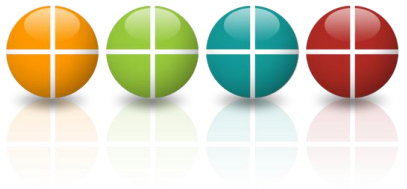
The PCI Security Standards Council

Bob Russo
June 2011

- What are the threats to card data?
- How can you defend your card data?
- What is the Council doing to help you?
- What tools are available to get you secure?
- How can you be involved?

- What are the threats to card data?
- How can you defend your card data?
- What is the Council doing to help you?
- What tools are available to get you secure?
- How can you be involved?



Why SECURITY matters…

"The attackers have changed with the emergence of organized crime into these cybercrimes...It's all about the money now ... Profit is driving these groups." - FBI agent J. Keith Mularski, May 2009

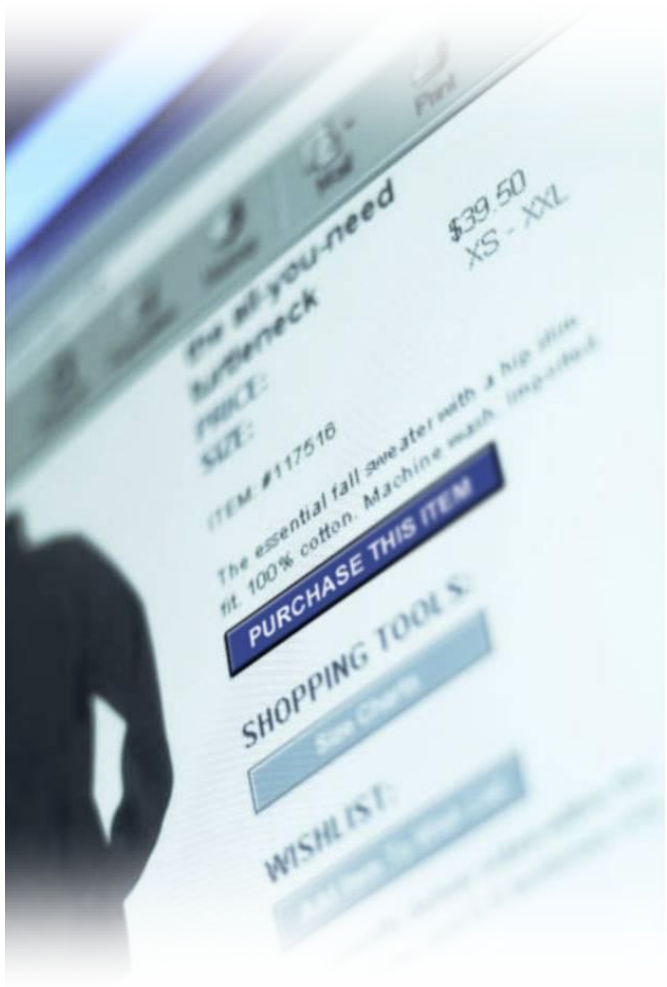
According to Gartner, payment card fraud was the method most actively used by crooks to steal money, claiming 36 percent more victims in 2008 than other types of fraud. - Gartner, March 2009

There were more than 222 million potentially compromised records in 2009 - Identity Theft Resource Center Breach Report, Jan. 8, 2010

"Nearly twice as many people who lost money to fraud in 2008 changed their shopping, payment and e-commerce behavior," said Avivah Litan, vice president and distinguished analyst at Gartner, March 2009

Is your focus on compliance audits rather than security making you a target? Is your risky behavior potentially causing you to lose customers?

