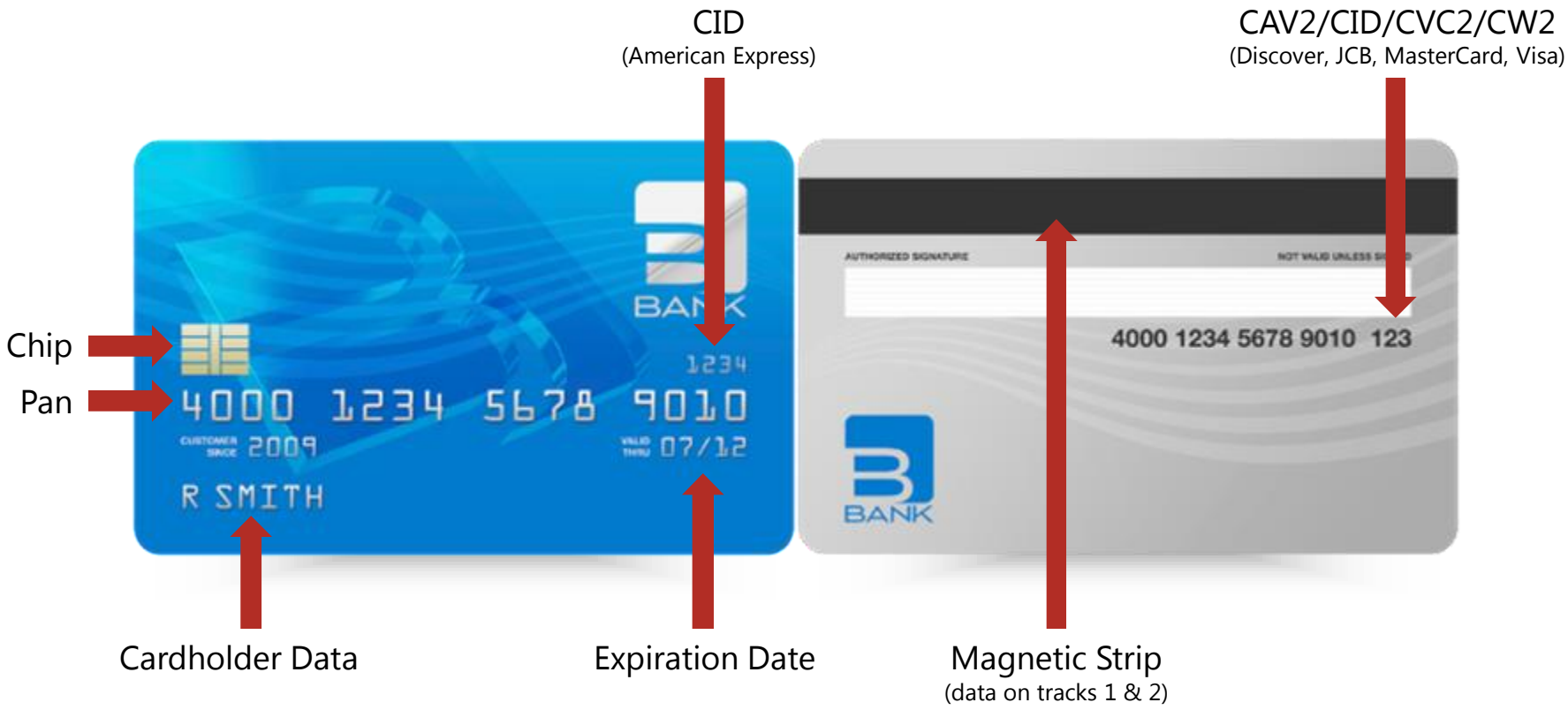
The future of PCI: Securing payments in a changing world

Jeremy King
2014

PCI Security Standards Council®

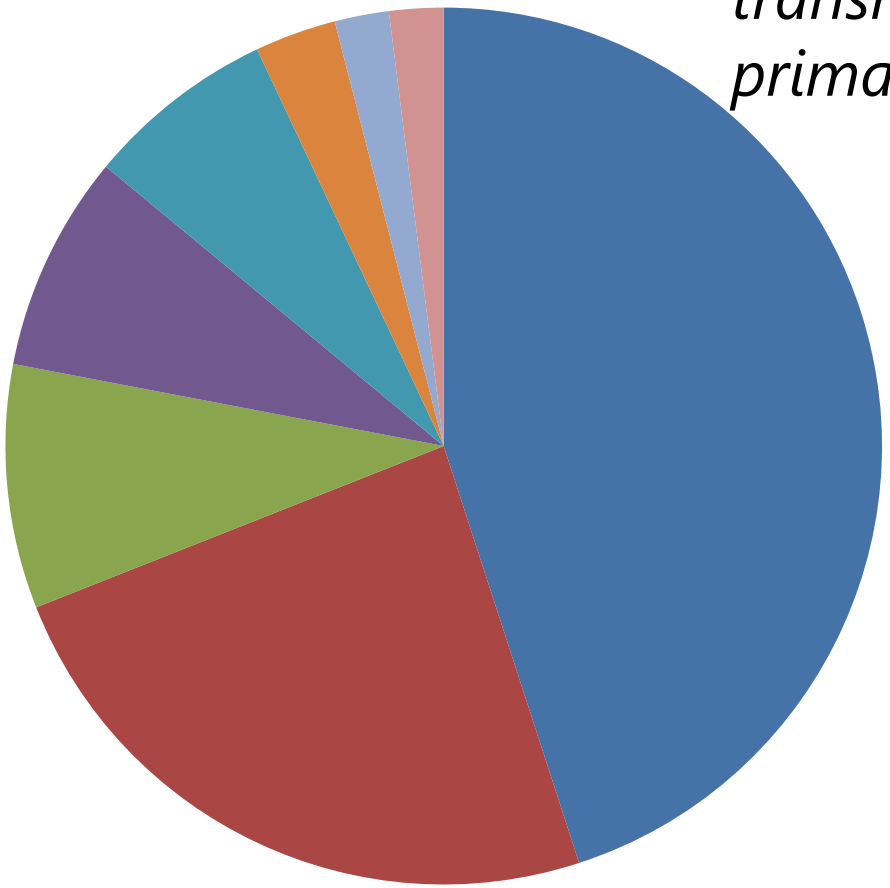
Your Card Data is a Gold Mine for Criminals

