Identifying Security Issues in the Retail Payment System

Federal Reserve Bank Chicago

Ellen Richey

Chief Enterprise Risk Officer

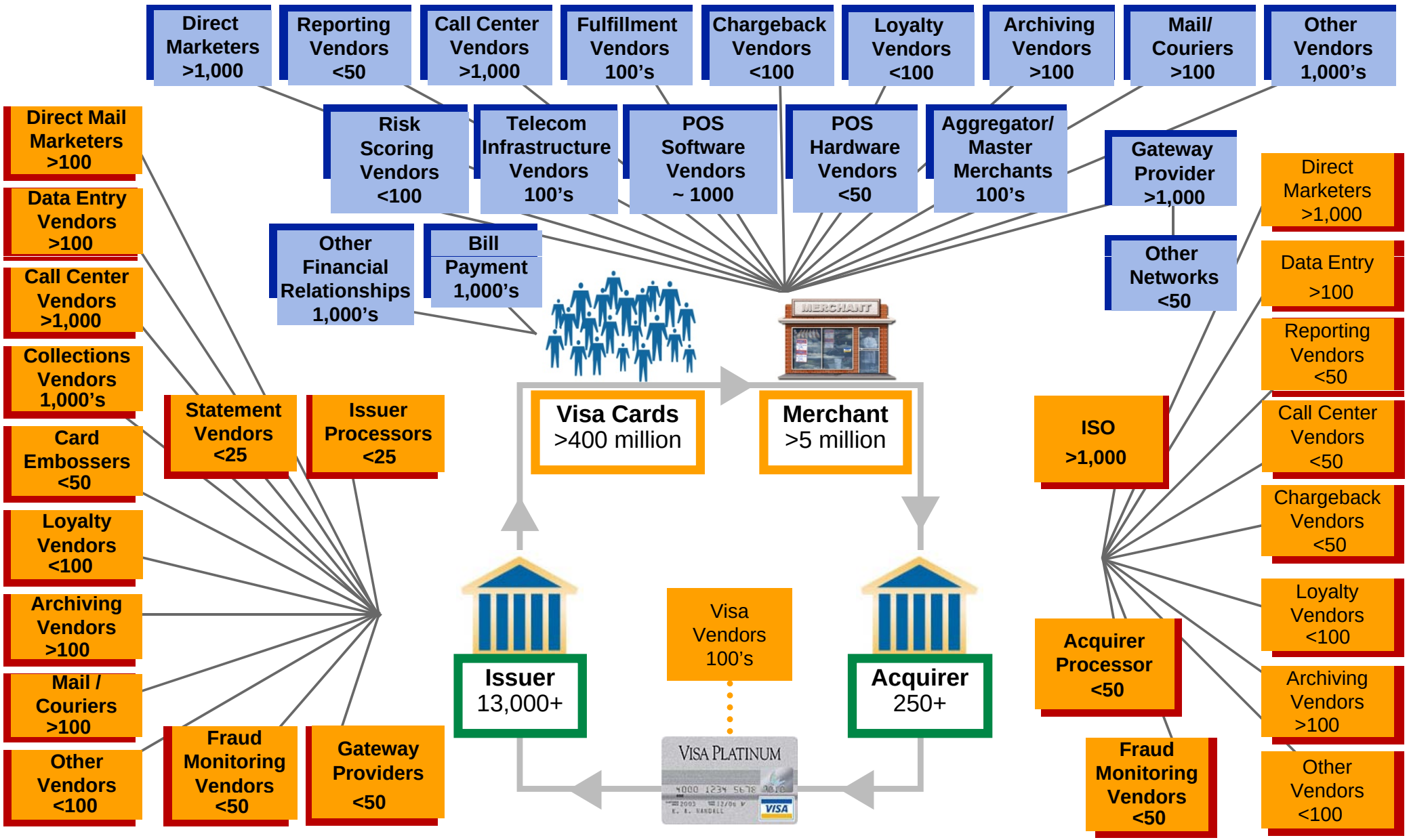
Visa Inc.