Remember, compliance is a byproduct of SECURITY



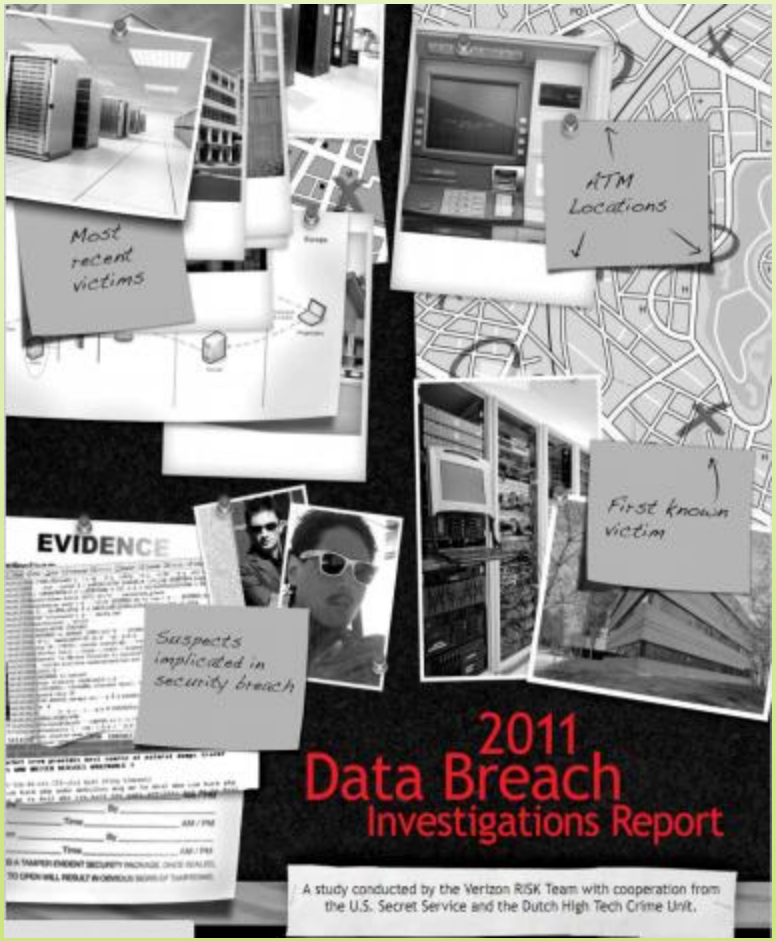
According to Verizon's 2011 Data Breach Investigations Report (DBIR)

79% of records were compromised through malware

2/3 of malware investigated was customized

79% of compromises were not discovered until, weeks, months or years had past

Data security is not all about prevention; it also requires detection and monitoring!



Breached organizations are 50 percent less likely to be PCI-compliant than a "normal population of PCI clients."

Top attack methods used to compromise payment card data:

- malware and hacking (25%)
- SQL injections (24%)
- exploitation of default or guessable credentials (21%)

Figure 4. Compromised records by industry group [1]

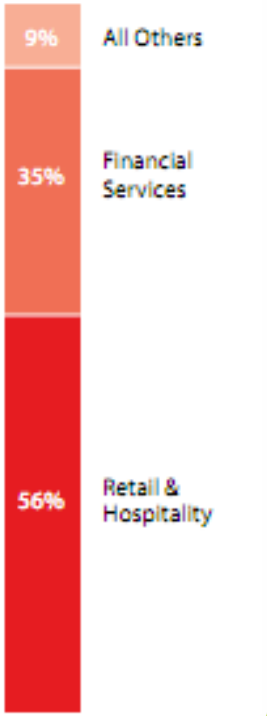
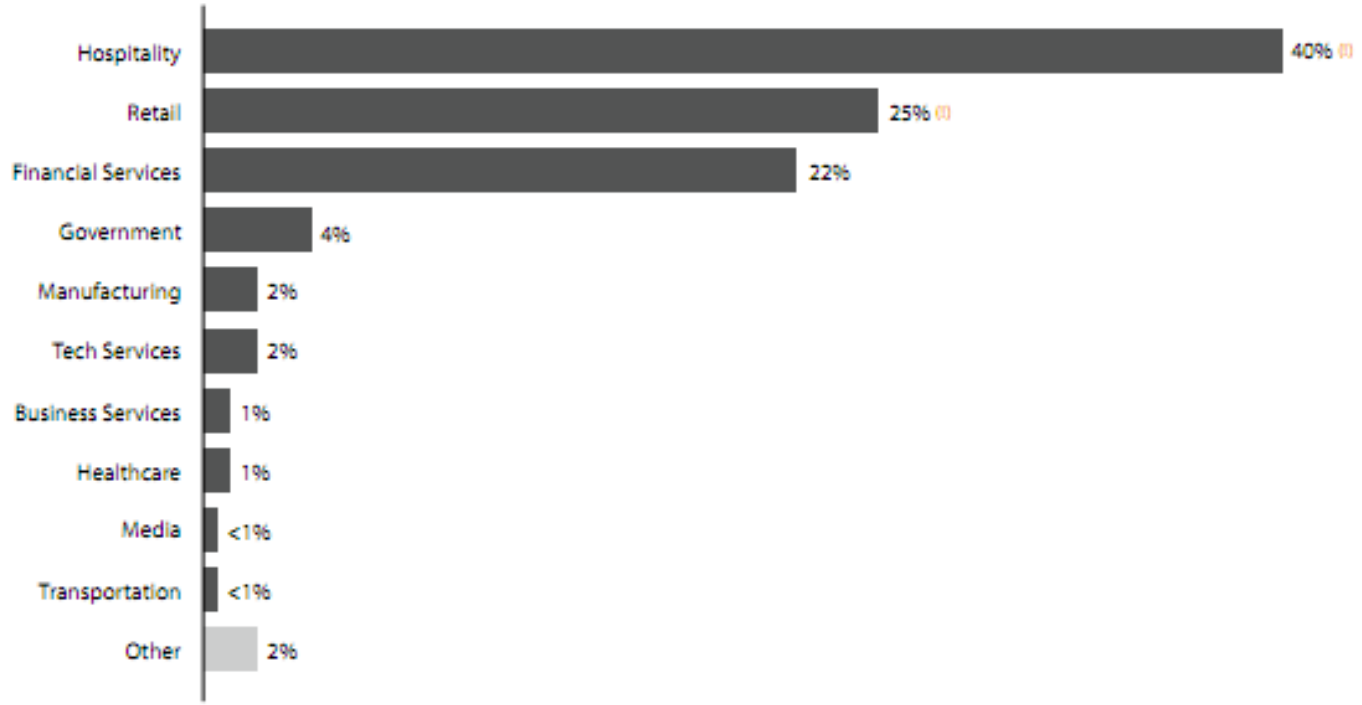


