Nonbanks in the Payments System

Presentation to the
Strategic Payments Forum
April 23, 2008

Richard J. Sullivan
Federal Reserve Bank of Kansas City

Outline

- Government oversight nonbanks in retail payments
- Where are nonbanks in payments, what are the risks, and how bad are they?
- Risk management in retail payments
- Options for improvement
- Discussion

Scope of government oversight of nonbank payment participants

- Regulation over competition, consumer protection, data security, safety and soundness, and legal requirements
- Nonbanks and banks are not treated equally in terms of safety and soundness, and data security
  - Many nonbank payment providers overseen as money transmitters
  - Retailers subject to oversight by FTC
  - Some payment processors are supervised
    - Most are large processors
    - Many payment processors are not supervised

Supervision of Nonbank Payment Providers

- Nonbank payment providers are one example of technology service providers (TSPs) of financial institutions
- TSP supervision
  - Conducted jointly among federal agencies
  - Two programs: regional and national
  - National program
    - Multi-district Data Processing Servicer (MDPS)
- Primary purpose: service to bank examiners

Business Lines Offered by Supervised Technology Service Providers

| | Bank affiliation status | | | | | |
| | All TSPs | | Nonbank | | Bank affiliated | |
Business Line	N	Percent	N	Percent	N	Percent
Core processing	68	54.6%	37	44.6%	31	73.8%
Any payments-related business line	87	69.6%	55	66.3%	32	76.2%
Other business line	21	16.0%	19	22.9%	2	4.8%
Total number of TSPs	125		83		42	

Notes: Year-end 2004. Percentages add to more than 100% because a TSP may offer several lines of business

Retail payment risk metrics

- Most available data concerns fraud
  - Data breaches
  - Identity theft
  - Payments fraud
    - Channel oriented (ACH, credit/debit cards)
    - Industry oriented (AFP, ABA, CyberSource, Dove/Pulse)
- Little or no systematic data on non-fraud related operational risk, illicit use, compliance risk
- Little or no information on sources of risk

