Michele Braun, James McAndrews, William Roberds, and Richard Sullivan

Understanding Risk Management in Emerging Retail Payments

- The retail payment landscape is shifting increasingly from paper to electronic form as the number of ways to make noncash payments grows.
- Payment products, services, rules, and technologies are changing at a rapid rate—as are the tools for perpetrating fraud, illicit use, and breaches of data security.
- Providers of emerging payment methods now face the same risks as providers of more established methods; failure to control these risks can lead to rejection in the market.
- By limiting access to payment networks, monitoring for compliance with risk mitigation standards, and enforcing penalties for noncompliance, emerging as well as established providers can contain many of the risks associated with fraud, illicit use, and data security breaches.

1. Introduction

Electronic checks, cell phones, and speed-through lanes at toll booths are just a few examples of new payment methods recently introduced to the market. Based on computer technology, online commerce, and telecommunications, these new payment methods rely on electronics for most or all of their functions. Many products based on these methods have failed, some have struggled to grow, and a few have become well accepted in routine commerce. All face a variety of risks.

Reflecting these risks, news reports of data breaches, identity theft, and fraud have become a part of the electronic payment landscape. Novel characteristics associated with "emerging" payments include low-cost ways to store and transmit data. These technologies can reduce risk, but they can also lead to new risks. It is timely now to develop a structure and vocabulary for examining how new payment technologies affect risk, particularly as the number of ways to make noncash payments grows and as payments shift from paper-based to electronic form.[1]

Understanding the structure of risk is useful, although assessing losses and mitigation efforts in a new payment

Michele Braun is an officer and James McAndrews a senior vice president at the Federal Reserve Bank of New York; William Roberds is an economist and policy advisor at the Federal Reserve Bank of Atlanta; Richard Sullivan is a senior economist at the Federal Reserve Bank of Kansas City.
Correspondence: <james.mcandrews@ny.frb.org>

This article began as a Federal Reserve System staff research project. The authors acknowledge those who participated in that research, each contributing significantly to the concepts and substance of this article: Eugene Amromin, Peter Burns, Marianne Crowe, Jim Cunha, Dan Littman, Mark Manuszak, Antoine Martin, James McGrath, and John Yanish. They thank Christine Cumming and Claudia Swendseid for sponsoring and supporting the research and for valuable comments, as well as Stephanie Heller, Ariel Stern, Nathan Halmrast, and Daniel Meyer for their assistance. The views expressed are those of the authors and do not necessarily reflect the position of the Federal Reserve Banks of Atlanta, Kansas City, and New York, or the Federal Reserve System.

product can be difficult. Low levels of fraud losses, for example, could imply that: 1) risk is low, 2) current mitigation practices are effective, or 3) weaknesses have not yet been discovered. However, high levels of losses demonstrate that risks are high, and it takes time to know whether mitigation efforts can succeed. In either case, only time and the monitoring of problems will reveal whether risk can be controlled sufficiently. In this article, we consider whether, in this period of uncertainty, the sponsor of an emerging payment method has enough incentives and tools to control risk before the harm from fraud or operational problems becomes widespread.

Our analysis suggests that the sponsors and providers of successful emerging payment methods must be aware of potential fraud risk and operational risk. Moreover, they must mitigate these risks or face rejection in the payment market. Service providers can contain risks by limiting access to their payment networks, monitoring for compliance with risk mitigation standards, and enforcing penalties for noncompliance. While much of this containment activity is voluntary, some is enforced by public authorities that can help coordinate activities as well as define and enforce standards.

> *It is timely now to develop a structure and vocabulary for examining how new payment technologies affect risk, particularly as the number of ways to make noncash payments grows and as payments shift from paper-based to electronic form.*

This article explores in several ways the structure and vocabulary of emerging payments system risks and their mitigation. We begin by recounting several incidents of fraud and losses associated with emerging payment methods. We then describe an economic framework for understanding risk control in retail payments. Next, we apply the framework to the risk experiences of three new payment types. These approaches—both deductive and inductive—are complementary ways to understand risk and its mitigation in emerging payment methods. Finally, we discuss some general observations derived from integrating the economic concepts and actual experiences, then offer conclusions.

2. True Accounts of Fraud and Operational Risks in Payment Innovations

The following accounts illustrate fraud and operational problems that exploited the novel characteristics of new payment methods. These incidents include a telemarketing scheme, a complex online fraud, and two data security breaches. The crimes that underlie these incidents—fraud, con artistry, and theft of money, property, or someone's good name—are not themselves new. The operational problems are also not necessarily new, but the potential scale and speed of the disruptions are of a magnitude untypical of their paper-based counterparts.

2.1 Telemarketing Fraud

In 2003, the Federal Trade Commission (FTC) announced that it had closed down the Assail Telemarketing Network and its affiliates. The FTC alleged that the Assail companies ran telemarketing activities from so-called boiler-room operations that offered credit cards to consumers with poor credit records.[2] Under the guise of charging membership fees, these firms persuaded consumers to provide the bank and account information from their checks.[3] The telemarketers then used this information to create electronic debits to consumers' checking accounts as payment for the "membership" fees. These credit cards appear to have been rarely, if ever, delivered. The consumers found, however, that they had also been signed up for expensive and dubious products (so-called upsell programs) such as auto club memberships, the fees for which were directly charged to their bank accounts. When consumers called to complain, the companies used elaborate scripts to avoid repayment or cancellation of the membership. The FTC alleged that Assail and its principals engaged in deceptive marketing activities that totaled more than $100 million.[4]

The particular type of electronic transaction that Assail used, a debit through the automated clearinghouse (ACH), must be processed, collected, and paid through participating banks. These banks are supposed to monitor the companies for

[1] In 2003, the number of electronic payments exceeded the number of check payments for the first time. See Federal Reserve System (2004).

[2] See Federal Trade Commission, "International Telemarketing Network Defendants Banned from Telemarketing," press release, January 24, 2005, available at <http://www.ftc.gov/opa/2005/01/assail.htm>, as well as other FTC press releases.

[3] Consumers provided the encoded information that runs across the lower edge of a check, which is also known as magnetic ink character recognition (MICR) information.

[4] ConsumerAffairs.com, "Bogus Credit Card Marketers Settle Federal Charges," January 26, 2005.

which they provide this ACH origination service. In this case, First Premier Bank admitted that it had failed to perform due diligence on the activities and legitimacy of its customers, but it then helped identify the telemarketers and supplied information to the investigative agencies. The bank later paid $200,000 to Iowa, South Dakota, and Minnesota as part of a wider settlement and agreed to engage vigorously in know-your-customer practices and ongoing monitoring of customer activity.[5]

Before the particular ACH transaction type used by Assail was introduced, this type of fraud was often perpetrated by creating a "remotely created check"—a check that contains a text legend in lieu of the payer's signature. This approach is still used to commit fraud, but it does not offer the speed and scale this fraudster achieved using automation.[6]

2.2 Transaction Fraud and Data Security Breach

The U.S. Department of Justice reported that, in 2000, two Russian men, Vasiliy Gorshkov and Alexey Ivanov, used unauthorized access to Internet service providers in the United States to misappropriate credit card, bank account, and other personal financial information from more than 50,000 individuals.[7] They allegedly hijacked computer networks and then used the compromised processors to commit fraud through PayPal and the online auction company eBay.

According to the Justice Department's press releases, the fraudsters developed elaborate programs to establish thousands of anonymous e-mail accounts at websites that, at the time, did not have the sophisticated tools required to distinguish human intervention at set-up. Gorshkov's programs created accounts at PayPal that were based on random identities and stolen credit card numbers. The programs then transferred funds from one account to another to generate cash and to pay for computer parts purchased from vendors in the United States. Additional computer programs allowed the conspirators to control and manipulate eBay auctions so that they could act as both seller and winning bidder in the same auction and then effectively pay themselves using the stolen credit cards.[8]

This was a case of fraudsters hacking into databases, stealing payment-related and other information, using the stolen identities to create fictitious accounts, manipulating online auctions, and using machine-based tools to proliferate their thefts and confound the transaction/audit trail.

Ultimately, the FBI used an undercover operation to lure the two hackers to Seattle, Washington, where they had been invited under the pretext of a job interview with "Invita," a fictitious computer security company. In October 2002, the two men were sentenced to three years in prison.

2.3 Unsecure Data

In 2005, the president and chief executive officer of CardSystems Solutions, Inc., a transaction processor, testified before a Congressional committee that, in September 2004, an unauthorized party had placed a clandestine computer program on the company's transaction processing system (Perry 2005). CardSystems reported that, on May 22, 2005, it suffered a "potential security incident." Records on 263,000 transactions were stolen—including account holders' names, account numbers, expiration dates, and security codes. Forty million records were potentially at risk.

CardSystems disclosed the breach to its bank as well as to MasterCard, Visa, and American Express. The three credit card companies determined that CardSystems had violated the credit card industry's prevailing security and data retention standards. Visa and American Express announced that they would not permit the firm to process their transactions after October 31, 2005. On October 15, Pay by Touch announced its acquisition of CardSystems Solutions because of the latter's network connections to 120,000 merchants, despite the demise of its card transaction processing business.[9]

More recently, in early 2007, the TJX Companies, which operate retail stores in the United States, Canada, Ireland, and the United Kingdom, reported that data security breaches from mid-2005 until late 2006 might have compromised more than 45 million customer records.[10] Company investigations also revealed breaches in 2003 and 2004, as well as compromised driver's license numbers and addresses. The Massachusetts Bankers Association reported fraudulent use of debit and credit cards issued by its members as a result of that breach. The

[5] This was the first time that the Federal Trade Commission tried to hold a bank responsible for the deceptive practices of its customer.

[6] To help reduce the potential for fraud in the use of remotely created checks, the Federal Reserve Board amended its Regulation CC effective on July 1, 2006, to create transfer and presentment warranties under which any bank that transfers or presents a remotely created check warrants that the check is authorized by the person on whose account the check is drawn. See Federal Reserve Board press release, November 21, 2005, available at <http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051121/>.

[7] U.S. Department of Justice, "Russian Computer Hacker Sentenced to Three Years in Prison," press release, October 4, 2002.

[8] Physor.com describes some of the techniques used by criminals to perpetrate fraud through online auction sites. See <http://www.physorg.com/news84545784.html>, December 5, 2006.