Figure 3. Industry groups represented by percent of breaches

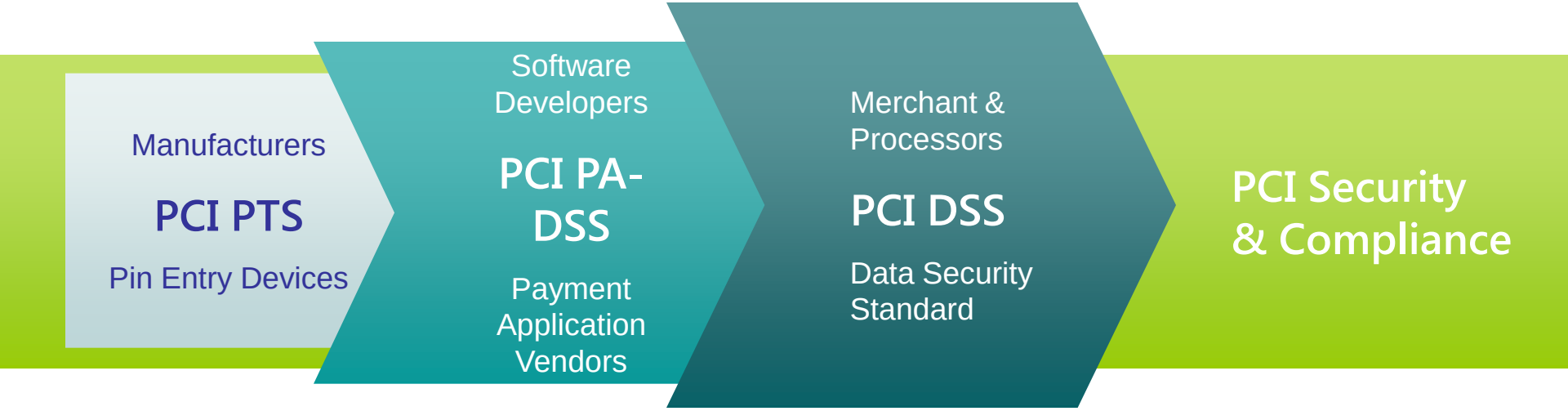


1. The 2010 Verizon Data Breach Investigations Report

- What are the threats to card data?
- **How can you defend your card data?**
- What is the Council doing to help you?
- What tools are available to get you secure?
- How can you be involved?