June 5, 2008

Agenda

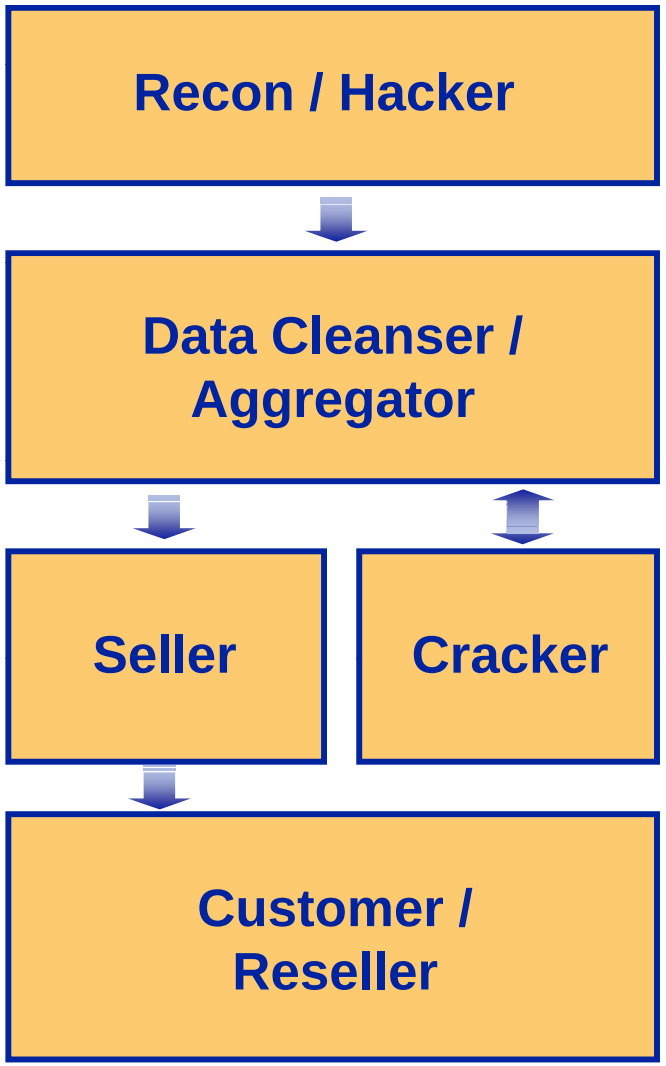
1. The Data Security Landscape
2. Recent Trends
3. Visa's Strategy
4. Working with the Public Sector