[9] Pay by Touch, "Pay by Touch to Acquire CardSystems Solutions, A Leading Provider of Integrated Payment Solutions," press release, October 15, 2005.

[10] TJX Companies, Inc., "The TJX Companies, Inc. Victimized by Computer Systems Intrusion; Provides Information to Help Protect Customers," press release, January 17, 2007, available at <http://home.businesswire.com/portal/site/tjx/>.

Association's press releases recounted that fraudulent card data had been used to make purchases in many U.S. states, Hong Kong, Sweden, and other countries.[11]

The *Wall Street Journal* reported that hackers first tapped into data transmissions from handheld equipment used to manage store inventory and prices.[12] Reportedly, they used these captured data to crack encryption codes and to steal employees' user names and passwords at company headquarters. With the resulting access to TJX's network, they stole credit and debit card numbers and even left messages for each other. Stolen card numbers were then allegedly sold on the Internet. Press reports traced losses to banks across the country. In addition to direct purchases with stolen credit and debit card numbers, the thieves or their customers also purchased prepaid cards, which were in turn used to purchase goods and services.

3. Definitions and Economic Insights

The examples just offered illustrate some risks of financial loss that are present in payment methods. We now turn to an economic examination of these risks and their mitigation, beginning with three general observations. First, the risks present when new or still-emerging payment methods are used are not wholly different from those present in long-established methods of payment. Nonetheless, our analysis suggests that certain risks are more salient in *emerging* retail payments than elsewhere in the payment marketplace.

Second, new payment methods are generally based on, or emerge from, existing payment products. To focus this discussion, we define *established* payments to include paper checks, recurring transactions transferred through the ACH, credit card and debit card transactions made with magnetic-stripe cards, and wire transfers. To this base, enhancements, innovations, and rules are added to address newly identified market opportunities or to take advantage of expanding technical capabilities. Sometimes innovations are sufficient to yield a distinguishably new payment method. Thus, we define *emerging* retail payments as those newly introduced payment methods that differ from established payments in a significant way—that is, technologically, contractually, legally, or conceptually.

Third, every payment method involves risk. The Bank for International Settlements' Committee on Payment and Settlement Systems identifies five major categories of risk associated with payment transactions: fraud, operational, legal, settlement, and systemic.[13] Generally, other types of risk are subcategories of these five broad types. Emerging payment methods may be particularly susceptible to fraud and operational risks. They may also carry enhanced legal risk simply because case law is less well developed or because the drafters of established laws and regulations may not have foreseen some of the ways in which payments are initiated, processed, and settled. Definitions of the three risks mainly associated with emerging payments are presented in the box.

A payment method may also carry risks not directly associated with the success or failure to transfer value. Instead, indirect problems may arise that appear ancillary to the financial transaction. For emerging retail payment methods, two risks of this type are notable: data security risk and risk of illicit use. In these cases, the payment methods function and transfer value correctly, but something underlying the transaction is "bad."

Data security risk is a form of operational risk involving unauthorized modification, destruction, or disclosure of data used in or to support transactions. For example, a data security breach may facilitate identity theft, which could trigger later harm to a party in a transaction or an otherwise uninvolved party elsewhere in the system.

The risks present when new or still-emerging payment methods are used are not wholly different from those present in long-established methods of payment.

Risk of illicit use is the risk that a payment method may be used for illegal purposes, for example, money laundering, terrorism financing, or the purchase of illegal goods and services such as drugs or child pornography. Similarly, the ease with which criminals can launder stolen funds or finance terrorists with legitimately earned funds affects not only the victims of the crimes that give rise to the "dirty" funds, but society as a whole.

[11] Massachusetts Bankers Association, "Massachusetts Banks Now Reporting That Fraud Has Occurred Due to the TJX Data Breach," press release, January 24, 2007, available at <http://www.massbankers.org/pdfs/TJXfraudNR.pdf>. Also see "Massachusetts, Connecticut Bankers Associations and the Maine Association of Community Banks and Individual Banks File Class Action Lawsuit Against TJX Companies Inc.," press release, April 24, 2007.

[12] Joseph Pereira, "Breaking the Code: How Credit-Card Data Went Out Wireless Door: Biggest Known Theft Came from Retailer with Old, Weak Security," *Wall Street Journal*, May 4, 2007.

[13] Bank for International Settlements (2000).

Major Risks in Emerging Payments

Type of Risk	Definition
Fraud	Risk of financial loss for one of the parties involved in a payment transaction arising from wrongful or criminal deception. The risk that a transaction cannot be properly completed because the payee does not have a legitimate claim on the payer.
Operational	Risk of financial loss due to various types of human or technical errors that disrupt the clearing and settlement of a payment transaction. The risk that a transaction cannot be properly completed due to a defective device or process that precludes the completion of all the steps required in a transaction.
Legal	Risk that arises if the rights and obligations of parties involved in a payment are subject to considerable uncertainty.

Source: Bank for International Settlements (2000).

3.1 Some Insights from Economic Theory

Risk Containment as a Good

Economic theory offers some useful concepts for understanding risk in payments systems. All payments systems are systems for managing valuable information: They keep records of transactions and communicate transaction data. Any information stored and transmitted by a payments system can be described as an economic *good*, an item having value in exchange.

Thanks to modern information technology, emerging payment methods can offer tremendous efficiency gains over traditional methods of making payments. Electronic data can be easily stored at a few locations and then shared among payments system participants at very low cost. Payment data thus meet Varian's (1998) description of a *digital good*, a good that can be stored and transferred in digital form.

Varian argues that digital goods are different from standard, physical goods (such as cornflakes, sneakers, and minivans) in that they are *nonrival goods.* A nonrival good is one whose value does not diminish with any one individual's use or consumption of it. A textbook example of a nonrival good is broadcast television: One's consumption of a TV show does not diminish the quantity available for consumption by another individual. Other examples of digital goods that are nonrival goods are recorded music, video, and computer software. The data managed by modern payments systems are another example of this type of good: The use of a credit card in one electronic transaction does not diminish the ability to use it in another transaction so long as the credit limit is not exceeded. (Credit, cornflakes, and sneakers are not nonrival goods; they get used up.)

Any information stored and transmitted by a payments system can be described as an economic good, an item having value in exchange.

Central to the value of any digital good is data integrity—garbled music or video is useless, for example. The usefulness of payment data can be diminished by fraud and security breaches or by operational disruptions that make it difficult to transmit data. Consequently, we argue that the integrity of payment data is also a nonrival good. If a payments system participant secures a facility against operational disruptions and fraud, it creates an environment conducive to smooth operation of the payments system, generating benefits for other participants as well.

Nonrival goods are classified as *club goods* or *public goods* according to whether access to the good can be limited. A club good is a nonrival good that a group or individual can be stopped or excluded from consuming. For example, cable television firms exclude nonsubscribers from their service by encoding their signals and giving decoders only to paying subscribers. A public good is a nonrival good for which access cannot be limited. National defense, for example, is a nonrival public good because everyone in a country is covered and no one can be excluded from the benefits.

In the case of actions to contain fraud and operational risks in emerging payments, the club good description is perhaps the most appropriate. Successful private sector payment providers (for example, credit cards, debit cards, and ATM networks) have by and large managed to contain fraud.[14] They also maintain operating procedures and auditable controls to limit operational risk. Participation in these systems is limited by membership rules, and participants (individuals, merchants,

[14] Reported fraud rates for credit card transactions are about 5 basis points of value, and similar fraud rates are reported for checks (Nilson Report). Industry representatives report that actual rates may be a little higher (Green Sheet). Visa reports an operational "reliability rate of 99.999 percent" ("Securing Payments: Building Robust Global Commerce," 2005, available at <http://whitepapers.zdnet.com/whitepaper.aspx?&scname=Bank+Management&docid=152783>).

banks, and processors) associated with high levels of fraud or operational snafus can be expelled.

There are natural limits to the power of exclusion, however. Since every payments system is a type of communications network, excluding too many network participants lowers the network's value for those parties that remain. There will always be a trade-off between security and inclusiveness.

Why Containing Fraud and Operational Risks Is Difficult

Hirshleifer (1983) describes a model of a nonrival good that is particularly applicable to data integrity in electronic payments systems. He describes the problem of people living in a "polder," a low-lying patch of land protected from flooding by a system of dykes. Each resident of the polder is responsible for maintaining the portion of the dyke that abuts his or her property. The dyke clearly provides a nonrival communal good: flood protection for all residents of the polder.

In this example, the degree of flood protection provided depends exclusively on the height of the lowest portion of the dyke. In other words, the degree of protection will not be determined by the *total* flood-mitigation efforts of everyone living inside the dyke, but rather by the one resident who exerts the *least effort* in maintaining the dyke. The analogy with emerging payments is straightforward: The risk mitigation effort of each party in the particular payments system to maintain data integrity prevents fraudulent data from circulating in the system, and a commitment to operational excellence allows others in the system to complete their transactions effectively.

A data breach or operational disruption in one portion of a payments system can open the metaphorical floodgates to problems throughout the entire system.

There are obvious parallels between flood protection in Hirshleifer's polder model and the mitigation of fraud and operational risks in payments systems. The 2005 data breach at CardSystems Solutions, for example, resulted in problems not only for CardSystems, but also for numerous other users of card payments systems—cardholders, merchants, banks, and processors. A data breach or operational disruption in one portion of a payments system can open the metaphorical floodgates to problems throughout the entire system. The potential for rapid propagation of fraud and operational disruptions is the flip side of the efficiency of electronic payments.[15]

Varian (2004) points out some difficulties in the provision of such nonrival goods. Because the amount of mitigation depends crucially on the participant that exerts the least effort, and because different system participants have different amounts at stake, there is a significant risk that participatory incentives will not be uniform. Participants with a lot at stake—that is, those with high net benefits from more mitigation activity—will prefer a higher level of protection from the risk in question than those with lower net benefits are willing to support. However, because overall protection depends on the participant that exerts the least effort, the latter group determines the overall level of risk mitigation.

The problem of nonuniform risk management incentives crops up regularly in payment situations. Various stakeholders in payments systems will naturally prefer different levels of mitigation in the system. The longer the supply chain or the larger the network for a given payment technology, the greater is the potential for disagreement about the appropriate level of mitigation.

Many different providers of services are integral to the processing of electronic payments. These providers include encryption firms, processors that route transaction data, and Internet service providers, among others. However, because minimizing fraud and operational risks requires effort from all participants, some mechanism is needed to give all participants the right incentives to "maintain the dyke." Private contracts, laws, and regulations can each play a beneficial role in creating such incentives.