Payment Card Industry Security Standards

Protection of Cardholder Payment Data

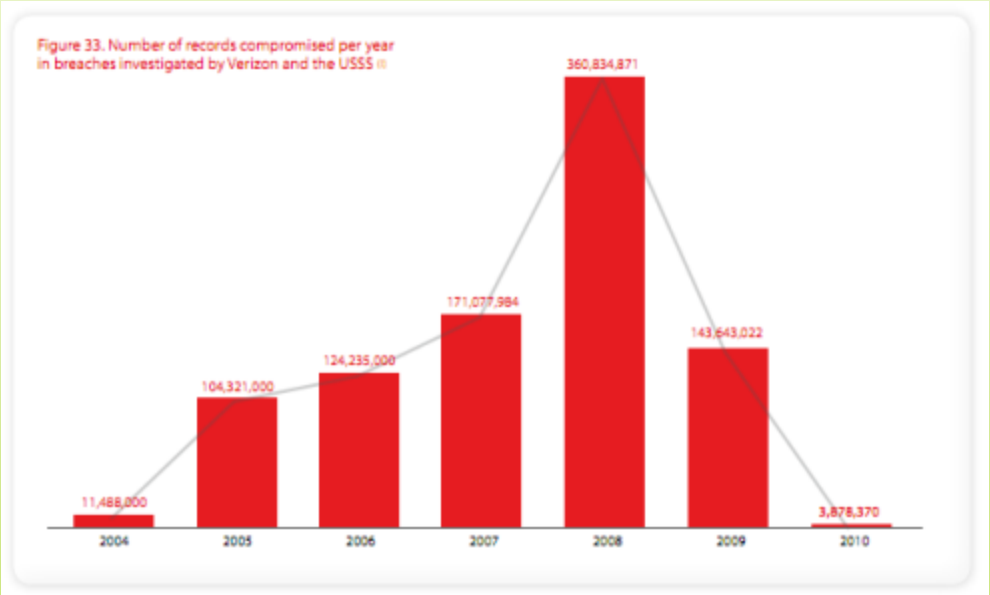


Ecosystem of payment devices, applications, infrastructure and users

PCI PTS

PCI PA-DSS

PCI DSS



Breached Records by Year

- *PCI compliant organizations suffer fewer data breaches*
- *Organizations reporting compliance with the standards has increased tremendously over the last year*
- *The volume of breaches reported in the Verizon DBIR decreased close to a hundredfold from their 2008 peaks*

1. The Ponemon Institute's *2011 PCI DSS Compliance Trends Study*

Open, global forum

Founded 2006

Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness

More than 600 organizations have joined

- What are the threats to card data?
- How can you defend your card data?
- **What is the Council doing to help you?**
- What tools are available to get you secure?
- How can you be involved?

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 2.0

October 2010

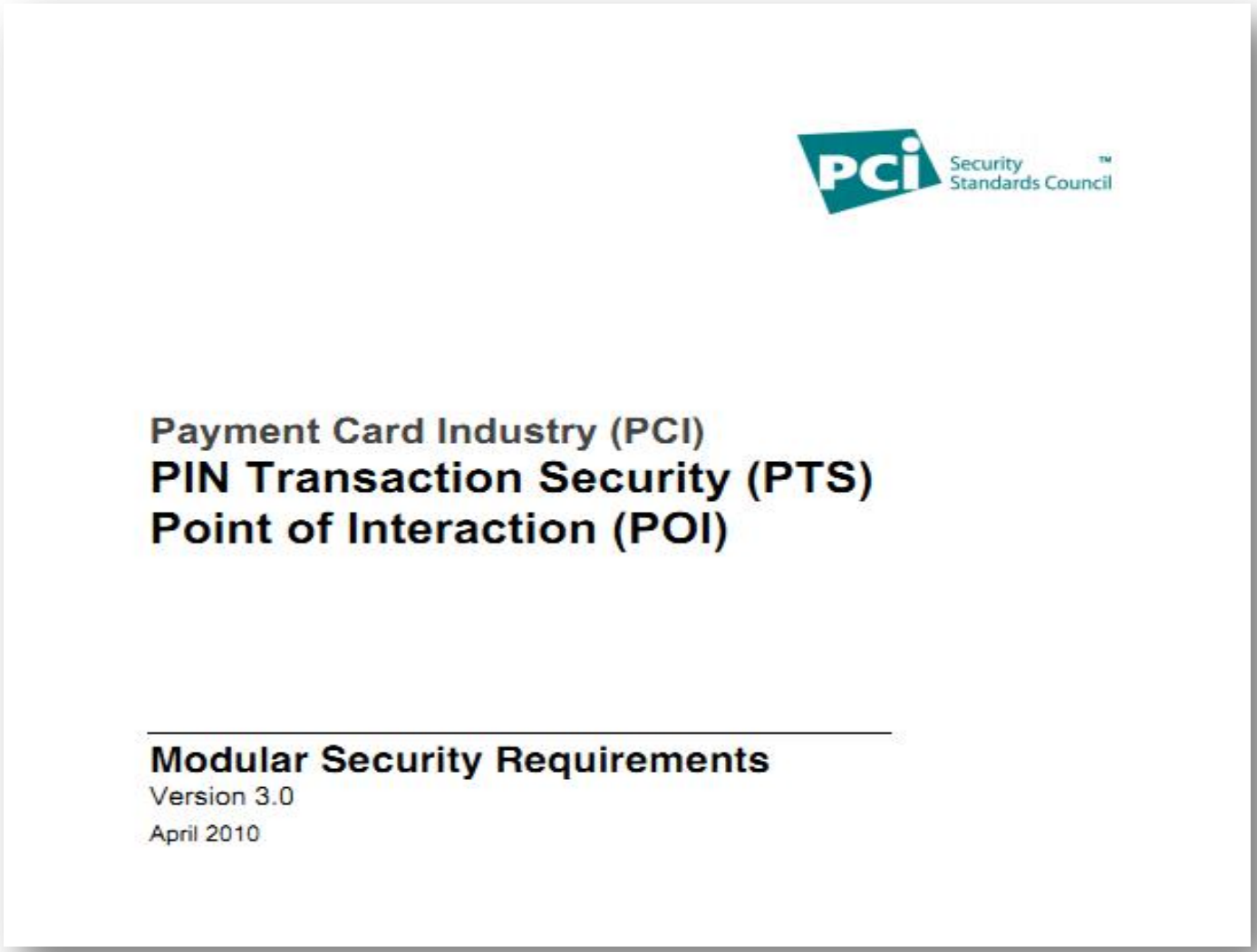
Payment Card Industry (PCI)

