ISACA Kansas City Chapter
PCI Data Security Standard v2.0 Overview

February 10, 2011

RSM McGladrey, Inc.

Quick Overview–RSM McGladrey, Inc.

- Greg Schu, Managing Director/Partner
- Kelly Hughes, Director
- When considered with McGladrey & Pullen, LLP, RSM McGladrey ranks as the fifth largest provider of accounting, tax and business services.
- We are a member of RSM International, a worldwide affiliation of accounting and consulting firms.
  - 24,000 employees in more than 600 offices worldwide
- We provide a full range of accounting, tax and consulting services to clients.

McGladrey

Agenda

- Before We Get Started
- Who Must Comply
- Why Comply
- Some Terms—Overview
- Visual Depiction
- PCI Levels—Merchants/Service Providers
- PCI Validation Requirements—Merchants/Service Providers

McGladrey

Agenda

- Planning
  - What to Consider
  - Cardholder Environment
- New Standards
- PCI Data Security Standard (DSS) Version 2.0
- Some of the More Significant Changes
- Support and PCI DSS
  - Common Compliance Challenges
  - Compensating Controls
  - The PCI Security Standards Council
- Best Practices
- Questions

McGladrey

Before We Get Started

- What is your background with PCI DSS?
  - High level of knowledge
  - Moderate level
  - Just learning what it means and possible impacts on your organization
- What are you interested in having us discuss today? What do you want to learn about PCI DSS requirements?
- Any questions before we begin?

Who Must Comply

- Any entity that stores, processes and/or transmits cardholder data must comply with the PCI DSS.
- Normally these entities include:
  - Service providers
  - Merchants—compliance mandated by merchant banks
- Each payment card brand has their own set of validation and reporting requirements.
- Financial institutions are currently in a grey area, but this will change in the next couple of years.

McGladrey

Why Comply

Keep Your Name Out of the “Media”

- New data breaches reported daily
  - Stealing credit card numbers has become a business.
  - Organized crime groups look for any way to get numbers for various purposes.
  - Loss of customer confidence is breached.
- Famous breaches
  - TJMMAX, Heartland, Hannaford, etc.

Why Comply

The “Media”

- News spreads quickly
  - Facebook
  - Twitter
  - Blogs
  - E-mail
- May include information about the breach or other company data and be available quickly

Why Comply

"Safe Harbor" Status

- Safe Harbor status provides organizations protection from fines and compliance exposure in the event of a compromise.
- To attain Safe Harbor status:
  - Members MUST be in FULL COMPLIANCE with the PCI DSS at the time of the breach (as demonstrated during a forensic examination).
  - Members MUST have validated FULL COMPLIANCE PRIOR TO the compromise.

