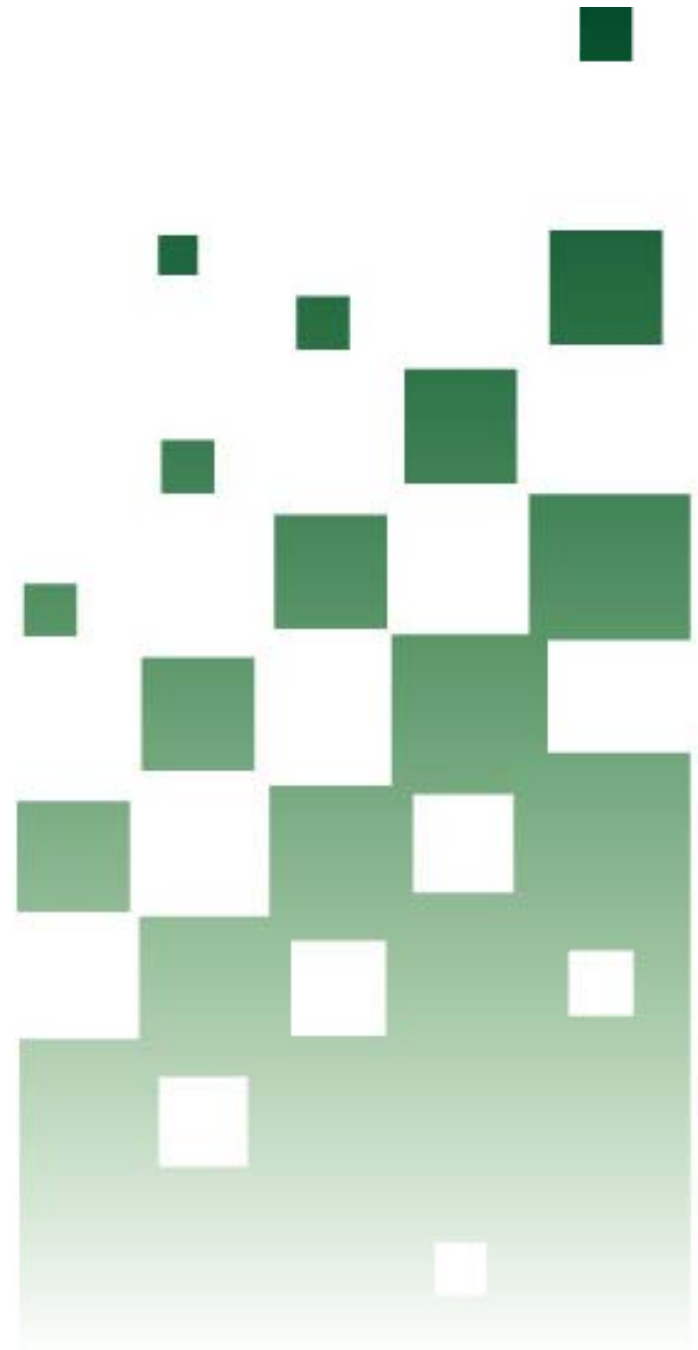


PCI DSS: Update and Case Study

Walt Conway
Marc Henkel
Kevin Noland



Background

- ◆ State Contract
- ◆ Operational Issues
- ◆ Costs
- ◆ Opportunity To Introduce Fee
 - Fund Equipment
 - Some PCI Related Costs
- ◆ More Engaged QSA

Conversion Process

- ◆ Existing Inventory Issues
- ◆ Outdated Equipment
 - Tranz 330 and 380
- ◆ Merchant Visit
 - Ask Questions
 - Learn Process
 - Begin Documentation

Quick Wins

- ◆ Office Reorganization
- ◆ Truncate All Receipt Paper
- ◆ New Terminals
 - PCI PED (PIN Entry Device)
 - MasterCard PTS (POS Terminal Security)
- ◆ New Tracking and Posting System
 - Authoritative Source of Merchant and Terminal Info
 - Automated Daily Posting To ERP
 - Contact Management
 - Simplified Transaction Search

Peripheral Benefits

- ◆ Single Point of Contact to Acquirer
- ◆ Merchant Boarding Process Offloaded
- ◆ Better Quality Settlement Data
- ◆ Identify and Educate “Rogue” Merchants
- ◆ Opportunity to Revise Merchant Policy
 - Made PCI DSS a requirement
 - Added Additional Detail

Managing the QSA

- ◆ Set Expectations
- ◆ Need to Understand Higher Ed
 - Hotel, Restaurant, Retail, Web
- ◆ Regular Communication
- ◆ Full Disclosure

Lessons Learned

- ◆ Merchant Cooperation
- ◆ PCI Affects Merchant Strategy
- ◆ Are We Going Backwards?
- ◆ Interpretation of PCI DSS Can Vary
- ◆ Staying Informed A Challenge
- ◆ Vendors Still Learning Too
 - PABP Certification Documentation

PCI: What's New in 08

- ◆ Outsourcing:
Payment Application Best Practices (PABP)
becoming Payment Application Data Security
Standard (PA DSS)
- ◆ Home grown systems:
Application layer security
(Requirement 6.6)

PA DSS

- ◆ Do you know PABP?
 - Third-party providers and applications
 - Validated by Visa
- ◆ Are your vendors on the list?
- ◆ PABP becoming PA DSS in 3Q08
 - Acceptance by all brands
 - Voluntary for now, but...

Visa PA DSS Mandate

| <i>Phase</i> | <i>Compliance Mandates</i> | <i>Effective Date</i> |
|--------------|--|-----------------------|
| I. | Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors ("VNPs") and agents must not certify new payment applications to their platforms that are known vulnerable payment applications | 1/1/08 |
| II. | VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant | 7/1/08 |
| III. | Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications | 10/1/08 |
| IV. | VNPs and agents must decertify all vulnerable payment applications | 10/1/09 |
| V. | Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications | 7/1/10 |

- ◆ Migrate to PA DSS for all outsourcing

Application Layer Security (6.6)

- ◆ Protect all web-facing applications against known attacks by either:
 - Application code review, or
 - Application layer firewall
- ◆ “Best practice” until June 30, 08
- ◆ Issue: Will you be ready July 1st?

Other PCI Developments

- ◆ New SAQs
- ◆ Wireless security
- ◆ Pre-authorization data
- ◆ PIN Encryption Device standard
- ◆ Compensating Control worksheet
- ◆ Enhanced documentation, FAQ
- ◆ Monitoring QSAs, ASVs for quality

Want to Know More?

- ◆ Treasury Institute's PCI DSS Workshop in May
- ◆ Register online:
www.treasuryinstitute.org

PCI DSS: Update and Case Study

- ◆ Thoughts?
- ◆ Comments?
- ◆ Questions?