



compliance
spectrum

The Payment Card Industry

10.07.08

Compliance Spectrum Confidential

Presenter

- Steven Helwig, CISSP, CGEIT
Compliance and Policy Analyst
steve.helwig@compliancespectrum.com
www.compliancespectrum.com

PCI Objectives

- Building and maintaining a secure network
- Protecting cardholder data
- Creating and maintaining a vulnerability management program.
- Implementing strong access control measures
- Monitoring and maintaining the networks
- Maintaining an information security policy

PCI-DSS and the PCI-SSC

- PCI Security Standards Council was launched on Sept. 7th, 2006
- Founding Brands
 - JCB and Visa International
 - American Express
 - Discover
 - MasterCard
- Key 3rd Parties
- PCI SSC Scope
 - Develop and manage the PCI-DSS
 - Manage the approval process for assessors and scanning vendors
 - Develop and publish PCI-DSS related documents
- PCI SSC not in scope
 - Compliance tracking and enforcement
 - Forensics and Account Data Compromise (ADC) event response

PCI-DSS: a regulation or a standard?

- Regulation
 - To regulate is to bring under the force of law or a governing authority
 - The regulators are empowered to interpret how the laws are to be implemented and to establish rules for following those laws. Those rules are then documented as regulations.
- Standards
 - Standards are not enforceable by law. However, failure to follow standards may result in actions contrary to regulations which are enforceable by law
 - A standard is a criterion, a means of determining what rules, principles, and measures established by an authority should apply to a given situation in order to improve efficiency.
- PCI-DSS is a hybrid
- The Payment Card Industry Association also mandates the use of its PCI-DSS standard as the audit standard that must be followed when proving that you've met their guidelines
 - Anyone wanting to accept credit cards as a form of payment is required to contractually agree to comply with this standard and failure to comply can result in a variety of fines and, potentially, the loss of the right to accept credit cards at all.

PCI Standards

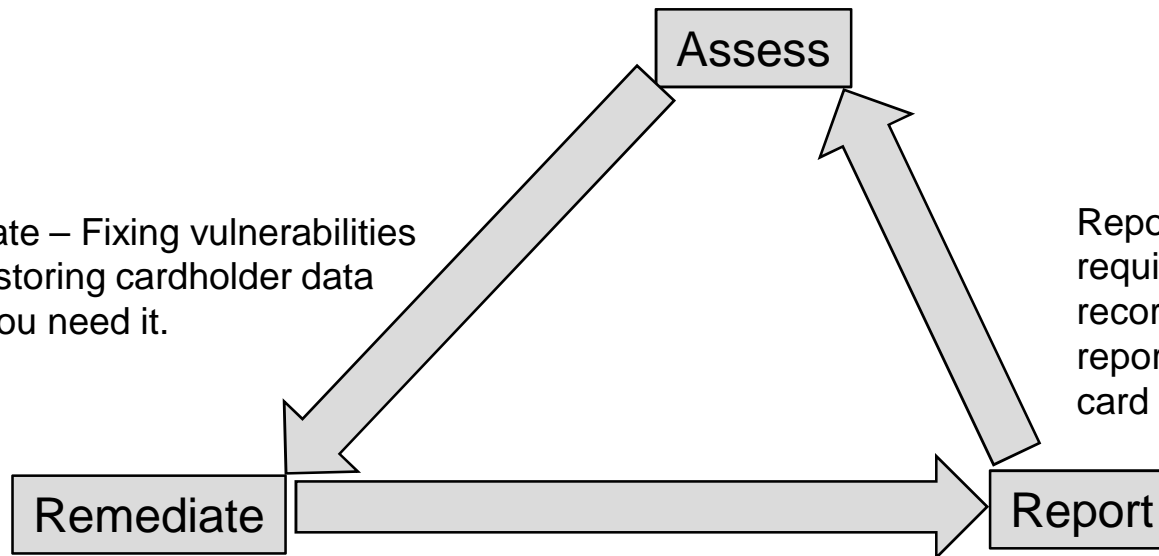
- Manufacturers
 - PCI PED (PIN Entry Device)
- Software Developers
 - PCI PA-DSS
 - Payment Application Vendors
- Merchants and Processors
 - PCI-DSS
 - Data Security Standard

PCI Compliance Life Cycle

Assess- Identifying cardholder data, taking inventory of your IT assets and business processes for payment card processing, and analyzing then for vulnerabilities that could expose cardholder data.

Remediate – Fixing vulnerabilities and not storing cardholder data unless you need it.

Report – Compiling and submitting required remediation validation records, and submitting compliance reports to the acquiring bank and card brands.