Types of Data on a Payment Card



Business Sectors With the Most Breaches

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

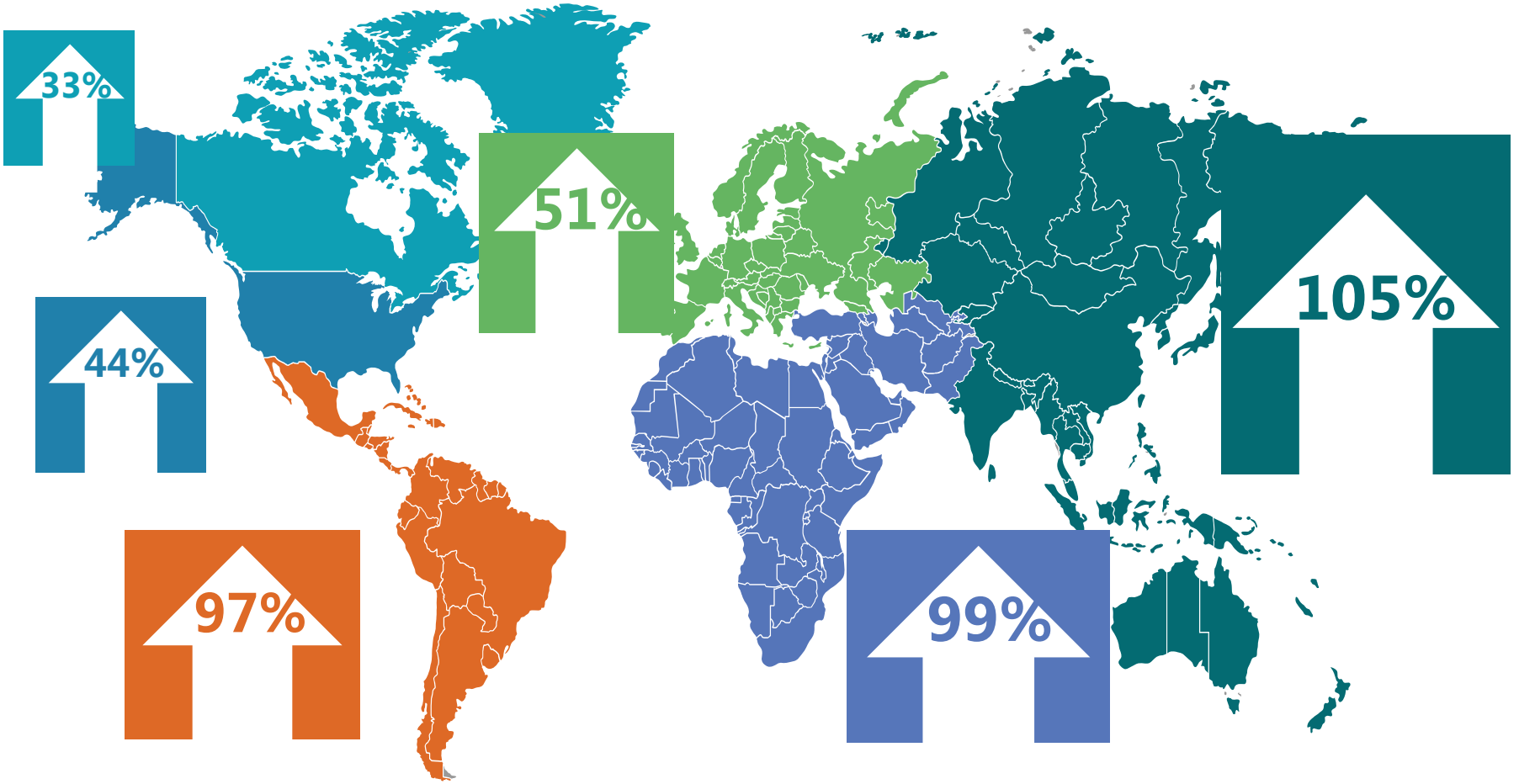


Source: Trustwave 2013 Global Security Report

Who's High Risk?

People in Payment Chain Cause Most Internal Breaches!