Confronting Fraud and Operational Risks

Despite the difficulties outlined above, experience has shown that all successful payments systems have learned to keep fraud and operational risks at fairly low levels. Competition among payments systems gives important incentives to service providers to mitigate these risks. Systems that fail to contain risks do not survive in the payment marketplace.[16]

Service providers have developed three broad approaches to managing various kinds of payment risk: pricing, insurance, and containment.

[15] For a formal exposition of this point, see Kahn and Roberds (2005).

[16] "Thinking Like a Criminal," *Arizona Republic,* August 24, 2006, recounts how an entity that tried to compete with PayPal in the mid-1990s was closed down by Visa because as many as "three out of five . . . transactions turned out to be fraudulent."

- *Pricing* means that a party that bears a risk is compensated appropriately. Pricing is extremely important in allocating credit risk—banks that issue credit cards charge higher prices, in the form of higher interest rates on borrowing and higher annual fees for cards, to subprime cardholders who they believe are less likely to pay their balances. Issuing banks willingly bear a high level of credit risk on these cards because the higher interest earned compensates for the greater risk taken.[17]
- *Insurance* is an agreement between two parties as to who will bear a loss when one occurs. Thus, for instance, a merchant that receives a credit card payment is insured against the risk that the cardholder will not be able to pay the balance.
- *Containment* is a catchall term for activities that tend to deter or suppress risk. In the case of fraud risk, examples include swiping a credit card through a card reader to verify that the card is valid and asking for extra identification.

For fraud risk in particular, the effectiveness of the pricing and insurance approaches is limited by factors known as *adverse selection* and *moral hazard*.[18]

Adverse selection refers to situations in which undesirable outcomes result from asymmetric information among various parties to a transaction. Pricing works best to offset risks that are known and can be quantified in advance. When the payee and payer are anonymous to each other, the payee cannot know if the payer poses a bad risk and is likely to make a fraudulent payment. Correspondingly, the payer cannot know if the payee is selling legitimate goods. Particularly when commerce is conducted remotely (for example, over the Internet or by telephone), adverse selection undermines incentives to play by the rules. "Bad actors" can optimize their own malign incentives, undermining the confidence of legitimate merchants and consumers.

Moral hazard describes the effect of insurance on the incentives and thus behavior of an insured party. The availability of insurance can lead to opportunistic behavior on the part of the insured at the expense of the insurer. For example, a merchant that accepts payments via cards branded by a major network like Visa, MasterCard, or American Express is insured against credit risk (and sometimes fraud risk) and consequently may not have an incentive to make sure that a payment is legitimate and within a cardholder's credit limit. The card networks and their issuing banks, which provide the insurance, contain the risks by imposing on merchants authorization and authentication procedures that create appropriate incentives and guard against fraudulent card use.

Of course, moral hazard can arise on the payer's side, too—for example, when the right of a credit card holder to dispute a transaction may tempt the cardholder to claim that fraud was committed when it was not. Authentication procedures, particularly the collection of signatures at the point of sale, are designed to contain this form of moral hazard.

Experience has shown that all successful payments systems have learned to keep fraud and operational risks at fairly low levels.

Moral hazard can also lead to opportunistic behavior that magnifies operational risk in payments systems. A payment processor might fail to spend the resources to maintain sufficient backup facilities—in the case of, say, a natural disaster knocking out a key data center—because the negative consequences of failing to maintain backup data do not accrue fully to the processor, but rather to thousands of other individuals and businesses as well. Card networks impose backup and resiliency standards to offset the lack of private incentives and contain this particular risk.

But pricing and insurance alone are not sufficient risk management techniques: Credit card issuers do not seek out cardholders who are likely to commit fraud, then attempt to recover the costs through differentially higher fees or interest rates; ACH operators do not offer two fee schedules, one for reliable and another for unreliable originating banks; and providers of payment services are generally reluctant to give unknown buyers and sellers guarantees against loss.[19]

Containment Techniques

Containment of fraud and operational risks requires cooperation among payments system participants. All need to have incentives to undertake actions that will keep fraud and operational risks down to acceptable levels. These incentives can be provided by monitoring system participants and then imposing penalties for inadequate risk controls that can lead to significant losses or disruptions.

Monitoring is the foundation of containment: Checking on participants will reveal whether they are engaging in appropriate levels of risk mitigation. But monitoring is unlikely to be

[17] About 4 percent of balances are never paid off.

[18] These problems generally plague information security; see Anderson and Moore (2006).

[19] Provisions in the Federal Reserve's Regulations E and Z, which implement the Electronic Funds Transfer Act and the Truth in Lending Act, respectively, impose some insurance requirements.

effective without some system of penalties for noncompliance. Monetary fines serve as deterrents. Contracts and laws assign legal liability for failures, which can be costly if breached, while some regulations establish performance standards and impose penalties when they are not met. Varian's (2004) theoretical analysis of the polder model, described earlier, suggests that relatively severe penalties—beyond the economic cost of a security lapse—may be necessary to ensure compliance.

Limitations on liability mean that penalties cannot do the whole job. In cases of fraud, the party most deserving of punishment, the fraudster, is usually long gone by the time the fraud is discovered. Even in cases where liability for a fraud or operational incident can unambiguously be assigned to a known party, there may be no practical level of penalty that could cause the guilty party to internalize the consequences of its inadequate risk controls. Sometimes the threat of the ultimate penalty—exclusion—may be the most effective deterrent: Payments system participants that fail to maintain adequate operational standards or fraud controls may be barred or expelled from the system.

> *[There are] a variety of techniques—pricing, insurance, and containment—for creating incentives for participants in retail payment transactions to mitigate fraud and operational risks.*

Thus, we have a variety of techniques—pricing, insurance, and containment—for creating incentives for participants in retail payment transactions to mitigate fraud and operational risks. Underlying structural aspects of many electronic retail payments—particularly their nonrival nature—and the concomitant ability to limit access to the payment networks make containment techniques especially useful for creating deterrence tools.

3.2 Special Concerns for Emerging Payments Systems

Any viable payments system must find ways to maintain the integrity of payment data, but certain concerns are unique to emerging payment methods.

First, there is a "newness factor." The novelty of emerging payment methods implies that various problems may not be anticipated and therefore adequate safeguards and procedures may not be in place to address them. Emerging methods face a learning curve when confronting these issues. As evidenced by their survival and success, established payment methods have devised ways to mitigate these risks. The key question regarding emerging payment methods is whether their providers have the incentives and means to overcome the risks that could otherwise hinder widespread adoption.

Competition gives important incentives to payment method providers to mitigate many of these risks. Users can choose from many payment methods, and their choices reflect the extent to which the methods best facilitate smooth, low-risk transactions. In competition with payment methods less susceptible to fraud or operational failures, providers of new payment methods have clear incentives to address those risks. Failure to do so jeopardizes a method's viability. As in other markets, competition among payment methods is an important mechanism to induce providers to address these problems.

New payment technologies can improve economic welfare by allowing diverse participants—consumers, merchants, banks, and nonbank service providers—to exchange payment data in ways not previously possible. The value of these technologies hinges, of course, on data integrity. Successful payments systems will find ways of coordinating the behavior of diverse parties to facilitate data exchanges that serve their mutual best interests.

Data Integrity and Privacy

Integrity of payment data is important not only as a safeguard against fraud and operational interruptions, but also for maintaining participants' privacy. Privacy issues have come to the fore in recent months. A group known as the Privacy Rights Clearinghouse reports that more than 165 million records have been compromised by data security leaks since February 2005.[20] Such data breaches create potential for fraud, identity theft, and general loss of privacy.

Similar to other aspects of payment data integrity, the maintenance of participants' privacy constitutes a nonrival good. By preserving the privacy of its legitimate participants, a payments system encourages widespread participation and enhances the value of the system to all users. But as discussed above, nonrivalness can make it difficult to reach agreement among payments system participants on the necessary level of privacy protection.

[20] See <http://www.privacyrights.org/> (accessed September 7, 2007).

Maintaining privacy is tricky because, by nature, it runs counter to the payment function: Every type of payment requires the exchange of some information, which under the wrong circumstances can be subject to misuse. For a consumer to use a credit card to buy something from a merchant, for example, he or she must give the credit card information to the merchant. The consumer's surrender of credit card information is essentially a compromise between the merchant's need to identify the consumer and the consumer's desire to remain anonymous to prevent misuse of his or her personal information. The merchant obtains enough information about the consumer to determine that the transaction is legitimate, but no more. Under some circumstances, maintaining privacy can conflict with the goal of preventing fraud, as Stigler (1980) points out. Moreover, Katz and Hermalin (2006) discuss efficiency reasons for privacy that suggest that the full sharing of private information within a payments system could be inefficient, even in the presence of fraud risk. Every successful payments system has to reach a workable compromise between these two facets of transaction privacy.

Illicit Use

Unlike many risks associated with payments systems, the use of a payment method for illicit purposes (such as money laundering, financing of terrorism or crime, or the purchase of illegal goods) rarely involves direct risk of financial loss to a participant in the payment transaction. Thus, unlike many operational risks, the use of a payment method for illegal activities does not pose a risk as such for other users of that payment method. In this case, the payment method works as designed, but individuals use the method for nefarious purposes external to the payments system itself. Rather than creating financial risk to direct participants in a transaction, illicit use introduces or carries broader societal risks. Since monetary gains are one determinant of the level of criminal activity, erecting obstacles and deterrents to these activities supports an important public good.

Unfortunately, many of the features that provide value for legitimate transactors can also make them susceptible to misuse by individuals engaging in money laundering and terrorism financing. Features that suggest the potential for a payment method to be used or misused for illicit purposes include speed of value transfer, transportability, intermediation, anonymity, quantity limits, network connectivity, and ease of interface. A common feature of many of these methods, especially electronic methods, is the speed with which value can be transferred. While the relative speed of the transactions is generally a desirable feature in the general market—it reduces certain types of fraud—it can also make it difficult to identify and preempt illicit transactions.

