



PCI Compliance Basics for Small – Medium Sized Retailers

NACS Webinar - March 6, 2008



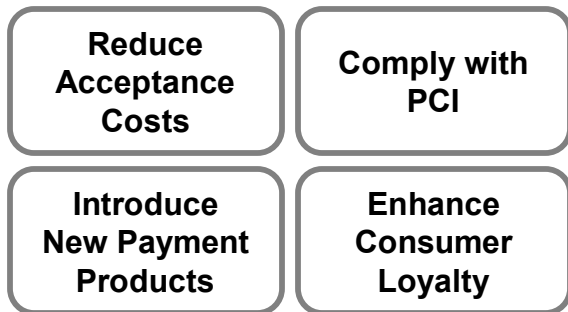
Introducing W. Capra

Mission: W. Capra Consulting Group is a consulting organization focused on *identifying, leading, integrating, and delivering solutions* to retail businesses

Focus: We help organizations leverage technology and supplier relationships to gain competitive advantages via two practices

Payment Practice

We provide merchants the best opportunity to minimize acceptance costs and construct a differentiated payment offer to maximize their value



Retail Consulting Group

We provide project leadership, retail technology expertise, architecture guidance, deployment management and operational strategies through a full lifecycle methodology



Introduction

Why is this important to my business?

Cardholder data theft and fraud – some real cases:

- **January 17, 2007** – TJX Companies Inc. disclosed they had experienced an unauthorized intrusion into the electronic credit/debit processing system. As many as 45M account numbers were stolen and TJX losses from the breach are estimated at \$130 million. ¹
- **February, 2008** – Thieves in Tucson compromised PIN pads by cracking them open and soldering in an electronic chip that functions as a wireless transmitter. When a customer swiped the card and subsequently entered their PIN, the digital information was transmitted wirelessly to thieves sitting in a car in the parking lot who then encoded the data on blank cards and used the cards at ATMs in Las Vegas. ²

Sources: 1. www.TJX.com; 2. AZBiz.com "The thieves who rode out of town with PINs", February 29, 2008

Key Questions for Retailers

- What Is PCI?
- Does PCI Apply to My Business?
- What Is The Timeline For Compliance?
- What Should I Do Now?

What is PCI?

- PCI DSS is the **Payment Card Industry Data Security Standard**
 - One uniform set of information security requirements for all national card brands (VISA, MasterCard, American Express and Discover)
 - Purpose of the DSS is to secure the payment system and protect:
 - Cardholders and Data
 - Merchants
 - Payment Processors
 - Banks and Card Issuers
- In addition to the DSS, PCI also includes standards for ***PIN Entry Devices (PCI PED)*** and ***Payment Applications (PA-DSS)***
- The DSS is comprised of 12 security requirements which are organized into 6 categories...

PCI DSS: Requirements 1-6

Build and Maintain a Secure Network

- 1: Install and maintain a firewall configuration to protect cardholder data
- 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- 3: Protect stored cardholder data
- 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- 5: Use and regularly update anti-virus software or programs
- 6: Develop and maintain secure systems and applications

Source: www.pcisecuritystandards.org

PCI DSS: Requirements 7-12

Implement Strong Access Control Measures

- 7: Restrict access to cardholder data by business need-to-know
- 8: Assign a unique ID to each person with computer access
- 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- 10: Track and monitor all access to network resources and cardholder data
- 11: Regularly test security systems and processes

