Risk Management and Nonbank Participation in the U.S. Retail Payments System

By Richard J. Sullivan

The retail payments system in the United States has changed significantly in recent years. Advances in technology have caused a greater reliance on electronic payment networks. And the industrial structure of the payment services industry has evolved, as more and more nonbanks deliver payment products to end users and supply back-end processing. In general, these changes have made the payments system more efficient and given more choices to consumers and more payment options to merchants and businesses.

At the same time, however, the rapid pace of change has introduced new risks to the payments system. For example, data breaches appear to be on the rise. Since 2005, 34 states have implemented new laws requiring nonbanks to disclose data breaches.[1] In January 2007, the retailer TJX Companies, Inc., announced that hackers had gained unauthorized access to 45.7 million payment card numbers—the largest data breach in U.S. history (Abelson).

Such recent changes have potentially introduced more risk to the payments system for three reasons. First, as more and more banks market payment services to nonbanks and outsource payments processing, the

---

Richard J. Sullivan is a senior economist in Payments System Research at the Federal Reserve Bank of Kansas City. Nathan Halmrast, a research associate at the bank, helped prepare this article. This article is on the bank's website at ***www.KansasCityFed.org****.*

differences in information possessed by payments participants can magnify difficulties in managing risk. Second, electronic payments have a significantly different risk profile than paper checks. Third, greater complexity of the payments network potentially reduces incentives to manage risk and may cause difficulties in coordinating risk mitigation.

This article lays the groundwork for a dialogue on policy to control risk in the U.S. retail payments system. The first and second sections give an overview of the shift toward nonbank payments providers and electronic payments and how the shift may expose retail payments to more risk. The third and fourth sections review the current supervisory structure over nonbank payments providers and risk management in the retail payments system. The fifth section discusses some of the options policymakers have that could strengthen the management of retail payments risk.

The article shows that while there are new or magnified risks, a substantial amount of private and public effort is directed at controlling risk in retail payments. Risk management by the payments industry is effective, but there are inherent difficulties in market mechanisms that control risk. These difficulties suggest some public involvement is needed to attain a socially desirable level of risk management in retail payments. Both private and public efforts at risk management could be made more effective by some policy adjustments.

The article concludes that a thorough review of supervisory authority relevant to retail payments would be valuable. In particular, the original authority to supervise nonbank payment processors was established over 40 years ago, when the primary reason for establishing that authority was the use of computer technology applied to bank accounting systems. Is that authority adequate given the revolutionary changes in the payments technology seen over the last four decades?

I. THE GROWING PRESENCE OF NONBANKS IN THE U.S. PAYMENTS SYSTEM

At the end of World War II, retail payments were made either by cash or checks. Since then many new options have been added, including credit cards, automated clearinghouse (ACH) payments, ATM machines, online debit cards, offline debit cards, stored value cards, and

online payments. These new choices have given nonbanks opportunities to service the payments process, and nonbanks have often innovated new payment options.

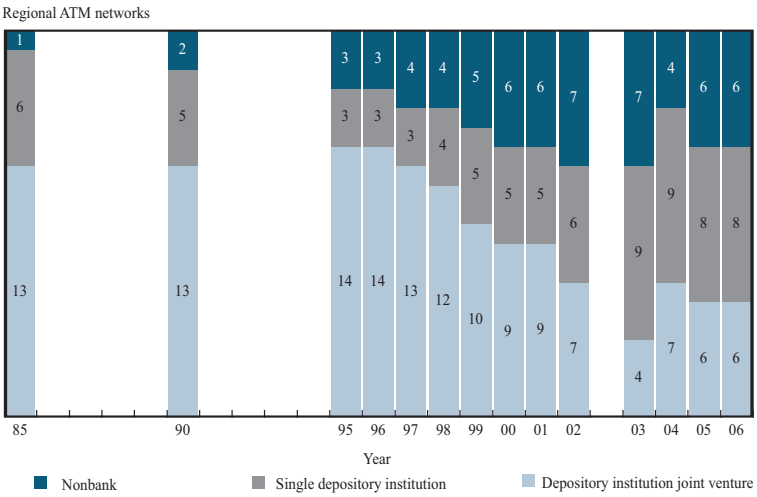
Nonbanks have become increasingly pervasive in both the front-end and in back-end processing of payments (Bradford, Davies, and Weiner 2003). While banks dominate in a number of areas (check processing, clearinghouses, credit card networks, ATMs, issuing of debit and credit cards), most payments activity has some nonbank presence. Nonbanks control virtually the entire market for check authorization and lead in online user authentication. Nonbanks are major suppliers of bank accounting systems and Internet banking software. Nonbanks have a large presence in provision of early-stage payments infrastructure (hardware, software, data processing of accounting systems) and dominate the hardware category. They originate roughly half of ACH payroll deposits. They dominate ACH outsourcing, card-issuer processing, business-to-business information exchange services, Web hosting, electronic bill presentment and payment services, person-to-person payments, retail wire services, money orders, and check cashing services.

Data revealing nonbank trends are scarce, but good data are available on regional ATM networks. Chart 1 shows the ownership information on the top 20 regional ATM networks from 1985 to 2006. Networks are classified as being owned either by nonbanks, single depository institutions, or joint ventures of two or more depository institutions. In 1990, nonbanks owned only two of the top 20 ATM networks. Moreover, as shown in Chart 2, the share of network transactions processed by these two ATM networks was small.[2] Starting in the 1990s control of transactions flowing through ATM networks shifted substantially toward nonbank-owned networks. In 1995 their control was minimal, but today nonbank-owned networks process nearly 60 percent of ATM transactions. The dramatic change is one reason that bankers and policymakers have begun to closely monitor changes in the structure of the payments processing industry.

Another reason that nonbank payment providers have drawn attention is the visible innovation they have brought to the market. The nonbank organizations CheckFree, Yodlee, Tempo, and PayPal have been major contributors to developments in areas such as electronic bill presentment and payment (EBPP), retailer issued debit cards, and online payments.

Chart 1

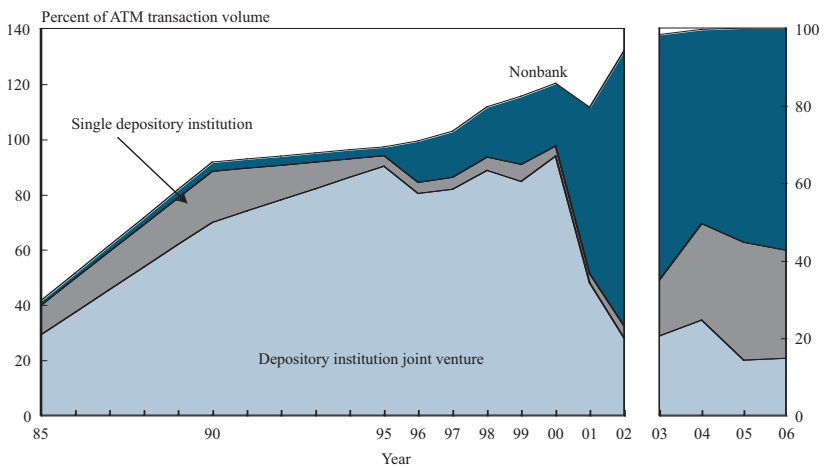
OWNERSHIP OF TOP 20 REGIONAL ATM NETWORKS
UNITED STATES, 1985-2006



Note: Data on ownership for 1986 to 1989 and 1991 to 1994 are not available.
Source: *EFT Network Data Book* (various years)

Chart 2

SHARE OF ATM TRANSACTION VOLUME BY OWNERSHIP OF ATM NETWORK



Notes: The break at 2002-2003 is due to different methods of calculating transaction volume. Prior to 2003, many ATM transactions were counted by more than one ATM network. As a result, measures of aggregate market share could be above 100 percent. Much of the double counting was eliminated for 2003 to 2005.

Source: *EFT Network Data Book* (various years)

While most EBPP is currently done directly on biller websites, growth of EBPP at consolidator sites has been estimated to be twice that of biller sites.[3] CheckFree Corporation is the dominant provider of this service (Wolfe 2006, 2004).[4] Yodlee offers bill consolidation services on behalf of an extensive number of billers and has partnered with America Online to offer EBPP (Ramsaran).

Another recent innovation is the retailer-issued debit card. Tempo Payments, Inc., provides origination and network processing services that facilitate retailer issuance of debit cards. Transactions processed through Tempo are less costly to retailer issuers, in part, because the transaction goes through the ACH network rather than the electronic funds transfer (EFT) network.

