

# Payment Card Industry A Case Study

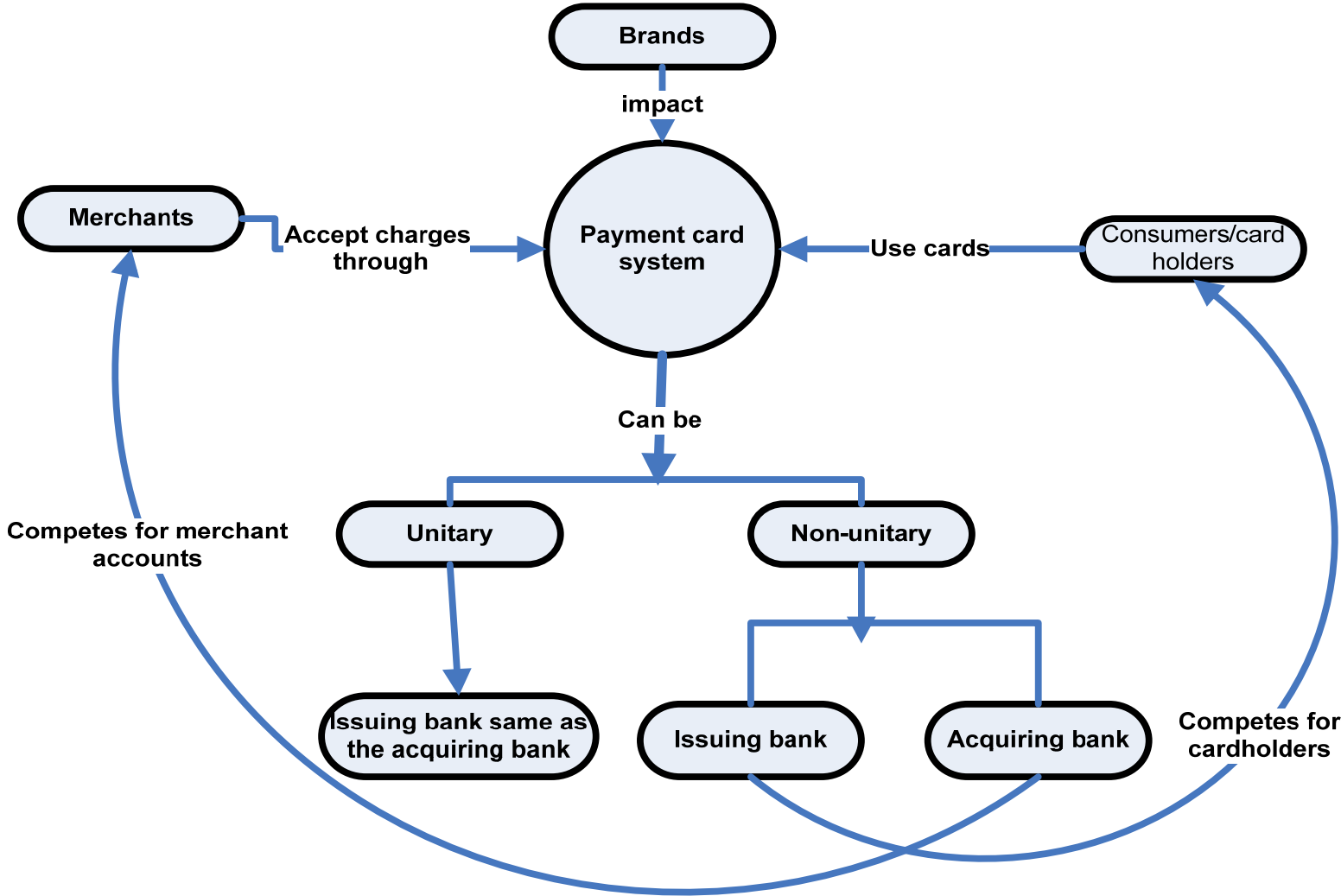
Vasant Raval

[vraval@creighton.edu](mailto:vraval@creighton.edu)

# Payment Card Industry (PCI) Overview

- In 2006, worldwide card usage figures:
  - 2.27 billion payment cards
  - 74 billion transactions
  - \$5.9 trillion (U.S.) in payment volume
  - Visa is dominant player
  - Others include Mastercard, American Express, Discover

