

# PCI Standards: A Banking Perspective

Bob Brown, CISSP  
Wachovia  
Corporate Information Security

# Agenda

---

1. Payment Card Initiative History
2. Description of the Industry
3. PCI-DSS Control Objectives
4. PCI Audit Process
5. Industry & Technical Factors Impacting Compliance
6. Q&A

# Identity Theft Complaints



# Short History

- 1996 Federal Government creates HIPAA
- 2000 Visa develops “Digital Dozen.” Rules that merchants had to follow to accept Visa’s credit/debit cards.
- 2001-2004 various standards from MasterCard, American Express, Discover
- 2005 Visa's Cardholder Information Security Program & MasterCard's Site Data Protection(SDP) Program Combine to form PCI
- 2006 Formation of the PCI Security Standards Council: American Express, Discover, JCB\*, MasterCard Worldwide and Visa International

# PCI Definition

---

- Payment Card Industry (PCI) Data Security Standard (DSS) is a set of internationally applicable requirements that merchants and payment service providers that accept, process, and store credit card information must meet in order to achieve compliance with the standard.

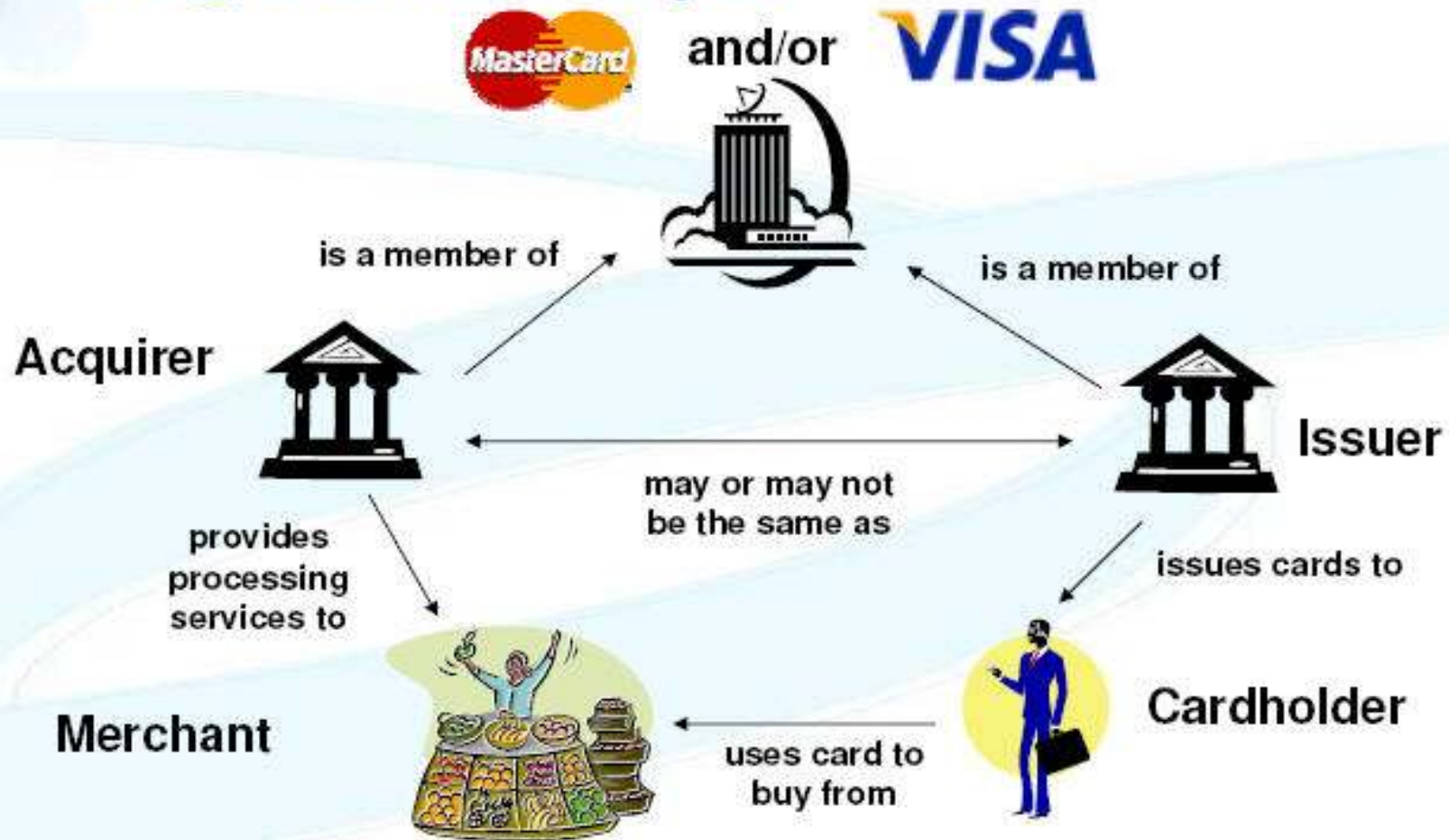
Merchants are expected to be compliant by  
June 30<sup>th</sup>.