As Global Use Rises, So Does Risk



Growth in Purchase Transactions Worldwide from 2011-2016

Top Mistakes Revealed by Forensic Audits

Weak or default passwords

Lack of employee education

Security deficiencies introduced by third parties

Slow self-detection

Source: 2013 Trustwave Global Security Report

Complex Passwords Don't Have to be Complicated

Password	***Time to Crack***
bigmac	0.077 seconds (not a dictionary word)
B1gMac	14 seconds (uppercase, lowercase, number
B1gMac1	14 minutes (7 characters)
leB1gMac	15 hours (8 characters)
B1gMac399	39 days (9 characters)
B1gMacfries	412 years (11 characters)
Bigmacandfries	511 years (14 characters, but only letters)
B1gMac&fries	344,000 years (12 characters)

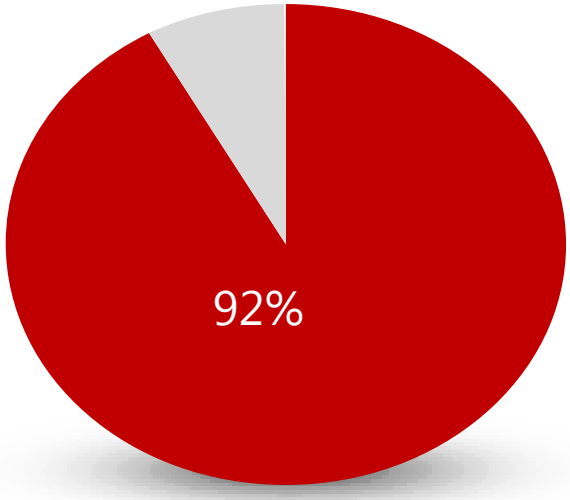
*25 Most Common Passwords of 2013**

1. 123456 (Up 1)
2. password (Down 1)
3. 12345678 (Unchanged)
4. qwerty (Up 1)
5. abc123 (Down 1)
6. 123456789 (New)
7. 111111 (Up 2)
8. 1234567 (Up 5)
9. iloveyou (Up 2)
10. adobe123 (New)
11. 123123 (Up 5)
12. admin (New)
13. 1234567890 (New)
14. letmein (Down 7)
15. photoshop (New)
16. 1234 (New)
17. monkey (Down 11)
18. shadow (Unchanged)
19. sunshine (Down 5)
20. 12345 (New)
21. password1 (up 4)
22. princess (New)
23. azerty (New)
24. trustno1 (Down12)
25. 000000 (New)

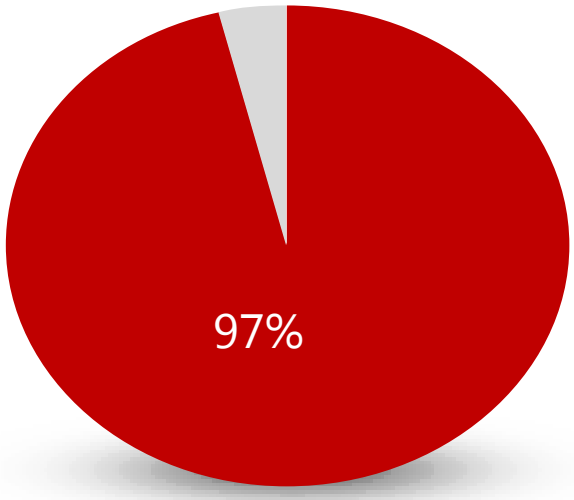
*CBS News, 21 January 2014

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

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

Source: Verizon 2012 Data Breach Investigations Report

Why?

Why we fail to maintain secure environments

- Lack of awareness by IT practitioners
- Incentive to keep security a primary focus
- Quickly evolving technology landscape
- Rapid development and distribution of new solutions
- Still unnecessary exposure of card holder data

