Paul Baker
Vice President, Payment System Integrity
MasterCard Worldwide

MasterCard Worldwide

PCI-DSS – Update on the evolution of the standard

Madrid, Spain

Agenda

- Security Landscape
- MasterCard Response - SDP
- PCI Security Standards Council
  - Recent Developments
- Summary

Security Landscape - Current Trends

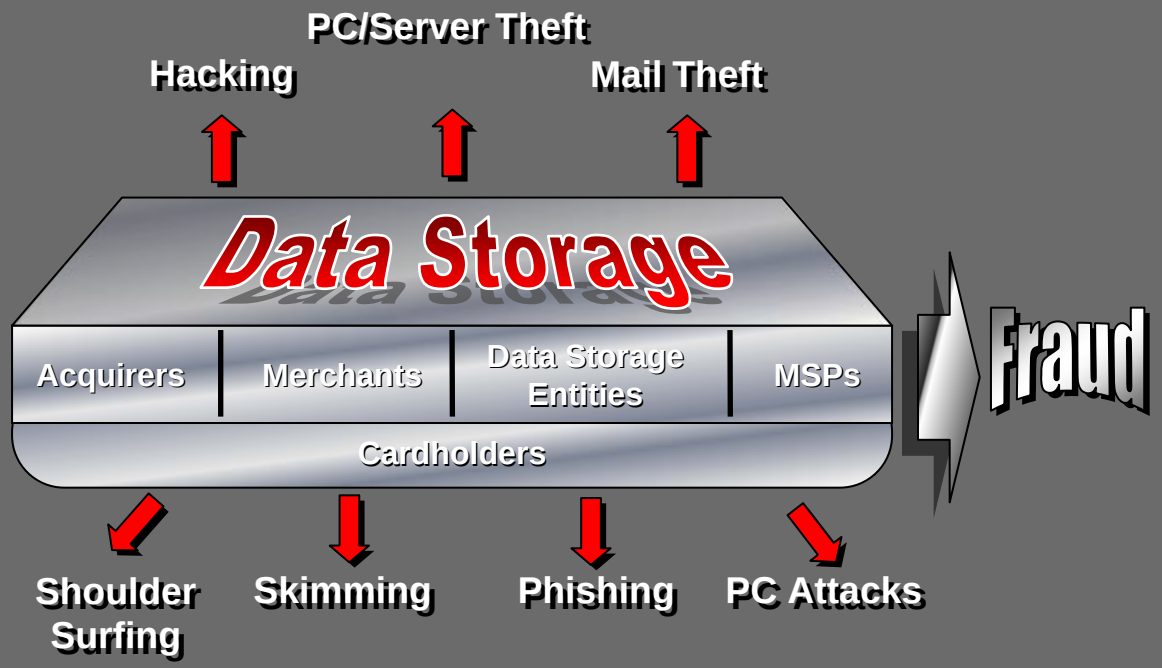
- Cyber crime is growing in diversity and sophistication
- Integrated POS Systems are increasingly targeted
  - In most cases, magnetic stripe data is stolen from log files as opposed to traditional databases
  - Sensitive data is often unknowingly stored leading to risk
  - Hackers are targeting centralized servers with Internet connectivity, not just an e-commerce issue

Security Landscape - Current Trends

- SQL injection is the most common attack method
  - First attempt is almost always SQL injection
  - Thieves can directly extract data from databases including log-in credentials or payment card information
- Remote control software
  - PC Anywhere/VNC commonly used
  - Poor access controls

How do Account Data Compromises occur?

- **Physical theft**
- **Remote Access**
  - Internet
  - Direct connect
  - Wi-Fi
  - SQL Injection



