



PCI Updates: Securing the future of payments

Bob Russo, General Manager
2014



Everyone is Aware of Breaches!

NEWS Attacks and Breaches

**Survey: Cyberattacks Greater Threat Than
Physical Attacks**

2.5 million Californians
to identity theft in

09 July 2013

Evolution of Cyber Attacks

Viruses

Worms

Trojan
Horses

Custom
Malware

Advanced
Persistent
Threats

Modern Malware Hides Itself



About the PCI Council

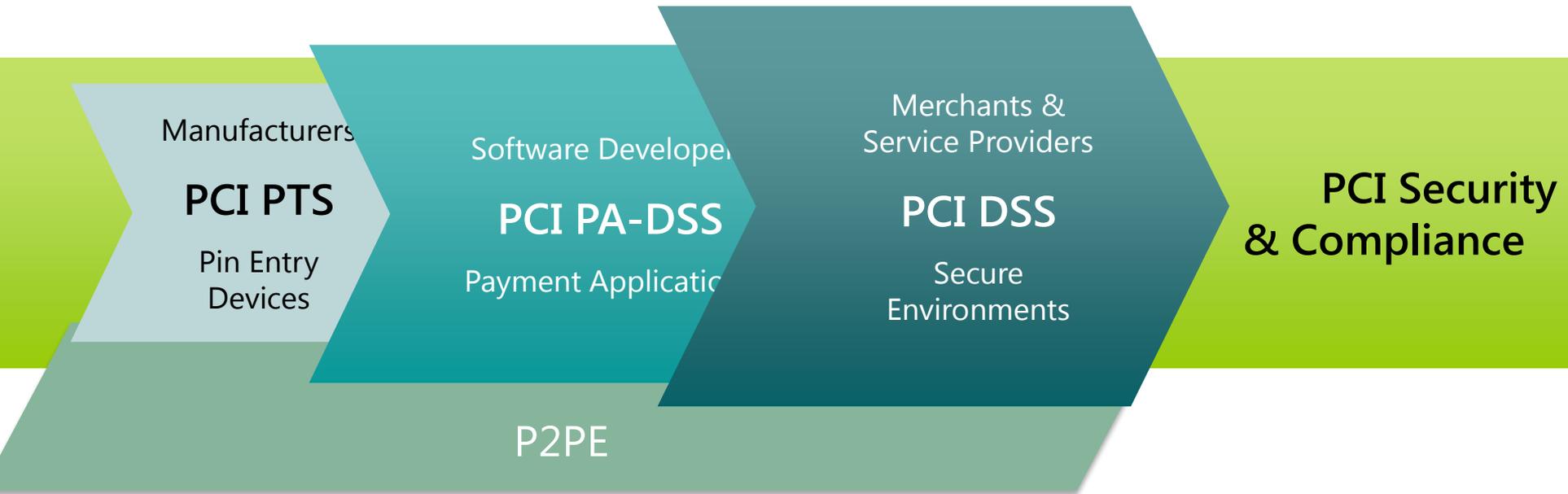
*Founded in 2006 -
Guiding open standards for
payment card security*

- Development
- Management
- Education
- Awareness



PCI Security Standards Suite

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

The Formula for PCI Success



PCI Standards Help Secure Your Data

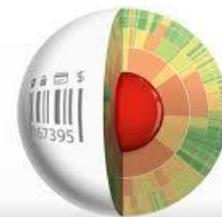
With version 3.0, PCI DSS is more mature than ever, and covers a broad base of technologies and processes such as encryption, access control, and vulnerability scanning to offer a sound baseline of security.

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



VERIZON 2014
PCI COMPLIANCE
REPORT



The Standards Continually Evolve



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

PCI DSS, PA-DSS 3.0 – Key Themes



**Education
Awareness**



Flexibility



**Security as a
Shared
Responsibility**

Make PCI your compass, not your roadmap

Effective Dates for v3.0 PCI DSS

Version 3.0 was effective on 1 January 2014

Version 2.0 is valid until 31 December 2014

Different supporting documents

Check our website for the latest documents

Do not mix and match

EMV Chip in US – It's Almost Here...