Why Comply

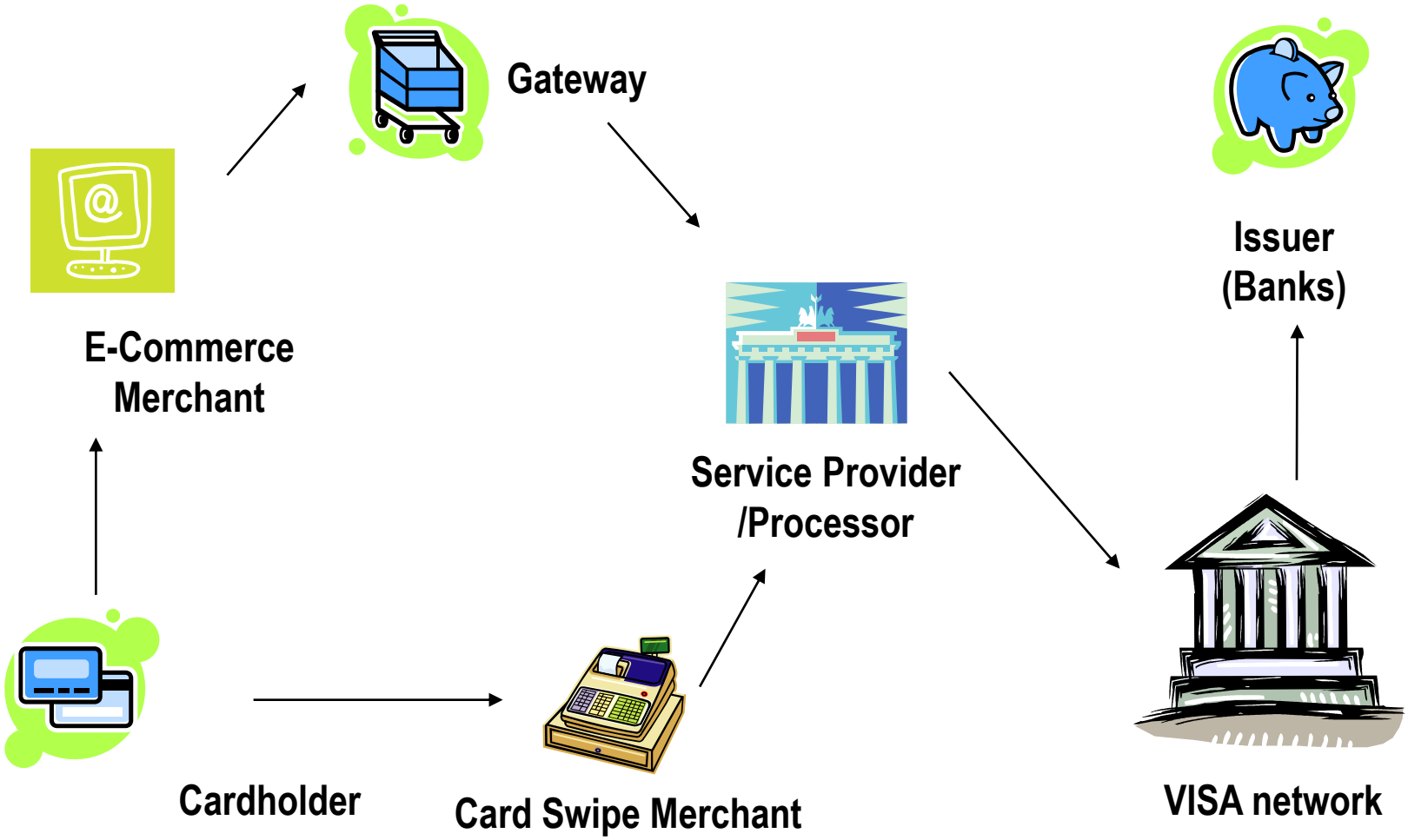
Fines, Penalties, Other Operating Costs

- Members proven to be noncompliant or whose merchants or agents are noncompliant may be assessed:
  - Noncompliance fine (egregious violations up to $500K)
  - Forensic investigation costs
  - Issuer/acquirer losses
    - Unlimited liability for fraudulent transactions
    - Potential additional issuer compensation (e.g., card replacement)
  - Dispute resolution costs

Some Terms—Overview

- Service provider
  - Any organization that stores, transmits or processes cardholder data on behalf of a merchant
- Merchant
  - Retailers/stores that take credit card payments from cardholders in exchange for products or services
- Third-party agent
  - Service provider without a direct connection to a card brand—must be registered with the card brand via card brand client
- Cardholder data environment
  - People, processes and technology that store, process or transmit cardholder data or sensitive authentication data

Visual Depiction



McGladrey

PCI Levels (Merchants)

Merchant Level 1	Any merchant processing over 6M transactions per year, **compromised in the last year** or identified by another payment card brand as Level 1
Merchant Level 2	Any merchant processing between 1M to 6M transactions or 150K MasterCard eCommerce transactions per year
Merchant Level 3	Any merchant processing 20K to 1M transactions or over 20K MasterCard eCommerce transactions per year
Merchant Level 4	Any merchant processing less than 20K eCommerce transactions per year and all other merchants processing up to 1M transactions per year

PCI Levels (Service Providers)

Service Provider Level 1	Any service provider processing or storing over 300,000 transactions/account numbers per year or **compromised in the last year**.
Service Provider Level 2	Any service provider processing or storing less than 300,000 transactions/account numbers transactions per year

McGladrey

PCI Validation Requirements (Merchants)

LEVEL	VALIDATION ACTIONS	SCOPE	VALIDATED BY
1	• Annual on-site security audit ** AND ** • Quarterly network scan	• Authorization and settlement systems • Internet-facing perimeter systems	• Qualified Security Assessor (QSA) or internal Auditor if trained by PCI • Approved scan vendor (ASV)
2 & 3	• Annual self-assessment questionnaire ** AND ** • Quarterly network scan	• Any system storing, processing or transmitting PCI cardholder data • Internet-facing perimeter systems	• Merchant (self-assessment) • Approved scan vendor (ASV)
4	• Annual self-assessment questionnaire recommended • Network scan recommended	• Any system storing, processing or transmitting PCI cardholder data • Internet-facing perimeter systems	• Merchant (self-assessment) • Approved scan vendor (ASV)

McGladrey

PCI Validation Requirements (Service Providers)

LEVEL	VALIDATION ACTIONS	SCOPE	VALIDATED BY
1	• Annual on-site security audit ** AND ** • Quarterly network scan	• Any systems storing, processing or transmitting PCI cardholder data • Internet-facing perimeter systems	• Qualified Security Assessor (QSA) or internal auditor if trained by PCI. • Approved scan vendor (ASV)
2	• Annual self-assessment questionnaire • Network scan recommended	• Any system storing, processing or transmitting PCI cardholder data • Internet-facing perimeter systems	• Service provider (self-assessment) • Approved scan vendor (ASV)

McGladrey

Planning—What to Consider

- What can cause problems
  - Inappropriate scope
  - Insufficient documentation
  - Application issues (particularly legacy applications)
  - Unnecessary (or inappropriate) data storage
  - Compensating controls (that don’t compensate)
  - Bad timing
  - Incident response plan

Planning—Cardholder Environment

- Remember, the assessment scope applies only to the cardholder data environment (CDE).
  - CDE: people, processes and technology that store, process or transmit cardholder data or sensitive authentication data
- The assessor must include everything in scope that is not segmented from the CDE.
- The organization (merchant, service provider) is responsible for documenting where cardholder data resides and how it flows through the environment.