Complex Payment Landscape



Visa Inc. and Visa Europe

Sophisticated and Organized Criminals



Estimated market value of compromised accounts*

Account number and CVV2	Classic track data	Gold/Plat/Corp track data
		
No Plastic	No Plastic	No Plastic
$1	*$15*	*$30*

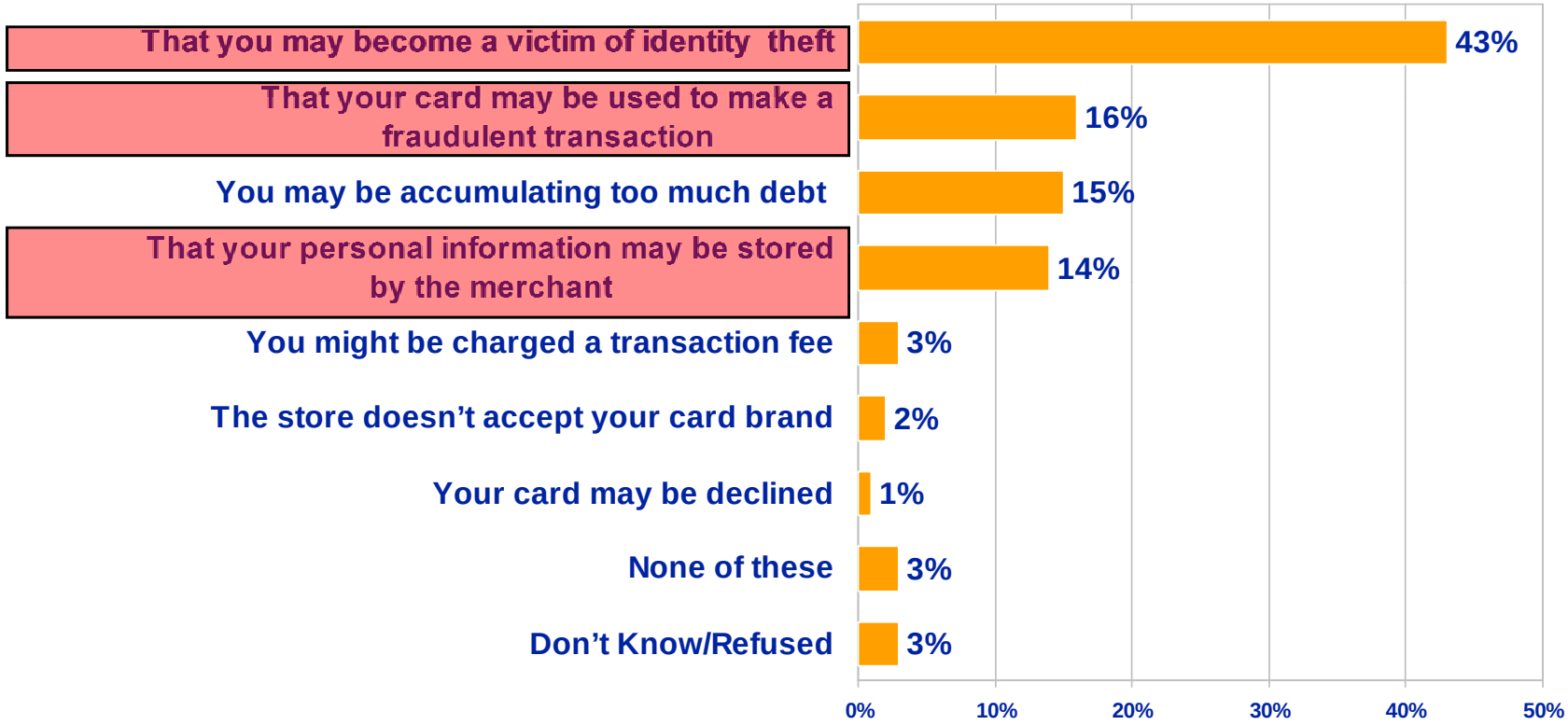
Semi-finished blank plastic	Complete counterfeit Gold plastic	Track data and PIN
		
White-Plastic	Finished	Finished
$80 - $100	*$250*	*$1,000***

**Source: The United States Secret Service*

***Typically track data and PIN not for sale; profit share arrangement amongst criminals; estimated criminal profit per card*

Cardholder Concerns About Card Use

Security and protection of personal information now tops consumer concerns…Despite concerns, Visa cardholders recognize they are protected from fraud