Payment Application Data Security Standard

Requirements and Security Assessment Procedures

Version 2.0

October 2010

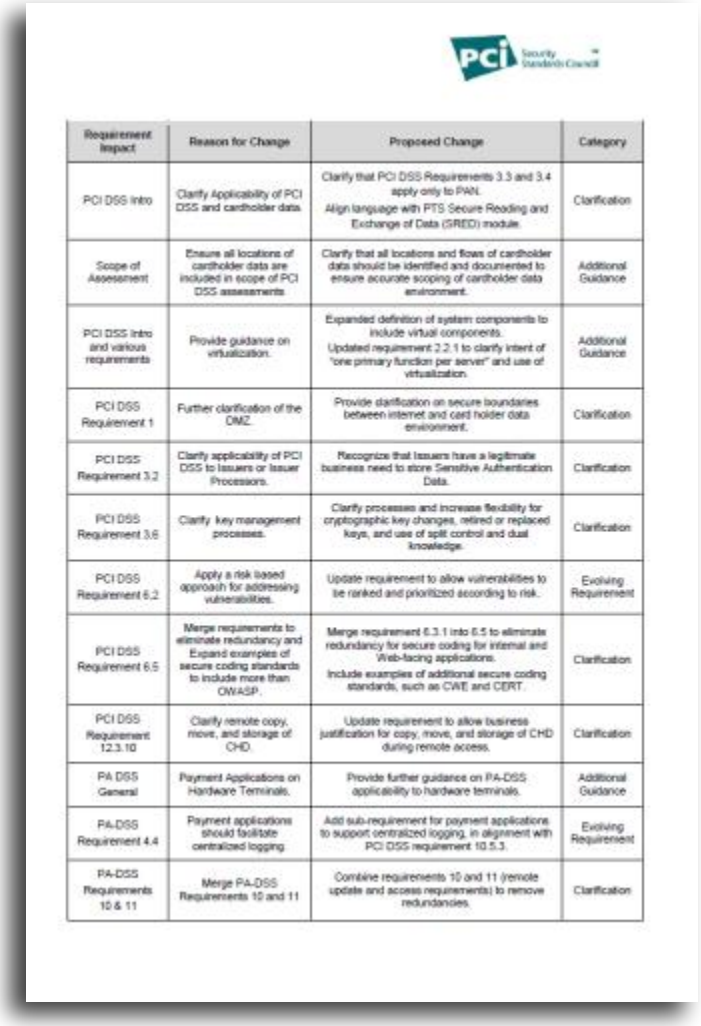

PCI Security Standards Council
Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)
Modular Security Requirements
Version 3.0
April 2010

Clarifications

Additional guidance

Evolving requirements

Your feedback has made the standard more mature and will help secure payment card data well into the future!



Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Intro	Clarify Applicability of PCI DSS and cardholder data.	Clarify that PCI DSS Requirements 3.3 and 3.4 apply only to PAN. Align language with PTS Secure Reading and Exchange of Data (SRED) module.	Clarification
Scope of Assessment	Ensure all locations of cardholder data are included in scope of PCI DSS assessments.	Clarify that all locations and flows of cardholder data should be identified and documented to ensure accurate scoping of cardholder data environment.	Additional Guidance
PCI DSS Intro and various requirements	Provide guidance on virtualization.	Expanded definition of system components to include virtual components. Updated requirement 2.2.1 to clarify intent of "one primary function per server" and use of virtualization.	Additional Guidance
PCI DSS Requirement 1	Further clarification of the DMZ.	Provide clarification on secure boundaries between internet and card holder data environment.	Clarification
PCI DSS Requirement 3.2	Clarify applicability of PCI DSS to Issuers or Issuer Processors.	Recognize that Issuers have a legitimate business need to store Sensitive Authentication Data.	Clarification
PCI DSS Requirement 3.6	Clarify key management processes.	Clarify processes and increase flexibility for cryptographic key changes, retired or replaced keys, and use of split control and dual knowledge.	Clarification
PCI DSS Requirement 6.2	Apply a risk based approach for addressing vulnerabilities.	Update requirement to allow vulnerabilities to be ranked and prioritized according to risk.	Evolving Requirement
PCI DSS Requirement 6.5	Merge requirements to eliminate redundancy and Expand examples of secure coding standards to include more than OWASP.	Merge requirement 6.3.1 into 6.5 to eliminate redundancy for secure coding for internal and Web-facing applications. Include examples of additional secure coding standards, such as CWE and CERT.	Clarification
PCI DSS Requirement 12.3.10	Clarify remote copy, move, and storage of CHD.	Update requirement to allow business justification for copy, move, and storage of CHD during remote access.	Clarification
PA-DSS General	Payment Applications on Hardware Terminals.	Provide further guidance on PA-DSS applicability to hardware terminals.	Additional Guidance
PA-DSS Requirement 4.4	Payment applications should facilitate centralized logging.	Add sub-requirement for payment applications to support centralized logging, in alignment with PCI DSS requirement 10.5.3.	Evolving Requirement
PA-DSS Requirements 10 & 11	Merge PA-DSS Requirements 10 and 11	Combine requirements 10 and 11 (remote update and access requirements) to remove redundancies.	Clarification

- Scoping
- Logging
- Risk-based approach
- Alignment between PA-DSS & PCI-DSS
- Recognition of small merchant environments
- New website and updated supporting documentation

Tokenization

Encryption

Wireless

EMV

Virtualization

Mobile

- What are the threats to card data?
- How can you defend your card data?
- What is the Council doing to help you?
- **What tools are available to get you secure?**
- How can you be involved?

Website


PCI Security Standards Council, LLC [US] https://www.pcisecuritystandards.org
PCI Security Standards Council
Home · Contact · FAQs · Change Your Language
Search
For Merchants
PCI Standards & Documents
Approved Companies & Providers
Training
News & Events
About Us
Get Involved
Welcome to the PCI Security Standards Council
MERCHANTS
Find out why and how to become compliant with PCI Security Standards
Learn More
FINANCIAL INSTITUTIONS
Resources to assist with compliance efforts for your organization
Learn More
HARDWARE / SOFTWARE
Resources designed for developers and device manufacturers
Learn More
SERVICES AND PROFESSIONALS
Quick access to resources developed for industry professionals
Learn More
PCI DSS 2.0 and PA-DSS Version 2.0 Now Available!
Please click here to download the new standards and supporting documents from the document library.
EVENTS
NRF 100th Annual Convention & Expo
January 09, 2011
European Card Acquiring Forum
February 06, 2011
2011 Hospitality Law Conference
February 09, 2011
NEWS
December 10, 2010
PCI Security Standards Council Announces PCI Forensic Investigator (PFI) Program
October 28, 2010
PCI ROCK
Payment Card Security
Meet our Participating Organizations

PCI Security Standards Council

Lifecycle for Changes to

The Payment Card Industry PIN Transaction Security (PTS) requirements are used primarily by point-of-sale equipment manufacturers to secure cardholder data at the physical point of sale. The standard is managed by the PCI Security Standards Council (PCI SSC). Input for proposed changes to the standard are also made by PCI SSC stakeholders – Participating Organizations, including merchants, banks, processors, hardware and software developers, point-of-sale vendors, and approved security evaluation laboratories.