Records Compromised in Publicly Reported Data Breaches
U.S., Monthly, April 2005-March 2008
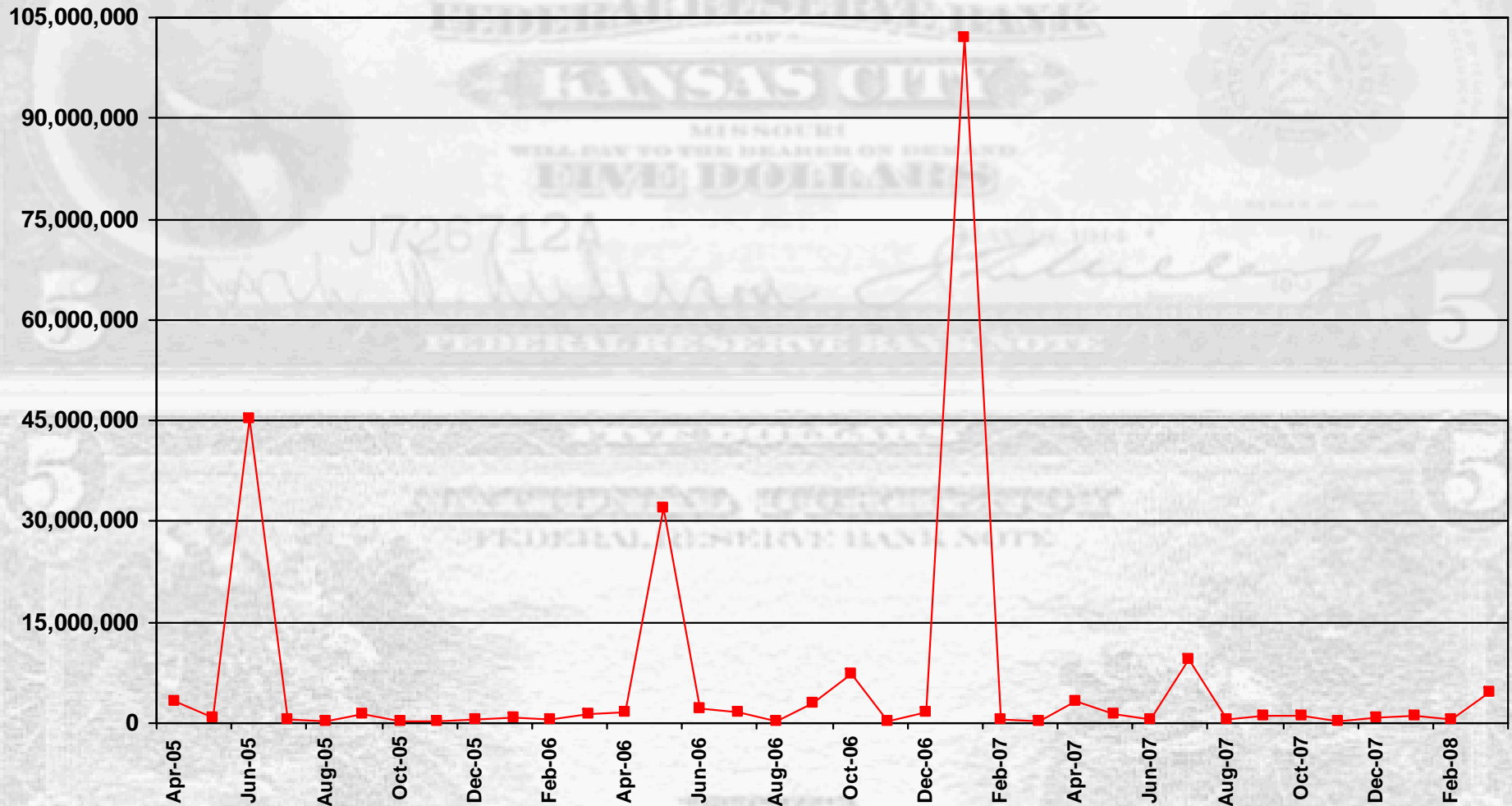
Source: Privacy Rights Clearinghouse website and author calculations.