00:03

You May Have Heard...

EMV Chip will solve all security problems

The payment landscape will be transformed, no need for PCI

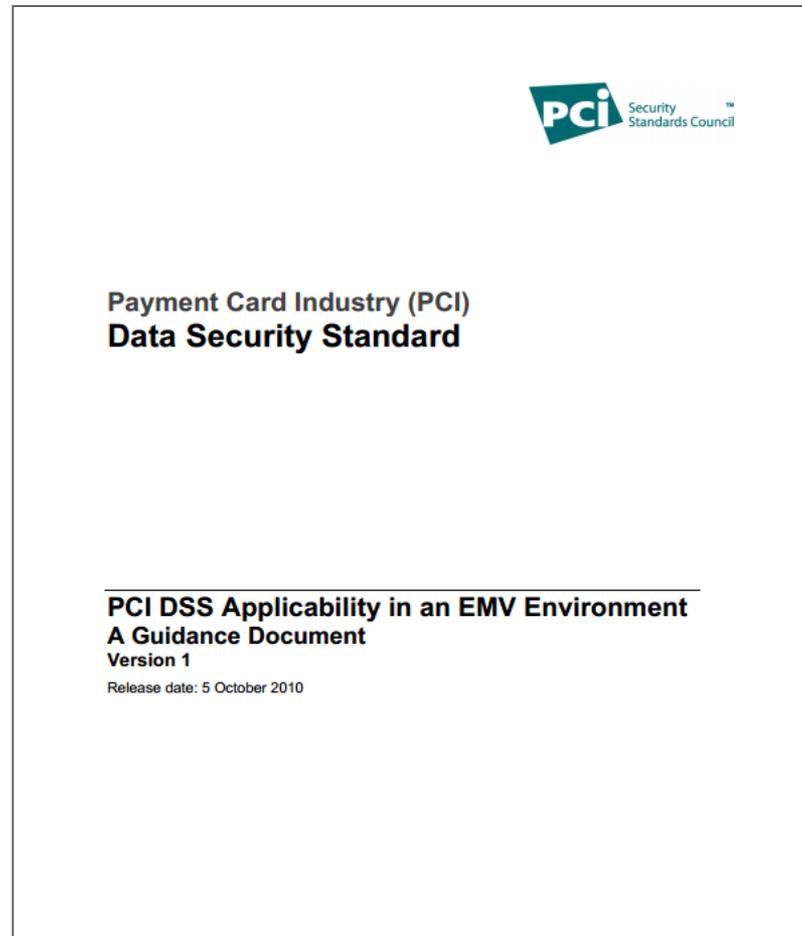
Card payments will be revolutionized with EMV Chip

