

# Information Security Policy in the U.S. Retail Payments Industry

Mark MacCarthy  
Communications Culture & Technology  
Georgetown University  
June 2010

# Agenda

- Information Security Externalities
  - System externalities
  - Liability rules
- PCI Data Security Standard
- Current Public Policy Issues
  - FTC Unfairness Authority
- System Upgrades
  - Chip and PIN

# System Overview

- Payment system
  - Financial institutions
  - Merchants
  - Networks
- Transaction flow
  - Relevant card details
  - Role of security code
  - Counterfeit cards

# System Externalities

- Static authentication
- Weakest link vulnerabilities
  - Vulnerability at any node
- Centralized, not end-to-end system
  - Nodes cannot upgrade system security on their own
  - Innovation needs to come from system operator

# Liability Rules

- Federal statute
  - Protects cardholders
- Industry practice
  - Liability to issuing bank
- Costs of breaches are not borne by the breached entity

# Misaligned Financial Incentives

- Merchants and processors can create vulnerabilities for others in the system
- They do not pay the full costs of data breaches
- Insufficient incentive to invest in information security
- Security precautions will not be optimal

# Data Breaches

- BJs - 2004
- DSW - 2005
- CSSI - 2005
- TJX - 2007
- Hannaford -2008
- Heartland -2009

# PCI

- Standard
- Validation
- Compliance



# Standards

- Storage of security codes prohibited
- Install and maintain firewalls
- Encrypt data transmitted over public networks
- Layers of security

# Validation

- Certification that a system is in compliance
- Role of assessor

# Compliance (End of 2009)

- Largest merchants
  - 94- 96% had validated compliance
  - 100% compliance with rule against storing prohibited data
  - 63% of Visa volume
- 5 million small merchant compliance is “moderate.”

# Public Policy

- Private cost recovery
- Cost recovery legislation
- Specific security legislation
- Data breach notification
- FTC Unfairness authority
- Generic security legislation

# Dissatisfaction

- Merchant resentment
- Financial institution concern
  - Law suits
  - Lobbying to shift costs to merchants
- Substantial discussion of upgrades

# Upgrades

- Cost benefit test
- End to end encryption
- Chip and PIN
- Static data creates widely distributed vulnerability at millions of nodes

# Chip and PIN

- Dynamic authentication
- Devalues previously used authentication information
- Adopted in Europe and UK
- Adoption on track in Asia, Canada, Latin America
- Uncertain timing in US

# Results

- UK results suggest marked improvement on counterfeit fraud at point of sale in UK
- Increase in fraud abroad
  - Cards are backwards compatible for use with magnetic stripe terminals abroad
- Increase in Internet fraud



# Process

- Public private partnership to guide transition
- Liability shift
  - Liability moves to party that implements chip and PIN late
- Interchange incentive

# United States

- Ellen Richey: the right long-range goal is to make data unusable by criminals – reducing the incentive to steal it.
- Work with agencies and private associations to guide details of upgrade