Number of Publicly Reported Data Breaches
U.S.,Monthly, March 2005-March 2008

Number of states implementing breach notification laws:
21 through May 2006, 19 additional June 2006 to March 2008
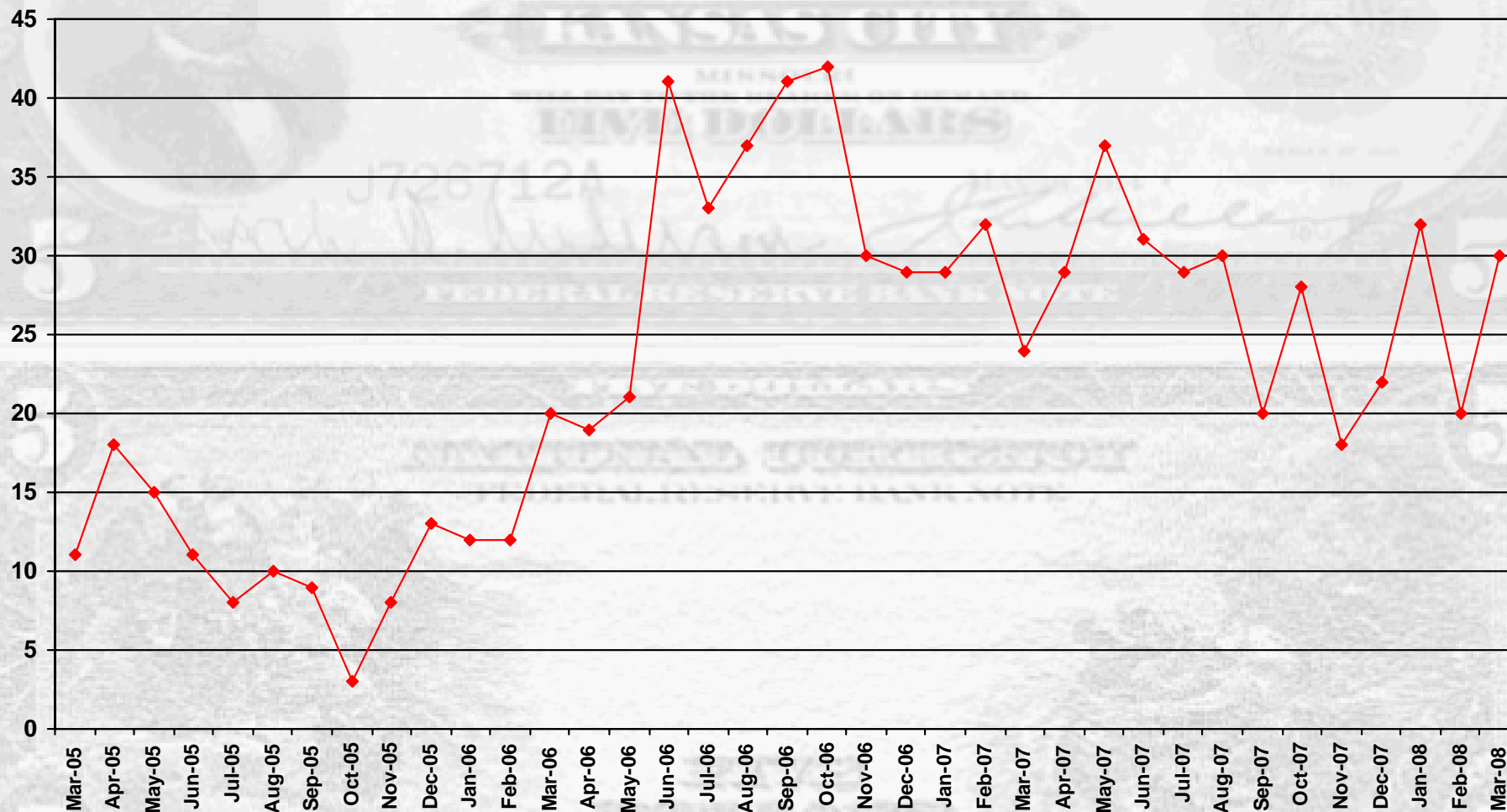
Sources: Privacy Rights Clearinghouse website; Perkins Cole law firm; author calculations.

Industry Sources of Data Breaches

U.S., April 2006-March 2008

	Incidents	Records
Banks and Credit Unions	5%	4%
Nonbank payment processors	2%	21%
Insurance and Fin. Services	6%	2%
Education	28%	2%
Retail and Commerce	18%	49%
Medical	11%	1%
Government	24%	19%

Source: Privacy Rights Clearinghouse website and author calculations.

Where are risks and how bad are they?

- Nonbanks are important for many elements of payments
  - How important?
- More risk: operational (disruptions, security, fraud) compliance, illicit use
  - How much?
  - Where?