PCI is on its way to extinction

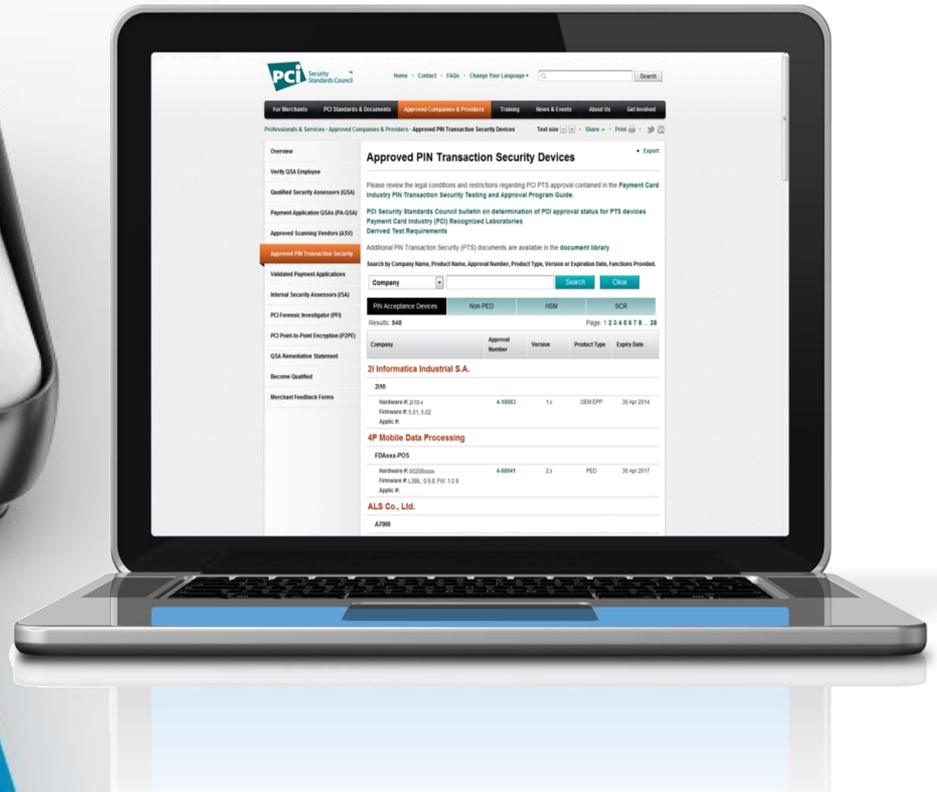
**EMV
Chip
Helps
Reduce
Face-to-
Face
Fraud**



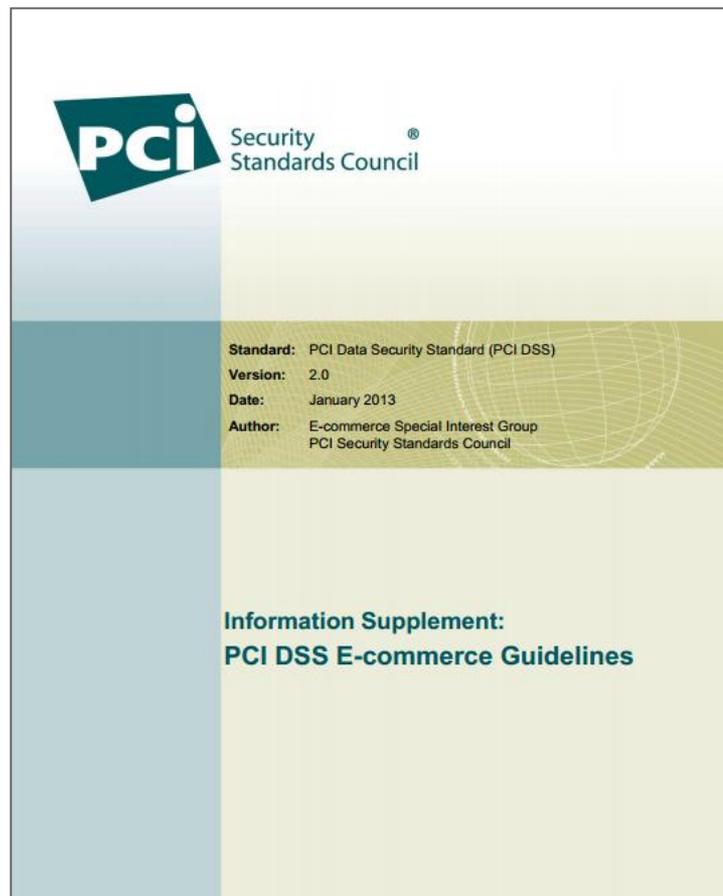
Even EMV Chip Needs PCI



Terminal Security



Don't Forget About E-commerce!



View at

www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf

Looking Forward ...

PCI Standards will continue to evolve...