Similarly, some emerging payment methods involve highly transportable stores of value, either in physical or electronic form. Diverse participation and a high degree of privacy, both of which are features that make a payments system attractive for legitimate users, can make it easier to mask illicit use. Some emerging payment methods operate with little or no involvement of conventional financial intermediaries such as banks, making it difficult for authorities to monitor and identify illicit use. Network connectivity addresses the breadth of uses of a payment method and may alter its attractiveness as a store of value. The interfaces through which transactions are initiated may alter the ability to identify illicit transactions. In practice, it may be hard to distinguish between "user-friendly" and "illicit-user-friendly" platforms.

> *Rather than creating financial risk to direct participants in a [payment] transaction, illicit use introduces or carries broader societal risks.*

Like other types of nonrival goods, payments systems can guard against illicit use through the use of monitoring and penalties (including criminal penalties) and through the exclusion of miscreants. But the high degree of similarity between the needs of legitimate and illegitimate users of payment technologies, as well as the need to balance societal costs and benefits, suggests that some amount of criminal use and other socially undesirable activity will always slip through. Society's determination of what constitutes an acceptable threshold of illicit use is a complex and thorny issue that goes beyond the scope of this article.

4. Three Examples of Risk and Its Management in Emerging Payments

We present three informal case studies to illustrate how characteristics of new payment methods affect potential risk, how key participants act to mitigate those risks, and how participants' actions demonstrate the economic principles described above. The three payment methods are: 1) general-purpose prepaid cards, 2) e-check payments through the ACH system, and 3) proprietary online balance-transfer systems such as PayPal. Each incorporates new technologies, new networks, and new rules to create an entirely new payment method. These examples are not intended to demonstrate the full range of payment options. They are used in different venues, employ different means for initiating payments, and clear and settle transactions differently; yet they employ similar risk mitigation strategies. (The appendix describes our selection of the case studies.)

While the payment methods in these case studies are not immune to all types of risk, we concentrate on fraud, operational, and illicit use risks because emerging methods appear particularly susceptible to these problems. The case studies focus on those areas of emerging payments that differ from established payment types. To the extent that an emerging payment is initiated using new technology but clears and settles through an established settlement network, our discussion examines the new front-end mechanism but excludes the clearing and settlement portion.

4.1 General-Purpose Prepaid Cards

General-purpose prepaid cards, branded by a payment network such as Visa, MasterCard, American Express, or Discover, can be used by all merchants that accept that network brand. Introduced in the 1990s, the cards function similarly to credit and debit cards at a point of sale: A customer swipes a plastic card through a standard reader, and the transaction is authorized and settled through a card network. In addition, some cards can be used to withdraw funds from ATMs and to make remote purchases or pay bills, similar to debit cards.[21] Cardholders can often check the balances available on their cards through a website or telephone response system.

General-purpose prepaid card programs differ in price, product functionality, customer identification requirements, value limits, and levels of cardholder protection. Their distinguishing characteristic is that they require cardholders to turn over funds in advance for future purchases of goods and services. Frequently, the funds on these cards can be reloaded at a variety of outlets, such as at merchants, over the Internet, or through ATMs. This feature allows a cardholder to use a single card without replacement or interruption, thus increasing the card's value as a potential substitute or complement to a formal banking relationship.[22]

Risk Analysis

The advance-payment feature substantially mitigates credit or nonpayment risk in general-purpose prepaid card products, allowing such cards to be marketed widely and distributed directly to consumers by nonbank third parties, referred to as card sponsors. Although every payment card must be issued by a bank, a nonbank sponsor's logo often appears as the most prominent brand name on the card. The broad involvement of nonbank institutions in the distribution of general-purpose prepaid cards stands in contrast to the common practices of traditional debit and credit card programs.

Since general-purpose prepaid cards use the credit and debit card infrastructure for transactions, clearing, and settlement, they share the risks inherent in these more mature financial products. These cards also exhibit a number of new risks, including a complex supply chain that often involves nonbank third parties at vulnerable stages of delivery and an increased susceptibility to money laundering and illicit transactions.

For general-purpose prepaid cards, nonbank institutions often stand between the cardholder and the bank that issues the card. In many cases, the nonbank institutions maintain the primary relationship with the cardholder. This prominent role for a third party in initiating and maintaining customer relationships can complicate the regulatory treatment of cards and introduce credit risk for the bank issuers and, potentially, the cardholders. The third-party entities could go bankrupt or be subject to various operational failings that would be less likely to impact accounts at a supervised and FDIC-insured financial institution. The involvement of the major card associations and the fraud detection that they bring to bear appear to deter illegal activity. News reports recount instances of fraud, however, such as using stolen credit cards to purchase prepaid cards at a self-serve checkout counter.[23]

Since general-purpose prepaid cards use the credit and debit card infrastructure for transactions, clearing, and settlement, they share the risks inherent in these more mature financial products.

[21] Payroll cards are a similar application, but differ dramatically in terms of the business model used for marketing and distribution and in terms of regulatory coverage. Payroll card programs are not discussed here.

[22] See McGrath (2007) for further discussion of the functionality and market position of prepaid cards.

[23] David Hench, "Savvy Thieves Use Gift-Card Scam to Fool the System," *Portland Press Herald/Maine Sunday Telegram*, February 21, 2007.

Additionally, third-party nonbanks may not have the same level of data security that banks have, potentially exposing consumer data to greater risk of theft. In particular, third-party distributors may fail to impose uniform data security standards for their retailers, a security lapse that increases risks for data gathered and stored at the point of sale.

A downside of the flexibility provided by cards able to facilitate nearly anonymous transactions is that they are attractive vehicles for abuse by illegal enterprises.[24] The Drug Enforcement Administration, Immigration and Customs Enforcement, and Internal Revenue Service–Criminal Investigation each allege that prepaid cards are used in bulk cash smuggling. They explain that drug dealers load cash onto prepaid cards and send them to their drug suppliers outside the country who use the cards to withdraw money from a local ATM.

This potential for illicit use is exacerbated if card issuers or sponsors operate offshore because it makes it harder to enforce relevant regulatory requirements. In fact, some general-purpose prepaid card products are openly marketed as a convenient way to circumvent law enforcement and tax authorities. For example, a prepaid card called the Freedom Card used to promise, among other things, "a fully anonymous ATM debit card . . . requiring no phone numbers or IDs . . . no daily cash withdrawal or loading limits . . . real-time card funding with any e-currency, PayPal, Western Union or bank wires."[25] The card was originated by an offshore financial institution, but it could be used to obtain funds throughout the world. This product appears not to exist any more. While such offerings are often short-lived, dubious new products emerge regularly.

Mitigation

Efforts are also under way to deal with the illicit use and data security risks. An industry task force says it is in the process of creating "AML [anti-money laundering] best practices guidelines" in response to anticipated regulations from the U.S. Treasury's Financial Crimes Enforcement Network aimed at thwarting money laundering and terrorist financing through prepaid cards.[26] The major card networks have issued guidelines to the issuing banks that are intended to reduce the attractiveness of prepaid cards for money laundering.[27] These include capping the stored dollar amount per card, limiting the frequency with which and the value of funds that can be reloaded, obtaining and confirming certain customer data prior to approving card applications, and providing liability protection for consumers in the event of card loss or fraudulent usage.

The operational and fraud risks of general-purpose prepaid cards are evidenced by: 1) a more complicated supply chain for providing the cards, often involving nonbank third parties in primary customer relationships, and 2) the potential for illicit transfer of funds. Domestic and international law enforcement officials are particularly interested in mitigating the latter risk.

> *The major card networks have issued guidelines to the issuing banks that are intended to reduce the attractiveness of prepaid cards for money laundering.*

4.2 ACH e-Checks

Over the last decade, the National Automated Clearing House Association (NACHA), which sets rules for ACH transactions, has gradually developed rules and formats for six new electronic debit transactions, referred to as *e-checks*. These e-checks allow banks and their clients to convert checks or information from checks into ACH debits.[28] The following discussion describes two types of e-check transactions—accounts-receivable conversion (ARC) and telephone-initiated (TEL) transactions—to illustrate the risk factors and mitigation trade-offs associated with these new transaction types.

ARC rules permit businesses to transform checks mailed by bill-paying consumers into ACH debits. In the fourth quarter of 2006, the 613 million ARC transactions initiated accounted

[24] See Money Laundering Threat Assessment Working Group (2005), Financial Action Task Force (2006), and Sienkiewicz (2007).

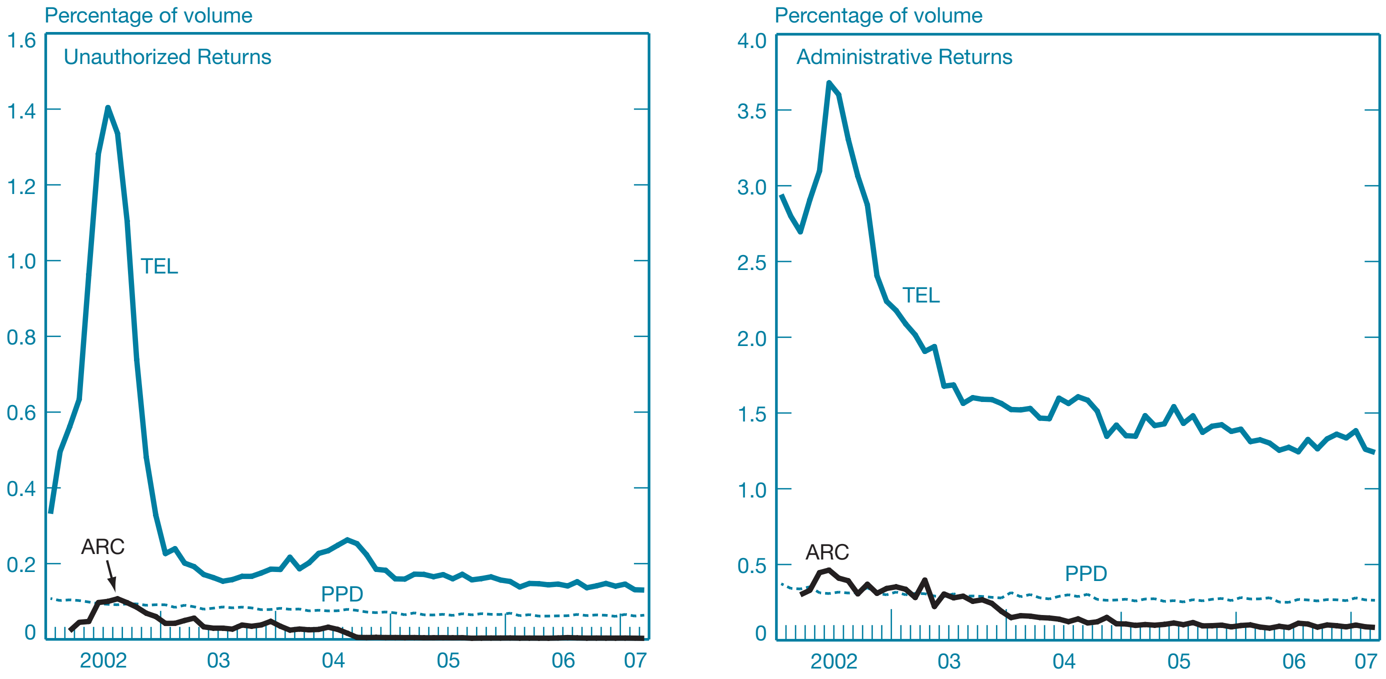
[25] See <http://www.freedom-cards.com> (accessed mid-2006).