Arguably the most visible nonbank that has made major payment innovations in recent years is PayPal, the payments subsidiary of eBay. PayPal dominates the business of person-to-person online payments and has pioneered the provision of payment services to small online retailers. Founded in 1998, it now has 133 million account holders worldwide. During fourth quarter 2006, the value of PayPal's total transaction volume was $11 billion, up 36 percent from fourth quarter 2005.[5] PayPal continues to develop its services and has launched initiatives to offer credit to accountholders and to extend its payment services to retailers beyond the online auction market.[6]

II. IMPLICATIONS FOR RISK IN THE RETAIL PAYMENTS SYSTEM

Nonbanks participating in the payments system and new payment technology can introduce new risks or magnify existing risks in payments.[7] Nonbank participation disperses control of payment access beyond the banking system and exposes financial institutions to more outsourcing risk (Table 1). At the same time, economies of scale in payment services leads to market evolution that can concentrate risk in a few payments participants. Moreover, the network architecture of payments can lead to coordination difficulties and inadequate incentives to manage risk. While examples can illustrate these problems, empirical analysis would be valuable to inform policy on managing payments risk.

Table 1
PAYMENT RISK AND NONBANKS

Source of Risk	Novel Features	Potential Difficulty
Nonbanks in payments	• Access control • Outsourcing and marketing payment services • Concentration	• Fraudulent use of payments • Inadequate data security • Single point of failure • Operational breakdown
Electronic and network technology	• Electronic forms of payment • Open architecture • Large-scale processing • Network systems and rapid development	• Electronic modes of payment fraud • Easy access • Widespread disruptions • Cascading failures • Complex risk management
Interactions of nonbanks and technology	• Simultaneous risk exposure • Conflicts of interest	• Coordination challenges • Inadequate incentives to manage risk • Secrecy

Operational risk in payments can take many forms, such as fraud, exposure of sensitive data, operational breakdowns, single points of failure, and complicated coordination of risk management. The disruptions resulting from these risks are not at the level of systemic risk, where one participant in a settlement process fails to meet its obligations, causing other participants to fail to meet their obligations. But these operational risks can have widespread consequences, and they can be very costly due to the direct consequences of correcting the problem, the opportunity costs of lost economic activity, and the loss of public confidence in established and emerging payments. The Bank of England has called this type of risk *systemwide risk* and has identified it as a major concern in its oversight of the British payments system (Bank of England). While systemwide risk would not be associated with financial market instability, changes in the payments system suggests that large-scale disruptions are more likely than in the past.

Nonbanks and payments

Banks and nonbank payment providers are gatekeepers for the payments system and as such help control payments risk. One difficulty we face today is that access control may be more of a challenge. Established methods of screening and monitoring can prove to be inadequate given the development of new payment types and emergence of new types of

business (such as online retailing). Moreover, this gatekeeping function may be more important than in the past because the stakes are higher. Computer technology can be exploited in a manner that is fast, can be scaled to large values, and can be difficult to detect or trace.

On the simplest level, nonbanks pose risk because they offer alternative points of access for criminals into the payments system. For example, in 2000, two criminals gained unauthorized access to an Internet service provider in the United States and misappropriated credit card, bank account, and other personal financial information of more than 50,000 individuals. They then hijacked computer networks and used the compromised processors to commit fraud through PayPal and the online auction company eBay (U.S. Department of Justice).[8]

More broadly, banks provide nonbanks with access to the payments system either by outsourcing payment processing or by selling payment services. In recent years, the risk associated with such access appears to be more widespread (Breitkopf 2004). In 2005, for example, improper security and record retention practices allowed a data breach at the nonbank credit card processor CardSystems Solutions, Inc., which exposed 40 million cardholder account numbers. An incomplete audit prevented the bank that outsourced card processing to CardSystems from either requiring compliance with appropriate practices or working with an alternative compliant processor (Fest). As a second example, in 2005, the Federal Trade Commission (FTC) banned the Assail Telemarketing Network after it had defrauded hundreds of thousands of customers (FTC). Though not directly involved in the scheme, the bank that sold ACH services to the company agreed to perform appropriate screening of potential ACH clients in the future to help prevent this type of criminal activity (Iowa Attorney General).

Nonbank presence in payments also has implications on a system level. Economies of scale have concentrated key payment services in a few processors. In the United States today, the top three networks process nearly 80 percent of PIN debit transactions (Hayashi, Sullivan, and Weiner). Two of these networks are nonbanks and the third will become a nonbank in the near future.[9] These key payment services now represent potential single points of failure that, if failure does occur, could cause widespread operational breakdowns. Moreover, nonbanks do not have the cushion supplied by the federal safety net. Thus, a significant breakdown

or failure caused by a nonbank payment provider has greater potential for serious consequences than a failure caused by a bank-affiliated payment provider (Hoenig).

Electronic and network technology

Electronic payments—debit cards, credit cards, and ACH transactions—have grown rapidly. Now more than half of noncash retail payments are initiated electronically (Gerdes and Walton 2002, 2005). This trend will accelerate as new methods of using electronic payments are created. While electronic payments offer significant efficiency gains, they also pose a new set of risks compared to those in a paper-check based system because they depend on substantially different technology.

To provide perspective on these risks, it is useful to first review risks associated with checks. Check-based payments have customarily been closed systems. Whether processing is done internally at banks or outsourced, the closed system simplifies control of operational risk because access is limited to those who have paper checks (Lemieux; Office of Technology Assessment). Risk in check processing has largely been confined to returns of individual checks due to insufficient funds or to fraudulent checks (GAO). The potential for operational errors in check processing that would aggregate into large scale disruption is limited because checks require physical handling of individual items. Check clearing systems aggregate to large dollar values at the point of settlement, which is also the point of greatest potential for large-scale disruptions. Control of this risk is simplified by allowing only well-defined, approved parties access to Federal Reserve settlement accounts. Overall, years of experience have led to risks in check-based payments systems that are either well controlled or that pose limited widespread consequences.[10]

Electronic payment processing presents some challenges for risk control that are different from paper-based systems. Online debit transactions, for example, are processed in real time so that it may be impossible to reverse a fraudulent transaction. Moreover, conducting electronic payment fraud does not require a paper check—merely access to a computer and a few bits of information related to a credit card or bank account. One result is that eBay and its payment subsidiary PayPal are top targets of phishers attempting to get victims to reveal credit card or bank information using misrepresented e-mails.[11]

Open architecture typical of today's computer networks increases the risk of unauthorized access, and the scale of a successful hack of a payment database can be enormous. The TJX data breach, for example, was the result of a successful external attack on its computer system (Abelson). While experience has shown that only a small fraction of compromised records are exploited, large-scale data breaches can still cause widespread consequences. This data breach also highlights the role of retailers, a nonbank element of the payments system that is often excluded from discussions of payments system risk.

Operational disruptions in electronic payments can affect many end users. ACH systems process payments in batches that contain large numbers of transactions, which could cause wide disruptions if processing errors occur. A good example is the 2004 software glitch that caused a two-day crash of the U.S. Central Credit Union's network for handling ACH transactions. The disruption delayed thousands of transactions for up to four days (Wade).[12] Nonbanks are also exposed to this type of operational risk. In October 2004, a site redesign crippled some of PayPal's operations, leaving the website unavailable for two days, with intermittent outages for several days thereafter (Wagner). In June 2005, a power outage disrupted CheckFree's EBPP service (CheckFree).

Data security breaches can have similar cascading effects. Data breaches such as those at CardSystems Solutions and TJX have led banks to reissue payments cards. Banks often bear the direct cost of any fraud at points-of-sale or ATMs resulting from data breaches, but consumers can also spend considerable time and expense in protecting their assets and recovering their credit standing. Online merchants, who forgo payment guaranties by accepting card-not-present transactions, must pay the cost when fraudulent transactions are charged back to their accounts.

The network architecture and rapid development of electronic payments provide additional challenges (Bank of England; McPhail). Rapid development of electronic payments technology complicates risk control because new sets of hard-to-determine threats arise with each generation of technology (Kimball). The history of vulnerabilities offers less information, so effective risk control methods need to be more forward looking (McPhail). Payment technology is often complex, requiring banks, nonbank payments providers, and bank regulatory agencies to have sufficient internal expertise to understand, analyze, or implement an effective risk control environment.[13]

Interactions of nonbanks and technology

The trend toward electronic payments can exacerbate the risks posed by nonbank presence in the payments system. Compared to paper-based payments, risk control in electronic payment networks requires a high degree of simultaneous coordination among all participants. While both banks and nonbanks must cooperate, a wider variation in the types of organizations in the network complicates design, execution, and enforcement of security standards.

In addition, the interaction among participants in electronic payment networks generates conflicts of interest that make control of risk difficult. For example, dependence on electronic communications introduces a new set of vendors into payments processing that supply security as well as many interlinking services (website hosting, ISPs, and telecommunications companies). Security incidents at these providers reflect poorly on their services, and they have an incentive to limit the spread of news about any incident. But effective risk control of the payments system requires good information about security breaches, both to warn other participants about specific problems and to design effective mechanisms to control risk. This conflict of interest has motivated recommendations for regulatory mandates for the reporting of security breaches and operational disruptions (Glaessner, Kellerman, and McNevin 2002).