PCI: Architecture for Payment Card Security

Five major card brands drive efforts for payment card security

PCI Security Standards Council manages the technical standards and process

About the PCI Council

Open, global forum

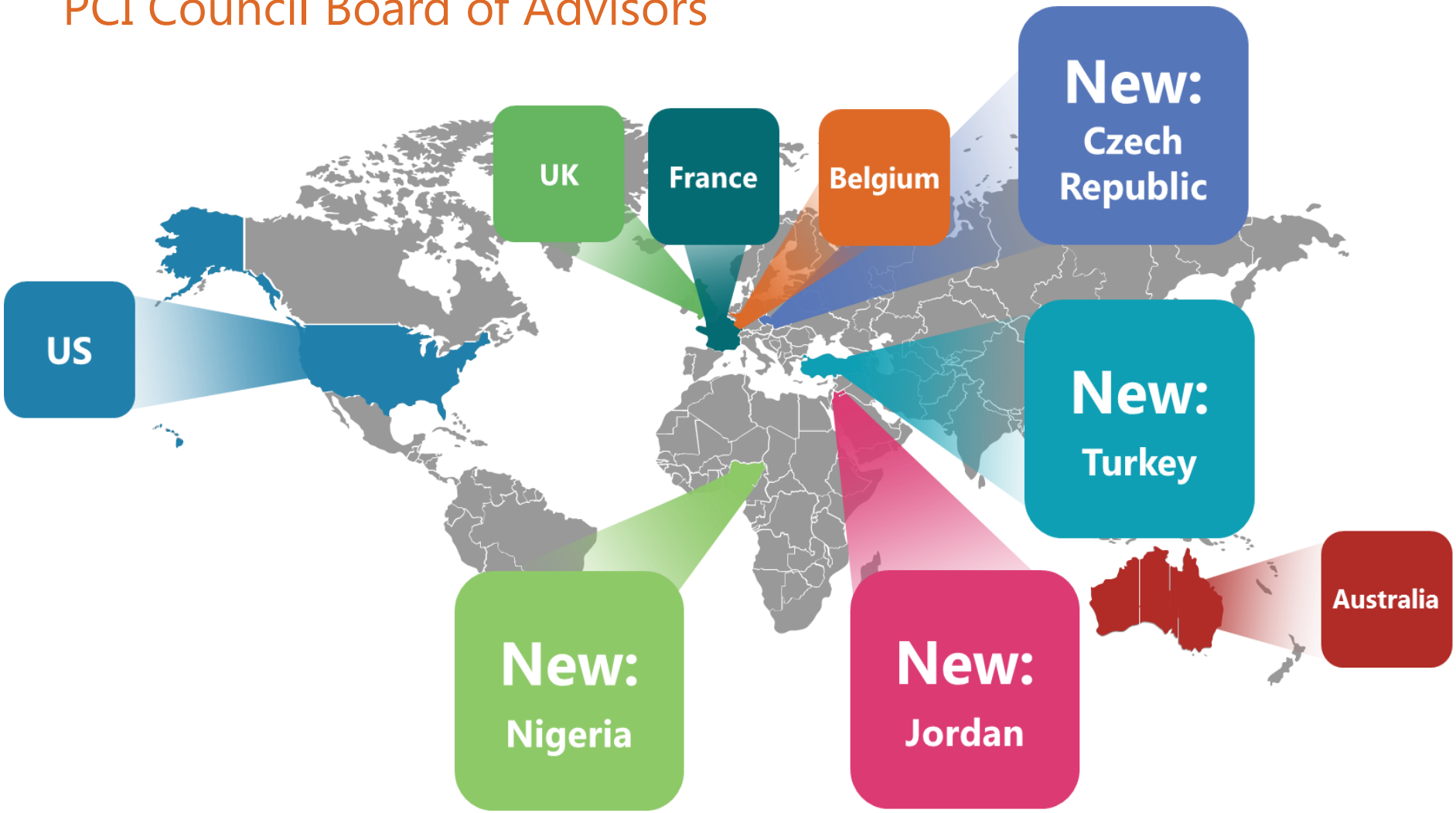
Founded 2006

Guiding open standards for payment card security

- Development
- Management
- Education
- Awareness

Expanding Global Representation

PCI Council Board of Advisors