Payment Activities and Selected Risks

Primary Activity		Subactivity	Liquidity	Credit	Settlement agent credit risk	Malfunctioning and/or other operational problems	Data security risk associated with fraud or violations of privacy responsibilities	Counterfeit and associated fraud	Compliance	Illicit use (AML, terrorist financing)
Activity			**Type of Risk**							
			Liquidity and Credit			Operational				
Pre-Transaction										
1 Customer acquisition	a	Registration and enrollment of customers as payers (consumers)		x			x		x	x
	b	Registration and enrollment for merchant accounts or deployers of ATMs	x	x			x		x	x
2 Services for issuer's front-end customer (payer) acquisition	a	Provision of credit evaluation/credit risk assessment tools		x		x	x			
	b	Application processing services				x	x			
3 Provision of payment instruments/devices to the front-end customer (payee or payer)	a	Card issuance, card production; card personalization; card delivery; card activation				x	x	x	x	
	b	Hardware and software production (such as a card reader) for usage with a consumer's online device (PC, mobile, handheld)				x	x		x	
	c	Provision of e-money wallet / access code to e-money values					x			
	d	Cheque manufacturing				x	x	x		
4 Provision of hardware to accept payment instruments/devices	a	Provision of ATM terminals (sell/lease; manage)				x	x		x	
	b	Provision of POS terminals				x	x		x	
	c	Provision of cheque readers/cheque POS terminals				x	x			
5 Provision of software to accept payment instruments/devices	a	Web hosting services				x	x		x	
	b	Provision of shopping cart software				x	x		x	
	c	Provision of software to connect payment gateway service providers				x	x		x	
	d	Provision of cheque verification software				x	x	x		
6 Provision of internet security-related technology/support	a	Certificate-authority services (such as PKI-based secure environments); provision of digital identity services for consumer authentication					x		x	
	b	Provision of online transaction security systems to front-end customers (payees, merchants...), and back-end customers (such as 3D-secured card transactions via internet)				x	x		x	
	c	Provision of e-signatures and other e-authorizations for payment authorization purposes				x	x		x	
7 Payment Card Industry (PCI) compliance services to merchants and/or payers	a						x		x	
8 Provision of data center services to back-end customers	a	Outsourcing complete data center functions/secured, supervised floor space/multi-site backup storage for disaster recovery				x	x		x	
9 e-invoicing	a	Creation and delivery of electronic invoices to front-end customers (payer)				x	x		x	
During-Transaction Stage 1										
10 Communication connection for merchants	a	Provision of gateway to acquirer/payment processors; a front-end service				x	x		x	
	b	Provision of gateway to various networks/check or ACH authorization vendors; a front-end service				x	x		x	
11 Transaction authorization (fund verification)	a	Provision of network switch services; a back-end service				x	x		x	
	b	Provision of communication connection between networks and payment instrument issuers; a back-end service				x	x		x	
	c	Provision of decision management/fraud screening/neutral network scoring system to card issuers for authorization; a back-end service		x		x	x			
	d	Process to verify and confirm if payer has sufficient funds (or credit lines) available to cover the transaction amount; a back-end service		x		x	x		x	
12 Fraud and risk management services to front-end customers (payees)	a	Verification services (address, IP address, card verification number, other data), Payment instrument authentication and authorization services		x			x		x	
	b	Identity authentication					x		x	
	c	Decision management/fraud screening/neutral network scoring system (hosted at third-party service providers)					x	x		
13 Fraud and risk management services to card issuers	a	Monitoring transactions and notifying cardholders of potential fraud, enabling them to take immediate action					x		x	
14 Initiate the debiting of the front-end customer's (payer's) account (during transaction)	a	Debiting the front-end customer's (payer's) account / e-money purse; a back-end service	x	x		x	x			
15 Ex-ante Compliance services	a	Anti-money laundering and terrorist financing regulation such as controls to identify suspicious transactions (database, software, and so on)							x	x

Payment Activities and Selected Risks (cont.)

