



## PCI Compliance

Presented to:

**NDSU IT Security Conference**

**Tuesday, October 21<sup>st</sup> 2008**

**John B. Weaver**

CISSP, CISA, CISM, CPP

President/CEO

Principal Consultant

# PCI Compliance

## Agenda

- ❑ Introduction
- ❑ What is PCI?
- ❑ Components
- ❑ Requirements
- ❑ Auditing for PCI Compliance
- ❑ Completing the Cycle

# JBW Group International Inc.

## ❑ Focus

- ❑ Full Service Information Security Consultancy Founded in 2002
- ❑ Information Security Management System Audit and Implementation (ISO 27001)
- ❑ Information Technology Service Management Audit and implementation (ISO 20000)
- ❑ Privacy Management and Corporate Governance
- ❑ Training- ISO 27001, ISO 20000 Implementation and Lead Audit; CISSP Preparation

## ❑ Experience

- ❑ Fortune 50 companies to small businesses
- ❑ Clients in the United States, Canada, Japan, Mexico and Central America
- ❑ Legal and Regulatory Compliance for Healthcare, Pharmaceutical, Financial Services Clients
- ❑ Energy, Banking and Finance, Telecommunications, Software, Legal

- ❑ Proven Methodology, based on Internationally Recognized Standards

- ❑ Over 20 years as an information security professional
- ❑ Former director of World-wide & IP network security for an international telecommunications company
- ❑ Taught standard Audit and Implementation for BSI Americas
- ❑ IRCA-certified ISO 27001 auditor
- ❑ IRCA-certified ISO 20000 auditor
- ❑ Subject matter expert in:
  - ❑ ITSMS and ISMS Audit
  - ❑ Security program deployment
  - ❑ Disaster Preparedness Planning
  - ❑ Incident response management
- ❑ Guided organizations in multiple verticals to successful certification on the first audit

# Background

## TJX Breach – Jan 17<sup>th</sup> 2007

- ❑ 215 million customer records from TJ Maxx, Marshalls, Winners, HomeSense & others in North America, the UK and Ireland
- ❑ According to TJX, cost of the breach \$216M, other sources estimate \$1B
- ❑ Fifth Third Bank paid over \$2.1M in fines and penalties
- ❑ TJX has set aside \$256M to cover fines and penalties
- ❑ Source [www.privacyrights.org](http://www.privacyrights.org)

# PCI-DSS

- ❑ Payment Card Industry Data Security Standard
- ❑ Evolution of multiple standards into one global security standard for credit/debit card processing
- ❑ Current version is PCI Data Security Standard version 1.2 (released Oct. 1<sup>st</sup> 2008)
- ❑ Includes (IT) security management, architecture, software design, policies and procedures
- ❑ Recognizes that not all organizations are created equal

# PCI Compliance and the Law

- ❑ Minnesota Statute 365E.64 is the 1<sup>st</sup> state to put PCI into law (August 1, 2007)
- ❑ Only a portion of the standard concerning retention of credit card information is addressed
- ❑ Provides recourse for the consumer and financial institutions
- ❑ Similar legislation is under consideration in at least five other states
- ❑ The payment card industry enforces harsher penalties
- ❑ 34 States have enacted breach notification laws similar to California Code 1798

# Terminology

- ❑ Merchant levels
  - ❑ Level 1 – More than 6,000,000 transactions per year
  - ❑ Level 2 – 1,000,000 to 6,000,000 transactions per year
  - ❑ Level 3 – 20,000 to 1,000,000 transactions per year
  - ❑ Level 4 – Fewer than 20,000 transactions per year

# Terminology

- ❑ Information contained on the magnetic stripe or smart card chip
- ❑ Cardholder Data
  - ❑ Cardholder name
  - ❑ Primary account number (PAN)
  - ❑ Service code
  - ❑ Expiration date
  - ❑ Proprietary and discretionary data
- ❑ Sensitive Authentication Data
  - ❑ Full magnetic stripe data
  - ❑ PIN/PIN Block
  - ❑ Card verification code