And will be applied as required, such as with EMV chip



Mobile

PCI Standards focus on merchant-acceptance

Mobile payment acceptance still evolving

Understand risk and use PCI SSC resources

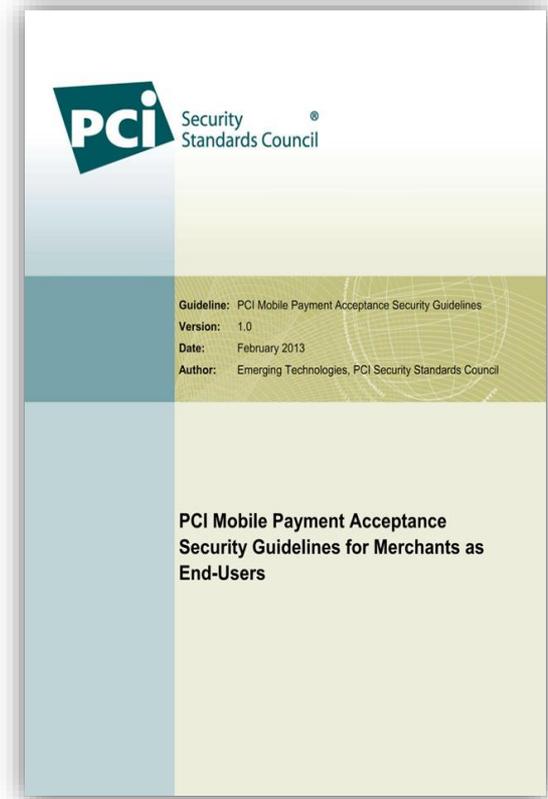
PCI SSC is working with industry

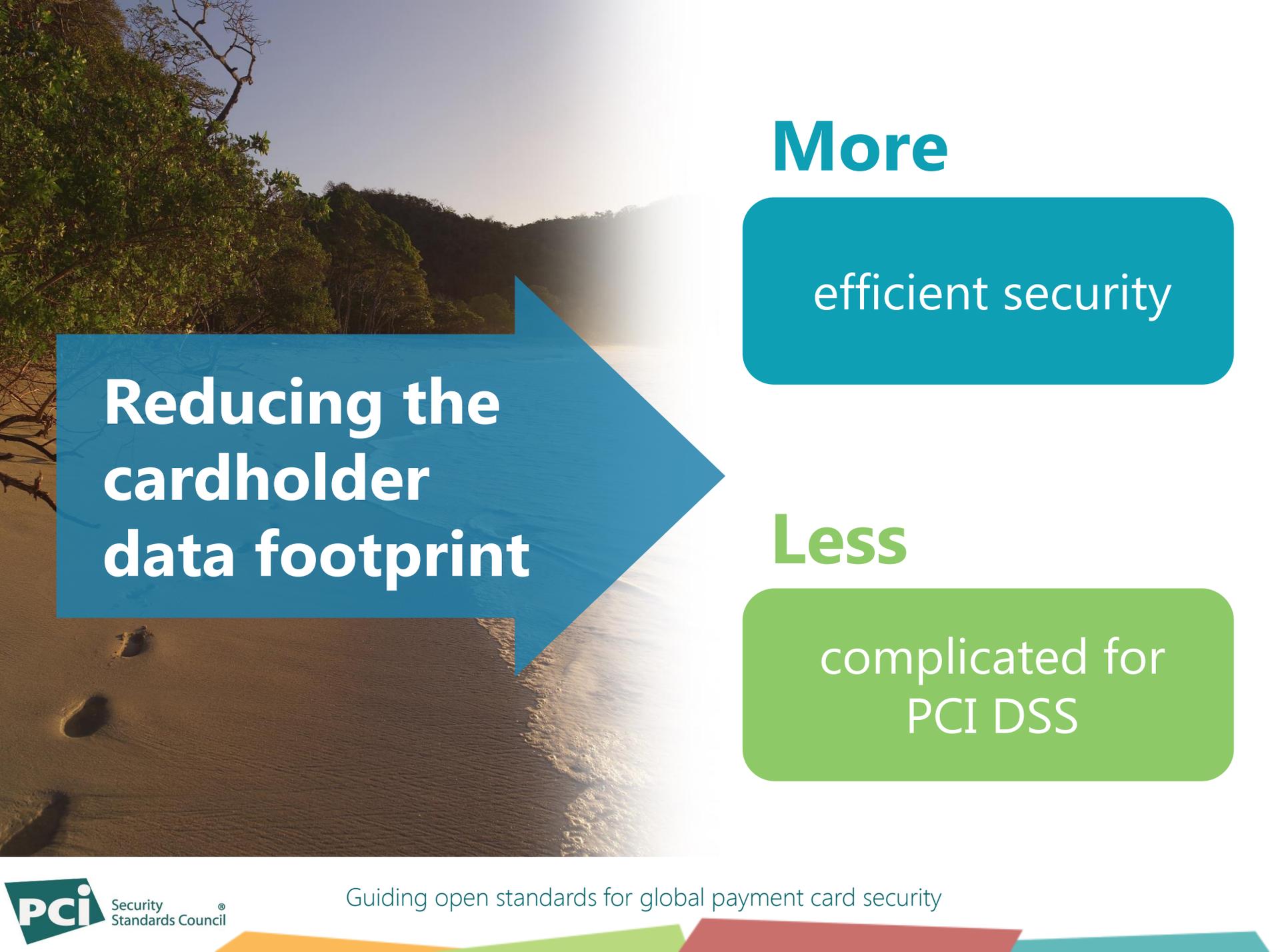


Mobile Guidelines and Best Practices

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





**Reducing the
cardholder
data footprint**

More

efficient security

Less

complicated for
PCI DSS

Where the Footprint Begins

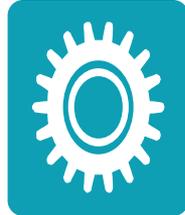


66% of data breaches, the organization didn't know the data was on the compromised system

VERIZON DATA BREACH INVESTIGATIONS REPORT

Ways to Reduce Footprint

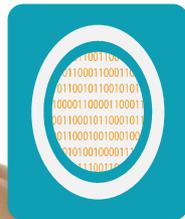
Reduce the need or ability to store or transmit cardholder data



Business process for retention



P2PE



Tokenization

Point-to-Point Encryption

Bluefin Payment Systems				
PayConex P2PE				
Version #: 2014-00897.001	Validated According	403 Labs, LLC	13 Mar 2015	13 Mar 2016
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 to P2PE Ver 1.1	Foregenix	18 Nov 2014	18 Nov 2015
	Solution Type:			
	Hardware/Hardware			

What is a PCI P2PE Solution?