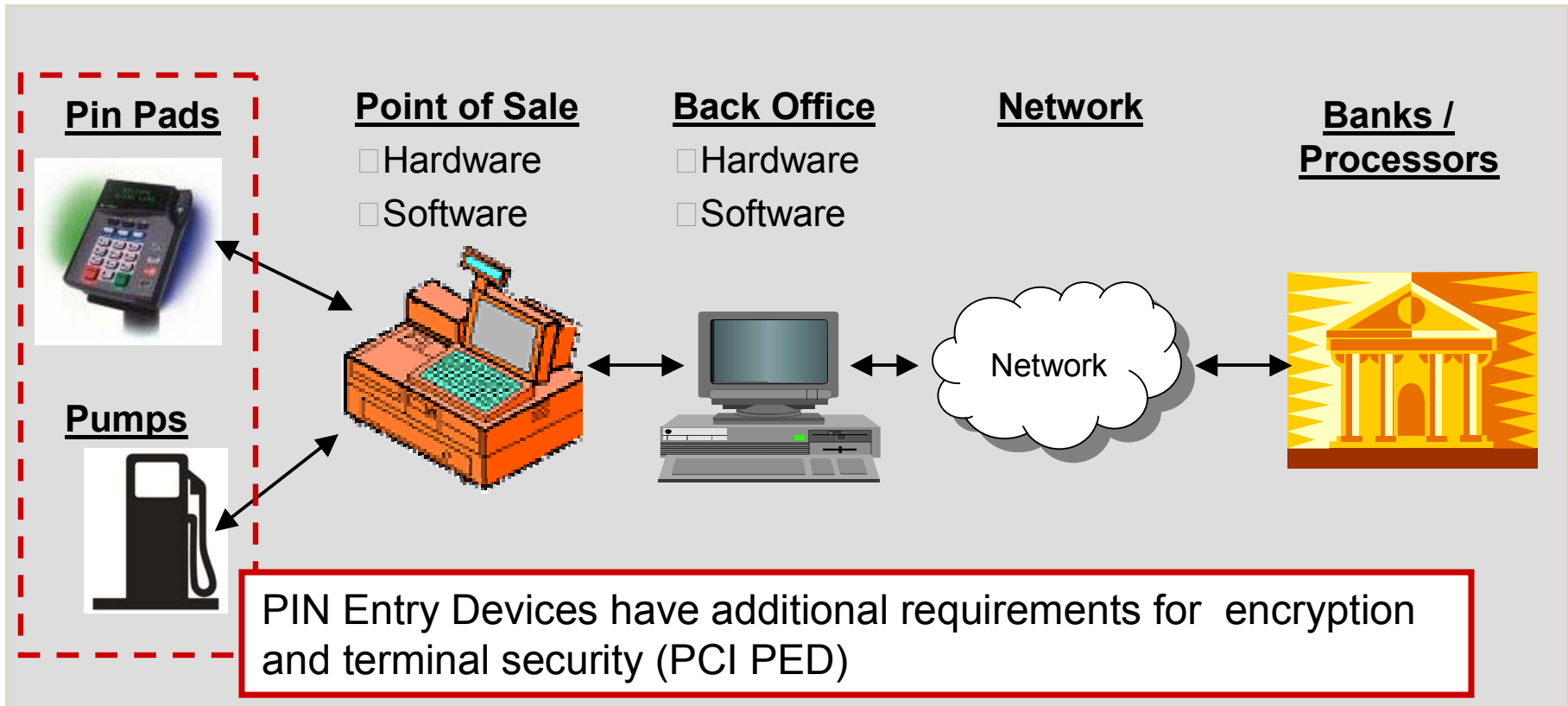
Maintain an information security policy

- 12: Maintain a policy that addresses information security for employees and contractors

Source: www.pcisecuritystandards.org

PCI DSS Applies to:

DSS applies to all components of the payment system that touch card data



Does PCI DSS Apply to Me?

- **If you accept credit or debit cards, YES!**
 - All merchants must be compliant – regardless of size
 - Requirements for validation of vary by number of transactions and by card brand.

- **Consequences of non-compliance?**
 - Consequences vary by card brand.
 - Published fines from individual card brands could be up to \$500,000 *or more* per brand per incident if data is compromised and merchants are found to be non-compliant.
 - Merchants risk losing the ability to process credit card transactions.
 - Merchants risk exposure to legal action by the card issuing banks both to recover the cost of fraud committed with stolen card information – and– the cost to re-issue new cards.

Source: www.GFI.com


Merchant Levels for Validation

Visa & MasterCard have similar definitions → **check with your bank/processor**

| Level | Level Definition | Validation Action |
|-------|--|--|
| 1 | <ul style="list-style-type: none"> • Merchants processing over 6 million transactions annually • Merchants from whom cardholder data has been compromised | <ul style="list-style-type: none"> • Annual On-site Data Security Assessment by Qualified Security Assessor (QSA) or internal auditor • Quarterly network scan by Approved Scanning Vendor (ASV) |
| 2 | <ul style="list-style-type: none"> • Merchants with 1 million to 6 million transactions annually | <ul style="list-style-type: none"> • Annual PCI DSS Self Assessment Questionnaire • Quarterly network scan by ASV |
| 3 | <ul style="list-style-type: none"> • Merchants with 20,000 to 1 million e-commerce transactions annually | <ul style="list-style-type: none"> • Annual PCI DSS Self Assessment Questionnaire • Quarterly network scan by ASV |
| 4 | <ul style="list-style-type: none"> • All other merchants (< 1 million transactions regardless of channel; < 20,000 e-commerce) | <ul style="list-style-type: none"> • Annual PCI DSS Self Assessment Questionnaire • Quarterly network scan by ASV (if applicable) |