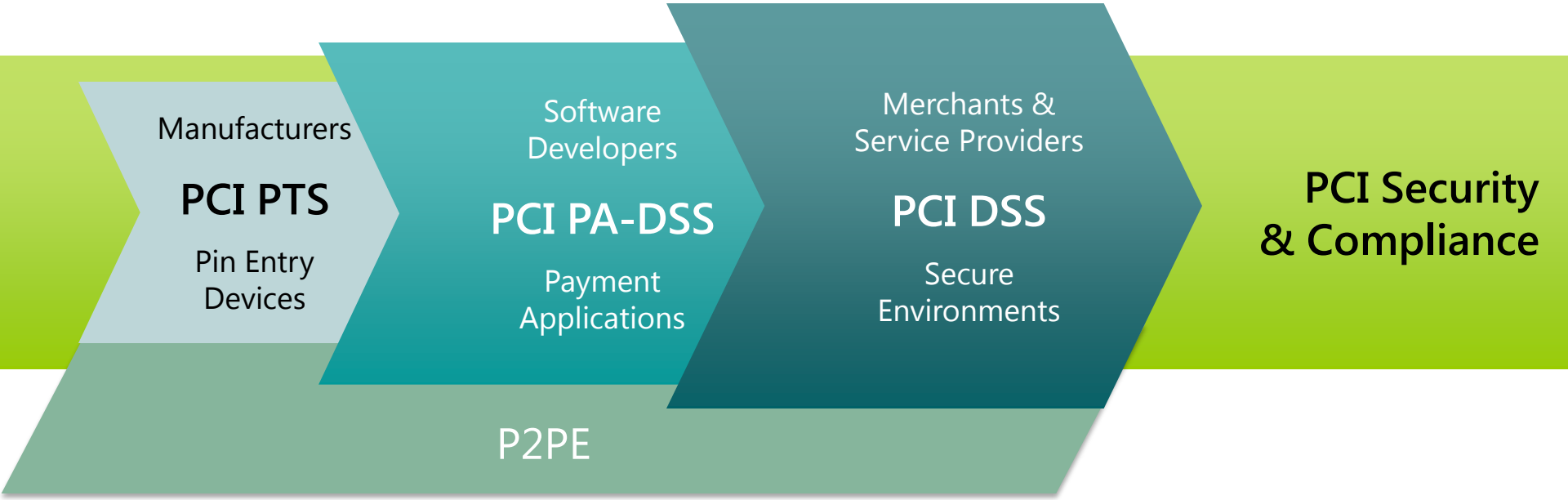


PCI Security Standards Council

Guiding open standards for global payment card security

PCI Security Standards Suite

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

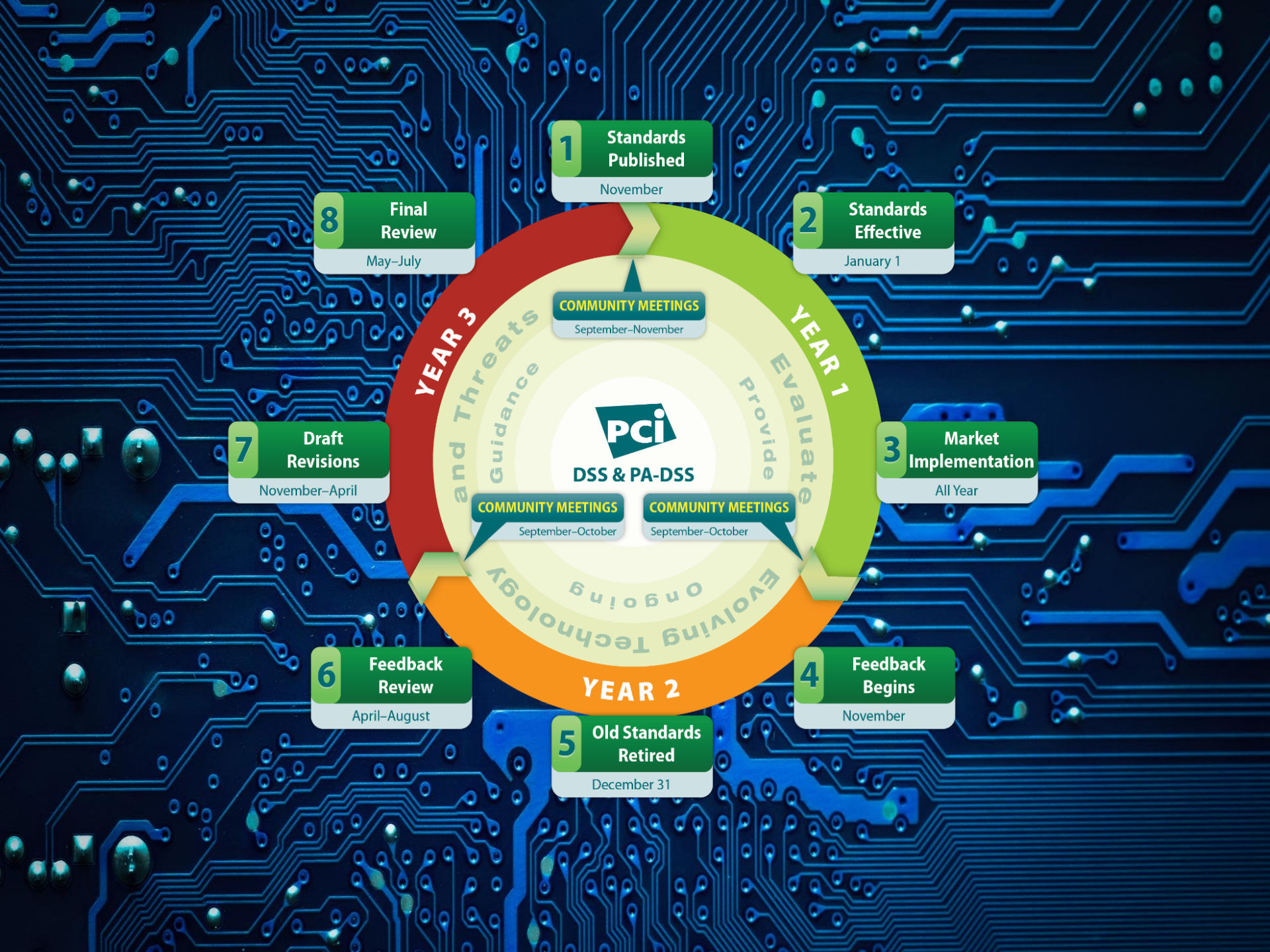
PCI Standards Help Secure Your Data

9 out of 10 security pros recommend PCI.

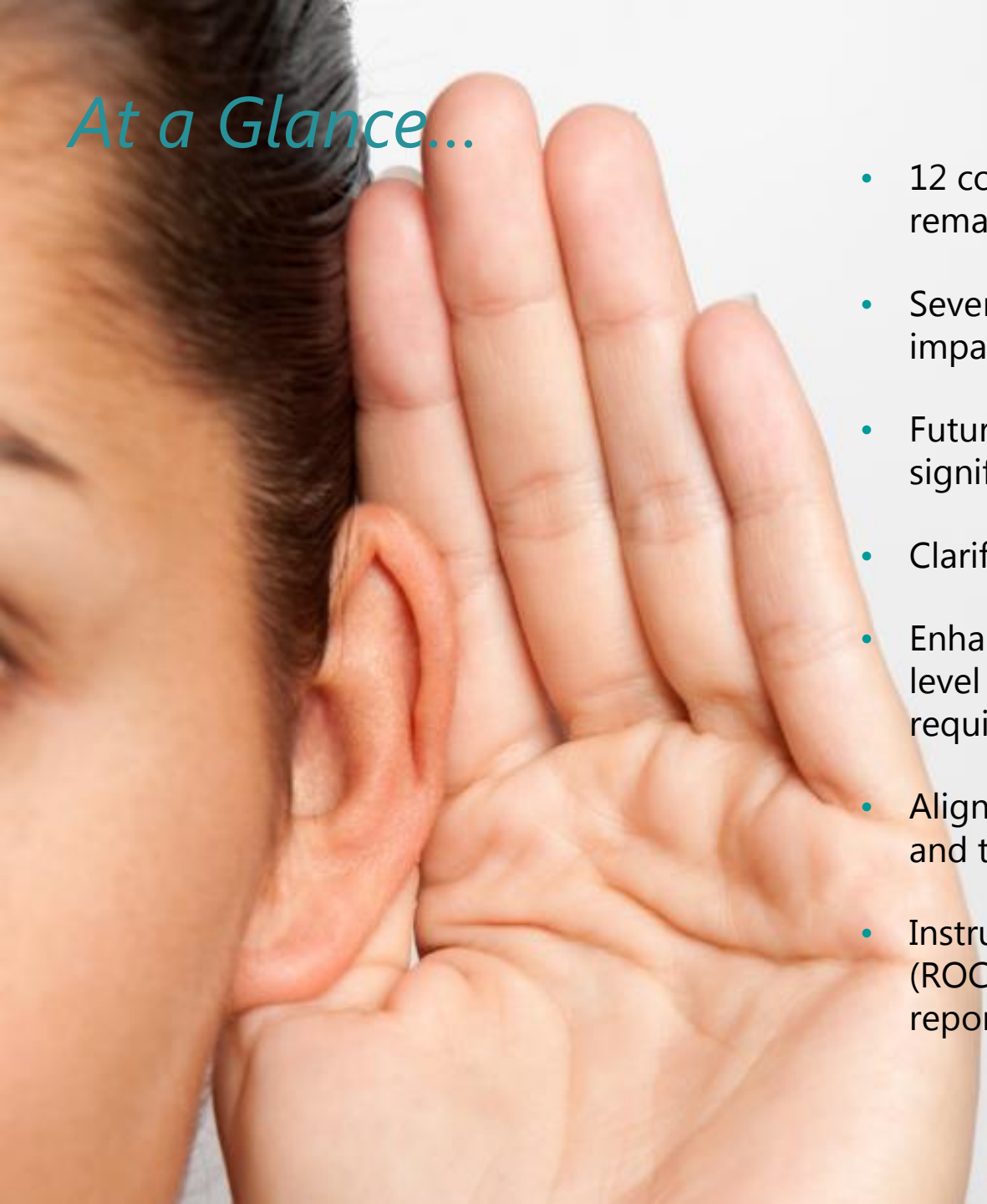
Source: Real Cost of Security Report, 451 Group

