

Deloitte.

Payment Card Industry Data Security Standard (PCI DSS).

A roadmap to PCI DSS certification

1 August 2007



Recent incidents of data compromise



Date made public	Name (Location)	Number of records
1 April 2008	Okemo (Vermont, US)	<p>Approximately 40,000 transactions are affected.</p> <p>Hackers broke into the resort's computer network and gained access to thousands of credit cards.</p> <p>The data was stolen during a two-week period in February.</p> <p>A similar breach occurred in March 2006.</p>
December 2007 to March 2008	Hannaford Bros. (New England/New York/Florida, US)	<p>Estimated 4.2 million credit and debit card numbers were illegally accessed from the supermarket's computer systems during transmission of card authorisation.</p> <p>More than 1,800 cases of fraud had been linked to the theft.</p> <p>A targeted malware attack is being blamed for the data breach .</p>
2007	TJX (Massachusetts, US)	<p>Reported at least 45.6 million cards were exposed, while banks' court filings put the number at more than 100 million.</p>

TJX credit card breach



- TJX the Massachusetts-based operator of discount chains including T.J. Maxx and Marshalls
- Estimated at least 45.6 million credit cards stolen
- In addition, more than 450,000 names, addresses and personal ID numbers also taken
- Breaches spanned 17 month period
- Resulting fraud \$17 million to date
- Three states' banking associations (MA, CT, and ME) filed a class action lawsuit against TJX to recover the costs of damages totalling "tens of millions of dollars" incurred for replacing customers' debit and credit cards.
- Banks' court filings put the number at more than 100 million.
- TJX agreed to pay MasterCard \$24 million for losing records of 29 million MasterCard transactions and agreed to pay Visa \$41 million for losing 65 million Visa records.
- It has also paid an \$880,000 fine for violating PCI DSS requirements

What is the PCI-DSS?



- **A comprehensive set of requirements for enhancing cardholder data security**
 - Storage and handling of customer credit card information/data
- Developed by the founding payment brands
 - MasterCard Worldwide
 - Visa International
 - American Express
 - Discover Financial Services
 - JCB
- To help facilitate the broad adoption of consistent data security measures on a global basis
- The five founding members jointly formed an independent regulatory organisation called the PCI Security Standards Council to promulgate the Standard
- The PCI DSS reflects an agreed position on the combination of each of the credit card brands' security standards

To help organisations ensure they are adequately protecting customer account data

View of PCI governance and relationships



PCI Security Standards Council

- Help facilitate the broad adoption of consistent data security measures on a global basis
- Owns, develops, maintains and distributes the PCI Data Security Standards
- Fosters adoption of a single set of data security standards for all key stakeholders (merchants, banks, SPs, POS vendors)
- Invite stakeholders to participate in the ongoing development of the PCI Data Security Standards

- Create and manage global pool of qualified ASVs and QSAs to ensure that the standards are consistently implemented.
- Defines qualifications for QSAs and ASVs
- Trains, test and certifies

Qualified Security Assessors (QSAs)

- Provides guidance on compliance process
- Conducts comprehensive on-site audits

Approved Scanning Vendors (ASVs)

- Performs quarterly external network scans

Merchant /
Service Provider

The PCE DSS requirements



Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: No use of vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management programme