[26] See <http://www.cardassociation.org> for information on Network Branded Prepaid Card Association efforts.

[27] As reported in Money Laundering Threat Assessment Working Group (2005).

[28] NACHA members include financial institutions and regional clearinghouse associations. NACHA manages the development, administration, and governance of the ACH system. Its rules provide more than fifteen worktype codes for different types of payments—such as corporate-to-corporate payments, recurring payments, point-of-sale payments, and e-check payments—as a means to identify specific rules, formats, and uses. Historically, the ACH has typically been used for direct deposit of payroll and Social Security payments and to collect recurring monthly mortgage, insurance, student loan, and business-to-business payments. For more information, see <http://www.nacha.org/About/default.htm>.

Return Rates for Selected Automated Clearinghouse (ACH) Applications, 2002-07



Source: Federal Reserve System.

Notes: Return rates are calculated from monthly Federal Reserve ACH data; ARC, PPD, and TEL are accounts-receivable conversion, preauthorized payment and deposit, and telephone-initiated transactions, respectively.

for more than half of e-check volume. Use grew by about one-third over the prior year: Roughly 6 percent of checks written are now being converted to electronic debits under ARC rules.[29]

TEL transactions are debits to consumers' accounts authorized by the account holder via telephone to a merchant, vendor, or service provider. These transactions make one-time ACH payments available when written authorizations are not feasible.[30] The 76 million TEL transactions processed during the fourth quarter of 2006 reflect a 16 percent increase over the previous year. TEL transactions account for about 7 percent of e-check volume.

ACH transactions that fail to clear (because of, for example, insufficient funds, errors in processing, or suspected fraud) are returned along with a code indicating the reason for the return. Return rates are useful indicators of risk because the standardized return reason codes indicate what type of problem caused the clearing failure. Typically, high levels of specific return codes indicate high levels of specific risks. For example, various processing-problem codes identify administrative returns that can indicate operational problems, whereas returns of transactions not authorized by an account holder (known as unauthorized transactions) can indicate fraud problems.

The chart presents historical rates for ARC and TEL for the types of returns most likely to suggest administrative or fraud problems. It also shows parallel return rates for preauthorized payments and deposits (called PPD), which is the most widely used recurring, non-e-check debit transaction and serves as a useful comparison.

There are similarities and differences in the records of ARC and TEL returns. In the fourth quarter of 2002, ARC return rates for both unauthorized and administrative returns were similar to those for PPD debits, but by the fourth quarter of 2006 they had fallen below the rates for PPD debits. In the fourth quarter of 2002, TEL return rates were some six to eight times the rates for PPD debits, and although they have since fallen, TEL return rates remain at least twice those for PPD debits. Overall, ARC and TEL each had high return rates in their introductory periods and the rates declined over time. ARC return rates today are very low, whereas those for TEL remain relatively high.

[29] Bank for International Settlements (2006, p. 157) reports that 33.1 billion checks were paid in 2005. ARC transactions are written as checks but paid as electronic debits.

[30] NACHA rules restrict TEL transactions to prevent their use for "cold-call" telemarketing, but they can be used when there is a preexisting relationship between merchant and consumer or when the consumer initiates the call.

Risk Analysis

ARC and TEL transactions share some risks with other ACH debit transactions, but differ in risks that are driven by the location at which the payments are initiated and the relationships among the parties to each transaction.[31] For ARC, retail lockbox processors convert checks sent by consumers to billers. Lockbox staff use high-speed equipment to capture coded information from the remittance slips and checks. The lockbox business is highly concentrated, mature, and controlled. In many cases, these processors operate as subcontractors to the originating banks, supporting the banks' cash management product offerings. In contrast, TEL transactions rely on customer input of account information via telephone, a context in which the data and customer's identity cannot easily be verified.

For ARC, the largest risk is operational. ARC rules initially made business checks ineligible for conversion to an ACH debit. Early problems included inadvertent conversion of business checks, particularly those that are the same size as consumer checks. Banks on which these checks were drawn often returned the transaction.[32] Another early problem was that processors could not properly match the ARC payment to the appropriate checking account: During a pilot program, one bank reported its associated administrative returns were as high as 10 percent.[33]

Inadequately researched bank relationships can undermine the "gatekeeper" function in [the telephone-initiated] payments system.

For TEL transactions, fraud is a larger risk, perhaps augmented by operational risk caused by various participants in its supply chain. TEL is designed for ad hoc transactions between merchants and consumers, some of whom do not have a preexisting relationship. A long-standing business relationship is thus often absent, which increases the likelihood of either seller or buyer fraud. Adding to this risk is the fact that TEL opened the ACH network to new merchants and businesses, including some telemarketers and bill collectors, that may not have received sufficient scrutiny or monitoring from the banks through which they originate their transactions. Inadequately researched bank relationships can undermine the "gatekeeper" function in this payment method, making it difficult to deny dishonest originators access to the ACH network. Use of third-party service providers for TEL can compound the difficulty of identifying illegitimate initiators by adding an intermediary between the payment-originating bank and its ACH debit-originating clients.

Mitigation

Many of NACHA's rules and procedures aim to control and mitigate these risks. NACHA defines the rights and responsibilities of ACH participants, including originators (merchants, lockbox operators, and other businesses that initiate ACH payments) and originating banks (banks that provide ACH services to originators). Originators are required to follow NACHA rules and procedures when preparing and submitting ACH payments. Originating banks warrant certain aspects of ACH transactions and are financially liable for returned transactions. To help control this liability, originating banks typically use contract language to shift risk to originators. Originators are thus given financial incentives to correct and avoid processing problems.

When the problem arose of business checks being converted inappropriately, ARC originators reconfigured processing equipment to improve separation of business checks and worked to change NACHA rules to permit conversion of the business checks that were hardest to identify.[34] Originators also reduced administrative returns by building databases to match ARC payments and checking accounts.[35] NACHA requires a lockbox processor or its bank to keep check images for two years, but to destroy the physical check within fourteen days. Such measures help mitigate fraud risk and simultaneously decrease the risk of processing a check twice.

NACHA rules also require originating banks to gather sufficient information to understand the background and business of any new originator that may be given access to ACH services. This gatekeeping function generally keeps dishonest originators out of the ACH network, but it proved inadequate for TEL transactions. As illustrated by the Assail example

[31] Shared infrastructure and processes can contribute to risks in certain ACH payments. The ACH network does not use real-time authentication and authorization, and there are no centralized databases of originators accused of fraudulent use of the ACH system. These are mitigation techniques used by other payment networks.

[32] Daniel Wolfe, "Dealing with the Accidental Conversions," *American Banker*, December 8, 2004.

[33] Steve Bills, "Pilot Done, Wells to Widen Lockbox Conversion Effort," *American Banker*, October 18, 2002.

[34] Daniel Wolfe, "Dealing with the Accidental Conversions," *American Banker*, December 8, 2004. Note that effective September 15, 2006, business checks that do not carry an indicator in the auxiliary on-us field of the MICR line can be converted to ACH debits.

[35] Steve Bills, "Pilot Done, Wells to Widen Lockbox Conversion Effort," *American Banker*, October 18, 2002.

described earlier, telemarketing was one source of fraud that resulted in high return rates for TEL transactions.

As evidence of problems with TEL transactions mounted, NACHA intervened directly with originating banks and outside of its normal processes. NACHA and its member banks identified the specific TEL originators responsible for initiating many of the transactions that were subsequently returned, and these originators were shut down.[36]

Various participants in the ACH system have taken steps to improve the effectiveness of originating banks as gatekeepers. These steps include the introduction of NACHA rules requiring originating banks to screen and monitor originators and to execute the appropriate contracts.[37] Additionally, in June 2003, NACHA instituted a monitoring process to flag originators with TEL returns exceeding 2.5 percent. Outside of the NACHA framework, ACH operators have introduced risk monitoring services and rule changes, and federal regulatory agencies increased the attention given to these transactions in their guidelines on controlling risk in retail payments.[38] These actions were followed by a rapid decline in returns, suggesting that monitoring, enforcing rules, and limiting access to the ACH network have been successful strategies for risk mitigation.

Although these mitigation efforts reduced TEL return rates, the return rates remain higher than NACHA would like. Thus, NACHA is pursuing additional proposals to make monitoring return items and resolving problems more effective. To address risk issues beyond those of TEL more broadly, NACHA also reorganized its risk management infrastructure, creating a Risk Management Advisory Group to help implement a new risk management framework.[39] Subsidiary work groups are attempting to address three areas of risk mitigation: 1) control of access to the ACH system, 2) the monitoring and control environment, and 3) enforcement activity. Additionally, to increase the visibility of risk management at ACH originating banks, the Office of the Comptroller of the Currency issued a guidance document in September 2006 requiring that key ACH statistics be reported to banks' boards of directors and senior officials.[40]

4.3 Proprietary Online Balance-Transfer Systems

Among the payment options that arose for Internet commerce are proprietary online schemes to transfer balances of funds between accounts. In this type of scheme, customers establish an account with a service provider, such as PayPal, and use e-mail messages to initiate payments.[41] If both parties to a payment have accounts with the same service provider, the service provider simply transfers monetary balances between their accounts. At PayPal, most customers are buyers and sellers (small businesses and individuals) involved in online transactions, usually at an auction site. The service is also used by small online companies and by individual customers who value the ability to transfer funds from person to person. Neteller, a similar service provider, is widely used for payments to online gaming sites.[42] Other online person-to-person payment providers that follow a proprietary balance-transfer or similar model include GreenZap, StormPay, and eGold.[43] We call these providers *proprietary online balance-transfer systems.*

Among the payment options that arose for Internet commerce are proprietary online schemes to transfer balances of funds between accounts.