PCI DSS has made comprehensive security controls more commonplace in larger organizations. Therefore, the organizations become more difficult to compromise.

Source: 2013 Trustwave Global Security Report


1 Standards Published
November
2 Standards Effective
January 1
3 Market Implementation
All Year
4 Feedback Begins
November
5 Old Standards Retired
December 31
6 Feedback Review
April–August
7 Draft Revisions
November–April
8 Final Review
May–July
YEAR 1
YEAR 2
YEAR 3
Evaluate
Provide
Guidance
and Threats
Evolving Technology
Ongoing
COMMUNITY MEETINGS
September–November
COMMUNITY MEETINGS
September–October
COMMUNITY MEETINGS
September–October
PCI
DSS & PA-DSS

PCI DSS, PA-DSS 3.0



At a Glance…

- 12 core security principles of PCI DSS remain the same
- Several new sub-requirements that will impact PCI DSS security efforts
- Future implementation dates for more significant changes
- Clarified PCI DSS Applicability
- Enhanced testing procedures to clarify level of validation expected for each requirement
- Aligned language between requirements and testing procedures for consistency
- Instructions for Report on Compliance (ROC) reporting now separate ROC reporting template

Physical Security for POS Devices

9.9 Protect devices that capture payment card data from tampering and substitution

- Maintain an up-to-date list of devices
- Periodically inspect device surfaces to detect tampering or substitution
- Provide training for personnel to be aware of attempted tampering or replacement of devices

Penetration Testing and Effective Scoping

11.3 Implement a penetration testing methodology

11.3.4 If segmentation is used, perform penetration tests to verify that the segmentation methods are operational and effective.

Security as a Shared Responsibility

Guidance	• Outsourcing PCI DSS responsibilities
Requirement 8.5.1	• Service providers with access to customer environments to use unique authentication credential per customer
Requirement 12.9	• Added to support 12.8; Service providers must acknowledge that they will maintain applicable PCI DSS requirements to the extent that the service provider handles or manages customer's cardholder data