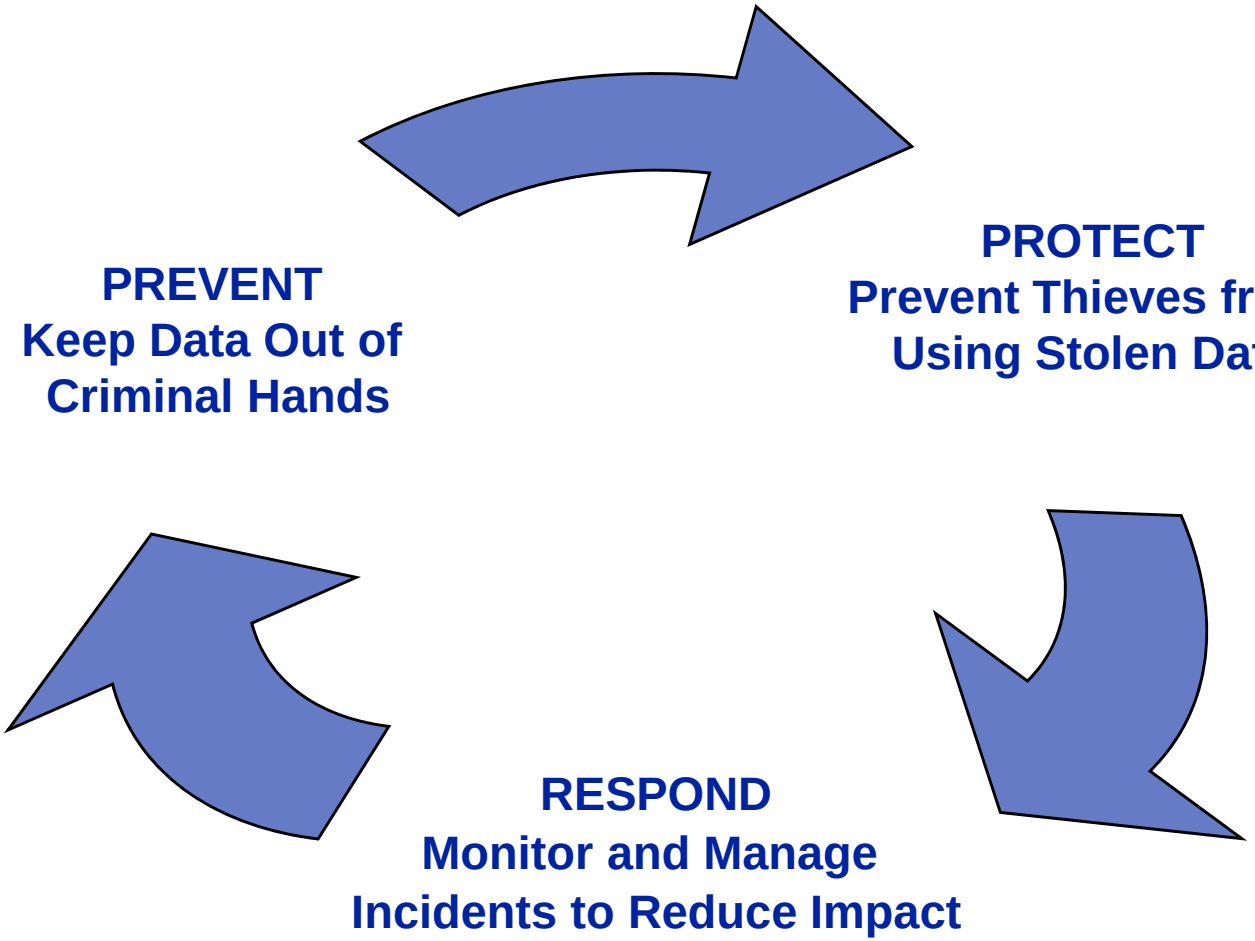
Source: Security and Fraud: National Survey of Cardholders, Fabrizio, McLaughlin & Assoc., Dec 2007

Recent Trends

- **The number of compromise incidents in the U.S. is rising**
  - Trend suggests Level 4 merchants targeted
  - Level 1 merchant compromises subsiding
- **Incidents outside the U.S. are also increasing**
- **But global fraud rates have remained stable since 2002**
  - Visa and system participants have been more effective at combating fraud
  - Mix of fraud is changing
    - Lost and Stolen is on the decline
    - Counterfeit and Card-Not-Present are now category leaders

Visa's strategy

Maintain Trust in Visa Payments



Partner with Clients & Stakeholders

Top System Vulnerabilities

Vulnerability	Remediation Efforts
Storing prohibited data (Track, CVV2, PIN)	***PCI DSS; PCI PA-DSS, PCI PED, PIN Security Requirements*** **Delete stored data; prevent future storage; replace vulnerable software**
Out of date security / systems patches	***PCI DSS, PCI PA-DSS*** **Establish policies, procedures and processes for maintaining and updating systems that handle sensitive data**
Inadequate perimeter security	***PCI DSS*** **Execute disciplined firewall policy management and network security; conduct routine penetration tests of all systems**
Weak wireless security	***PCI DSS*** **Utilize strong encryption to protect wireless environments**
SQL injection attacks	***PCI DSS*** **Conduct regular testing of susceptibility to SQL injection utilizing automated tools or manual techniques**

Working with the Public Sector

- **Public Officials:**
  - Consistent public policy to effectively and efficiently secure the payment system
  - Data security legislation with reasonable security requirements, risk-based notifications, and national uniform standards
  - Global law enforcement initiatives to prosecute criminal organizations

- **Visa:**
  - Education and training for public agencies, regulators, and law enforcement
  - Investigative support for law enforcement and other stakeholders

Final Thoughts on Security

Protecting the payment system is a shared responsibility for all payment system participants

Everyone has an important role to play:

- **Issuers**
- **Acquirers**
- **Merchants**
- **Cardholders**
- **Processors**
- **Third Party Agents**
- **Public / Government Officials**
- **Law Enforcement**