PCI RULES

- THE STANDARDS APPLY TO ALL ORGANIZATIONS THAT STORE, PROCESS OR TRANSMIT CARDHOLDER DATA
- KEEP YOUR SCOPE AS SMALL AS POSSIBLE

The Chain

- Brand
 - Acquirer
 - Service Provider / Processor
 - Merchant
 - » POS

Risk

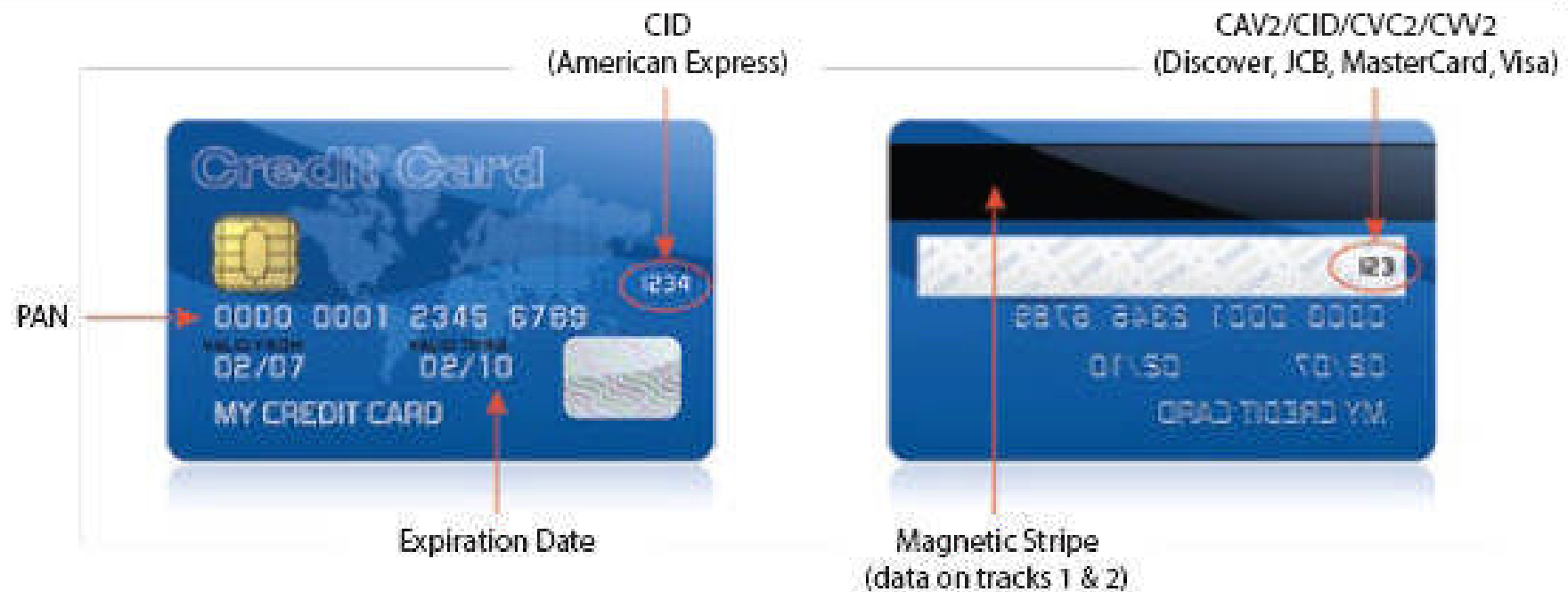
- Survey of US and European Businesses
 - 81% Store Payment Card Numbers
 - 73% Store Payment Card Expiration Dates
 - 71% Store Payment Card Verification Codes
 - 57% Store Customer Data from the Payment Card Magnetic Stripe
 - 16% Store Other Personal Data

PCI-DSS Applicability Information

	Data Element	Storage Permitted	Protection Required	PCI-DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN / PIN Block	No	N/A	N/A

Card Data

Types of Data on a Payment Card



Why Do Criminals Want The Card Data

- With the equivalent track 2 data the criminals can make magnetic stripe cards – lots of magnetic stripe cards
- These can be used to perform Cardholder not present fraud
- With the PIN the criminals can use the cards to withdraw cash at an ATM