Changes to the standard follow a defined 36-month lifecycle with eight stages, described below. The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implemen noncompliant when changes are published a Throughout the lifecycle, the Council will cont ongoing guidance about these standards.

NEW STANDARD PUBLISHED

- Major new release of PTS
- Presented at Community Meetings in October
- Initiates 3-year lifecycle
- Previous version remains effective for 12 months after the new standard becomes effective

Stage 1: Sta

Stage 1 occurs a new lifecycle t of security to th

Stage 2: Fee

Stage 2 is an en Feedback is acti laboratories, the goal is assessing enable guidance collectively use

If a new threat o will take immedi protect cardhold

PCI Security Standards Council

Overview of the PCI DSS W Information Supplement

The near ubiquity of wireless networks makes ther a top priority for organizations that store, process or transmit cardholder data. In response, the PCI Security Standards Council Special Interest Group Implementation Team has published an informatio supplement called PCI DSS Wireless Guideline. The goal of this document is to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as pertains to wireless, and provide practical method and concepts for deployment of secure wireless in payment card transaction environments. It is also intended for assessors who audit PCI DSS compliance. This At-a-Glance is a summary of the 32-page Guideline.

HIGHLIGHTS

- Provides guidance for testing or deploying 802.11 Wireless Local Area Networks (WLAN)
- Focuses on suggestions for deploying WLAN in the Cardholder Data Environment
- Includes operational procedures required to make WLAN part of a PCI DSS compliant network

Wireless Requirem

The wireless requirements f Cardholder Data Environme data is transferred, process that environment. The audit Wireless Guideline address Generally applicable wirel should have in place to pro access points and clients. technology is part of the C organizations that wish to

Requirements applicable organizations that transmit place to protect these syste scope for PCI DSS compli apply in addition to the un

Using the PCI DSS

Download the Guideline

The Guideline provides spe this At-a-Glance, left sidebar for complying with PCI DSS including authority docume v1.2 cross reference.

PCI Security Standards Council

Skimming Prevention: Overview of Best Practi

Skimming is the unauthorized capture and transfer of payment data to another source. Its purpose is to commit fraud, the threat is serious, and it can ha any merchant's environment. With skimming, thieve steal payment data directly from the consumer's payment card or from the payment infrastructure a merchant location. Both techniques typically requir the use of a rogue physical device planted onsite. PCI Security Standards currently contain a number requirements and recommendations to guard agai skimming. In addition, the Council has introduced overview document for merchants containing a "da diva" about skimming, examples, best practices an tools to thwart its use. This "At-a-Glance" provides snapshot of skimming and introduces areas requir countermeasures to ensure an appropriate level of security for cardholder data.

HIGHLIGHTS

Describes the problem of skimming with several examples of actual gear used to steal cardholder data

Provides best practices to mitigate the risk of skimming

Includes written methodology to quantify risk of skimming and a checklist for tracking assets in a specific merchant location and terminal environment

Merchants N

Skimming equipm back page). Mer at the merchant's familiar with the

Who Does It? Pe and organized cr unsophisticated

Targets for Attac data, often issue entry device; unu volume (allowing heavy volume of

Impact of Skimm process, employ There is a cost to and services.

Using the Gu

Download the gu www.pcisecurity

The document pr of this At-a-Glan best practices, s

PCI Security Standards Council

AT A GLANCE
PCI DATA STORAGE

PCI Data Storage Do's and Don'ts

Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public assumes merchants and financial institutions will protect data on payment cards to thwart theft and prevent unauthorized use. But merchants should take note: Requirement 3 applies only if cardholder data is stored. Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves.

For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only Council certified PIN entry devices and payment applications may be used. PCI DSS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