	Primary Activity		Subactivity	Liquidity	Credit	Settlement agent credit risk	Malfunctioning and/or other operational problems	Data security risk associated with fraud or violations of privacy responsibilities	Counterfeit and associated fraud	Compliance	Illicit use (AML, terrorist financing)
	Activity			**Type of Risk**							
				Liquidity and Credit			Operational				
During-Transaction Stage 2										
16	Preparation	a	Sorting merchant's sales information by payment instrument/network for clearing				x	x		x	
		b	Submission of sales information to each payment instrument network				x	x		x	
		c	Calculation of each network member's (either financial institution or processor) net position and transmission of net position information to each member				x	x			
		d	Provision of transformation services into other payment instrument formats (such as MICR to ACH)				x	x			
		e	Provision of sorting transactions by destination groups to Fis				x	x			
17	Clearing	a	Transmission of clearing orders (credit transfers,, direct debits, cards, cheques) to a financial institution				x	x			
		b	Transmission of clearing orders to ACH operator				x	x			
		c	Distribution of advices showing the amounts and settlement dates				x	x			
		d	Clearing (different from an ACH)				x	x			
18	Settlement	a	Posting credit and debit at each financial institution's central bank account	x	x		x				
		b	Posting credit and debit at each financial institution's commercial bank account	x	x	x	x				
		c	Posting debit (credit in case of a return) to front-end payer account	x	x	x	x				
		d	Posting credit (debit in case of a return) to merchant (payee) account	x	x	x	x				
		e	Check settlement	x	x	x	x				
Post-Transaction										
19	Statement	a	Provide statement preparation/delivery services for front-end customers (payers) (such as mobile credit advice or online bank/card account statements)				x			x	
		b	Provision of statement/payment receipt notification services for merchants (payees)				x			x	
20	Reconciliation, incl. collection and receivable management services	a	Matching invoices and payments				x	x		x	
21	Retrieval	a	Provision of chargeback and dispute processing services				x	x			
22	Reporting and data analysis services	a	to merchants, such as support services for treasury and accounting					x			
		b	to consumers					x			
		c	to financial institutions					x			
23	Ex post Compliance services	a	Compliance with anti-money laundering and terrorist financing regulation, such as reporting to authorities, back-feeding to ex-ante databases					x		x	x

Notes: Yellow shading of table cells indicate activities and components of settlement risk.
Data security risk is associated with the online environment.
Counterfeit and associated fraud is limited to physical payment instruments (checks and payment cards) used in an offline environment.

FRBKC, ECB, "Nonbanks and Risk in Retail Payments," ECB/Bank of England Conference Proceedings, November 2007.

Risk management in retail payments

- Pricing, insurance, containment
  - Pricing and insurance weakened by imperfect information and moral hazard
  - Payment industry relies heavily on containment
- Industry self-regulation
- Legal recourse
- Government policy

Options for improving risk management in retail payments

- Improve industry ability to manage risk
- Strengthen supervision
- Coordinate risk management across the industry
- Collect and analyze useful information

Questions

- Growth of nonbanks in payments
- Competition: disruption, advantages/disadvantages, level playing field
- Nonbanks and safety of payments
- Adequacy of oversight system in retail payments
  - Potential for industry self-regulation
- Methodology: payment activities, importance/risk of nonbanks, bank/nonbank risk if performing similar activities

Summary and Discussion

- Regulatory safeguards are in some cases designed assuming payments safety depends on banks only, what might be termed "legacy regulatory structures."

- There is a need for increased coordination and cooperation

  – Among banks and nonbanks within the industry.

  – Among bank and nonbank regulators/authorities

  – Among industry participants and regulators/authorities

  – At the international level.

References and Contact Information

Contact information

Richard J. Sullivan
Research Department
Federal Reserve Bank of Kansas City
1 Memorial Drive
Kansas City, MO 64198
816-881-2372
Rick.J.Sullivan@kc.frb.org

References

Bradford, Davies, Weiner, *Nonbanks in the Payments System*, FRBKC Book, 2003.

Bradford, Weiner, "Who's Processing Your Payments?" FRBKC *Briefing*, August 2005.

Sullivan, "The Supervisory Framework Surrounding Nonbank Participation in the U.S. Retail Payments System: An Overview," FRBKC Working Paper, April 2006.

Sullivan, "Risk Management and Nonbank Participation in the U.S. Retail Payments System, FRBKC *Economic Review*, 2nd Quarter 2007.

FRBKC, ECB, "Nonbanks in the Payments System: European and U.S. Perspectives," FRBKC Conference Proceedings, May 2007.

Sullivan, Wang, "Nonbanks in the Payments System: Innovation, Competition, and Risk—A Conference Summary," FRBKC *Economic Review*, 3rd Quarter 2007.

FRBKC, ECB, "Nonbanks and Risk in Retail Payments," ECB/Bank of England Conference Proceedings, November 2007.

Braun, McAndrews, Robards, Sullivan, "Understanding Risks Management in Emerging Retail Payments," *Economic Policy Review,* Federal Reserve Bank of New York.

Website

http://kansascityfed.org/home/subwebs.cfm?subweb=9