PayPal, the largest and most well-known online payment service provider, uses the proprietary online balance-transfer approach and intermediated almost $23 billion in transactions during the first half of 2007. PayPal is larger and more sophisticated than any of its competitors. eBay, the huge online auction business, acquired PayPal in 2002, and eBay

[36] Wells Fargo, "Waging War on ACH Fraud," <http://www.nacha.org/ACHNetwork/ACH_Quality/WellsFargo_DB.doc> (accessed January 12, 2007).

[37] This includes establishing limits on ACH transactions and on return items, conducting audits, and making ad hoc contact to verify that the originator has represented its business appropriately in terms of the products it is marketing, its financial strength, and so on.

[38] For information on Reserve Bank services, see <http://frbservices.org/Retail/fedachRisk.html>. For information on Electronic Payments Network services, see <http://www.epaynetwork.com/cms/services/processing/value/001477.php>. See also Federal Financial Institutions Examination Council (2004, pp. 43-4).

[39] See *NACHA Risk Management Newsletter* 2, no. 2, pp. 1-2 (2006).

[40] See OCC Bulletin no. 2006-39, "Automated Clearing House Activities: Risk Management Guidance," available at <http://www.occ.treas.gov/ftp/bulletin/2006-39.pdf>.

[41] This discussion is our interpretation based on information from public sources; it is not based on conversations with anyone at PayPal. For detailed descriptions of PayPal's processes, see Bradford, Davies, and Weiner (2003) and Kuttner and McAndrews (2001).

[42] Neteller describes "the online gaming industry" as its "main market" ("President and CEO's Report for the Six Month Period Ended 30 June 2006," available at <http://investors.neteller.com/neteller/upload/1NLRInterims2006releaseFINAL11sep062.pdf>). As of early 2007, Neteller, based in the United Kingdom, did not permit U.S.-based customers to make gambling payments. See <http://content.neteller.com/content/en/member_businessupdate.htm> (accessed February 2007).

[43] Companies that have tried but failed to provide online services for consumer-to-consumer and consumer-to-business payments include Citibank, Yahoo!, and eBay, with their respective products C2it, PayDirect, and BillPoint.

transactions currently generate almost 70 percent of PayPal's dollar volume.

These service providers act as agents by accepting deposits from customers and allowing money to be transferred from one in-house account to another. Although specific arrangements vary, in-house account balances typically are funded from a bank account by ACH transfer or a buyer's/sender's credit or signature debit card. Frequently, funds can be withdrawn by check or by co-branded debit/ATM card, transferred to the user's individual bank account by ACH credit, or used for future transfers within the network.

Risk Analysis

Although the volume of activity suggests that this type of payment meets a market demand for rapid online payments, it remains an emerging payment method accompanied by a variety of risks. Examples of fraud, operational, and illicit use risks include: 1) fraud associated with simple enrollment and anonymity; 2) operational errors and malicious attacks, such as "phishing" and "pharming";[44] 3) operational risk associated with technological complexity and a complex supply chain; and 4) susceptibility to illicit use. Specific rules, processes, controls, and screening capabilities vary across providers, yielding different levels of unmitigated risk and affecting the availability of mitigation options.

The core philosophy of the proprietary online balance-transfer model is to permit easy, quick entry and 24-hour availability. Under this system, an unknown, possibly anonymous, seller can be positioned to perpetrate fraud or simply fail to live up to his or her side of a transaction. Such a dishonest seller could take the money and not ship the product. The buyer would then have to try to recover funds under the rules of the payment provider's user agreement or protection policy. To be covered under PayPal's Buyer Protection Policy, the seller must enroll in the verification program and the buyer must comply with other eligibility requirements.[45] In contrast, the user agreement for GreenZap, a smaller but similar service provider, indicates that it is not liable for any purchases or services and does not issue refunds for a product or service if the seller does not fulfill on commitments. GreenZap also states that members send funds to third parties at their own risk.[46]

Online businesses are also vulnerable to the risk of outages, and businesses with high visibility seem to be most attractive to those seeking to disrupt services and overcome security features. The size of PayPal (about 133 million accounts as of year-end 2006) and the speed at which technical changes are made to support its growth have, indeed, led to some significant system downtime and made PayPal subject to hacker attacks.[47] In addition, in October 2004, a site redesign crippled some of its operations, leaving the website unavailable for two days and subject to intermittent outages for several days thereafter.[48] Moreover, PayPal and eBay were the top phishing targets in 2005, representing 62 percent of all attacks, according to Netcraft, a company that tracks and blocks phishing sites.[49]

> *Proprietary online balance-transfer payment methods depend on complex, multistep processes. For the user, the tasks are kept simple. Behind the scenes, however, many parties . . . are involved in completing a transaction.*

Proprietary online balance-transfer payment methods depend on complex, multistep processes. For the user, the tasks are kept simple. Behind the scenes, however, many parties (including individuals, merchants, third-party service providers, the buyer's and seller's banks, and the ACH, debit card, and credit card networks) are involved in completing a transaction. As is the case generally in complex networks, the large number of digital "hands" and handoffs increases the difficulty of identifying and assessing risk severity and the exposures that can vary by user, channel, or product.

Intentional user anonymity makes these services susceptible to illicit use, such as money laundering or payments for illicit purposes. Only the service provider has information about user identities. While this structure protects users from fraud and

[44] Phishing employs social engineering and technical subterfuge to generate "spoofed" e-mails that appear to be from a legitimate company. It uses the company's logo and style to lead consumers to counterfeit websites designed to trick them into divulging private data such as account user names and passwords. In contrast, a pharming attack redirects visitors from a legitimate website to an unofficial location by exploiting technical and procedural security weaknesses that compromise the domain-name server.

[45] Ralph F. Wilson, "Assessing Criticism of PayPal," *Web Commerce Today*, March 15, 2002. Available at <http://www.wilsonweb.com/wct5/paypal_assess.htm>.

[46] GreenZap claimed 777,600 users at year-end 2006. See <http://www.greenzap.com/newz/Company_Update_Q3_Q4_2007.pdf>. See also the GreenZap User Agreement, available at <www.greenzap.com>.

[47] eBay, Inc., "eBay Inc. Announces Fourth Quarter and Full Year 2006 Financial Results," press release, January 24, 2007. PayPal does not disclose how many of the accounts are active or have been used recently.

[48] Jim Wagner, "PayPal Scrambling to Fix Site Glitch," *Internetnews.com*, October 13, 2004. Available at <http://www.internetnews.com/ec-news/article.php/3421031>.

[49] Sean Michael Kerner, "eBay, PayPal Rank High on Phish Lists," *Ecommerce*, January 6, 2006.

identity theft, it can also make it easier for users to transfer funds illegally because traditional enforcement authorities do not have identifying information. In addition, theft of identities outside of the network could provide criminals with sufficient information to set up false accounts that can be used for illegal funds transfers. Further, if a service provider allows international transfers, the payment process might be used to launder funds between domestic and offshore accounts.

Mitigation

As the leading service provider, PayPal has an incentive to invest in good risk management tools and oversight to protect its payment method. Its risk management, in turn, protects legitimate users and establishes standards for other online payment service providers. The following examples illustrate that PayPal, in conjunction with eBay, appears to have learned from its losses and risk exposures, creating systems, technologies, and rules that help control the risks that emerged in its early years. As a result of its efforts, PayPal says that its loss rate is four-tenths of 1 percent, well below that of the credit card industry.[50]

> *Online payment service providers have addressed the risk of illicit use and international exposure by placing limits on transfers and account balances for unverified accounts.*

To combat machine-based attacks, PayPal developed an account creation process that requires manual human input, which has blocked unmanned computer "bots" from opening accounts. It also created multiple levels of service, in which higher levels of account service require additional identity confirmation. The verified member program, for example, protects PayPal and creates a product it markets to customers. PayPal also retains the right to terminate service to any participant it suspects of not complying with its rules.[51]

In addition, PayPal developed background computer monitoring programs (named Igor and Ilya) to search for transaction patterns consistent with suspicious buyer or seller behavior. While these efforts have not totally eliminated fraud, they appear to have had some success: Statistics reported in the press show that merchants using PayPal have loss rates due to fraud that are noticeably below the e-commerce average.[52]

To prevent the risk of a data breach, PayPal says that it collects, encrypts, and stores sensitive customer information on servers not connected to the Internet. Additionally, to counter phishing and pharming, PayPal provides clear instructions on what to do if customers suspect they have received a phishing e-mail. When notified of a phishing attack, PayPal attempts to close down the perpetrator's site within twenty-four hours.[53]

PayPal limits its own risk inherent in its complex supply chain by specifying its own rights and responsibilities as well as those of its users in cases where errors, disruptions, or unauthorized transactions occur. The user agreement is complex, and it is updated as needed. Information on how PayPal establishes contracts or manages relationships with its suppliers is not publicly available.

Online payment service providers have addressed the risk of illicit use and international exposure by placing limits on transfers and account balances for unverified accounts.[54] PayPal relaxes these limits for its verified accounts, but the verification process exposes would-be criminals. As a result, PayPal may have become less useful for money laundering. It does appear possible, however, to launder large sums of money by sending small increments to many accounts using a mass-pay type of function.[55] To counter the above risks, eBay and PayPal have established a joint fraud investigation team to track down problem transactions and users. Moreover, within the context of its legal obligations, PayPal has a strong history of cooperating with law enforcement agencies.[56]

Ultimately, the proprietary online balance-transfer model is a self-contained, closed payment method, albeit one open to a wide range of potential participants. All payment account activity occurs within a single entity, which can make it easier for a service provider to internalize and control risks. By operating as a closed system, a service provider can manage

[50] *Computer World*, "Q&A: PayPal Fights Back Against Phishing," February 12, 2007.

[51] PayPal's user agreements can be accessed at <http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/ua-outside>.

[52] Paul Cox, "PayPal and FBI Team Up," *Wall Street Journal,* June 22, 2001; Ralph F. Wilson, "Assessing Criticism of PayPal," *Web Commerce Today*, March 15, 2002; Rob Garver, "eBay and Banking: Is PayPal a Serious Rival?" *American Banker*, November 15, 2005.