Planning—Cardholder Environment

- No segmentation? Then the assessor must include everything in scope.
  - This is where most organizations start.
  - This approach rarely (never?) leads to a clean Report on Compliance (ROC).
- Perform a pre-assessment/readiness to help determine where cardholder data resides (risk assessment approach).
- PCI DSS requirements require planning and validation using a continuous approach vs. “once a year” event.

New Standards

- PCI DSS Version 2.0—October 2010
- Self-Assessment Questionnaires—October 2010
- PCI PA-DSS—October 2010
- Internal Security Assessor Program—September 2010
- PCI DSS v2.0 Scoring Guide—March 1, 2011

McGladrey

PCI DSS Version 2.0

- The requirements are fundamentally the same as Version 1.2.
- Twelve standards covering six domains:
  - Build and maintain a secure network.
  - Protect cardholder data.
  - Maintain a vulnerability management program.
  - Implement “strong” access control measures.
  - Regularly monitor and test networks.
  - Maintain an information security policy.

PCI DSS Version 2.0

- Many minor changes to better clarify the intent of requirements and test procedures
- Requirements divided into individual requirements to align with the ROC scoring
- Better categorization, i.e. moving test items from requirements to test column and vice versa
- Better documented requirements that were “unclear” or requirements emphasized at training to QSAs, i.e., all traffic inbound and outbound transits a DMZ

Some of the More Significant Changes

- Addressed virtualization within the context of the existing requirements
- Prohibition on WEP to secure wireless network as of June 10, 2010
- Secure coding requirements to apply to all internally developed applications, not just Web applications
- Secure coding to address newly identified high-risk vulnerabilities

Some of the More Significant Changes

- Additional sampling guidance
  - Does not reduce scope
  - Reiterates requirement for documenting sampling rationale
- Key changes—required when end of life is reached vs. annually
- Logs—clarified
  - Systems need to generate logs, not just be capable of generating logs.
  - Log data can be restored immediately, not just immediately available.
- Passwords—resets that require an immediate change after first use

Support and PCI DSS
Common Compliance Challenges

- Quarterly scans by ASV
- Documentation
  - Polices and procedures to specifically address CHD
- Segmentation of cardholder systems from network
- Logging requirements/file integrity monitoring
- Wireless implementations
- Application code reviews
- Internal and external penetration testing

Support and PCI DSS Compensating Controls

- Compensating controls need to meet the intent and the rigor of the original requirement.
  - Adding key management does not help you meet an authentication requirement.
- Compensating controls must be documented.
  - Compensating controls are subjective; document fully to build your case.
  - Even if you cannot meet a control, document why you cannot and what else you are doing to address the issue.
  - Your assessor wants to agree with you. Thorough documentation makes it easy for the assessor to agree.
  - The assessor must be able to validate the compensating control.
- Compensating controls have a shelf life.
  - They're a "stop-gap," not an "end state."

Support and PCI DSS
The PCI Security Standards Council

- Standards and fact sheets
  - Skimming prevention
    - Cameras, secured devices, security tape, maintenance
  - Wireless guidelines
    - Segmentation and firewalls (1.2.3), rogue access points, WPA2 and vendor defaults (2.1.1), scan for wireless (11.1), IDS/IPS (11.4), port detection

Support and PCI DSS
The PCI Security Standards Council

- Navigating the PCI DSS (v2.0)
  - Understanding the intent of the DSS
  - Guidance pertaining to the requirements
- Point-to-Point encryption (P2PE) (initial roadmap)
  - Helps determine if P2PE can help with compliance
  - Describes components of P2PE
- PCI storage do's and don'ts
  - Another way to describe what can/cannot be stored
  - Possible methods to protect data

Support and PCI DSS
The PCI Security Standards Council

- Fact sheets
  - Data storage
    - Do not store unless necessary, no prohibited data, do not print CHD on PED devices, encrypted at rest, cameras, limited access, hard copy data
- Prioritized approach
- FAQs
- URL—https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

Best Practices

- Discussed throughout this presentation
  - Segmentation
  - Understand cardholder environment
  - Limit where CHD stored
  - Limit access to CHD
  - Limit length of time data retained
  - Ongoing process
  - Do not try to “over control” business processes

McGladrey

Questions?

Greg Schu

Managing Director/Partner Director

greg.schu@mcgladrey.com

612.376.9520

Kelly Hughes

Director

kelly.hughes@mcgladrey.com

303.298.6461

McGladrey