An analysis of recent data breaches

Anecdotal examples are useful for understanding how nonbanks have magnified payments risk. But empirical analysis of data security incidents and operational breakdowns would be particularly helpful to inform decisions about risk management policy for the retail payments system. Table 2 shows an analysis of data breaches that have occurred in the United States from January 2005 to April 2007. The record of incidents was assembled by the Privacy Rights Clearinghouse, which relies on public information sources. They list breaches where information exposed would be useful for identity theft, which often manifests itself in fraudulent use of some type of payment. The information is sufficient to roughly identify the sectors of the economy where the data were compromised.

Table 2

PUBLICLY REPORTED DATA BREACHES IN THE UNITED STATES
JANUARY 2005-APRIL 2007

Sector of origin	Bank and financial services	Nonbank payment processor	Education	Retail	Health care	Government	Other or unknown	Total
			A: Number of incidents					
All incidents	51	16	149	101	51	118	55	541
	9.4%	3.0%	27.5%	18.7%	9.4%	21.8%	10.2%	
Before 4/1/2006	16	6	58	21	14	11	13	139
	11.5%	4.3%	41.7%	15.1%	10.1%	7.9%	9.4%	
After 4/1/2006	35	10	91	80	37	107	42	402
	8.7%	2.5%	22.6%	19.9%	9.2%	26.6%	10.4%	
			B: Records compromised					
All records	6,352,711	40,691,306	4,961,749	61,288,322	1,244,716	35,761,123	3,393,818	153,693,745
	4.1%	26.5%	3.2%	39.9%	0.8%	23.3%	2.2%	
Before 4/1/2006	5,725,850	40,200,526	2,491,827	2,765,590	391,300	960,183	1,227,330	53,762,606
	10.7%	74.8%	4.6%	5.1%	0.7%	1.8%	2.3%	35.0%
After 4/1/2006	626,861	490,780	2,469,922	58,522,732	853,416	34,800,940	2,166,488	99,931,139
	0.6%	0.5%	2.5%	58.6%	0.9%	34.8%	2.2%	65.0%

Notes: Data are based on information collected by the Privacy Rights Clearinghouse and accessed on their website April 8, 2007. Classification by sector of origin and other calculations are by the author.

During this 28-month period, 541 data breaches were publicly reported. Most of the breaches—402—occurred in the second half of the period (after April 1, 2006). We cannot conclude with certainty that the number of data breaches actually increased because numerous new laws on notification were implemented after the middle of 2005, at least partially causing a rise in publicly-disclosed data breaches.

Still, the publicly-disclosed data breaches can be interpreted as revealing one of two undesirable aspects of retail payments risk. Either the 139 incidents reported in the first half of the period significantly understate actual data breaches, or the number of breaches increased rapidly in the second half.

Data breaches compromised nearly 154 million records. Roughly three-quarters of the records were compromised in just three incidents: the large data breaches at TJX and CardSystems, and a data breach reported in May 2006 at the U.S. Department of Veteran's Affairs that compromised 28.6 million records. These three incidents compromised a total of 116 million records. Like many measures of risk, very few incidents can account for a large portion of losses.

Occurrences of data breaches and compromised records do not necessarily go hand in hand. The nonbank payment processor sector accounted for only 3.0 percent of all data breaches but 26.5 percent of compromised records. This sector was responsible for nearly 75 percent of compromised records in the first half of the period. On this data, a reevaluation of public policy towards risk management for nonbank payment processors may be valuable.[14]

The bank and financial services sector accounted for 9.4 percent of incidents and 4.1 percent of records compromised over the entire period. The worst blemish for bank and financial services was the 10.7 percent share of records compromised in the first half of the period. However, the share fell to only 0.6 percent in the second half.

This record may not reflect the true underlying risk associated across the sectors. Federal and state disclosure guidelines are not uniform. If disclosure standards were not equal, then data across sectors or states may not be comparable. In addition, records across sectors may not be equally useful for misuse. Data from the bank and financial services or the nonbank payments processing sectors may be particularly useful in perpetrating payments fraud compared to that of other sectors.

While data breaches in Table 2 suggest an upward trend, the uncertainty of that conclusion illustrates the shortage of good data on payments risk. Information that reflects the outcomes of data breaches suggests that consequences may be limited and trending downward. One analysis calculated the likelihood that exposed identity information is misused at less than one in 1,000 (ID Analytics). Survey data suggest that, from 2003 to 2006, the number of adult victims of identity fraud fell 12 percent (although the average fraud loss per case increased 22 percent) (Javelin Research). Some analysts have argued that fraud relating to these breaches is rare and that most of the cost related to identity theft is borne by businesses (Lindenmayer; Lenard and Rubin). On the other hand, a recent rise in debit transactions charged back to consumer accounts has been attributed to data breaches and at least one report documents a recent rise in measures of internet security threats (Breitkopf 2006a).[15]

In short, nonbank payments participants and electronic payments introduce new risks into the payments system, some of which compound one another. Threats and disruptions to payments are becoming commonplace, and while disruptions thus far have not risen to the level of a systemic problem, numerous disruptions qualify as systemwide disturbances. Data that measure payments risk are limited and must be interpreted carefully, but can be useful to inform policy decisions.

III. REGULATION OF NONBANK PAYMENT PROVIDERS

Public interest in the payments systems has the goal of ensuring safety, efficiency, and access. To achieve this goal, public authorities in the United States consider competition, consumer protection, data security, prudential supervision, and law enforcement.[16] Table 3 describes these areas of concern, their legal basis, and other details of regulation and enforcement. The extent and complexity of public involvement vary across elements of the payments process (from initiation to final settlement), institutional aspects of the payments industry, and the legal issues tied to payments.

The last column of Table 3 shows areas where banks and nonbank organizations are treated equally or unequally. Only in the areas of data security and prudential supervision is treatment unequal, which is

Table 3

PUBLIC REGULATION OF PAYMENTS IN THE UNITED STATES

Area of regulation	Description	Legal basis	Enforcement authority	Regulations or guidelines	Treatment of bank and nonbank organizations
Competition	Competitive implications of mergers, acquisition, and business practices	Antitrust laws	U.S. Department of Justice	Department of Justice Antitrust Division Manual	Equal
Consumer protection	Liabilities and responsibilities in check and electronic funds transfers	State check laws; Electronic Funds Transfer Act of 1978	For checks, state legal authorities; for electronic funds transfer, federal agencies (financial institution supervisory agencies* or the Securities and Exchange Commission according to their jurisdiction) with the FTC covering retailers and other payment participants not covered by other agencies	For electronic funds transfer, the Federal Reserve Board's Regulation E specifies disclosure, payment authorization, transaction record, and disputes resolution requirements	Equal
Data security	Safeguarding and disclosing to customers the use of sensitive nonpublic customer information	Gramm-Leach-Bliley Act of 1999; various federal and state laws concerning unfair and deceptive acts in business transactions	Federal financial institution supervisory agencies*; FTC	Federal Reserve Board's Regulation P and Regulation H (Appendix D2)	Unequal between financial and nonfinancial organizations
Prudential supervision	Periodic examination and ongoing monitoring of the financial health and prudential operation of the institution	Various laws enabling supervision of financial institutions; The Bank Service Company Act of 1962; state laws covering money transmitters	Federal financial institution supervisory agencies*	State and federal guidance provided by supervisory agencies; Federal Reserve regulations covering payments, such as Regulations J (check collection)and CC (check funds availability)	Generally unequal with the possible exception of where banks outsource payment processing to nonbanks
Law enforcement	Efforts to counter trends in illegal data breaches, identity theft, and money laundering	USA Patriot Act of 2001; Bank Secrecy Act of 1970; state law	FBI Cyber Operations group; Secret Service Electronic Crimes Task Force; Department of the Treasury Financial Crimes Enforcement Network; state and local law enforcement	Electronic Crimes Task Force website (*www.secretservice.gov/ectf.shtml*); FinCEN website (*www.fincen.gov/reg_guidance.html)*	Equal

*Federal financial institution supervisors include the Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

largely a result of enabling legislation that applies regulation specifically to financial institutions. This section describes nonbank regulation in the areas of data security and of prudential supervision.

One determinant of the authority to supervise payment providers in the United States is the provider's relationship with a bank. Some payment providers are affiliated with banks, either as subsidiaries or as separate entities in a bank holding company. Some of the largest payments processing operations in the United States are affiliated with banking organizations such as Fifth Third Bancorp, U.S. Bancorp, and JPMorgan Chase. Many organizations that provide or process payments in the United States have no affiliation with a banking company. Among the larger organizations without affiliation are First Data Corporation, MasterCard, and PayPal.