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

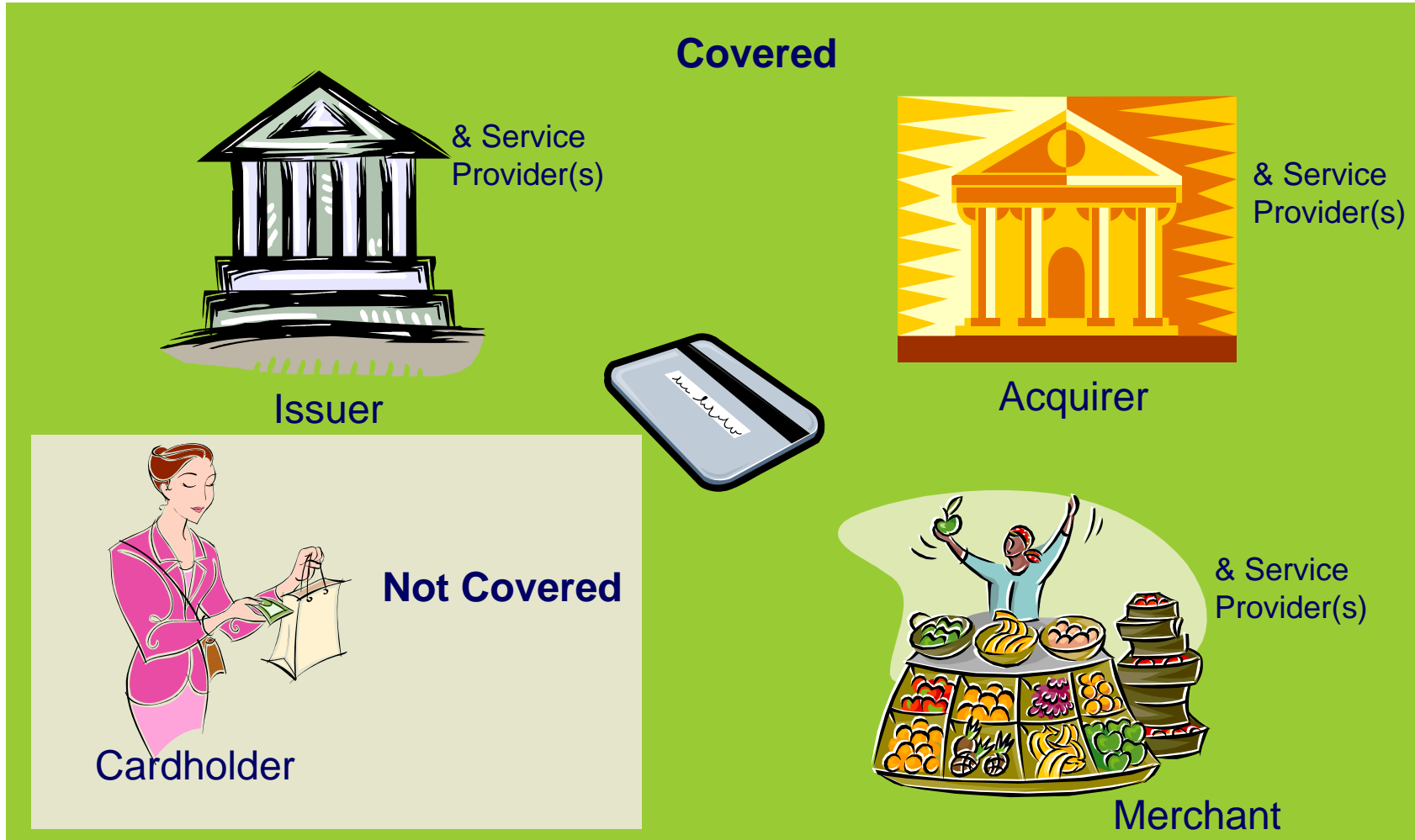
Requirement 10: Track & monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Who must comply with PCI DSS?



What will the QSA focus on?



- The flow and storage of credit card information
- Relevant standards that the organisation already aligns to
 - informs the PCI readiness efforts
- Who are your third-party relationships and service providers?
- Your architecture and operations
- The 12 requirements

What value you should seek from certification

- More than just 'avoid the fine'
- Achieving the intent of PCI DSS
 - Avoiding unnecessary risk altogether
 - Securing cardholder information
 - Reducing fraud risk
 - Secure the brand image / customer confidence
- Integrated cardholder information architecture
- Align with privacy principles
- Sustained ongoing compliance

PCI Relationships – The view for each player



The Acquirer

- Key Gaps
- Observations

Merchants & their Service Providers

- Awareness and Education
- Gap Analysis and Readiness
- Remediation
- Validation
- Service Provider Challenges
- New Merchant Acquisitions & Marketing

Service Providers & their Service Providers

- Awareness and Education
- Gap Analysis and Readiness
- Remediation
- Validation
- Service Provider's Service Provider Challenges

Questions



© Scott Adams, Inc./Dist. by UFS, Inc.