# Industry Features



# Industry Thrives on Trust

- Seamless and trustworthy network facilitates demand interrelationships between consumers and merchants.
  - Broad acceptance by merchants facilitates usage
  - Merchant acceptance depends upon demand
  - Industry profits depend on maximizing usage
- Confidence among cardholders
  - Protection from unauthorized charges
  - Protection from consequences of identity theft

# Data Breaches

<b>Year</b>	<b>NotForProfit</b>	<b>Government</b>	<b>Business</b>
<b>2000</b>	<b>1</b>	<b>0</b>	<b>2</b>
<b>2001</b>	<b>0</b>	<b>1</b>	<b>8</b>
<b>2002</b>	<b>0</b>	<b>0</b>	<b>3</b>
<b>2003</b>	<b>3</b>	<b>2</b>	<b>6</b>
<b>2004</b>	<b>8</b>	<b>2</b>	<b>6</b>
<b>2005</b>	<b>82</b>	<b>12</b>	<b>47</b>
<b>2006</b>	<b>127</b>	<b>108</b>	<b>122</b>
<b>2007</b>	<b>142</b>	<b>95</b>	<b>103</b>
<b>2008 (thru Sept.)</b>	<b>58</b>	<b>20</b>	<b>38</b>
<b>Total</b>	<b>421</b>	<b>240</b>	<b>335</b>

# Vulnerabilities of PCI are sourced in:

- An collaborative venture of business partners: merchants, banks, and payment card companies
- Pervasive and constantly expanding
- Global, cross-border presence
- Normally trusted
- But not necessarily secured
- Far too many interfaces and data transfers across systems with varying security measures.

# Threats to Cardholders

- Security breaches threaten consumer confidence and card usage throughout the payment card industry.
- Unauthorized charges within the network are handled through contract via merchant charge backs.
- Outside the network, contract protections are generally lacking; consumers are threatened through unauthorized disclosure of their data.

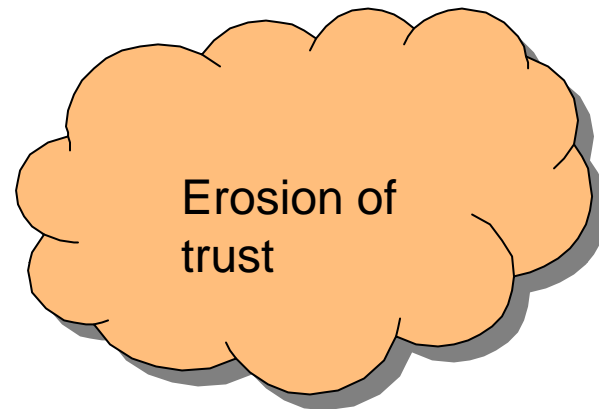
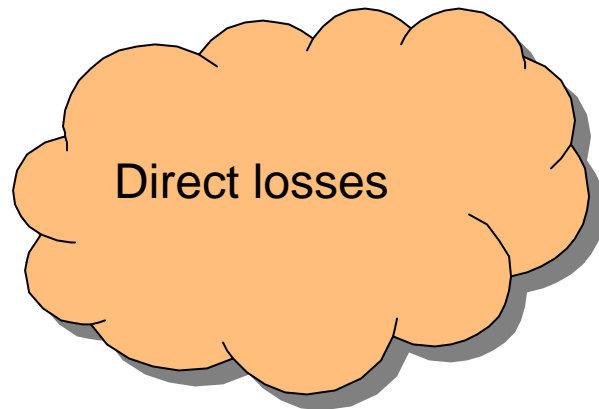
# Confronting Externalized Costs

- The costs resulting from lax security are potentially significant for consumers and businesses.
- Underground exchange services, such as SellCVV2, promote the sale of stolen card data. Organized crime may be involved. *See CLSR Briefing, § 1.15, 24 Computer Law and Security Report 292 (2008).*
- Who will bear these costs?

# Inadequate Merchant Incentives

- Merchants (Payees) do not naturally bear all the costs of their own lax security.
  - E.g., University disclosing card information unlikely to experience tuition losses.
  - Costs shifted to other businesses (perhaps those with card-not-present operations) and perhaps ultimately to other consumers.
- Returns for investments in security are indirect and uncertain.
  - Are consumers sufficiently sensitive?