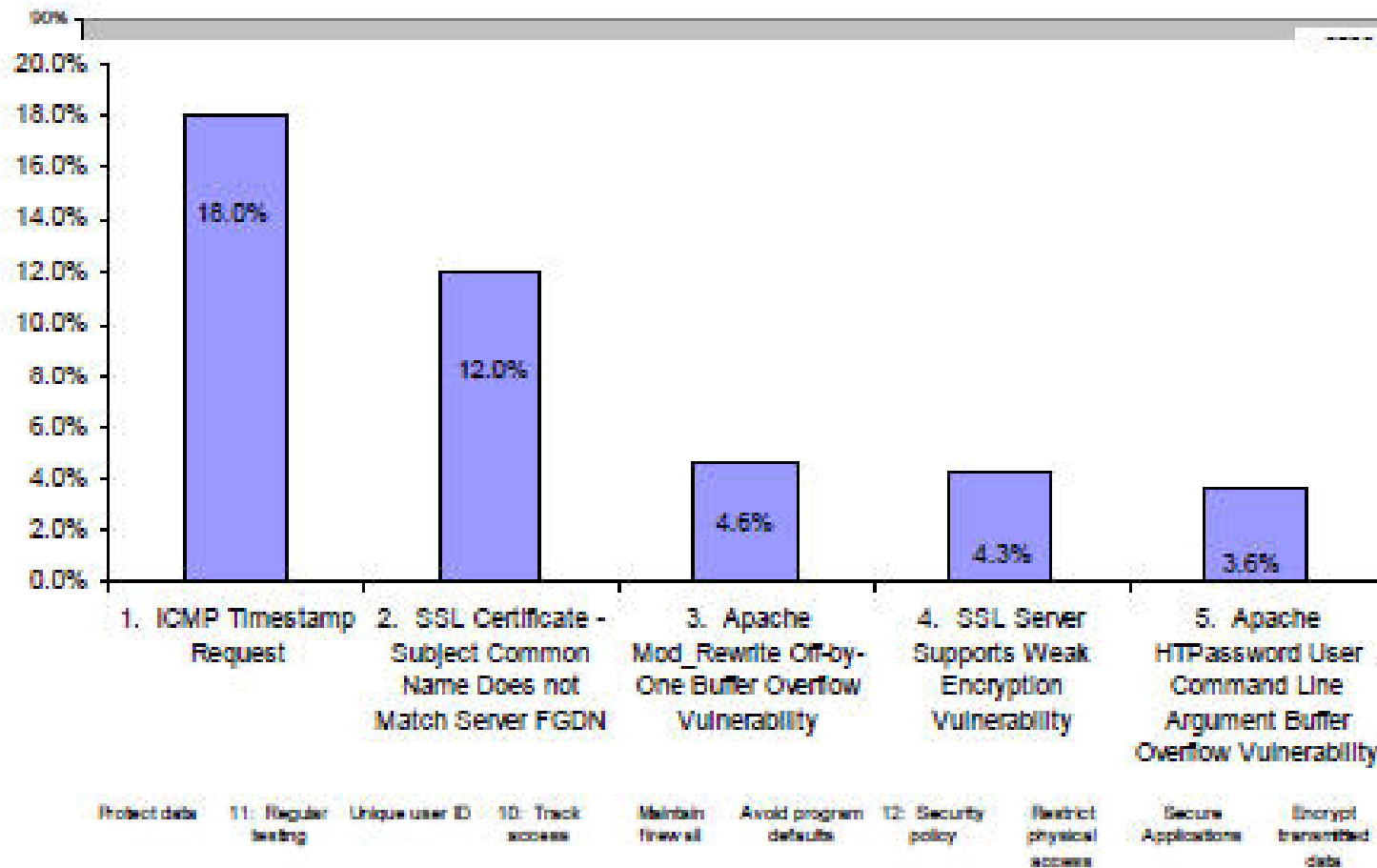
Who Should Comply?

- Anyone who takes credit card orders
 - Mail Order, Telephone Order (MOTO)
 - Point of Sale systems
 - E-commerce systems
- Size Matters Somewhat
 - There are 4 levels of PCI-DSS compliance, based upon the number of annual transactions
 - There is no difference for any other contractual obligation
- PCI-DSS
 - Level 1
 - >6 MM transactions
 - All TTPs
 - All DSEs storing data
 - Anyone compromised
 - Level 2
 - >150,000 transactions
 - Level 3
 - >20,000 transactions
 - Level 4
 - Everyone else

How Should We Comply with PCI-DSS

Level	Requirement	
Level 1	3 rd party Audit	Quarterly Network Scan
Level 2	Self Assessment	
Level 3		
Level 4		

Why Are Merchants Having Problems



Top Ten Vulnerabilities Sample Size: 85,000

- 10 - Telnet running
- 9 - Outdated Apache Mod_Frontpage
- 8 - Man-in-the-middle remote desktop attack
- 7 - Found telnet default password
- 6 - Outdated IIS
- 5 - Outdated OpenSSH
- 4 - Cross-Site Scripting
- 3 - Inconclusive Scan: (Port scan blocking at FW or IDS, or no required services present)
- 2 - Outdated SSH
- 1 - Using SSL version 2.0 (SAQ 4.2)