If a payment provider is affiliated, then federal bank supervisors have authority to examine its activities. If a payment provider is not affiliated, then it may or may not be subject to federal supervision depending on whether it has an outsourcing relationship with a bank (Sullivan).[17]

Data security

Federally mandated standards and enforcement for security of payments data can be different for bank and nonbank organizations. The Gramm-Leach-Bliley Act of 1999 set data security requirements for financial institutions and therefore applies to payments data. If a bank outsources payment processing to a nonbank, then the nonbank is subject to the same data security standards as banks. Otherwise, there is no similar federal data security requirement for nonfinancial institutions. To some extent, the FTC has filled this gap by enforcing data security standards for retailers and other organizations. The FTC views breaches of payments data security as an unfair and deceptive business activity. In cases of breaches of payments data, it has reached settlements with firms as diverse as retailers, payment processors, and software developers.[18]

Prudential supervision of nonbank payment providers

Supervision of nonbank payment providers is part of a broader program of supervising technology service providers. The primary focus of this supervision is to protect the provider's bank clients, with a

secondary benefit of protecting the payments system. Supervisory agencies use a risk-based approach that helps ensure that those nonbank payments processors posing the greatest risk are subject to more stringent supervision. But an unknown number of payments processors are not under any supervision. And in cases where inadequate control of risk require enforcement, the enforcement options for nonbanks are weaker compared to those available to bank supervision.

The main purpose of prudential supervision is to ensure financial health and safe operation of an organization. Banks, for example, are regulated and examined, and the historic goal of supervision is to protect depositors by ensuring banks operate in a safe and sound manner. Payments activity is within the scope of examination, which may help manage payment risk, but control of risk in the nation's payments system is a secondary benefit.

Supervision of nonbank payments processors is the responsibility of the same agencies that supervise financial institutions. Authority comes from the 1962 Bank Service Company Act. At that time, computer automation of crucial bank accounting systems and payments processing was growing important. The primary purpose of the act was to provide legislative authority allowing banks to invest in computer service companies. Section 5 of the act confirmed the supervisory authority of federal agencies over bank-owned computer service companies. More important, it made explicit that this authority extended to nonbank-owned servicers.[19]

Today, these service companies are called Technology Service Providers (TSPs). Supervision of TSPs uses resources of federal supervisory agencies but is coordinated by the Federal Financial Institutions Examination Council (FFIEC).[20] A risk-based approach used by these agencies determines the activities covered under the supervision program, the process used to select entities for supervision, and the frequency of monitoring and examination. The FFIEC oversees development of examination guidelines and establishment of uniform rating systems for providers of information system services to banks. It also establishes policy regarding agency responsibility, which TSPs get examined, the frequency of examination, and the scope of supervision.

Early examination of TSPs covered hardware and software associated with general ledger accounting, transaction recording, and check processing, such as transport, capture, and reconciliation. TSP exams subsequently expanded to match changes in technology employed by banks and now include information systems, electronic payments, telephone banking, and Internet banking.

Supervision of TSPs is administered either nationally or regionally (FFIEC 2003b). Those that are nationally administered are in the Multi-Regional Data Processing Servicer (MDPS) program. An organization is considered for the MDPS program when it provides core information system applications for a large number of depository institutions or if it works from a number of data centers located in different geographic regions. TSPs included in the MDPS program are considered to pose systemic risk. Supervised TSPs that service depository institutions from more than one charter class, but are not included in the MDPS program, are administered regionally.

The FFIEC uses a risk-based approach for TSP supervision and examination. The goal of the approach is to aim examination resources at areas of "highest potential risk to...[a TSP's] serviced financial institutions"(FFIEC 2003a). A TSP risk evaluation determines the time frame for examination and monitoring activity and helps identify TSPs that would come under the MDPS program (FFIEC 2003b).

At year-end 2004, 125 TSPs were supervised (Table 4). Both nonbank and bank TSPs are in the program, but twice as many nonbank TSPs are supervised. Core processing (computer processing of general ledger accounting and of information systems), offered by 68 of the supervised TSPs, is the single most important line of business.[21] Compared to nonbank TSPs, core processing is more likely to be offered by bank-affiliated TSPs. Core processing is offered by 73.8 percent of bank-affiliated TSPs but by only 44.6 percent of nonbank TSPs. While core processing is the most common activity, payments are also a focus of supervised TSPs.[22] Nearly 70 percent of supervised TSPs offer at least one type of payment processing service.

The national supervision program tends to focus on payments-related lines of business and on nonbank TSPs. Among the TSPs in the national program, 69 percent are nonbank and 81 percent offer at least one payment processing service. This correspondence could reflect the

Table 4

BUSINESS LINES OFFERED BY SUPERVISED TECHNOLOGY SERVICE PROVIDERS

			Bank affiliation status				Supervision program			
	All TSPs		Nonbank		Bank Affiliated		National		Regional	
Business line	**No.**	**Percent**	**No.**	**Percent**	**No.**	**Percent**	**No.**	**Percent**	**No.**	**Percent**
Core processing	68	54.6	37	44.6	31	73.8	7	43.8	61	56.0
Any payments-related business line*	87	69.6	55	66.3	32	76.2	13	81.3	74	67.9
Other business line**	21	16.8	19	22.9	2	4.8	2	12.5	19	17.4
Total number of TSPs	125		83		42		16		109	

*ACH processing/services, ATM processing/services/network/switch, bill payment service, credit card issuance, credit and/or debit card merchant processing, credit card network/switch, check processing, check processing software vendor clearing and settlement, POS processing/services/network/switch, and wholesale payments.

**Retail e-banking/transactional website hosting, electronic record safekeeping, imaging, loan or mortgage processing/servicing, corporate e-banking/cash management, website hosting (informational), disaster recovery, investment processing, aggregation, asset/liability management, credit scoring, other emerging technologies, employee benefit account processing, asset management processing, bank image processor, debit card "services," Internet services, IRA "services," payroll "services," safe deposit, student loan processor, trust processing services, Visa "services."

Notes: Many TSPs are double counted because they offer core processing, payments, and/or other business lines. As a result, the sum of the number of TSPs in each category is greater than the total number of TSPs, and the sum of percentages is greater than 100 percent. TSPs in the national supervision program are in the MDPS examination program. Other supervised TSPs are in the regional program. Bank affiliation status is determined by a significant ownership position by one or more depository institution, whether run as corporations, limited partnerships, or limited liability companies. A nonbank TSP has no significant ownership by a depository institution.

economics underlying payments processing which may lend itself to a large-scale operation and a nonbank form of organization. Regardless of the reason for the correspondence, it is likely that the resources brought to supervision in the national program are more extensive than in the regional supervision program, commensurate with the greater risk of the payment processors in the national program.

While the largest nonbank payments providers are probably represented in the TSP supervision program, it does not cover all TSPs that offer payments services. For example, after a 2005 security breach at a payments processor, news stories reported the existence of roughly 500 companies that process credit card payments (Dash).[23] But, at most, 87 payments processors were supervised at year-end 2004 (Table 4).

One reason that many nonbank payments providers are not supervised is that the Bank Service Company Act is sufficiently narrow to exclude many significant payment providers. In particular, nonbank TSPs must be in an outsourcing relationship with a bank to be eligible

for supervision. But many payment providers are customers of banks. For example, PayPal or Ceridian Corp. originate many payments and pass that information to banks for further processing.[24] In this instance, the originator is purchasing payment services from the bank. A similar relationship exists between banks and acquirers of point-of-sale transactions or originators of many automated clearinghouse transactions. As such, risk management via direct supervision is currently not an option for these elements of the payments network.

It is important to emphasize that the purpose of TSP supervision is not the survival of the TSP or the viability of its business model (Federal Reserve Board 2000). Rather, the TSP supervision program is targeted as a service to the supervisors of depository institutions. It is useful because examiners of depository institutions have a resource that they can draw upon to understand the risks that an outsourcing relationship might pose for the depository institution. The focal point is the risk to serviced depository institutions. Ultimately TSP examination seeks to ensure that there is a control environment that adequately addresses these risks.

Finally, supervisory agencies can examine nonbank payment providers but have limited enforcement power if they find weaknesses at the organization. Enforcement powers over financial institutions include voluntary agreements, cease and desist orders, removal or prohibition of individuals from an institution or the industry, civil money penalties, termination of deposit insurance, appointment of bank conservators, and divestment of activities (Spong). Enforcement powers over nonbank payment providers include only voluntary agreements and prohibitions on financial institutions from doing business with the service provider.

IV. MANAGEMENT OF RISK IN RETAIL PAYMENTS

Management of risk in retail payments in the United States involves a mix of private and public activity. Market mechanisms and self-interest lead the payment industry to continuously engage in this type of activity. Public intervention in the U.S. retail payments market has been relatively limited because market forces have generally been effective in managing risk.[25] But limitations inherent in market driven management of risk implies that public regulation and oversight also has value.