# Who's Who in PCI Compliance?

Entity	Role	Requirement	Example
PCI SSC	Maintain PCI DSS, manage QSA and ASV approval Process	Work with the SSC Exec Committee and Participating Organizations and modifications to PCI DSS	PCI SSC
Card brand	Credit card branding and Network	Member of PCISSC, final enforcement point for PCI (or brand-specific) Compliance	American Express, Discover, JCB, MasterCard, Visa
Issuing Bank	<i>Members of the Visa or MasterCard organisations that issue the cards to Cardholders</i>	Comply with PCI Standards	Capital One, Wachovia
Acquiring Bank	The merchants' and PSPs' bank that processes the credit card Transactions	Validate merchant and PSP PCI compliance	Bank of America, Washington Mutual
Merchant	Sell goods and maintain systems that store, process, or transmit cardholder data	Self-attestation, annual on-site audits, quarterly network scanning	Amazon, Barnes & Noble, eBay
PSPs	Provide payment services to merchants that store, process, or transmit cardholder data	Self-attestation, annual on-site audits, quarterly network scanning	PayPal, VeriSign
QSAs*	Perform Onsite Audit	Maintain qualifications w/ PCI SSC	CTG, Vigilar
ASVs*	Perform Network Scans	Maintain good standing with PCI SSC	Accuvant, Qualsys

# Who's Who? (cont)

## Diagrammatically...



# PCI-DSS Control Objectives\*

- **Build and Maintain a Secure Network:**
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use 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 Program:**
  - 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 and 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

# PCI-DSS Appendix

## *Appendix A:*

### PCI DSS Applicability for Hosting Providers

- *Hosting providers protect cardholder data environment.* As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS.

## **Appendix B**

### *Compensating Controls – General*

- Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. See the PCI DSS Glossary for the full definition of compensating controls.

# What Can Be Stored?

	Data Element	Storage Permitted?	Protection Required?	PCI DSS Requirement 3.4
Cardholder Data	PAN	Yes	Yes	Yes
	Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Exp Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Strip	No	N/A (Do not store)	N/A (Do not store)
	CV2/CVV2/CID	No	N/A (Do not store)	N/A (Do not store)
	PIN/PIN Block	No	N/A (Do not store)	N/A (Do not store)

# PCI-DSS Audit Process

1. **Self Attestation and Readiness:** The PCI SSC provides a self-attestation document that can be used as proof of PCI compliance for merchants and PSPs that do not perform a high volume of card transactions.
2. **External Scanning:** For PCI, all merchants and PSPs, regardless of size of transaction base, are required to undergo quarterly network scans. These scans must be performed by an Approved Scanning Vendor (ASV) as defined by the PCI SSC.
3. **On-Site Audit:** High-transaction merchants and PSPs, known as Level 1 in Visa's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection (SDP), are required to undergo an annual on-site audit conducted by either a qualified internal auditor or a PCI DSS QSA.

# Merchant Levels & Requ's

	Description	QSA Onsite Review	Self Assessment	Network Security Scan
<b>LEVEL 1</b>	Any Merchant processing over 6,000,000 transactions per year, compromised in the last year, or identified by another payment card brand as Level 1	Required Annually	Not Required	Required Quarterly
<b>LEVEL 2</b>	Any Merchant processing between 150,000 and 6,000,000 e-commerce transactions per year, or identified by another payment card brand as Level 2	Not Required	Required Annually	Required Quarterly
<b>LEVEL 3</b>	Any Merchant processing between 20,000 and 150,000 ecommerce transactions per year, or identified by another payment card brand as Level 3	Not Required	Required Annually	Required Quarterly
<b>LEVEL 4</b>	Any Merchant processing less than 20,000 e-commerce transactions per year, and all other Merchants processing up to 6,000,000 transactions per year	Not Required	Recommended Annually	Recommended Annually

