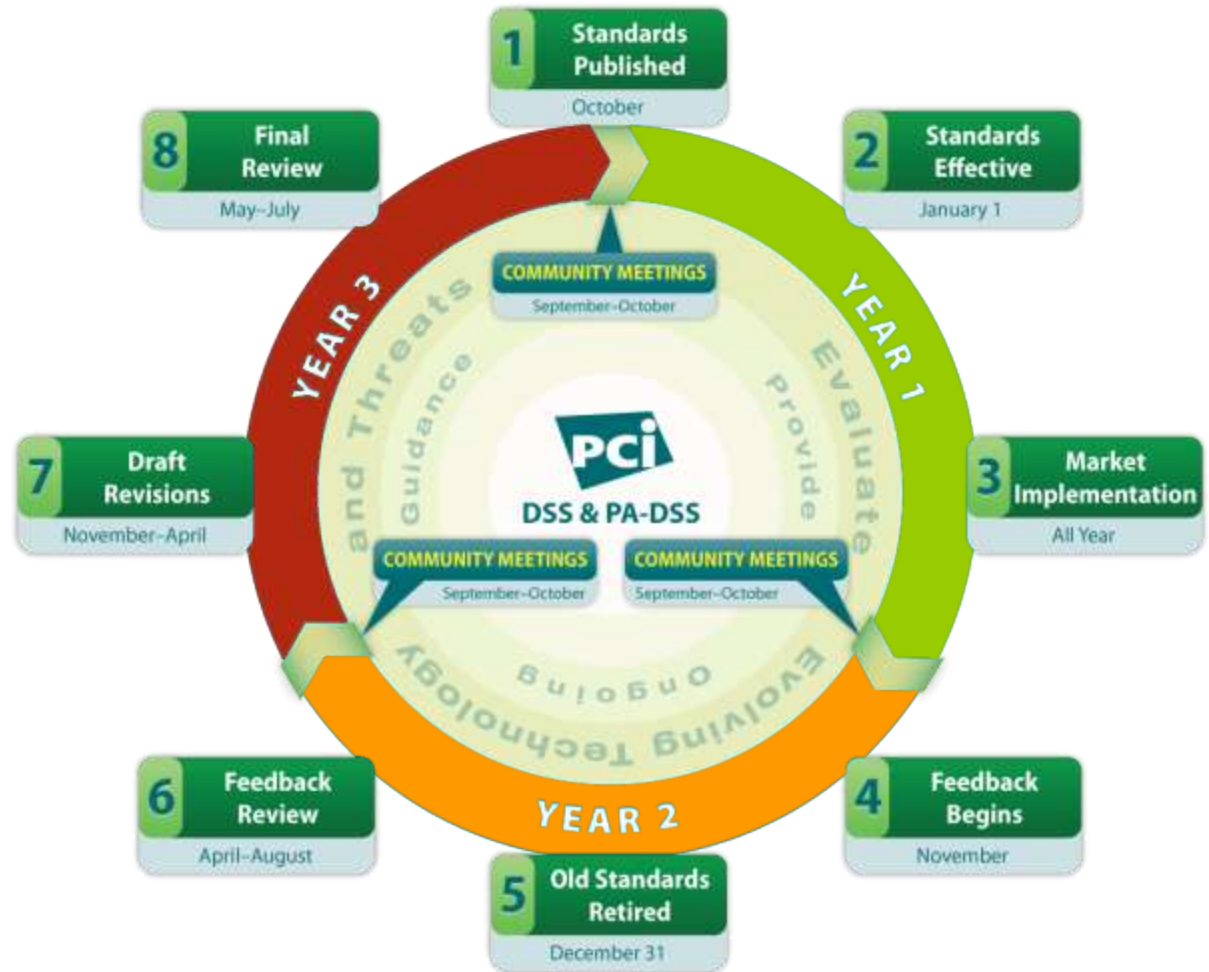
Source: Verizon 2012 Data Breach Investigations Report

You Drive the Open PCI Standards Lifecycle

Implementation
Feedback

Formal
Feedback

Draft Revisions
Feedback



Guiding open standards for global payment card security

Your Feedback Shapes the Standards

1

Feedback reviewed and categorized (April '12 – August '12)

2

Feedback shared with PCI community (August – September '12)

3

Feedback presented at 2012 Community Meetings (September '12 – October '12)

4

Revisions drafted for PCI DSS and PA-DSS (November '12 – April '13)

5

Final Review Period (May '13 – July '13)

6

Standards Published (October '13)

PCI Security is a Journey...



...but reaching the summit holds immense value for your organization

96% of breach victims that are subject to PCI DSS had not achieved compliance

Source: Verizon 2012 Data Breach Investigations Report

Use the Standards to Make Security Part of Your DNA



Reduce the attack surface



Continuous Awareness & Protection



Prevent New Types of Exposure



Measure success and identify opportunity

Focused Guidance on Payment Technology



Mobile



P2PE



Virtualization



Wireless



Tokenization



Telephone-based
Payment Card Data



EMV

Even EMV Security Needs PCI



EMV



- Council released guidance on EMV within an overall data security framework defined by the PCI Data Security Standard
- Guidance highlights benefits both systems bring to tackling fraud
- EMV does help prevent some types of fraud, but for a merchant to secure payment data they must also adopt all elements of the PCI DSS
- In today's EMV market, PCI DSS must be fully implemented to protect cardholder data

Point-to-Point Encryption



2012 Target Deliverables

General Requirements

- *P2PE Hardware encryption and hardware decryption*
- *P2PE "Hybrid" Hardware encryption and hardware decryption, with transaction keys in software at decryption*
- *P2PE next phase*

Point-to-Point Encryption

- P2PE Assessor Qualification Requirements released
- Testing Procedures, Program Guide, SAQ and P2PE Assessor training now available
- Solutions listing for Fall 2012

Sign up for P2PE Training today:
administration@pcisecuritystandards.org

Mobile Update



Deliverable

Guidance and Best Practices

- *Mobile Transactions Using SCR & P2PE for Merchants*
- *Mobile Acceptance Best Practices*

Mobile

- Key areas of focus include:
 - Devices
 - Applications
 - Service Providers

Mobile Update



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.