Industry efforts at risk containment

Traditional market mechanisms, such as insurance and pricing, are important to industry efforts to managing risk in payments. In an attempt to align pricing with responsibility for errors, the National Automated Clearing House Association (NACHA) has proposed return entry fees on ACH originators who initiate unauthorized payments (Digital Transactions). Credit card issuers insure merchants against payment fraud if they follow proper procedures when accepting some payment cards. Insurance can be particularly effective if it reallocates risks to those that can better control the risk. Payment card networks can offer payment guarantees at a reasonable price because a centralized method of detecting fraud is more efficient than having millions of merchants install their own fraud detection systems.

But there are inherent difficulties in pricing and insurance.[26] Appropriate pricing of risk can be impossible without adequate information, and insurance can induce risky behavior. Payment card holders, for example, may not be sufficiently careful because they often do not face any cost if they lose their card and it is used fraudulently. These difficulties have led the payments industry to embrace containment as an approach to risk management. Containment includes such activities as setting standards for data security and operational risk, monitoring for trends in risk and for compliance, and penalizing payment participants for noncompliance. The ultimate penalty is exclusion from the payments system.

Containment can be most effective at a network level, where risk management can be comprehensive to include all participants and where there is some control over membership in the network. Credit card networks have developed the Payment Card Industry (PCI) data security standard, which began a phased implementation in 2005. It sets 12 requirements involving topics such as data encryption, intrusion detection, activity monitoring, and access controls. The standards apply to all card network members, merchants that accept credit cards, and credit card payments processors. Similarly, the NACHA recently created a Risk Management Advisory Group to help implement a new risk management framework (NACHA).[27] Subsidiary work groups are addressing three areas of risk management: control of access to the ACH system, the monitoring and control environment, and enforcement activity.

The payments industry has also established mechanisms designed to foster cooperation across the industry in developing techniques to manage risk and to share information that can assist in fighting fraud. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) was established by the financial services industry in 1999.[28] This private sector initiative allows members to share information about security incidents that represent threats to the U.S. financial infrastructure. By allowing confidential reports of security incidents, FS-ISAC can overcome the reluctance of firms to release information that can damage a firm's reputation. As a result, FS-ISAC can build a large database of security events, which FS-ISAC can analyze to determine vulnerabilities and develop responses to threats in a timely manner (*Cards International*).[29]

Another private industry effort addresses one shortcoming of risk management at a network level. Historically, each payment channel—checks, ACH, EFT networks, and credit card networks—has developed separate standards and approaches to reducing risk. The Partner Group is an private organization sponsored by the financial industry whose goal is to foster cooperation among payment channels and address emerging risks that may cross payment applications.[30] To accomplish its goal, The Partner Group has established three working groups with representatives from each payment channel to address sharing of fraud information, liability assignment among networks, and access of third parties to the payments system.

Risk management by public authorities

Despite diligent efforts, market imperfections such as the presence of externalities can limit effectiveness of industry risk management.[31] Payments participants will manage risk in relation to the private cost and benefit of their effort. But this effort also benefits other payment participants because of the interdependency of risk management in a network environment. This type of externality implies that the sum of the risk management efforts of payments participants may be less than socially desirable. Public involvement may also result in some efficiency gains. For example, small banks have limited ability to monitor their TSP providers, leading some to suggest that there would be value in a

central bank role in developing standards and infrastructure (Lemieux). Most important, trust in the payments system is a public good that warrants attention by public authorities.

As a result, there is a role for public involvement of managing risk in the payments system. Some of these efforts involve setting risk control standards as well as monitoring and enforcing their implementation. In this regard, public authorities are involved in risk containment activities that are similar to industry efforts.

The public sector manages payments risk in a number of ways, most directly by examining the payment activities of banks and supervised TSPs. This can help the financial industry improve data security and enhance resiliency and operational integrity of the payments system. Partly because of limited jurisdiction, other public authorities (such as the FTC and law enforcement) have taken the lead in addressing payments data security outside of the financial industry.

The Federal Reserve System has a number of programs that directly or indirectly manages payments system risk. The Federal Reserve has responsibility to oversee the payments system by monitoring payments systems, assessing them for safety and efficiency, and inducing change when necessary (Committee on Payment and Settlement Systems 2005). The Federal Reserve System issued its Policy on Payments System Risk to provide guidance on principles and minimum standards for managing risk in systemically important payments systems (Federal Reserve Board 2007). While aimed primarily at wholesale, large-value payment systems, it is also relevant to retail payments systems. The Federal Reserve applies these standards to the retail payments systems (ACH and checks) that it operates and where it has explicit supervisory authority over financial institutions that operate clearing and settlement systems. The Federal Reserve also participates in national and international policy processes that set standards for operating and controlling risk in payments systems.

The authority of the Federal Reserve System to oversee payments, however, is limited. Recently Chairman Ben Bernanke stated that "[i]n contrast to the situation in some other countries, the Federal Reserve lacks explicit legal authority to oversee systemically important payments systems."[32] Federal Reserve examiners can review payment activities of the banks in their jurisdiction, and they also participate in the TSP

supervision program. Federal Reserve authority to set regulations also has important influence on some operational aspects of payments and on incentives to control risk by determining liability in cases of fraud and operational disruptions.

But neither the Federal Reserve, nor any other federal agency, has explicit authority to manage retail payments risk from a system perspective. Private industry efforts to manage risks across payment channels are helpful in this regard, but implementation of their recommendations may be hampered by inherent difficulties of coordinating many participants in the payments system.

V. STRENGTHENING RISK MANAGEMENT IN RETAIL PAYMENTS

In light of recent changes to the payments system, risk management in the retail payments system might be strengthened in three ways: improve the ability of the market to manage risk, strengthen supervision of payment activities, and help coordinate risk management from a system perspective (Table 5). This section reviews options for reforms that address nonbank presence in the payments system. It then closes with a discussion of proposals to better allow gathering and analysis of data relevant to risk in retail payments.

Improve the ability of the market to manage payment risk

One barrier to industry efforts to manage risk in payments is that private incentives can inhibit implementation. Efficient risk management requires that those in the best position to control risk should also face financial consequences of failure, but this is not always the case in the payments industry. Options to correct this may require some legal reforms. Enhancing information useful to managing risks can also help industry efforts.

Some payments participants may not follow adequate security and operational standards because they do not face the entire cost of breakdowns. A 2004 data breach at the retailer BJ's Wholesale Club caused several financial institutions to reissue thousands of debit cards at a cost of $10 to $20 each. Lawsuits that sought to recover these costs were dis-

Table 5

OPTIONS FOR STRENGTHENING RISK MANAGEMENT IN RETAIL PAYMENTS

Purpose	Reform	Benefit
Improve ability of the market to manage risk	• Align legal responsibility with cost of operational breakdowns • Redefine revocability of payments • Provide information on quality of risk management	• Improve incentives to manage risk • Tie ability to control risk with responsibility • Enable payment participants to judge quality of risk control
Strengthen supervision of payment activities	• Mandate control of payments risk • Add enforcement options for TSP supervision • Expand eligibility for supervision • Redefine mission of the FTC	• Focus supervisory activity • Tailor sanctions to shortcomings • Actively supervise risky payment processors • Clarify and enforce security among retailers and other nonbank organizations
Coordinate risk management from system perspective	• Create institutions to coordinate risk management • Mandate umbrella risk management of retail payments	• Target specific public policy goals • Provide robust perspective on risk management
Collect and analyze useful information	• Require payments participants to report risk-related information • Assign responsibility for collecting and analyzing data	• Better understanding of payments system risk • Guidance for private and public risk management

missed because the financial institutions did not have a direct contractual relationship with BJ's (Pereira). Similarly, when credit cards are used online for fraudulent purchases, merchants pay for the fraud, not the issuer of the card. Merchants argue that this reduces the incentive of card issuers to implement anti-fraud measures and to track down fraudulent activity for online purchases (Becket and Sapsford). Perhaps more important, critical software and payments processing services are sometimes contracted so that the vendor does not face liability in case of failure (Menta; Funnell). In other words, the vendor may not face the full cost of errors for which it may be responsible.

BJ's incentive to implement appropriate risk mitigation systems is incomplete because it was not held responsible for all costs associated with failure of its system. Software makers may have insufficient incentive to produce high-quality, low-risk services and software. Reforms to legal responsibilities or to limits on litigation could help to align liability and ability to control risk.[33] To protect the payments system, analysts

have proposed legal reform and regulation to rationalize liability and responsibility for risk in contracting relationships for payments processing (Glaessner, Kellerman, and McNevin 2002, 2004).