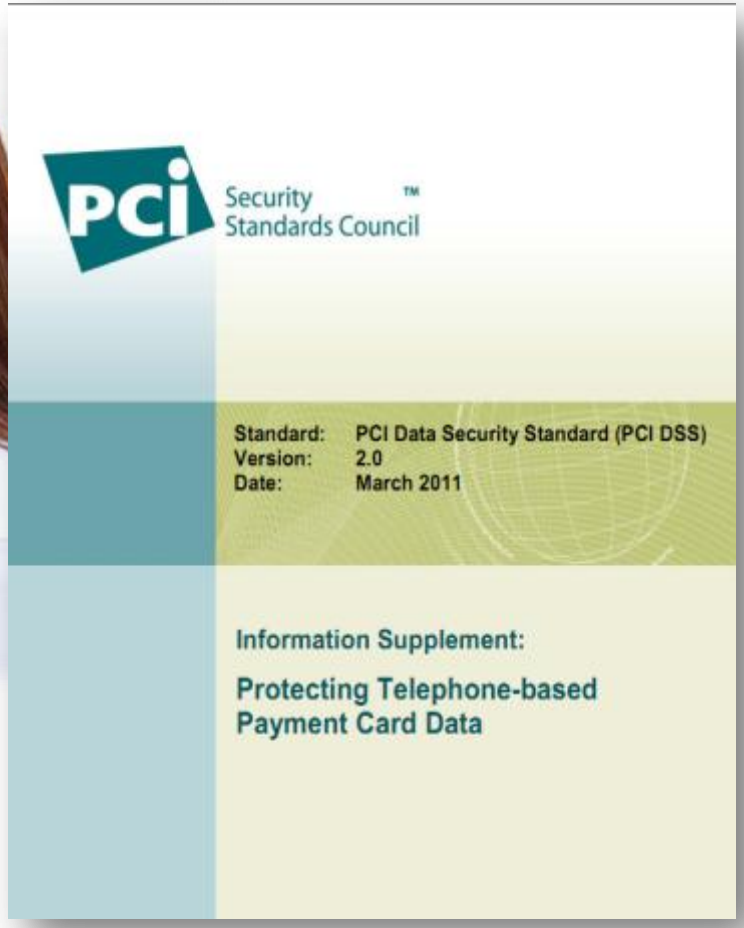
Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors

Basic PCI Data Storage Guidelines for Merchants

Cardholder data refers to any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side. The front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization.

In general, no payment card data should ever be stored by a merchant unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and merchants must use technical precautions for safe storage (see back of this fact sheet for a summary). The matrix below shows basic "do's" and "don'ts" for data storage security.

Data Do's	Data Don'ts
Do understand where payment card data flows for the entire transaction process	Do not store cardholder data unless it's absolutely necessary
Do verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements	Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization
Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS)	Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked
Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it's protected	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals	Do not locate servers or other payment card system storage devices outside of a locked, fully-secured and access-controlled room
Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable. Have clear access and password protection policies	Do not permit any unauthorized people to access stored cardholder data


PCI
Security Standards Council
Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: March 2011
Information Supplement:
Protecting Telephone-based Payment Card Data

HITEC 2011

A service of HFTP

Who Should Attend?

Open to anyone who is interested in learning more about PCI, with a focus on those individuals working for organizations that must meet compliance with the PCI DSS or have a vested interest in the Payment Card Industry

Upcoming Training Dates

August 24th, 2011 – Boston, MA, USA

PCI Awareness Training – Online!

- At your home or office, at your pace
- Offers general PCI training across your business to ensure a universal understanding of PCI compliance
- Provides **four** CPE hours
- Available all the time, anytime!

Number of Employees Registered	Price Per Person
1 - 24	$495 USD
25 - 99	$395 USD
100+	$295 USD

Discounts are available for group registration. Please contact the PCI SSC Training Coordinator at training@pcisecuritystandards.org for more information.

https://www.pcisecuritystandards.org/training/non_certification_training.php

Security standards and supporting documents

Quick Reference Guide

Searchable Frequently Asked Questions

List of approved QSAs, ASVs, PA-QSAs, PED Labs

Education and outreach - e.g., fact sheets, webinars

Participating membership, meetings, collaboration

A global voice for the industry

HITEC 2011

A service of HFTP

2011 Community Meetings:

Scottsdale, Arizona
September 20 – 22, 2011

London, UK
October 17 – 19, 2011

Join us as a Participating Organization to get involved in setting global PCI standards!

Focus on security, not compliance

Understand the process of PCI standards development

Join us as a Participating Organization and increase our global presence

Take advantage of the Council's resources and guidance

Participate in the 2011 Annual Community Meetings

Adopt version 2.0 and share the PCI SSC roadmap with internal stakeholders

Any Questions?

Please visit our website at www.pcisecuritystandards.org

What Did You Think?

In order to help us create/provide a better HITEC experience in the future, please take a second to fill out the short survey that will be sent to you via e-mail at the end of the day.

And THANK YOU for attending HITEC!

HFTP
Hospitality Financial and Technology Professionals

Learn how HFTP membership can benefit you, visit www.hftp.org