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 with a Validated Point of Interaction (PCI) that have been tested to work securely with the solution provider. The solution provider is responsible for ensuring that any PCI used with the solution is validated as compliant with the appropriate PCI SSC security standard, such as the Secure Reading and Exchange of Data (SRED). The solution provider will also tell you how to safeguard your mobile payment acceptance is contained in a P2PE Instruction Manual (P2PE-IM). The solution provider may ask you to complete a P2PE Self-assessment Questionnaire (P2PE-SAQ) as part of your annual PCI DSS validation - including confirming that the solution provider's P2PE-IM. You should coordinate with your

NEW

Accepting Mobile Payment Acceptance Security Fact Sheet for Merchants

- Understand PCI DSS responsibilities in mobile environments
- Leverage benefits of P2PE program
- Choose a mobile payment acceptance solution that complements the merchant's PCI DSS responsibilities

2012 Training Highlights

- ✓ *Qualified Integrators and Resellers (QIR) Program*
- ✓ *Corporate PCI Awareness – Let Us Come To You!*
- ✓ *Online Awareness Training in Four Hours*

To learn more, visit:

<https://www.pcisecuritystandards.org/training/index.php>

Make 2012 the Year of Data Security Training

PCI SSC Internal Security Assessor (ISA) Program
Helps security professionals improve their organizations' understanding of PCI DSS and validate and maintain ongoing compliance



PCI Awareness Training
Offers general PCI training across your business to ensure a universal understanding of PCI compliance

PCI Awareness Training online anytime!

Check out our
Training Webinar!

2012 Training Schedule

ISA Training: Boston, MA, USA 20-21 August

QSA Training: Boston, MA, USA on 22-23 August

ISA Training: Lake Buena Vista, FL, USA on 6 – 7 September

PA-QSA Training: Lake Buena Vista, FL, USA on 8 – 9 September

QSA Training: Lake Buena Vista, FL, USA on 10 – 11 September

ISA Training: Lake Buena Vista, FL, USA on 10 – 11 September

P2PE Training: Lake Buena Vista, FL, USA on 15 – 16 September

Guiding open standards for global payment card security



New Certification and Training Opportunity Coming Soon!

Become PCI Certified as a Qualified Integrator and Reseller (QIR) – earn PCI credentials and exclusive listing on the PCI SSC website!

What is the Qualified Integrators and Resellers (QIR) Program? PCI SSC certification program to educate, qualify, and train organizations involved in the implementation, configuration, and/or support of a PA-DSS validated payment application on behalf of a merchant.

Who can participate? Any eligible company involved in implementing and configuring PA-DSS validated applications into merchant environments, including both brick-and-mortar and e-commerce environments.

What are the benefits?


- Achieve industry-recognized certification
- Be included on merchants' go-to global list of certified integrators and reseller
- Receive specialized training from PCI SSC experts on guidelines for implementing and maintaining payment applications
- Earn CPE credits

Online training will begin in fall 2012.

For more details, visit www.pcisecuritystandards.org/training/qir_training.php.

Please contact QIR@pcisecuritystandards.org with any questions.

Guiding open standards for global payment card security

A rowing team of men in yellow tank tops is shown in a rowing boat on a body of water. The focus is on the rowers in the foreground, with others visible in the background. The water is dark and reflects the sunlight.

Why PCI?

How The
Council Can
Help You

How You Can
Participate

Agenda

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

Special Interest Groups (SIGs) Are For You



Risk Assessment



eCommerce



Cloud

sigs@pcisecuritystandards.org

Email today to join!

2013 SIG Proposal & Election Timeline

June 1, 2012

**Proposal
Period Open**

July 31, 2012

**Proposal
Period Close**

The Special Interest Groups (SIGs) leverage the valuable business and technical experiences of PCI SSC Participating Organizations to collaborate with the Council on any supporting guidance or special projects relating to the PCI Security Standards.

Submit your 2013 SIG proposal today!

- After the close of the SIG proposal period a shortlist of proposals will be drawn up by PCI SSC and those selected notified.
- Presentations from POs and assessors on shortlisted SIG proposals will be given at the North American and European Community Meetings.
- Electronic vote on which proposals to move ahead with will follow in November.

NEW for 2013: Online Proposal Form now available at
<https://www.pcisecuritystandards.org/site/sig-2012.php>

Guiding open standards for global payment card security

2012 PCI Community Meetings

Orlando, Florida, USA

September 12-14, 2012



Dublin, Ireland

October 22-24, 2012



Register today:

http://www.regonline.com/pcissc_cm_orlando2012

http://www.regonline.com/pcissc_cm_dublin2012

Summary

Learn!

Take advantage of the Council's resources and guidance, and training courses

Join!

Become a Participating Organization today

Share!

We want your feedback on the Standards

Participate!

Get involved in a Special Interest Group

Questions?



Please visit our website at www.pcisecuritystandards.org