Proper design of legal liability can also help in the fight to control illicit activity such as fraud and money laundering. Payments service providers—both bank and nonbank—are often in the best position to screen and monitor customers so as to exclude those with illicit intent. One option is to redefine revocability rules in payments to make it easier to recover illicit funds. This would also make payments service providers more responsible for the costs associated with clients engaged in illegal transfer of funds and enhance incentives of payments service providers to improve their gatekeeping responsibilities (Anderson).

Providing information on data security and resiliency could also help the market manage payments risk. For example, a SAS 70 audit is an evaluation of the control structure of an organization over information security risks, and the written report can provide information to a TSP's clients about potential exposure.[34] Licensing or certification of payment providers can convey a level of competence and allow potential clients to judge providers on the quality of the providers' security controls. Proposals to more widely release exam reports for major vendors in the TSP supervision program have a similar purpose (Lemieux). Done properly, this can convey information about a firm's risk control environment without compromising security and allow clients to seek out vendors with high-quality internal controls.

Strengthen supervision of payment activities of banks and technology service providers

As noted earlier, the primary goal of the supervision of depository institutions is to protect the institution's depositors. An explicit goal of controlling payments system risk could be added to the mandate of supervisors. By doing so, supervisors would be encouraged to look beyond narrow consequences of problems in the payments activities of financial institutions or of TSPs. This would require modification of the policies and procedures used in supervision of financial institutions and TSPs to attain objectives tied to protecting the payments system.

Supervisors of TSPs could be given additional enforcement options. Enforcement should provide options that range from mild to severe to allow tailoring sanctions to the severity of shortcomings. In addition, assuming some details of enforcement actions are disclosed, payment participants would gain more information on potential consequences of weaknesses in risk management.

Policymakers could also consider expanding eligibility requirements for supervision of nonbank payment participants. Expanding supervision to other payment processors would be consistent with the current expertise and practices of financial institution supervisory agencies. It is instructive that even smaller payments processors can accumulate large databases of payment card information, as was the case at CardSystems Solutions, and so there may be some value in adding smaller payments processors. Similarly, there may be value in extending eligibility to significant payments processors who are not in an outsourcing relationship with a bank.

Table 2 suggests that it may be particularly important to strengthen data security in the retail sector of the economy. Because it has jurisdiction over commercial firms in data security matters, policymakers could consider strengthening the mandate and enforcement powers of the FTC.

Coordinate risk mitigation across elements of the payments system

Industry efforts to coordinate risk mitigation, both within and across payment channels, represent significant progress. Policy changes just discussed would assist those efforts. But incomplete incentives to control risk and interdependence among payments participants suggests that some public policy steps aimed at improving coordination of risk mitigation in the payments system would be valuable.

At least nine federal agencies can influence risk management in payments (Table 3).[35] In addition, state authorities, private industry, and international agencies each have some role. At the present time, many of these authorities have a great degree of independence in their mission. There are some informal and formal coordination among these authorities. A good example is the process undertaken in the aftermath of

September 11 in a federal interagency effort to improve the resiliency of systemically important payments systems in the United States.[36] None of these initiatives, however, considers the payments system as a whole.

One potential model could be the European Commission's Fraud Prevention Expert Group (FPEG).[37] This group consists of different parties involved in fraud prevention, including various payment networks, banks, public authorities, law enforcement, consumer groups, and others. The FPEG provides a forum where participants can exchange information and best practices to prevent fraud. Such participation can help facilitate cooperation among participants. The group also provides advice to the European Commission. While the FPEG provides a forum on fraud prevention, the model could be applied to all aspects of risk management in payments.

An alternative is what might be called an umbrella model for management of risk in the payments system. This model stresses the systemic nature of payments and provides a more robust perspective of risk than when each element of that payments network is analyzed separately (McPhail). This model does not necessarily involve regulation. Rather, it could use a range of actions (such as legal reforms) that might enhance private efforts at managing risks, establish institutions to coordinate risk management across payment platforms, act as a liaison for public and private interests in risk management. Regulation might be called for when there is a clear public interest, regulation is cost effective, and other ways of addressing risk management shortcomings are ineffective.

Who would take on this responsibility? A central bank may be in a position to successfully implement this responsibility because of its unique position in the payments system (McPhail). However, central bank linkage to the payments system is primarily with other financial institutions, and the risk in retail payments clearly extends beyond financial institutions. Effective management of risk in the U.S. retail payments system may need to involve interaction among all federal and state agencies that influence payments risk management.

Collect and analyze information useful to understand payments system risk

More and better data would help provide the information to guide decisions. Policymakers should consider proposals that allow gathering and analysis of data relevant to risk in retail payments. In recognition of the value of these data, some central banks have significant powers to gather information on payments useful for monitoring and surveillance purposes.[38]

The analysis of data breaches shown above is based on flawed data but illustrates the value that empirical information can have in understanding payments system risk. It allows a breakdown of the sources of data breaches by bank and nonbank organizations. It allows a distinction between an incident and the number of compromised records, the latter of which is a better measure of risk exposure. Comprehensive and uniform data breach notification requirements would make this type of analysis more helpful to policymakers.[39]

More facts relevant to a number of questions would be useful to determine whether and where more public action is warranted. What is the nature of operational risk in payments processing? How many incidents are there and how costly have they been? How often have payments disruptions occurred at vendors that are outside of the TSP supervision program and how significant are they? How effective are private institutional arrangements that facilitate the sharing of information on security and operational disruptions to payments systems?

VI. CONCLUSION

A 1997 report on risks in payments, settlement, and clearing by the U.S. General Accounting Office (GAO) identified credit risk, fraud, and malicious activity as the main risks in retail payments. Given the prevalence of checks in payments and the early stage of the Internet at the time of the report, the GAO conclusion was reasonable. But today, with the great reliance of payments on electronic networks and on nonbank payment providers, the risk profile of retail payments is significantly different. Unauthorized access, virus infections, malicious attacks, and operational breakdowns have become part of the payments

landscape. Some of the disruptions to payments caused by these problems are severe enough to qualify as systemwide risks and seem to be coming with greater frequency.

Nonbanks bring new technology and perspectives that can significantly contribute to reducing risk in the payments system. Nonbanks are developing innovations related to security (such as biometrics), payment processing improvements, and real-time controls over payment authentication. These contributions improve security, reduce fraud, and improve the resiliency of the payments system. But the emergence of nonbanks as elements in the payments system, at a minimum, alters the mix of risks in the payments system and potentially magnifies some old or introduces new ones. Nonbanks complicate control of outsourcing risk and can introduce weaknesses to the payments system by adding locations for access or by complicating coordination of mitigation efforts.

Policymakers have a number of options that could help to reduce risk in the retail payments system. The ability of the market to self-regulate could be enhanced by better aligning responsibility and control in matters of data security and operational integrity and by improving information relevant to risk mitigation. Public involvement in managing retail payment risk could be strengthened by providing an explicit mandate to protect payments, authorizing regulation where weaknesses in data security or operational integrity are apparent, and by giving supervisors appropriate enforcement tools. In recognition of the network structure of payments, efforts that assist coordination of oversight and risk management would be valuable. Policy choices would be clearer if more useful data were collected and analyzed.

Lastly, primary authority for supervision of nonbank payment providers in the United States comes from the Bank Service Company Act. This act was passed more than 40 years ago and reflects technology in service at that time. Since then, there have been vast increases in the sophistication of technology applied in payments and significant changes in payment options. A review of the authority for public involvement in managing risk in payments would therefore be useful. This type of review would be particularly valuable in areas where risk exposure of payment participants arises from their interrelationships in a payments network.

ENDNOTES

[1]Crowell Moring LLP website at *www.crowell.com/pdf/SecurityBreachTable.pdf*, accessed 4-13-07. Thirty-five states and the District of Columbia now have notification laws. California enacted its disclosure law in 2003, while the effective date for other states was mid-2005 or later.

[2]Chart 2 has a break at 2002/2003 because the transaction volume was measured differently beginning in 2003. Prior to that, many ATM transactions were counted by more than one ATM network. As a result, measures of aggregate market share could be above 100 percent. Much of the double counting was eliminated after 2003.

[3]A consolidator site can present billing information for many billers on a single Web page and typically offers an option to pay the bill (Wolfe 2004, p. 17.)

[4]CheckFree has estimated that it has a 75 to 80 percent share of this market ("Paper Costs Cut through e-Payment Option," p. 14).

[5]From eBay's fourth quarter 2006 earnings report press release dated January 24, 2007, *http://investor.ebay.com*.

[6]"Card Issuers Beware: PayPal to Offer Credit," "PayPal Targets Music Download Micropayments;" and "PayPal, The Fifth Credit Card?"