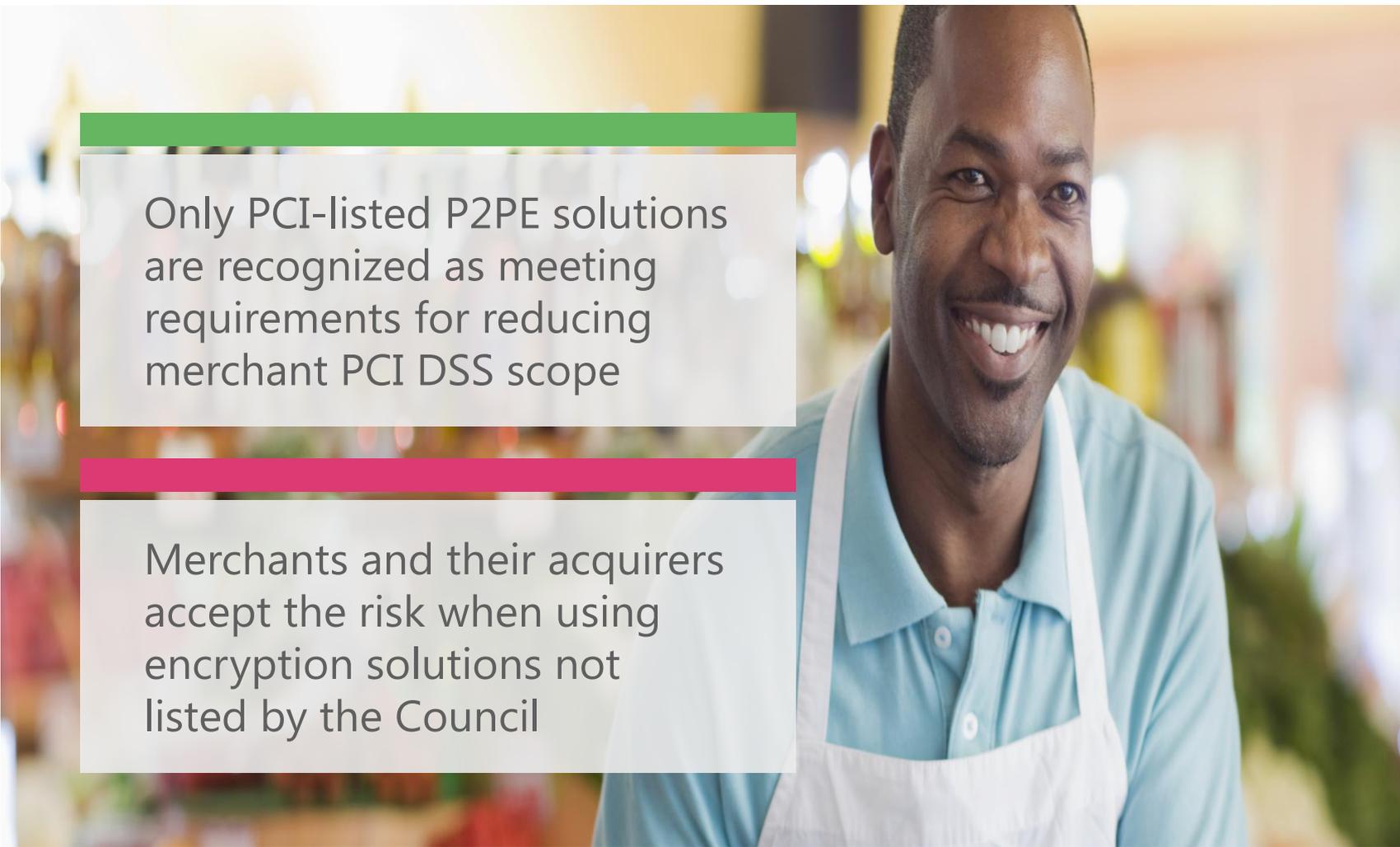
PCI PIN Transaction Security (PTS)
approved devices with Secure
Reading and Exchange of Data
(SRED)