# Service Provider Levels & Requ's

	Description	QSA Onsite Review	Self Assessment	Network Security Scan
<b>LEVEL 1</b>	All Service Providers that process, store or transmit over 600,000 transactions or accounts annually (or that store card data for Level 1 or 2 Merchants for MasterCard)	Required Annually	Not Required	Required Quarterly
<b>LEVEL 2</b>	Any Service Provider that is not in Level 1 and stores, processes or transmits more than 120,000 accounts or transactions annually (and that store card data for Level 3 Merchants for MasterCard)	Required Annually (for MC)	Required Annually (for Visa)	Required Quarterly
<b>LEVEL 3</b>	Any Service Provider that stores, processes or transmits less than 120,000 accounts or transactions annually (and all other Storage Entities not in Levels 1 or 2 for MasterCard)	Not Required	Required Annually	Required Quarterly

# Consequences of Audit Failure

- Payment card brands can levy fees on the “offending” merchant, PSP or Acquiring Bank. Fines could reach +\$500,000.
- Suspend doing business
  - In 2005 Cardsystems Solutions was cutoff from processing Visa & AmEx
- Compliance gaps treated as a way to create a timeline for resolution w/ “Target Dates”

# Fines/Penalties To Date

- Other than CardSystems Solution in 2005 there have been no fines or penalties.

# PCI Council Adaptation

- Visa has announced that it will start making PCI compliance a requirement for some reductions in the interchange fees they charge to merchants who accept credit card payments.

# Successes

- Web application security given more prominence
- Increased emphasis on Identity/role-based access control and privilege limitation
- Robust audit and monitoring
- Enhanced, more detailed usage policies

# Challenges\*

- **Cost of compliance:** Estimated costs of annual audits range from \$20,000 to \$100,000, the average was less than \$50,000, and no company reported spending more than \$200,000
- **Legacy constraints:** Many applications, databases, and networks that process and store credit card data were in use well before the PCI DSS existed. Some customers reported that legacy constraints made it difficult to meet all of the PCI DSS requirements.
- **Subjectivity concerns:** Requirement 6.6 (which is currently a “best practice”), calls for performing source code reviews or “installing an application-layer firewall.” The definition of what constitutes an “application layer firewall” is not clearly explained
- **PCI and other requirements:** Requirement 10.3 of the PCI DSS requires audit trails that log entries for user identification, type of event, date and time of access, or origination point of the event. However, recording and tracking some of this information could negatively intersect privacy requirements in certain jurisdictions.

# “An Evolving Standard”

- **Transference of Risk:**
  - “If a central organization says, ‘We certify ChoicePoint,’ who gets sued when ChoicePoint has a problem? If you did that, you would have to have a limitation of liability that says something like, ‘We’ll review them, but don’t hold us accountable if something happens to them.’ Therefore the certification doesn’t mean too much.”
- **PCI standard also requires that data be encrypted at rest**
  - Many databases cannot meet this standard currently. Even if they can, it requires massive re-writing of application code.
- **The requirement for two-factor authentication.**
  - The standard stipulates that a user name and password are not enough to authenticate an employee, administrator or third party who gains remote access to any system that holds debit or credit card data.
- **The Stop&Shop Vulnerability**
  - Involved criminals who tampered with the equipment customers use to swipe their credit cards and input PINs, is not currently addressed in the PCI standard.

# References

- Payment Card Industry Data Security Standard:  
[http://usa.visa.com/download/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_PCI\\_Data\\_Security\\_Standard.pdf](http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf)
- PCI Self-Assessment Questionnaire:  
[https://sdp.mastercardintl.com/pdf/758\\_PCI\\_Self\\_Assmnt\\_Qust.pdf](https://sdp.mastercardintl.com/pdf/758_PCI_Self_Assmnt_Qust.pdf)
- VISA Security Information web site:  
<http://www.visa.com/cisp>
- Managing Sensitive Data Initiative web site:  
<http://lct.msu.edu/security>
- Ambiron TrustWave:  
<http://www.atwcorp.com/>
- [http://www.csoonline.com/read/040107/fea\\_pci\\_pf.html](http://www.csoonline.com/read/040107/fea_pci_pf.html)

# Q&A

A hand holding an American Express card in front of a blurred document with the word 'PAYMENT' visible. The entire image is overlaid with a blue tint.