[7]The Committee on Payments and Settlement Systems (2000) identifies five major categories of risk associated with payments transactions: fraud, operational, legal, settlement, and systemic risks. Rather than discuss these general principles, this article focuses on risks of particular relevance to paper and electronic payments systems. For example, Bradford, Davies, and Weiner argue that nonbanks pose limited settlement risk (though they warn of indirect nonbank access to settlement facilities through "captive bank" relationships). See pp. 9-11 for a more complete discussion of payments system risk.

[8]Since this incident, PayPal has developed state-of-the-art data security and fraud detection systems to the point where loss rates due to fraud for merchants who use PayPal are noticeably below the e-Commerce average (Cox; Garver). See "Computer Scientists" for a description of some recent techniques used by criminals to perpetrate fraud through online auction sites.

[9]The two nonbank networks are Star and Pulse. The third is Visa's Interlink, which will become a nonbank network when Visa completes plans to become a publicly held organization (Berry and Breitkopf).

[10]For example, since 1997, bank losses have been fairly steady despite a fivefold increase in attempts to commit check fraud (Bills).

[11]Phishers target PayPal and eBay in 77 percent of their recent e-mail (Sancho and Yaneza, p. 13).

[12]When made aware that funds were not going to arrive on time, one credit union extended $1.8 million in credit to cover expected deposits for its members.

[13]When asked about challenges they face in hiring new employees, community banks rank skills of potential employees as a significant challenge (Myers, p. 18).

[14]Given the flaws in this data, this is a tentative conclusion that should be explored further as better data and more experience with existing risk management processes become available.

[15]Threats such as worms, trojan horses, bots, spyware, and phishing increased 163 percent between December 2005 and December 2006 (Sancho and Yaneza). Creators of these threats are increasingly motivated by financial gain and are participating in underground markets to trade stolen data and malicious code.

[16]Another important area of oversight is systemically important payments systems, which is governed in the U.S. by the Federal Reserve System's *Policy on Payments System Risk*. Because this article is focused on retail payments, it will not go into any depth for systemically important payments systems, which are clearing and settlement systems for large value (wholesale) payments.

[17]For the purposes of this article, the term "nonbank" refers to any payment provider with no bank affiliation. Whether a particular payments processor is supervised is not publicly available information.

[18]Examples include the retailer DSW, the credit agency ChoicePoint, and software vendor Guidance Software.

[19]A 1996 amendment allowed bank service companies to incorporate, so the act is sometimes referred to as the Bank Service Corporation Act.

[20]Members of the FFIEC represent all of the federal agencies responsible for regulating and supervising of U.S. depository institutions, including the OCC, the Federal Reserve System, the FDIC, the Office of Thrift Supervision and the National Credit Union Administration. It promotes uniformity across agencies in the federal examination of depository institutions by prescribing uniform examination principles, developing common reporting systems, and conducting schools for examiners.

[21]Business activities shown in Table 4 are based on information provided by examiners. Examiners do not expect that these reports would be subject to statistical analysis and therefore the completeness of the reported lines of business is uncertain. However, it seems unlikely that any misreporting would be biased regarding payments activity and so the relative position of bank versus nonbank payments providers should not be misleading.

[22]Whether a TSP is counted as providing payment services is based on it offering at least one of 11 payment-related lines of business: ACH processing/services, ATM processing/services/network/switch, bill payment service, credit card issuance, credit and/or debit card merchant processing, credit card network/switch, check processing, check processing software vendor clearing and settlement, POS processing/services/network/switch, and wholesale payments.

[23]There is no comprehensive data source that would show the number of companies that provide payment services to financial institutions.

[24]If they do provide outsourced services to banks, these organizations may be eligible for the TSP supervision program.

[25]In a speech delivered in April 1998, Roger Ferguson, former vice chair of the Board of Governors, stated that "I do not believe that the market for new retail electronic payment services reflects the existence of market failures.... The government should avoid regulatory actions that may inhibit the evolution of emerging payments products and services or prevent the effective operation of competitive market forces. It is not clear whether, or what type of, regulation will be needed for many new products and it is important to avoid jumping to the conclusion that such regulations are inevitable over the longer term(Ferguson)."

[26]Economists refer to these complications as asymmetric information and moral hazard (Braun and others).

[27]NACHA consists of financial institutions, industry councils, and other stakeholders in the ACH system. It sets rules and standards for ACH transactions and has some monitoring and enforcement responsibilities.

[28]For more information, see the FS-ISAC website at *www.fsisac.com*.

[29]Similarly, in 2006, First Data and five large banks formed a joint venture called Early Warning Services LLC as a vehicle for payments providers to share information and expertise on fraud prevention and screening of customers (Breitkopf 2006b).

[30]The Partner Group is sponsored by BITS, a financial industry consortium that is a vehicle for industry collaboration on emerging issues. For more information, see the BITS website at *www.bitsinfo.org/index.html*.

[31]For example, after nearly two years of implementation, some observers feel that the adoption of the PCI data security standards has been slow (Sidel). Visa has recently increased sanctions for noncompliance and has implemented a reward program to encourage implementation (Aplin).

[32]In addition, Chairman Bernanke stated that "Federal Reserve powers in this area derive to a considerable extent from its bank supervisory authority. Notably, some key institutions providing clearing and settlement services hold bank charters that place them under Federal Reserve oversight.... The Fed is also either the direct or umbrella supervisor of several large commercial banks that are critical to the payments system through their clearing and settlement activities" (Bernanke). By contrast, the Banque de France has broad power to oversee noncash payments (European Central Bank Oversight Division, p. 21).

[33]In the aftermath of the TJX data breach, the state of Massachusetts is considering legislation that would make commercial firms responsible for data breaches liable for the associated costs of reissuing payment cards (Pereira).

[34]A description of SAS 70 audits, *www.sas70.com*.

[35]Some of these actions are indirect because there is a trade-off between risk and efficiency in payments (European Central Bank Oversight Division, p. 45).

[36]Guidelines for this effort were presented in Board of Governors and others 2002. A 2006 report to congress discusses private sector implementation of the guidelines (Board of Governors and others).

[37]See their website at *http://ec.europa.eu/internal_market/fpeg/index_en.htm*.

[38]For example, see Monetary Authority of Singapore.

[39]The recently implemented data breach notification requirement in the Federal Reserve's *Operating Circular 1* is a step in the right direction. Information on the new requirements, *www.frbservices.org/OperatingCirculars/index.html*.

REFERENCES

Abelson, Jenn. 2007. "Breach of Data at TJX is Called the Biggest Ever," *Boston Globe*, March 29.

Anderson, Ross. 2007. "Closing the Phishing Hole—Fraud, Risk, and Nonbanks," Paper presented at the Federal Reserve Bank of Kansas City, *Conference on Nonbanks in the Payments System.*

Aplin, Donald G. 2006. "Visa Offers Banks PCI Compliance Rewards, But Will also Increase Enforcement Sanctions," *BNA Banking News*, December 22.

Bank of England. 2000. "The Bank of England's Oversight of Payments Systems," *Financial Stability Review*, December, p. 173.

"Bank Service Companies." 2000. Title 12, chapter 18, § 1865, *U.S. Code*, 2000 ed.

Becket, Paul, and Jathon Sapsford. 2003. "Signature Problems: As Credit Card Theft Grows, a Tussle Over Paying to Stop It," *The Wall Street Journal*, May 1, p. A1.

Bernanke, Ben S. 2007. "Central Banking and Bank Supervision in the United States," Remarks given at the Allied Social Sciences Association, January 5, *www.federalreserve.gov/boarddocs/speeches/2007/20070105/default.htm.*

Berry, Kate, and David Breitkopf. 2006. "Big Step for Visa May Prove Bigger For Industry; Merchants Gain More Clout; Association Model Fades Further," *American Banker*, October 26.

Bills, Steve. 2004. "Report Suggests Anti-Fraud Measures are Having Impact," *American Banker*, November 23.

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and Exchange Commission. 2002. "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," *www.federalreserve.gov/boarddocs/srletters/2003/SR0309a1.pdf.*

_____. 2006. "Joint Report of Efforts of the Private Sector to Implement the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," *www.federalreserve.gov/boarddocs/rptcongress/soundpractices/soundpractices200604.pdf.*

Bradford, Terri, Matt Davies, and Stuart E. Weiner. 2003. *Nonbanks in the Payments System.* Federal Reserve Bank of Kansas City.

Braun, Michele, Jamie McAndrews, William Roberds, and Richard J. Sullivan. Forthcoming 2007. "The Economics of Managing Risks in Emerging Retail Payments," Federal Reserve Bank of New York, *Economic Policy Review.*

Breitkopf, David. 2004. "Scams Expose Weaknesses: Do Processors Vet Merchants Well Enough?" *American Banker*, June 9.