PCI P2PE validated applications
and processes

Listed by PCI SSC



P2PE and Merchants

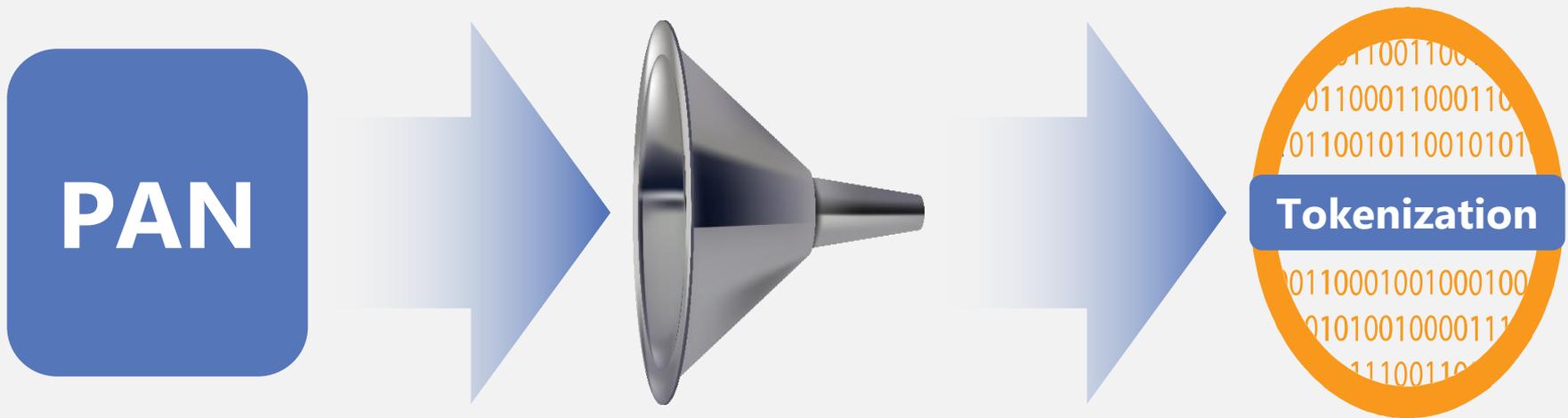


Only PCI-listed P2PE solutions are recognized as meeting requirements for reducing merchant PCI DSS scope

Merchants and their acquirers accept the risk when using encryption solutions not listed by the Council

Tokenization – Standard Expected in 2014

Work on tokenization standards has begun



Industry Coordination

Continued cooperation to align tokenization efforts for the benefit of payment industry

EMVCo

ANSI X9

NIST

The Formula for PCI Success



Preparation

What are your personal PCI education goals for the next three years?

For yourself

For your staff



**People in
Payment
Chain
Cause
Most
Internal
Breaches!**



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"

Training Highlights



- ✓ **Online Internal Security Assessor (ISA) Training**
- ✓ **P2PE Assessor Training**
- ✓ **Corporate Group Training– 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

New! Quick Resources for card security



It's time to change your password

Are you still using the default password that came with your point of sale (POS) terminal? Or, using 12345 or password? If so, you need to change it right away to protect your customers' confidential payment card data. Passwords are an easy way for criminals to sneak in to access information if not updated from the default or, if passwords are too simple, it can also make it easy for data thieves to break in.



The idea of changing your passwords may be overwhelming. You want it to be something easy for you and for your employees to remember, while also keeping unwanted predators out. Complex passwords don't have to be complicated. Look at the chart below:

[Click here to learn more!](#)



Stay Smart on Protecting Against Card Fraud!

Trying to understand what you can do to keep your customers' card data safe and protect against fraud? Unsure of where to begin?



Take a look at these ten simple steps to help you get started in your security efforts:

1 Educate

Employees should be trained annually on both online and physical security threats as well as on the best practices for protecting cardholder data.



[Click here to learn more!](#)



Increasing Security and Reducing Fraud with EMV Chip and PCI Standards



When data is exposed, it puts your customers and your reputation as a business at serious risk. EMV chip technology combined with PCI Security Standards offer a powerful combination for increasing card data security and reducing fraud.



What they are – Fraud protection & data security

EMV chips
= Technology that uses secret



[Click here to learn more!](#)

Windows XP Support is Ending



If you're running outdated software on your computer, your business could be at risk.

[Find out why](#)

www.pcisecuritystandards.org/news_events/quick_resources.php

Guiding open standards for global payment card security

Get Involved – We Need Your Input



Join



Learn



Input



Network



Nominate



Vote



Share



Influence

Be Part of SIGs



Security Awareness



Penetration Testing
Guidance

Save the Dates – 2014 Community Meetings

North America



9-11 September
Orlando, Florida

Europe



7-9 October
Berlin, Germany

Asia-Pacific



18-19 November
Sydney, Australia

Questions?



Security
Standards Council[®]



**Please visit our website at
www.pcisecuritystandards.org**