# Mitigating Threats



Dissipating these threats:

LAW	PRIVATE ORDERING
Security/Privacy rules	PCI DSS
Disclosure	Monitoring
Legal remedies	Enforcement

# Legal Measures

- The U.S. lacks comprehensive legal protections for consumer privacy and security
- Attempts to legislate are fragmented
- Keeping the law current with payment industry's technological innovations presents a major challenge

# Legal Approaches

U.S. lacks a comprehensive data privacy framework.

There is no single law, statute, or regulation that governs a company's obligations to provide security for its information. Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement actions, as well as common law fiduciary duties and other express and implied obligations to provide “reasonable” or “appropriate” security for corporate data.

Source: Thomas J. Smedinghoff, It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law, Michigan State J. of Int'l Law, I, 10 (2007).

# Varying legal approaches include:

- Segment specific legislation (e.g., banks, health care)
- FTC enforcement efforts directed at “unfair practices”
  - Privacy as a subset of security
  - FTC has a general basis for discretionary intervention
  - But only 20 complaints have been investigated out of thousands of data breaches
- State-specific privacy and security-breach disclosure provisions
  - Enacted in more than 40 states
  - State privacy laws provide general requirements for *reasonable* security
  - Limited jurisdiction on a netcentric problem
- Common-law claims, such as tort

# Private Ordering

- Represented by PCI Data Security Standards (DSS)
- The development of PCI DSS is led by payment card brands
- Somewhat collaborative due process to set standards
- Rooted in economic incentives