Source: Visa USA; PCIComplianceGuide.org

Compliance Timeline

| | 2008 | 2009 | 2010 | Future |
|--|---|--|--|--|
| PCI Data Security Standard | Today: Merchants must be DSS Compliant. | <ul style="list-style-type: none"> Maintain compliance Annual Audit or Assessment Quarterly scans |  | |
| PCI PIN Entry Device (Including Triple DES) | Jan 1: All Non-PCI PED compliant terminals may no longer be sold; those installed may be used / deployed | | Jul 1: All terminals and AFDs accepting debit must support and be using Triple DES encryption | 2014: PED1 and PED1 Spec 2 terminals good until 2014 2017: PED2 Spec2 good until 2017 |
| PCI Payment Application-DSS (Visa PABP) | | | Jul 1: Must use Visa PABP compliant POS (and other payment) applications | |

What Should I Do Now?

Step 1: Begin Learning about PCI DSS, PCI PED, and PCI PA-DSS:

- The following are some resources to begin your
- PCI Security Standards Council: www.pcisecuritystandards.org
- Visa : www.usa.visa.com/merchants/risk_management/cisp.html
- MasterCard: www.mastercard.com/us/merchant/security
- PCI Compliance Guide: www.pcicomplianceguide.org
- NACS: www.nacsonline.com/NACS/Resource/CreditCards

Step 2: Contact Your Bank Processor/Third-Party Service Provider:

- Ask your processor about PCI
 - How does PCI affect my business?
 - What do I have to do to become compliant?
 - Identify processor requirements and documentation
- Determine merchant level qualifications and the subsequent validation requirements
- Document these conversations
- If you use more than one processor, perform the same step for each one
- Ask your processor about their own PCI compliance and validation status

Branded Marketers:

- Follow these steps as outlined
- Review compliance status with your Brand
- Check with your Brand before replacing PIN pads or automated fuel dispensers

What Should I Do Now?

Step 3: Inventory Your Systems:

- Utilize the information obtained from your processor to conduct a thorough inventory of your payment-related systems
- Recognize that PCI impacts all systems related to or involved in the payment processing chain, from consumer all the way to the bank
 - Inside PINPads
 - Outside PINPads in Pumps/Dispensers
 - Point of Sale
 - Back Office
 - Networks
 - Banks & Processors

Branded Marketers:

- Review compliance status of with your Brand, especially POS and networks
- Get information in writing

Step 4: Contact All Systems Vendors:

- Gain written confirmation on the compliance and validation status of each system your sites use against each relevant PCI standard (PCI DSS, PCI PED, and PCI PA-DSS)
- Be persistent in getting complete, **written** information from vendors
- If a component is not compliant, obtain written confirmation on vendor's plans to become compliant

What Should I Do Now?

Step 5: Conduct Self Assessment:

- Obtain self assessment forms from PCI Security Standards Council Web Site
- Assess where your systems and operations are in relation to requirements—and be brutally honest with yourself!
- Get help from experienced consultants or personnel. Do not underestimate time and skill/experience involved in accurately assessing your PCI situation.

Step 6: Fix What You Can Today:

- Close gaps identified in the assessment to position your firm for the best possible results in Step 7

Step 7: Perform Assessment and Security Scan:

- Hire an approved PCI Qualified Security Assessor (QSA) to audit your systems and operations, plus perform an external “security scan”