Top 5 Reasons for Account Data Compromise

MasterCard Worldwide

Based on MasterCard Forensics Examinations of Hacked Entities

#1 Ineffective Patch Management

#2 No Security Scanning

#3 Weak Network Level Security

#4 SQL Injection

#5 Lack of Real Time Security Monitoring

PCI Compliance Levels

Category	Criteria	Requirements	Compliance Date
Level 1	• Merchants >6 MM annual transactions (all channels) • All TPPs • All DSEs storing data for Level 1, 2, 3 • All compromised merchants, TPPs and DSEs	• Annual Onsite Audit [1] • Quarterly Network Scan	30 June '05 [2]
Level 2	• All merchants > 1 million total MasterCard transactions < 6 million total MasterCard transactions annually • All merchants meeting the Level 2 criteria of a competing payment brand	• Annual Self-Assessment • Quarterly Network Scan	31 December 2008
Level 3	• All merchants with annual MasterCard e-commerce transactions > 20,000 but less than one million total transactions • All merchants meeting the Level 3 criteria of a competing payment brand	• Annual Self-Assessment • Quarterly Network Scan	30 June '05
Level 4	All other merchants	• Annual Self-Assessment • Quarterly Network Scan	Consult Acquirer

1 TPPs and DSEs must use a certified third party to perform the onsite audit
2 TPPs and DSEs were previously required to completed quarterly scans and self-assessments by 30 June 2004

MasterCard PCI Update: Data Storage Clarification

	Component	Storage Permitted	Protection Required	Encryption Required**
Cardholder Data	PAN	YES	YES	YES
	Expiration Date*	YES	YES	NO
	Service Code*	YES	YES	NO
	Cardholder Name*	YES	YES	NO
Sensitive Authentication Data	Full Magnetic Strip	NO	N/A	N/A
	CVC2/CVV/CID	NO	N/A	N/A
	PIN	NO	N/A	N/A

* Data elements must be protected when stored in conjunction with PAN
** Compensating controls for encryption may be employed

PCI and SDP Compliance

PCI Compliance

- PCI Onsite Assessment
- PCI Self Assessment
- PCI Quarterly Network Scanning

The successful completion of the above applicable compliance requirements means the merchant is compliant with the PCI Data Security Standard.

SDP Compliance

- Compliance Validation with Acquirer
- Acquirer Registration of Merchant with MasterCard

The successful completion of the above compliance requirements means the merchant is compliant with the PCI Data Security Standard AND compliant with the MasterCard SDP Program requirements.

PCI Compliance + SDP Compliance = Safe Harbor

PCI Merchant Education Program – Launched 15 October 2007

- MasterCard has developed a series of customizable, interactive modules and will work with financial institutions to develop training sessions and materials tailored to their merchants.
- Offered to acquirers:
  - Comprehensive education and training for acquiring banks and merchants to broaden their understanding of PCI DSS through interactive sessions with industry security experts.
  - The new PCI Merchant Education Program is adaptable and delivered through various channels based on the needs of each individual acquirer and their merchant base.

PCI-Education Delivery Options & Timeframes

- The education program offers several training options including:
  - **On-Site** (OS) In-person training for acquirers at designated locations. This option provides the best opportunity for high-contact interaction. (Available after November 1, 2007)
  - **Live Web Meeting** (LM) –Real-time online interface and teleconference. This option is ideal for presenting one to three modules and may be followed by Q&A sessions. (Available after November 1, 2007)
  - **On-Demand Webinar Series** (WS) –Pre-recorded content available through an online interface. This option is low-contact and can be viewed as the merchant's schedule allows. (Available after October 15, 2007)

Content Library

- *An Introduction to the PCI Security Standards Council*
  - Presented by Bob Russo, PCI Security Standards Council
- *A Detailed Look at PCI DSS Requirements*
  - Presented by Andrew Henwood, One-Sec/ Trustwave
- *A Merchant's Journey Towards Compliance*
  - Presented by Alexander Grant, British Airways
- *Understanding Account Data Compromise*
  - Presented by Bryan Sartin, Cybertrust / Verizon Business
- *Preparing for a Successful PCI Assessment, Lessons from the Field*
  - Presented by Michael Walter, Arsenal Security Group
- *Reducing Your Risk: A Look into PCI Vulnerability Scanning*
  - Presented by John Bartholomew, Security Metrics
- *Security and the Payments System*
  - Presented by Jeremy King & John Verdeschi, MasterCard
- *Compliance Validation & Beyond*
  - Presented by Sally Ramadan, MasterCard