[53] Similarly, Neteller's annual report describes significant expansion in its fraud, security, and IT capabilities. See <http://investors.neteller.com/neteller/upload/1AR2005_0406.pdf>.

[54] See, for example, <http://www.PayPal.com>.

[55] The mass-pay feature allows PayPal Premier or business account holders to pay up to 10,000 recipients in varying amounts at one time.

[56] See Paul Cox, "PayPal and FBI Team Up," *Wall Street Journal,* June 22, 2001. Also see Dawn Kawamoto, "PayPal Charged with Breaking Patriot Act," CNET News.com, March 31, 2003.

fraud by denying or restricting access to users who do not meet its membership eligibility requirements or who fail to provide the required authentication. It can temporarily or permanently block users who do not comply with its rules or who are suspected of fraudulent or unauthorized activities. PayPal's experiences illustrate that a provider must aggressively battle new operational and fraud threats with vigilant monitoring of payment transactions.

5. Lessons Learned

The foregoing case studies offer many useful lessons for managing the problems that arise in emerging payment methods. Although each case is unique, there are common themes, which can be organized into three basic lessons.

5.1 Recognize the Problem

The very features that contribute to the efficiency of new payment forms—their scalability, speed, and relative anonymity—can also enable the rapid proliferation of various types of payment risk. As information moves more easily among payments system participants, more intensive management is needed to safeguard this data flow. Moreover, the more widespread and successful the system becomes, the bigger the potential for disruptions.

The incident reported earlier concerning two Russian men scamming PayPal offers a striking illustration of this principle. The perpetrators first breached the security arrangements at Internet service providers, gaining an initial cover of anonymity. They then used electronic means to create anonymous e-mail accounts, which in turn were used to create bogus accounts at PayPal. The speed and extent to which this was possible relied fundamentally on computers and the Internet.

To date, most innovative payment methods still have relatively low volumes of transactions. So even if risks are not well controlled, the overall risk of loss is limited.[57] Complacency, however, would be irresponsible. Significant flaws or fraud risks to ACH products have the potential to reach more institutions and individuals than most emerging payment products. And, as demonstrated by the Assail, CardSystems, and TJX incidents, even interruptions of low-value payments can result in large losses and disruption of business for many participants.

5.2 Maintain a Perimeter

All legitimate payments system participants—consumers, merchants, banks, and other service providers—share a common interest in risk mitigation. The nonrival nature of risk mitigation means that all these participants operate behind the same common protective perimeter of security and reliability. Successful payment methods find ways to encourage an appropriate buy-in of all participants in terms of contributing to this shared resource. As the case studies illustrate, wrongdoers need to be kept outside this perimeter—even in the most inclusive payment methods.

PayPal offers a good illustration of this principle. A key aspect of PayPal's market positioning is its openness, inclusiveness, and ease of use. It claims that all anyone needs to participate in PayPal is an e-mail address. However, as PayPal has become more sophisticated and has placed increased value on avoiding fraud and operational losses, it has accordingly tightened its perimeter and imposed participation standards.

All legitimate payments system participants—consumers, merchants, banks, and other service providers—share a common interest in risk mitigation.

Today, PayPal screens each participant, requiring not only an e-mail address but also some identifying information as well as credit card, debit card, or bank account information (all of which can be independently verified) before a participant is permitted to send funds.

Telephone-initiated ACH transactions offer another example of adaptation to new risks. The highly decentralized nature of the ACH, in which debit transactions are created by a wide variety of entities, has facilitated a relatively high fraud rate in the case of TEL transactions. Recent and proposed changes to NACHA rules are meant to encourage buy-in from banks in controlling this problem. They do so by imposing monitoring of problematic originators and, under some proposed rules, penalties for violators. This process is necessarily more complicated than it is in a proprietary system such as PayPal, given the diverse composition of the ACH. Yet

[57] The volume and value of e-money payment transactions in the United States are negligible. In contrast, ACH e-check transactions grew more than 40 percent last year, totaling about 2 billion transactions for the first half of 2006. See Bank for International Settlements (2006, Tables 7 and 8 and pp. 145-6).

there now seems to be widespread acceptance of the idea that stringent rules—such as exclusion—are required to keep fraud rates down to manageable levels.[58]

Prepaid cards are something of an intermediate case, being neither purely proprietary like PayPal nor as decentralized as the ACH. On the one hand, anyone can purchase a prepaid card at a retail outlet and anyone, not necessarily the same individual, can make a purchase with the card at a participating retailer. On the other hand, the card association whose name is on the card (for example, MasterCard or Visa) screens issuing banks and binds them contractually to particular provisions. The card associations also screen the card-selling merchants for a variety of risks, including the effectiveness of their security to prevent large-scale theft. Finally, the card associations impose contractual and monitoring provisions on merchants that accept their cards.[59]

> *For prepaid cards, the card associations serve as enforcers to ensure the integrity of the network, for example, by minimizing operational and fraud risks.*

For prepaid cards, the card associations serve as enforcers to ensure the integrity of the network, for example, by minimizing operational and fraud risks. Thus far, this control appears to be effective, even though the nominal issuers of general-purpose prepaid cards—merchants and various third parties—are neither typical card issuers nor regulated financial institutions. In a broader context, the aftermath of the May 2005 data breach at CardSystems illustrates the efficacy of such control:[60] Visa and American Express subsequently barred CardSystems from participating in their networks, forcing the firm out of business.[61]

The CardSystems case also highlights the difficulties posed by lengthening supply chains in the payment industry. Again, tensions can arise between efficiency and security. Specialization along the payment supply chain represents a source of efficiency, but the heavy involvement of nonbank or third-party participants means that the defensive perimeter for data integrity cannot be monitored by the banking system alone.

Historically, the role of third-party processors was limited to back-office services, such as lockboxes. In conjunction with emerging payment methods, some third-party entities have moved into the more prominent position of maintaining primary relationships with customers. Conversely, in some cases, banks have moved from maintaining primary relationships to becoming back-office service providers. This role reversal for bank and nonbank institutions has raised policy concerns and is a topic that warrants additional study.[62]

5.3 Trust the Marketplace—but Not Blindly

Producing a nonrival good is always a difficult and often a controversial business. Computer software, recorded music, and video, three common examples, are frequent objects of public controversy, regulation, and litigation. But somehow, the market finds innovative ways to provide these goods fairly—though rarely without growing pains along the way.

Electronic payment services also demonstrate both market-driven discipline and creativity, including for their security and reliability components. New payment products are immediately subjected to the forces of a market's "invisible hand," including ramifications of exposure to operational, fraud, and data security risks. As a result, operators are forced to learn about previously undetected operational problems. Outages of almost any sort can rapidly undermine user confidence in the reliability of a product, a particular service provider, or a new form of payment generally. New products also seem to attract the attention of fraudsters eager to exploit flaws before they are rectified. Only if a payment provider can address such problems quickly and effectively can it stay in business. Thus, for many of these risks, market mechanisms provide significant incentives for service providers to see that they are addressed promptly and thoroughly.

New products in their early stages repeatedly show patterns of operational or fraud problems and unmitigated risk, after which containment efforts follow. When PayPal faced fraud losses early on, it took steps to reduce those losses. It also implemented new authentication techniques and introduced innovative technology. PayPal continues to revise

[58] NACHA has recently approved a code of conduct that establishes standards of behavior and "*specifies NACHA's right to disassociate itself* from any organization that, in NACHA's opinion, fails to meet the standards and principles stated in the code" (emphasis added). See Elliott C. McEntee, "Open Letter," NACHA, April 13, 2006.

[59] See, for example, BankInfoSecurity.com, "Visa Takes Aim at Data Companies," August 8, 2006.

[60] See Perry (2005).

[61] CardSystems was purchased by Pay by Touch for its merchant network, according to a company press release dated October 15, 2005.

[62] Concerns about the role of nonbank third parties in the payments system have been raised, but they remain unresolved. See, for instance, Hoenig (2000) and Sullivan (2007).

its contracts and participation agreements to increase controls and limit risk.

Some providers of similar online payment services have failed, at least in part because of fraud losses, and others have run into trouble with law enforcement authorities over illicit payments.[63] The service providers that survive are those that are able to identify and mitigate losses quickly. When NACHA introduced the TEL product in 2001 and return rates began to soar, it took steps to identify the source of the problems. As a result, return rates fell to more acceptable levels. The WEB transaction, another recently created ACH e-check application useful for Internet transactions, had a return rate of 0.68 percent in 2002, but it fell to 0.08 percent in 2004.[64]

As payments systems grow and flourish, however, so too does the potential for disruption. Recent developments in the payment card industry provide an illustration. Card networks, historically quite vigilant in the protection of their data integrity, have nonetheless been subject to significant data breaches. Increasing volume and a more diffuse supply chain have posed new difficulties. The card networks have responded by putting more pressure on merchants to comply with data security standards, but this effort remains a work in progress.[65]

As payments systems grow and flourish . . . so too does the potential for disruption.

The vitality of the market for payment services does not rule out a role for public policy. Well-designed regulations can help coordinate industry efforts and maintain industry standards. Laws and criminal penalties can serve as deterrents to activities such as fraud. In addition, the importance of confidence in the overall payments system—a public good—should not be underestimated. Policymakers will always have an interest in ensuring that disruptions in one method of payment, however unlikely, do not spill over into other segments of the payments system.

In contrast to other risks considered here, the steps needed to reduce the risk of illicit use are not always fully supported by general market incentives. The federal government and many states respond to this risk by enacting laws and regulations to prohibit the use of payment methods for such purposes and by creating incentives for payment providers to screen out prohibited transactions. A measured policy response again seems appropriate, as the risk of illicit use must be balanced against the costs of compliance.

6. Conclusion

Innovative payment mechanisms, such as the ones described in this article, are making transactions less expensive and easier, while opening new commercial venues for payment transactions. As with more established forms of payment, however, the ultimate success of these inventive arrangements will depend on their ability to control risk.

For retail payments, the predominant risks are operational, fraud, illicit use, and data security risks. Providers mitigate these risks through techniques such as pricing, insurance, and containment. In the growing market of electronic transactions, these techniques have shared value that does not decline with additional use and can be enhanced with additional contributions—in other words, they are nonrival.

This article examined three emerging payment methods to draw some lessons from their operation and markets. The payment methods explored here carry transactions that are relatively low in value, and, during their start-up phases, most had a small number of users. However, some ACH-based transactions quickly reached substantial volume levels. With low values and generally limited breadth, the payment methods do not currently pose systemic risks or demonstrate substantial policy gaps. We note, however, that the risks discussed here are not confined to emerging payments.