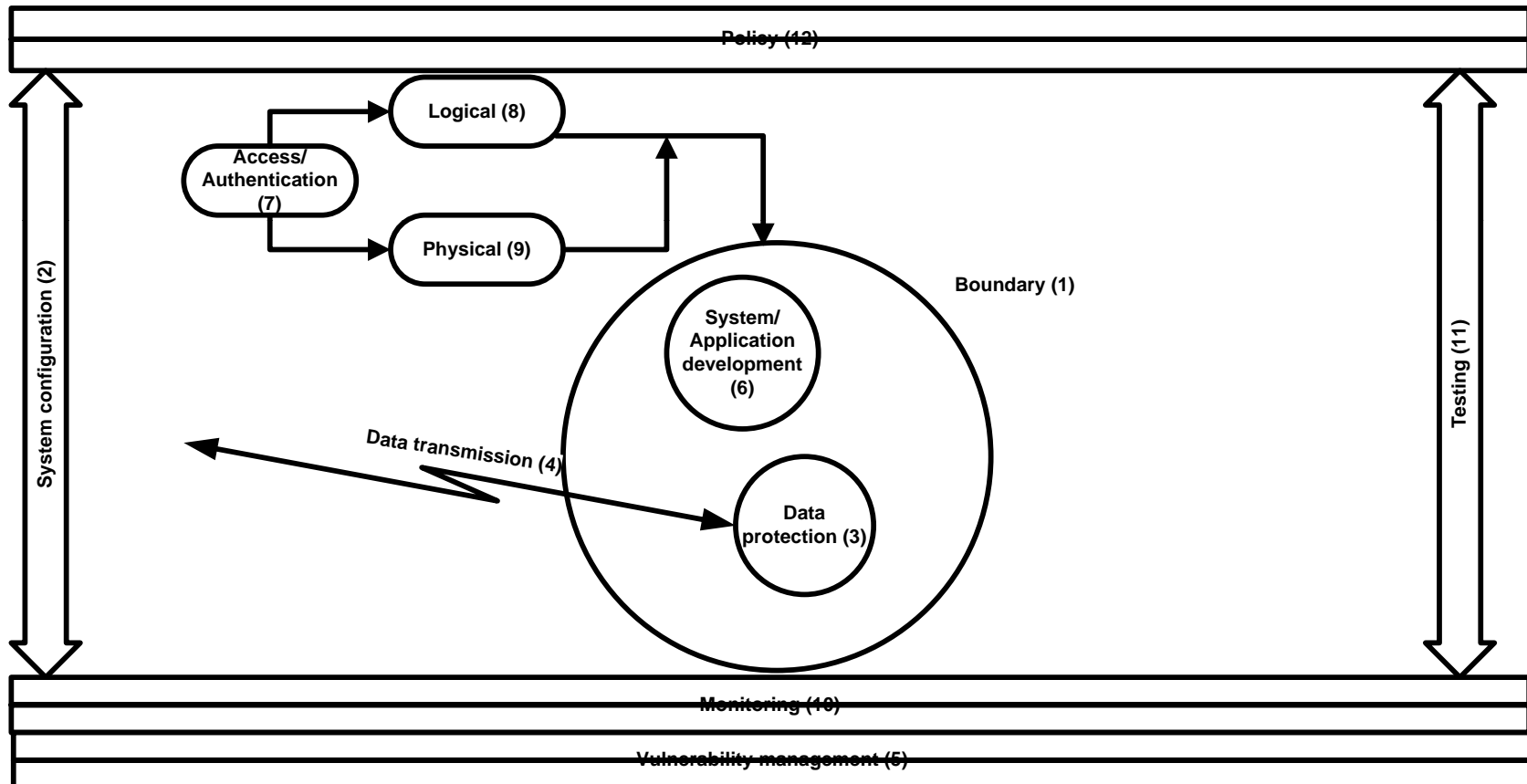
# PCI DSS

- Agreed upon by affected parties
- Currency of practices and procedures to limit/avoid data breaches (compared to the legal requirements)
- Cost effective
  - Requirements are aligned with risk, as measured by volume and complexity of the environment
  - Tiers are defined based on the risk criteria
- Assessment requirements

# Private Ordering through Standards: PCIDSS

- Network relationships within the Payment Card Industry lend themselves to an alternative solution, which is based on contractual relationships within the industry.
- Consumer protection also results from industry pursuit of its own self-interest in security.

# PCI DSS: A Systemic Overview



# Economic Incentives Driving PCI DSS

- Consequences of failure are non-trivial
  - Branding, post-breach consumer behavior/reaction
- Cleanup costs are sizable, and could ruin a perfectly viable business
- Cooperation across systems and processes owned by different legal entities

# Economic Justification

Level	Definition, based on annual volume of Transactions	Compliance requirements	Possible economic justification
1	Merchants with more than six million card transactions. Includes merchants from whom card data have been compromised.	Annual assessment by a certified assessment firm and quarterly network scans.	Market-wide exposure; widespread impact of a breach; cost of correction; penalties
2	Merchants with between one and six million card transactions.	Annual self-assessment and quarterly network scans.	Cost-sensitive monitoring, potentially smaller economic impact of a breach; lesser brand exposure
3	Merchants with between 20,000 and one million card transactions.	Annual self-assessment and quarterly network scans.	Cost-sensitive monitoring; focus on better procedures
4	All other merchants.	Annual self-assessment and annual network scans.	Training and education. Focus on merchant awareness

# Enforcing the Standards

- Limits of Contract
  - PCI-SSC has no authority to enforce.
  - Each card network is responsible for its own enforcement standards.
  - Privity issues: e.g., merchant contracts with acquiring bank, who contracts with Visa. Visa imposes fines and penalties on acquiring banks with noncompliant merchants, who pass those costs along
  - Are consumers third-party beneficiaries?

# Enforcing the Standards

- Who will Monitor?
  - Qualified Security Assessors (QSAs) are trained and credentialed by PCI-SSC.
  - QSAs address larger merchants
  - Self-assessment questionnaires address smaller merchants
  - Standards may nevertheless be interpreted differently by different card brands – how will merchants address variations?

# Practical Constraints

- Industry protections address largest merchants first.
- Smaller merchants get less protection; do they present greater risks for consumers?
- Even standards are not fool-proof if implementation is inconsistent or intermittent (e.g., TJX breach occurred despite certification of compliance)

# Selected Future Issues

- Will laws develop to codify risk-bearing for data security breaches? Who will bear those costs?
- Would merchant disclosure of PCI DSS compliance improve consumer protection?
- How will auditors take into account liability concerns for PC data security breaches? How about corporate boards? (Issues of financial vs. nonfinancial impacts)
- Influence of PCI DSS on global standards (and vice versa).
- Application of PCI DSS concepts to other payment system environments (e.g., virtual worlds, mobile payment systems, e-z pass systems, etc.)