

Keep Your Data Safe Stay PCI Compliant

Kevin Wright

Vice President of Information Technology

Knowledge is Power! Series





Agenda

- Data Security
- Credit Card Security
- Steps to PCI Compliance
- Resources
- Question & Answer



Data Security

- History
- Data to Protect
- Importance of Data Security
- Best Practices for Data Security



Importance of Data Security

- Loss of reputation
- Loss of customers
- Legal or other regulatory requirements
- Potential financial liabilities
- Litigation



Importance of Data Security

- Fidelity National – 8.5 million
- Britain's Tax & Customs - 25 million
- Dai Nippon Printing – 43 million
- TD Ameritrade – 6.3 million
- Monster – 1.3 million
- TJX – 46 million
- Card Systems – 40 million



Best Practices for Data Security

- Take Stock – Know what you have.
- Scale Down – Keep just what you need
- Lock It – Protect what you keep.
- Pitch It – Dispose of what you don't need.
- Plan Ahead – Have an incident plan.



Credit Card Security

- Current PCI Security Standards
- Merchant Compliance Levels
- High Level Merchant Requirements
- Nebraska Book Company Applications



Current PCI Security Standards

- Payment Card Industry Data Security Standard
 - Version 1.1, September 2006
 - Currently in effect for all merchant levels
 - Twelve high level requirements for Merchants
- Payment Application Data Security Standard
 - Version 1.1, April 2008
 - Currently recommendation, will be required as of July 2010
 - Specification for payment application vendors
 - VISA website lists validated payment applications



Merchant Compliance Levels

Level	Annual Visa/MC Transactions	Validation	Deadline	In Compliance with PCI (as of Jan 2008)
Level 1	More than 6 million	Annual Audit Quarterly Scan	9/30/04	77%
Level 2	1 to 6 million	Self Assessment Quarterly Scan	9/30/07	62%
Level 3	20,000 to 1 million	Self Assessment Quarterly Scan	6/30/05	54%
Level 4	Less than 20,000	Self Assessment Quarterly Scan	Merchant Bank Determines	N/A



High Level Merchant Requirements

- Build & Maintain a Secure Network
- Protect Cardholder Data
- Maintain Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor & Test Networks
- Maintain an Information Security Policy



Nebraska Book Company Applications

- Tender Retail – Merchant Connect Multi
 - Validated against PA-DSS / PABP
- WebPRISM Hosting Center – PCI Compliant
- PRISM / WinPRISM Applications
 - Includes encryption and PCI required features
 - Will be validated against PA-DSS in 2009
 - Requirement as of July 2010
- Also Integrating with Third Party Service Provider



Steps to PCI Compliance

- Select a knowledgeable and qualified partner for compliance effort.
- Follow data security best practices – especially scale down.
- Rate level of compliance.
- Show progress!!!

- Danger Signs
 - Lack of firewall
 - Lack of data encryption
 - Use of sensitive information for account numbers



Resources

Federal Trade Commission's Guide for Information Security

www.ftc.gov/infosecurity

PCI Security Standard Council (Standard, QSA's, self assessment)

<https://www.pcisecuritystandards.org/>

VISA's List of Validated Payment Applications

http://usa.visa.com/download/merchants/validated_payment_applications.pdf

VISA's List of Certified Service Providers

http://usa.visa.com/download/merchants/cisp_list_of_cisp_compliant_service_providers.pdf



Thank you!