The Formula for PCI Success

Technology in Payments

Mobile

P2PE

Virtualization

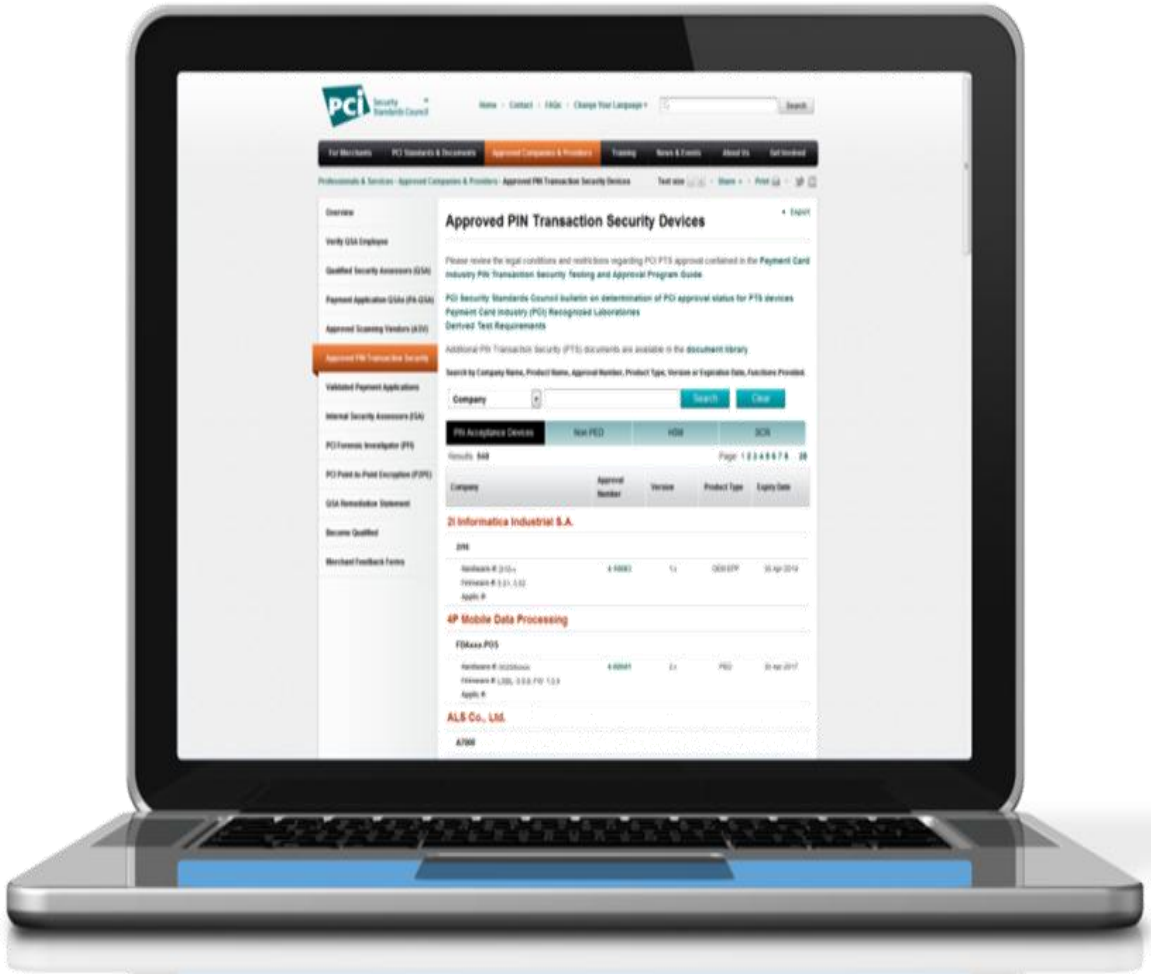
Wireless

Tokenization

Telephone-based
Payment Card Data

EMV Chip

EMV Chip + PCI Working Together for Greater Security

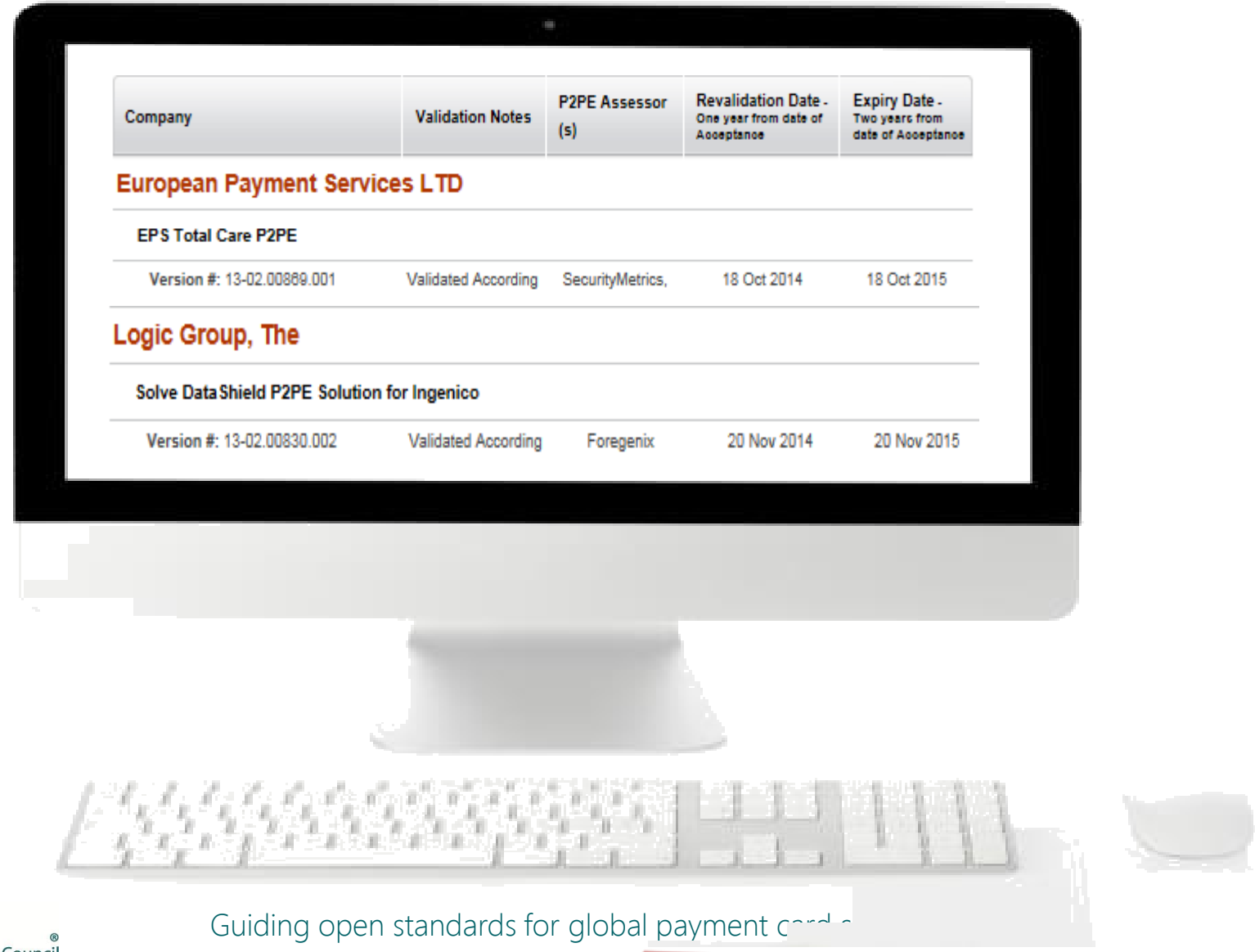


PCI Security Standards Council

EMV Chip Helps Reduce Face-to-Face Fraud

EMV Chip Needs PCI

Point-to-Point Encryption



Company	Validation Notes	P2PE Assessor (s)	Revalidation Date - One year from date of Acceptance	Expiry Date - Two years from date of Acceptance
European Payment Services LTD				
EPS Total Care P2PE				
Version #: 13-02.00869.001	Validated According	SecurityMetrics,	18 Oct 2014	18 Oct 2015
Logic Group, The				
Solve DataShield P2PE Solution for Ingenico				
Version #: 13-02.00830.002	Validated According	Foregenix	20 Nov 2014	20 Nov 2015

Work on tokenization standards has begun

PAN

Tokenization

Mobile

PCI Standards focus on merchant-acceptance

Mobile payment acceptance still evolving

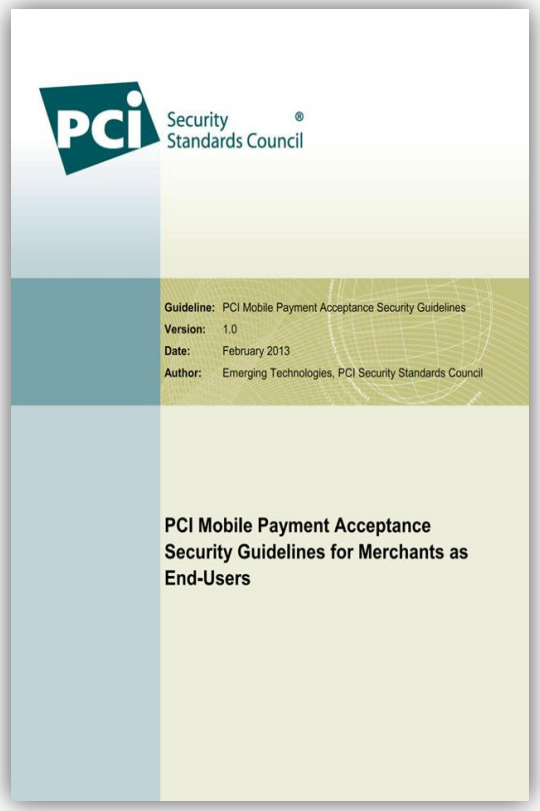
Understand risk and use PCI SSC resources

PCI SSC is working with industry

Mobile Guidelines and Best Practices

Guidelines published 2012-2013

- PCI Mobile Payment Acceptance Guidelines for Developers
- PCI Mobile Payment Acceptance Guidelines for Merchants as End-Users
- Accepting Mobile Payments with a Smartphone or Tablet



PCI SIG Guidance Documents

Cloud

E-Commerce

Tokenization

Visit www.pcisecuritystandards.org
to download this guidance

Special Interest Group (SIG)

Maintaining PCI DSS Compliance

183 members

Third Party Security Assurance

196 members

Multilingual Resources on the PCI Website

- *Chinese*
- *French*
- *German*
- *Japanese*
- *Italian*
- *Portuguese*
- *Russian*
- *Spanish*