_____. 2006a. "Rise in Chargebacks Linked to Fraud and Data Breaches," *American Banker*, January 17.

_____. 2006b. "Fight vs. Fraud Spurs Five-Bank First Data Deal," *American Banker*, May 26, p.1

"Card Issuers Beware: PayPal to Offer Credit." 2004. *Electronic Payments International*, July, p. 1.

"CheckFree EBPP Service Halted by Power Outage." 2005. *Finextra, www.finextra.com/fullstory.asp?id=13824.*

Committee on Payment and Settlement Systems. 2000. *Clearing and Settlement Arrangements for Retail Payments in Selected Countries,* Bank for International Settlement, September, *www.bis.org/publ/cpss40.htm.*

_____. 2005. *Central Bank Oversight of Payment and Settlement Systems*, Bank for International Settlement, May, *www.bis.org/publ/cpss68.pdf.*

"Computer Scientists Uncover Online Auction Fraud." 2006. *Physorg.com,* December 5, *www.physorg.com/news84545784.html.*

Cox, Paul. 2001. "PayPal and FBI Team Up," *The Wall Street Journal*, June 22.

Dash, Eric. 2005. "Take a Number," *The New York Times*, July 30, p. 1.

European Central Bank Oversight Division and Federal Reserve Bank of Kansas City Payments System Research Department. 2007. "Nonbanks in the Payments System: European and U.S. Perspectives." Paper presented at the Federal Reserve Bank of Kansas City, *Conference on Nonbanks in the Payments System.*

Federal Financial Institution Examination Council. 2003a. *IT Handbook Presentation: Supervision of Technology Service Providers*, April, *www.ffiec.gov/ ffiecinfobase/presentations/tsp_presntation.pdf.*

_____. 2003b. *Supervision of Technology Service Providers*, IT Examination Handbook, March.

Federal Reserve Board. 2000. "Information Technology Examination Frequency," Supervision and Regulation letter SR00-3 (SUP), February 29.

_____. 2007. *Federal Reserve Policy Statement on Payments System Risk,* January 11, *www.federalreserve.gov/paymentsystems/psr/policy07.pdf.*

Federal Trade Commision. 2005. "International Telemarketing Network Defendants Banned from Telemarketing," January 24, *www.ftc.gov/opa /2005/01 /assail.htm.*

Ferguson, Roger W., Jr. 1998. "The Federal Reserve's Role in the Payments System and Its Effect on Competition," Remarks before the Bankers Roundtable, Phoenix, April 4, *www.federalreserve.gov/boarddocs/speeches/1998/ 19980404.htm.*

Fest, Glen. 2005. "CardSystems Takes a Bullet After Breach," *Bank Technology News*, August.

Funnell, Kevin J. 2005. "Holding a Bank's Technology Service Providers Accountable," *Journal of Internet Law*, December, pp. 3-6.

Garver, Rob. 2005. "eBay and Banking: Is PayPal a Serious Rival?" *American Banker*, November 15.

Gerdes, Geoffrey R., and Jack K. Walton. 2002. "The Use of Checks and Other Noncash Payment Instruments in the United States," *Federal Reserve Bulletin,* Spring, pp. 360-74.

_____. 2005. "Trends in the Use of Payment Instruments in the United States," *Federal Reserve Bulletin*, August, pp. 180-201.

Glaessner, Thomas, Tom Kellerman, and Valerie McNevin. 2002. "Electronic Security: Risk Mitigation in Financial Transactions," Policy Working Paper 2870, The World Bank, June.

_____. 2004. "Electronic Safety and Soundness: Securing Finance in a New Age," Working Paper Number 26, The World Bank.

Hayashi, Fumiko, Richard J. Sullivan, and Stuart E. Weiner. 2006. *A Guide to the ATM and Debit Card Industry: 2006 Update.* Federal Reserve Bank of Kansas City.

Hoenig, Thomas M. 2000. "Payments and Settlement Systems: Future Players and Issues," Remarks before the BAI Money Transfer 2000 Conference, Chicago, November 9, *www.kansascityfed.org/SPCH&BIO/chicago.htm.*

ID Analytics. 2006. *National Data Breach Analysis.* San Diego: ID Analytics.

Iowa Attorney General. 2005. "First Premier Bank Agrees to Deny Automatic Withdrawal Services to Telemarketing Scams," July 6, *www.state.ia.us /government/ag/latest_news/releases/july_2005/First_Premier.html*.

Javelin Research. 2006. "New Research Shows Identity Fraud Growth is Contained and Consumers Have More Control than They Think," press release, *www.bbbonline.org/IDtheft/safetyQuiz.asp*.

Kimball, Ralph C. 2000. "Failures in Risk Management," Federal Reserve Bank of Boston *New England Economic Review*, January/February.

Lemieux, Catharine. 2003. "Network Vulnerabilities and Risks in the Retail Payments System," Federal Reserve Bank of Chicago, Emerging Payments Occasional Papers Series 2003-1F.

Lenard, Thomas M., and Paul H. Rubin. 2005. "An Economic Analysis of Notification Requirements for Data Security Breaches," *Progress on Point* Release 12.12, July, Progress and Freedom Foundation.

Lindenmayer, Isabelle. 2005. "Study: Breach-Related Fraud Rarer than Thought," *American Banker*, December 9, p. 11.

McPhail, Kim. 2003. "Managing Operational Risk in Payment, Clearing, and Settlement Systems," Working Paper 2003-2, Department of Banking Operations, Bank of Canada, February.

"Members Reject NACHA's Return Fee Proposal, but NACHA still Backs Idea." 2005. *Digital Transactions*. June 10, *www.digitaltransactions.net/ newsstory.cfm?newsid=613*.

Menta, Richard. 2004. "Don't Sign Software Contracts that Leave Vendors Off the Hook," *American Banker*, February 13, p. 11

Monetary Authority of Singapore. 2003. "Payments Systems Oversight Act," Consultation Paper 01-2003, April.

Myers, Forest. 2001. "Management and Staffing Challenges," Federal Reserve Bank of Kansas City, *Financial Industry Perspectives*, December.

NACHA. 2006. *Risk Management News*, vol. 2, issue 2, pp. 1-2.

Office of Technology Assessment. 1982. "Security in Electronic Funds Transfer," Chapter 5 in *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity*, March, pp. 45-54.

"Paper Costs Cut through e-Payment Option." 2004. *Electronic Payments International*, April 15, p. 14.

"PayPal Targets Music Download Micropayments." 2004. *Electronic Payments International*, December, p. 1.

"PayPal, the Fifth Credit Card?" 2004. *Internet News*, May 3, accessed on October 29, 2004, *www.internetnews.com/dev-news/article.php/3348451*.

Pereira, Joseph. 2007. "Bill Would Punish Retailers for Leaks of Personal Data," *The Wall Street Journal*, February 22.

Ramsaran, Cynthia. 2004. "AOL Introduces Free Online Bill Payment," *Bank Systems & Technology*, June 1, p. 56.

Sancho, David, and Jamz Yaneza. 2006. "2006 Annual Threat Roundup and 2007 Forecast," Trend Micro, December, *http://uk.trendmicro-europe.com/global/products/collaterals/white_papers/2006AnnualThreatRoundup.pdf*.

Sidel, Robin. 2006. "Credit Firms Push to Thwart Fraud," *The Wall Street Journal*, September 25, p. C1.

Spong, Kenneth. 2000. B*anking Regulation: Its Purposes, Implementation, and Effects*. Federal Reserve Bank of Kansas City.

Sullivan, Richard. 2006. "The Supervisory Framework Surrounding Nonbank Participation in the U.S. Retail Payments System: An Overview," Federal Reserve Bank of Kansas City, Payments System Research Working Paper 04-03, April 24, *www.kansascityfed.org/PUBLICAT/PSR/ RWP/Sullivan_Supervision_nonbank_pmt_providers_WP0403.pdf.*

"U.S. Banks Collaborate on Data Security." 2006. *Cards International*, June 13, 2006.

U.S. Department of Justice. 2002. "Russian Computer Hacker Sentenced to Three Years in Prison," October 4, *www.cybercrime.gov/gorshkovSent.htm.*

U.S. General Accounting Office. 1997. *Payments, Clearance, and Settlement: A Guide to the Systems, Risks, and Issues*, GAO report GGD-97-73, June.

Wade, Will. 2004. "CU Outage Sparks Questions about ACH Network Resilience," *American Banker*, April 14, p. 1.

Wagner, Jim. 2004. "PayPal Scrambling to Fix Site Glitch." *Internetnews.com*, October 13, 2004, *www.internetnews.com/ec-news/article.php/3421031.*

Wolfe, Daniel. 2004. "Environment for EBPP Seen Shifting in Bankers' Favor," *American Banker*, June 29, p. 17.

_____. 2006. "CheckFree Shares Tumble Despite 19% Profit Gain," *American Banker*, October 26.