What Is The Scope

PCI-DSS applies to all system assets/components that are *in scope*

E-commerce sites are different than POS networks

- *E-commerce Fundamentals*
 - *Online payment configurations*
 - *E-commerce modes of operation*
- *The POS systems*
 - *POS systems*
 - *Kiosks*
 - *In-store processor*
 - *LOB servers*
- All sites have some common components
 - Border routers
 - Firewalls
 - The network
 - Authentication servers
 - DNS servers
 - Operating environments
 - Stored data
 - E-mail
 - Notebooks
 - Operational logs
 - Users

PCI – DSS Standard

Goals	PCI DSS Requirement
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need – to – know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors

Summary of Changes PCI-DSS 1.1 / 1.2

- Based on a Life Cycle of 24 months
- No new major requirements
- Provide greater clarity on PCI DSS requirements
- Offers improved flexibility
- Incorporate best practices
- Clarify scoping and reporting
- Eliminate redundant sub-requirements
- Consolidate documentation
 - Requirements and Testing Procedures

Consequences

- Acquiring Banks
 - Financial institutions that grant retailers and other entities the approval needed to accept credit cards
 - Contractually responsible for ensuring merchant members comply
 - Determine merchant level
 - \$5000 per instance per month for Mid Sized Merchant
 - \$25000 per instance per month for Larger Merchants
 - Loss of the ability to take credit cards
- Verisign report on 9/17/07 – Nearly 2/3s compliant

Challenges

- Know data flow
- Scoping
- POS systems as apply to Requirement 5 and 6
 - *Requirement 5: Use and regularly update anti-virus software*
 - *Requirement 6: Develop and maintain secure systems and applications*
- Cost
- Implementation (installing / maintaining)
- Firewalls and Anti-Virus
- Data ownership – encrypting of stored data at rest
- Testing and Maintaining
- Annual rotation of encryption keys
- Securing Applications
- Minimizing amount of data stores
- Logging and protecting data

Possible Solutions

- Report any incidents to Visa or other brand
 - Breaches
 - Even if not sure – let the brand determine
- Limit the scope
 - Know where data is
 - Know where data is stored
 - Verify encryption
 - Reduce these areas
- Use certified applications and hardware for POS
- Know what level required to be compliant with
 - Acquirer makes this determination

Possible Solution (con't)

- If doing self-assessment, try to have third party verify
- Have a change management process
 - Know how changes affect the compliance
- Have Incident Response plan
 - Include Visa, Acquirer
 - Know regulations
 - State
 - Federal
 - Other
- Keep up with PCI changes
 - Check PCI SSC Website periodically
 - <https://www.pcisecuritystandards.org/>
- Quickly remediate issues

Qualified Security Assessors (QSA)

- Contracted directly with PCI SSC
- Only QSA can determine compliance
- Instituted for consistent and proper application of security measures and controls
- Qualifications requirements are exacting and detailed
- Both company and employee must be certified
- Process
 - Apply as a firm for qualification in the program
 - Provide document adhering to the Validation Requirements for Qualified Security Assessors
 - Qualify individual employees, through training and testing, to perform assessments
 - Execute an agreement with PCI SSC governing performance
- Renew yearly
- High costs

Approved Scanning Vendor (ASV)

- Validate compliance
- Perform a rigorous remote test on the PCI SSC test infrastructure, which simulates a typical customer
- Deliberate introduce vulnerabilities and misconfigurations for the vendor to identify and report as part of the compliance testing process
- Primary test addresses:
 - Scan administration – how the vendor collects and manages scan requests from its customers
 - Scan performance – the ability of each vendor to identify vulnerabilities and misconfigurations in the network and web applications
 - Scan report – how the vendor presents the scan results to its customers
- Subject to annual recertification
- Costly

Payment Application Qualified Security Assessor (PA-QSA)

- Must be employed by QSA company
- Must utilize the testing procedure documentation in PA DSS document
- Must assess to laboratory where validation process
 - Simulates real world use of the payment application
- Follow requirements for the laboratory and laboratory processes
- Must complete and submit Appendix B in PA-DSS document completed for payment application under review as part of completed PA-DSS report

Incidents – TJ MAX

- WEP compromise
- Minimum 18 month break in
- Affected 98 million credit card numbers
- Violated 9 of the 12 PCI requirements
- Fined \$880,000 by Visa

Incident - Hannaford Brothers Grocery

- Company claimed PCI compliance in 02/08
- Timeline
 - Happened Dec. 7, 2007
 - Discovered Feb. 27, 2008
 - Contained March 10, 2008
- Exposed 4.2 million credit / debit card numbers
- 1800 credit / debit numbers stolen
- Inside job
- Sniffed while cards were processed

Contact Information

- Compliance Spectrum
11044 Research Blvd., D-300
Austin, TX 78759
www.compliancespectrum.com
- Steve Helwig
steve.helwig@compliancespectrum.com

The End

Q & A

Thanks for Attending / Drawing

Please submit a business card or Lead slip (with email address) for a copy of this presentation and chance to win an Ipod