Security
Standards Council

Recent Developments

13 November, 2007

The PCI Security Standards Council Members

PCI Data Security Standard

- PCI Data Security Standard
  - PCI DSS v1.1
  - PCI Security Audit Procedures v1.1
  - PCI Security Scanning Procedures v1.1
  - PCI DSS v1.1 Summary of Changes
  - Glossary
- QSA and ASV Requirements
  - PCI Validation Requirements for QSAs
  - PCI Validation Requirements for ASVs
  - PCI Technical and Operational Procedures for ASVs

PCI DSS - Translations

- Chinese (simplified and traditional)
- French
- French Canadian
- Korean
- Japanese
- German
- Spanish
- Portugese
- *Italian (coming soon)*

Six Goals, Twelve Requirements

The Payment Card Industry Data Security Standard (PCI DSS)

Build and Maintain a Secure Network	1. Install 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 data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems 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
Regularly 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 DSS v1.1 – Revision examples

- **Clarity and Consistency:**
  - Incorporated a clarification of data definitions, distinguishing between cardholder data that must be protected by PCI vs. sensitive authentication data that must never be stored
- **Flexibility:**
  - Defined compensating controls for data encryption, and provided ability for compensating controls to be applied to various requirements based on technical and business constraints
- **New Security Requirements**:
  - Created new application level requirement (6.6) to address significant trend in account data compromise cases, effective date June 30, 2008

Frequently Asked Questions

- Over 1100 questions submitted to TWG by QSAs, ASVs and Merchants
- Responses developed by all five payment brands help “pave-the-way” for PCI DSS evolution
- *Technical FAQ planned availability on PCI SSC website in 3Q 2007*

Self-Assessment Questionnaire

- Validation and reporting tool used to facilitate self-evaluation against the PCI DSS requirements
- Used by non-level 1 merchants and smaller service providers
- SAQ v1.0 is not fully aligned with the DSS and takes a “one-size fits all” approach

New SAQ Objectives

- Alignment with the PCI DSS v1.1
- Based on industry feedback
- Flexibility for multiple merchant types
- Providing guidance for the intent and applicability of the underlying requirements
- May be used as a basis for an automated tool in the future

Draft SAQ v1.1

- SAQ Instructions and Guidelines
- Navigating the PCI DSS: Understanding the Intent of the Requirements
- SAQ A: Attestation only
- SAQ B: Imprint and standalone POS merchants
- SAQ C: IP Based POS merchants with no data storage
- SAQ D: For all other merchants

Top PCI DSS Feedback Issues

Panel Discussions

1. Application Layer Security (6.6)
   - Code Reviews
   - Application Firewalls
2. Pre-Auth Data Security (3.2)
3. WEP and wireless security (2.1.1)
4. PA-DSS – Discuss adoption of PABP into PCI SSC

Quick Hits

1. Clarification on connected entities (12.10)
2. Guidance for penetration testing (11.3)
3. PCI DSS Audit Scope
4. Clarification of Public Networks (4.1)
5. The use of production/mag stripe data for testing (6.3.4)
6. Logging and monitoring requirements (10.6/10.7)
7. Risk reduction through the use of Chip based technology/EMV
8. Compensating controls - flexibility vs. consistency

Additional Standards

- Pin Entry Device Standard
  - All Brands will Grandfather previously approved POS PEDs
  - Lab Qualification
  - Approval Letters
  - Approved Product Listings
  - Approval Process – 10 business days
- PA DSS
  - New standard based on PABP
  - PA-QSA Training & Testing
  - Compliant Product Listings