# Terminology

- ❑ PED – Pin entry device
- ❑ SAQ – DSS Self-Assessment Questionnaire (4 actually)
- ❑ QSA – Qualified Security Assessor
- ❑ ASV – Approved Scanning Vendor

# PCI Requirements

## Build and maintain a Secure Network

1. Build 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

# PCI Requirements

## Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure system and applications

## 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

# PCI Requirements

## 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

# PCI Requirements

## PCI Requirements for Shared Hosting Providers

- ❑ Protect the cardholder data environment

## Compensating Controls

- ❑ Alternates to most PCI requirements required because of technical or other business constraints

# Differences from Previous Versions

- ❑ Numerous clarifications and explanations from the previous version
- ❑ Enhancement to requirements and testing procedures for wireless (4.1.1)
- ❑ Enhancement to included all operating system types (5.2)
- ❑ Attestation of compliance for on-site assessments – Merchants (Appendix D)
- ❑ Attestation of Compliance for On-site Assessment – Service Providers (Appendix E)

Source Payment Card Security Standards Counsel

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

# PCI Documentation

<b>Document</b>	<b>Audience</b>
<b>PCI Data Security Standard</b>	<b>All merchants and services providers</b>
<b>Navigating PCI DSS: Understanding Intent</b>	<b>All merchants and services providers</b>
<b>PCI DSS: Self-Assessment Guidelines and Instructions</b>	<b>All merchants and services providers</b>
<b>PCI DSS: Self-Assessment Questionnaire A</b>	<b>Merchants</b>
<b>PCI DSS: Self-Assessment Questionnaire B</b>	<b>Merchants</b>
<b>PCI DSS: Self-Assessment Questionnaire C</b>	<b>Merchants</b>
<b>PCI DSS: Self-Assessment Questionnaire D</b>	<b>Service Providers &amp; all other merchants</b>

# Common Errors

## PCI compliance as implementation of controls

- ❑ PCI is not considered in the context of an overall approach to information security
- ❑ Information security objectives are separated from critical business objectives and functions

## Focus on passing the audit

- ❑ Emphasis on the presence/absence of controls
- ❑ No linkage to wider organizational information security needs

# Common Errors

## Not a risk-based approach

- ❑ Implementation of controls based on best practices
- ❑ Difficult to articulate compensating controls

## Limiting technological approach

- ❑ Activities driven by the audit cycle
- ❑ Absence of a process-based approach

# Auditing for PCI Compliance

## PCI Self-Assessment Questionnaires

- ❑ Audit for compliance based on identified criteria
- ❑ Utilize self-assessment questionnaires for checklist audits
- ❑ White hat hacker tools to assess secure network monitoring and testing

## PCI Controls

- ❑ Over 250 requirements testing procedures

## Certification for Compliance by QSA

- ❑ Compliance assessed by qualified QSA
- ❑ Network scans by ASV validate security posture

# Completing the Cycle

## Reporting on Compliance

- ❑ Complete the Report on Compliance
- ❑ Ensure passing vulnerability scans by an approved ASV
- ❑ Complete the Attestation of Compliance
- ❑ Submit the ROC, passing scan results and Attestation (and other documentation as required)

# Completing the Cycle

- ❑ Integrate PCI compliance in the context of an overall approach to information security
- ❑ Establish linkages between critical business objectives and functions information security objectives
- ❑ Focus on integrating PCI control requirements and compensating controls based on an enterprise risk management framework
- ❑ Process approach to information security with foundations in regulatory guidance, identification of relevant components, planning, development, maintenance and continuous improvement



**John B. Weaver**

CISSP, CISA, CISM, CPP

President/CEO – Principal Consultant

**JBW Group International**

PO Box 19393

Minneapolis, MN 55419 USA

**+1.877.97.27001**

**[www.JBWGroup.com](http://www.JBWGroup.com)**