All payment processes have risks that must be controlled. Fraudsters seem especially drawn to new technologies, becoming early adopters in their attempts to exploit any identifiable weaknesses. But fraudsters can also perpetrate innovative attacks against established systems. Moreover, even low-value retail payment providers can be the targets of machine-based attacks that can cause substantial damage; the speed of corruption and potential for proliferation of damaging problems are certainly shared by all payment methods that use electronic and networked technologies.

An important lesson to be taken from this study of emerging payment methods and their risks is that the products, services, rules, and technologies are all changing—and doing so at what appears to be an accelerating rate. So, too, are the tools for perpetrating fraud and data breaches as well as the techniques for mitigating them. This study provides a new structure for

[63] See, for example, Neteller Lawrence Complaint: *United States of America v. Stephen Eric Lawrence*, Southern District of New York. January 16, 2007, available at <http://www.casinocitytimes.com/news/article.cfm?contentID=163591>. Also see Neteller Lefebvre Complaint: *United States of America v. John David Lefebvre*, Southern District of New York, January 16, 2007, available at <http://www.casinocitytimes.com/news/article.cfm?contentID=163594>.

[64] Furst and Nolle (2005, p. 37).

[65] Robin Sidel, "Credit Firms Push to Thwart Fraud: Merchants Face a Penalty If Steps Aren't Taken to Curb Identity Theft; Visa Misses Own Security Deadline," *Wall Street Journal*, September 25, 2006.

considering risk and mitigation strategies that can be used to analyze new as well as established payment methods.

Our analysis of the risk mitigation techniques used by payments system providers concludes that containment is the dominant means of controlling risk. Generally, market mechanisms appear to encourage providers to mitigate risks appropriately: Most private-sector providers have the tools to manage many of these risks, particularly because they treat the integrity of the network as a club good; in other words, they retain the option to exclude any party that fails to comply with the network's safeguards. The applicability of this approach to the risk of illicit use, however, appears less certain.

More cooperative, open systems, which derive some of their utility from their universality, have less ability to exclude particular users and thus face greater risk mitigation challenges. Nonetheless, the problems, risks, and gaps in processes can be addressed only if the providers and participants remain vigilant while applying the lessons we described.

Appendix: How the Case Studies Were Selected

In general, new payment methods are built on top of existing products. Enhancements, significant innovations, and various levels of rule changes are added to these products to address newly identified market opportunities or to take advantage of expanding technological capabilities. To identify the extent to which a payment method is new rather than more established, we grouped the components of a generic payment process into two broad categories: the *access channel* and the *payment method*.[a] An access channel is used at the beginning of the transaction process; it provides the user interface or front end (for example, a plastic card with a magnetic stripe) and may or may not include verification of the identity of the involved parties and validation of the payment instrument. The payment method includes the remaining parts of the payment process governed by applicable laws, regulations, and contracts.

These various factors—new versus established components of access channels and payment methods—can be organized into a 2 x 2 matrix, as shown in Exhibit 1. Payment methods that have the fewest changes from established methods fit into the upper-left quadrant, although rule changes or new combinations of established characteristics can yield a new payment method. The lower-right quadrant includes emerging payment methods that incorporate the greatest number of new characteristics in terms of both access channels and payment methods. The remaining two quadrants, upper right and lower left, are hybrids of new and established components.

Exhibit 2 provides examples of payments that might be found in each of these four cells. For the case studies, we selected one payment method from each quadrant (shaded).

- ACH payments initiated via telephone (TEL) fall in the upper-left quadrant, since neither the telephone access channel nor the ACH clearing and settlement portions are new.
- General-purpose prepaid cards use established card-swipe technology to create a new payment and therefore fall in the upper-right quadrant.
- Accounts-receivable conversion (ARC) uses the new access channel of scanning technology and software to read paper checks and create transactions that flow over the established ACH network, as represented in the lower-left quadrant.
- Proprietary balance-transfer systems meld a new access technology—the Internet—with new transaction methods—e-mail and balance transfers—and therefore fall into the lower-right quadrant.

The TEL and ARC payments are types of ACH e-checks that share a clearing and settlement network and many rules (these are addressed jointly in the analysis above).

[a] See Bank for International Settlements (2000) for a description of the components of payment processes.

Exhibit 1

Access Channels and Payment Methods

Access Channels Front End	Noncash Payment Methods Transaction, Clearing, and Settlement Processes: Established	Noncash Payment Methods Transaction, Clearing, and Settlement Processes: New
Established	Well-known technologies initiate commonly known types of payments or use new rules to create new types of payments.	Existing access technologies initiate a new type of payment.
New	New technologies or networks access established payment method.	New technologies and networks initiate new types of payments.

Exhibit 2

Examples of Payments

Access Channels Front End		Noncash Payment Methods Transaction, Clearing, and Settlement Processes: Established	Noncash Payment Methods Transaction, Clearing, and Settlement Processes: New
Established	Established	Credit card payments Paper checks in general PPD ACH debit PPD ACH credit PIN debit Signature debit	General-purpose prepaid cards Closed network and gift cards
	New combinations of established components	ACH debit card ACH TEL Micropayment aggregators Check 21 substitute check	
New		ACH POP ACH ARC ACH WEB Check image presentation (not IRD) Cell-phone payment Highway toll booths Contactless card payments (debit or credit) Charge to phone bill Biometic authentication License ID to create ACH debit ACH credit push	Proprietary balance transfer Secured proprietary balance transfer Proprietary balance transfer via cell phone Prepaid wallet Instant credit

References

Anderson, R., and T. Moore. 2006. "The Economics of Information Security." Science 314, no. 5799 (October 27): 610-3.

Bank for International Settlements. 2000. "Clearing and Settlement Arrangements for Retail Payments in Selected Countries." Basel, Switzerland.

———. 2006. "Statistics on Payment and Settlement Systems in Selected Countries." Preliminary version, November. Basel, Switzerland.

Bradford, T., M. Davies, and S. E. Weiner. 2003. Nonbanks in the Payments System. Federal Reserve Bank of Kansas City. Available at <http://www.kansascityfed.org/publicat/psr/BksJournArticles/NonBankPaper.pdf>.

Federal Financial Institutions Examination Council. 2004. Retail Payments System: IT Examination Handbook. March. Available at <http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf>.

Federal Reserve System. 2004. "The 2004 Federal Reserve Payments Study: Analysis of Noncash Payments Trends in the United States: 2000-2003." Available at <http://www.frbservices.org/Retail/pdf/2004PaymentResearchReport.pdf >.

Financial Action Task Force. 2006. "Report on New Payment Methods." October 13. Available at <http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf>.

Furletti, M., and S. Smith. 2005. "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: ACH E-Checks and Prepaid Cards." Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper no. 05-04, March. Available at <http://www.philadelphiafed.org/pcc/papers/2005/ConsumerProtection.pdf>.

Furst, K., and D. Nolle. 2005. "What's Your Risk with the Growing Use of ACH Payments?" Office of the Comptroller of the Currency Quarterly Journal 24, no. 4 (December): 21-43.

Hirshleifer, J. 1983. "From Weakest Link to Best Shot: The Voluntary Provision of Public Goods." Public Choice 41, no. 3 (January): 371-86.

Hoenig, T. M. 2000. "Payments and Settlement Systems: Future Players and Issues." Remarks delivered at the BAI Money Transfer 2000 Conference, Chicago, Illinois, November 9. Available at <http://www.kansascityfed.org/SPCH&BIO/chicago.htm>.

Kahn, C. M., and W. Roberds. 2005. "Credit and Identity Theft." Federal Reserve Bank of Atlanta Working Paper no. 2005-19, August.

Katz, M., and B. E. Hermalin. 2006. "Privacy, Property Rights, and Efficiency: The Economics of Privacy as Secrecy." Quantitative Marketing and Economics 4, no. 3 (September): 209-39.

Kuttner, K., and J. McAndrews. 2001. "Personal On-line Payments." Federal Reserve Bank of New York Economic Policy Review 7, no. 3 (December): 35-50. Available at <http://www.newyorkfed.org/research/epr/01v07n3/0112kutt.html>.

McGrath, J. C. 2007. "General Use Prepaid Cards: The Path to Gaining Mainstream Acceptance." Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper no. 07-03, March. Available at <http://www.philadelphiafed.org/pcc/papers/index.cfm>.

Money Laundering Threat Assessment Working Group. 2005. "U.S. Money Laundering Threat Assessment." Report Prepared by an Inter-Agency Working Group and Issued by the United States Treasury Department, December. Available at <http://www.ustreas.gov/press/releases/reports/js3077_01112005_MLTA.pdf>.

Perry, J. M. 2005. Statement of John M. Perry, President and CEO, CardSystems Solutions, Inc., Before the U.S. House of Representatives, Subcommittee on Oversight and Investigations of the Committee of Financial Services. July 21.

Sienkiewicz, S. 2007. "Prepaid Cards: Vulnerable to Money Laundering?" Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper no. 07-02, February. Available at <http://www.philadelphiafed.org/pcc/papers/index.cfm>.

Stigler, G. J. 1980. "An Introduction to Privacy in Economics and Politics." Journal of Legal Studies 9, no. 4 (December): 623-44.

Sullivan, R. J. 2007. "Risk Management and Nonbank Participation in the U.S. Retail Payments System." Federal Reserve Bank of Kansas City Economic Review 92, no. 2 (second quarter): 5-40. Available at <http://www.kansascityfed.org/publicat/econrev/PDF/2q07sull.pdf>.

Varian, H. R. 1998. "Markets for Information Goods." Remarks prepared for a Bank of Japan conference, June 18 and 19. Available at <http://www.sims.berkeley.edu/~hal/Papers/japan/>.

———. 2004. "System Reliability and Free Riding." Available at <http://www.ischool.berkeley.edu/~hal/people/hal/papers.html>.

The views expressed are those of the authors and do not necessarily reflect the position of the Federal Reserve Banks of Atlanta, Kansas City, New York, or the Federal Reserve System. The Federal Reserve Bank of New York provides no warranty, express or implied, as to the accuracy, timeliness, completeness, merchantability, or fitness for any particular purpose of any information contained in documents produced and provided by the Federal Reserve Bank of New York in any form or manner whatsoever.