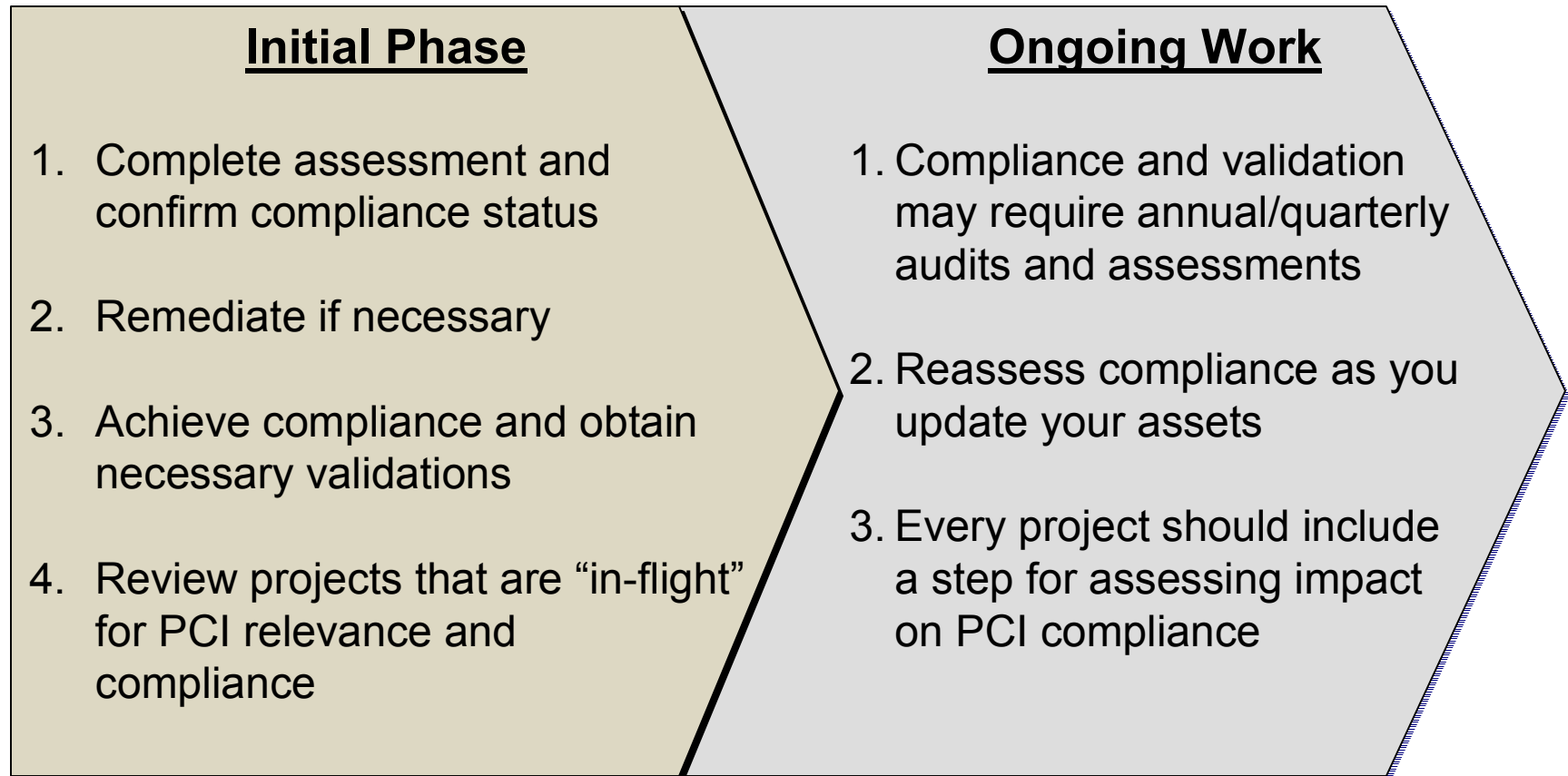
Step 8: Fix Additional Items Identified in Assessment:

- Remediate any items uncovered in assessment (or remaining from self-assessment), and begin planning for next cycle of assessment while continuing to make operational improvements. This is because...

Process Review

PCI Compliance is a process, not a project!

While there are deadlines, it is not a 2008 only endeavor



Summary

- PCI applies to every merchant accepting card payments
- Begin now!
 - Work with your processor/bank to determine your specific compliance requirements
 - Compliance is ongoing – plan accordingly
 - Seek help from experienced, knowledgeable source as necessary
 - Use certified, compliant products and services
- Information available at www.pcisecuritystandards.org
- Be aware of PCI PED, PCI PA-DSS, Triple DES, and other emerging requirements and upcoming deadlines
- *Presentation and other information may be found at www.wcapra.com*