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)™ Program***
- ✓ ***PCI Professional Program (PCIP)™***

To learn more, visit:
www.pcisecuritystandards.org/training

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

PCI Security Standards Council

Guiding open standards for global payment card security

Qualified Integrators and Resellers (QIR)™

QIR Addresses Common Misconceptions

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

I'm using a "reputable" 3rd party, so they must be doing a secure installation.

This applies only to brick and mortar establishments.

Payment Card Industry Professional (PCIP)™

Now Available

PCI Security Standards Council®

Guiding open standards for global payment card security

Get Ready for the Future

Personal PCI training is essential to keep on top of emerging threats

PCI training by the Council is the most effective, targeted way to accelerate mastery and stay current

Validation proves your value to your employer and sets you apart from so-called “experts”

PCI Security Standards Council

Guiding open standards for global payment card security

Save the Dates – 2014 Community Meetings

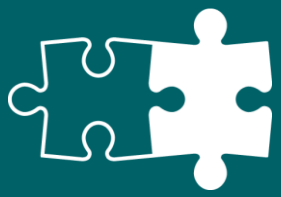
North America	Europe	Asia-Pacific
		
9-11 September **Orlando, Florida**	7-9 October Berlin, Germany	18-19 November Sydney, Australia

Stand Out From the Crowd – Become a PO

Benefits of Participating Organization (PO):

- Two free passes to Community Meetings
- Savings on Council training
- Ability to vote for Board of Advisors officers
- Opportunity to participate in SIGs
- And more!

Get Involved – We Need Your Input



Join

Learn

Input

Network

Nominate

Vote

Share

Influence

Questions?

PCI Security Standards Council®

Please visit our website at www.pcisecuritystandards.org