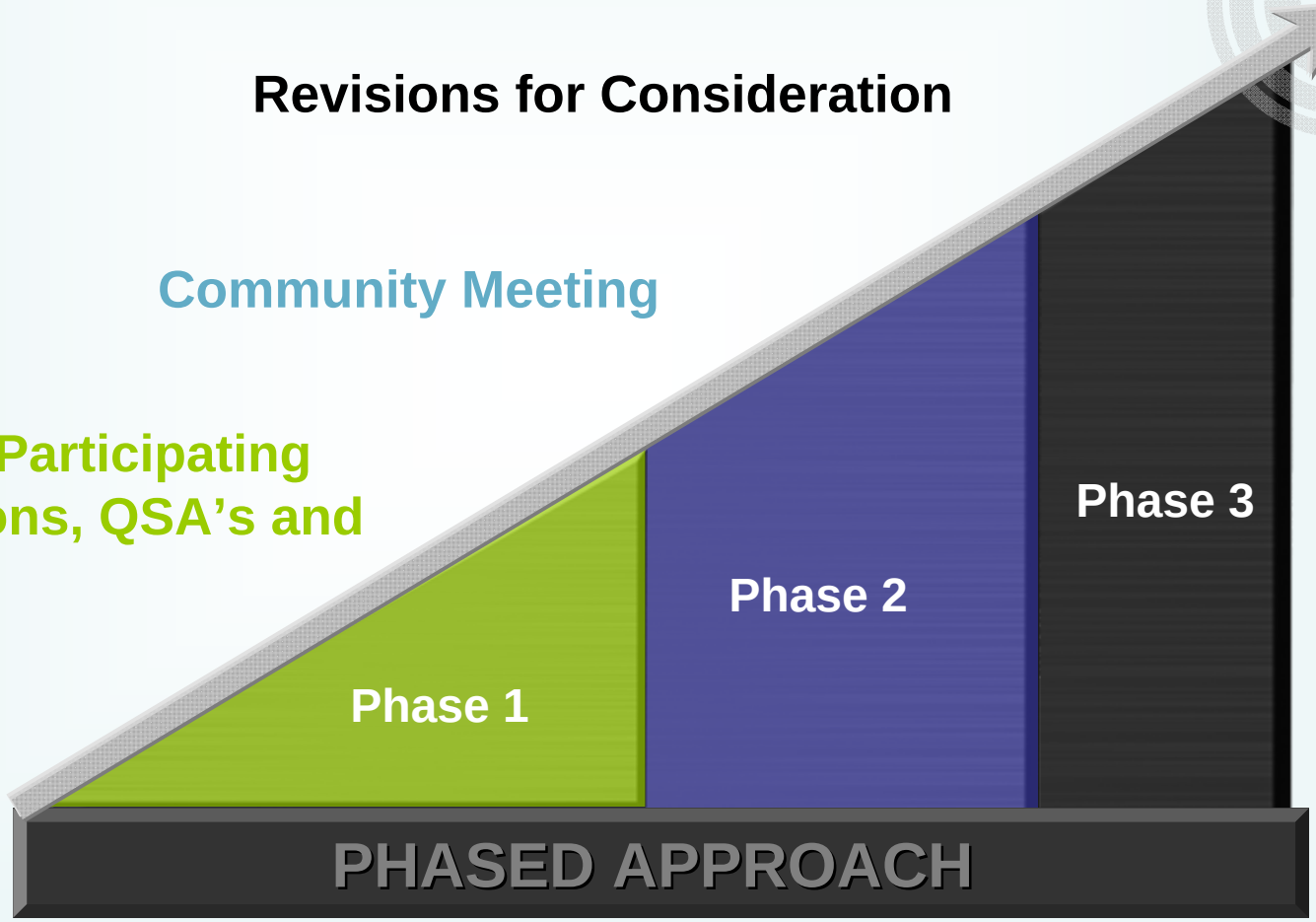
Security Standards Council

Revised PCI Standard

Revisions for Consideration

Community Meeting

Input from Participating Organizations, QSA's and ASV's



PA-DSS

- Based on Visa USA's PABP
- Applies to third party payment applications implemented in merchant and service provider environments as opposed to home grown applications which are covered in the DSS
- Distinct from but aligned with PCI DSS
- Will be updated based on industry feedback
- Using a PA-DSS compliant application does not in itself provide PCI DSS compliance

Payment Application Data Security Standard (PA-DSS) formerly PABP

- Publish PA-DSS and testing procedures

- PA-QSA testing approval

- Payment application validation

PA-DSS Deployment

PCI SSC

- PA-DSS Standard
- PA-QSAs
- List of compliant payment applications

Payment Brands

- Mandates and enforcement
  - Due Dates
  - Non-compliance Assessments if applicable

Summary

- PCI-DSS is aimed at reducing the risk of an account data compromise
- New tools available to assist in compliance
- PCI-SSC now responsible for PA-DSS and PCI-PED / EPP
- Collectively we can evolve this standard to protect card data
- Become a participating organisation in the PCI-SSC & / or encourage other stakeholders

Navigating The Future of Commerce

MasterCard Worldwide