

# Keeping the bad guys out: risk management and retail payment innovation<sup>1</sup>

**Michele Braun**

Officer, Federal Reserve Bank of New York

**William Roberds**

Research Economist and Policy Adviser,  
Federal Reserve Bank of Atlanta

**Richard Sullivan**

Senior Economist, Federal Reserve Bank  
of Kansas City

## Abstract

New technologies used in payment methods can reduce risk, but they can also lead to new risks. Emerging retail payments are prone to operational and fraud risks, especially security breaches and potential use in illicit transactions. This article describes an economic framework for understanding risk control in retail payments. Risk control is a special type of good because it can protect one payment participant without diminishing the protection of other participants. As a result, risk containment is critical, primarily through the establishment and enforcement of risk management policies. Informal case studies of several recent emerging payments suggests that a payments system can successfully manage risk if it quickly recognizes problems, encourages commitment from all participants to control risk, and uses an appropriate mix of market and public policy mechanisms to align risk management incentives. Providers of emerging payment methods must mitigate risk effectively or face rejection in the payment market.

<sup>1</sup> Additional discussion of the issues explored in the paper can be found in Braun et al. 2008. The views expressed in this paper are those of the authors and not necessarily the views of the Federal Reserve Banks of New York, Atlanta, or Kansas City, or of the Federal Reserve System.

## Keeping the bad guys out: risk management and retail payment innovation

As retail payments shift increasingly from paper to electronic form, payment products, services, rules, and technologies are changing rapidly. “Electronic checks,” cell-phone payments, prepaid cards, and speed-through lanes at highway toll booths are just a few examples of recent innovations in retail payments. These payment innovations combine computer technology, telecommunications, and information to provide new ways to pay for things and to conduct commerce. The risks associated with emerging payments, such as operational disruptions, fraud, illicit use, and breaches of data security, are also changing. News headlines that frequently report data breaches, identity thefts, and frauds have become a part of the electronic payments landscape. Because using electronics and new technologies reduces some risks but also introduces others, it is now timely to examine how innovative payment technologies affect risk and to develop a structure and vocabulary through which to explore these risks.

Understanding the structure of risk is useful, although assessing losses and mitigation efforts in a new payment product can be difficult. Low levels of fraud losses, for example, could imply that the risk is low, current mitigation practices are effective, or weaknesses have not yet been discovered. On the other hand, high levels of losses demonstrate that risks are high, but it takes time to know whether mitigation efforts can succeed. In either case, only time and monitoring of problems will reveal whether risk can be controlled sufficiently. In this paper we ask whether, in this period of uncertainty, the sponsor of an emerging payment has enough incentive 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 payments can often manage these risks by employing the right techniques. They need to be aware of potential fraud and operational risks, especially in the early stages of their introduction. Emerging payment services must mitigate risk or face rejection in the payments market. Service providers can contain risks by limiting access to their payments 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 who can help to coordinate activities as well as define and enforce standards.

### Risks in retail payment innovations

We begin our examination of these risks and their mitigation with three general observations. First, the risks present when new or still-emerging payments methods are used are not wholly different from those present in long-established modes of payment. Every payment method involves risks. Nonetheless, our analysis suggests that certain risks are more salient in emerging retail payments than elsewhere in the payments marketplace. The Committee on Payments and Settlement Systems (CPSS) identifies five major

Types	Definitions
<b>Fraud risk</b>	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.
<b>Operational risk</b>	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.
<b>Legal risk</b>	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)

Figure 1 - Major risks in innovative payments

categories of risk associated with payments transactions: fraud, operational, legal, settlement, and systemic risks [BIS (2000)]. 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 particularly associated with emerging payments are shown in Figure 1.

Second, payment method innovations are generally based on, or emerge from, existing payment products. To focus this discussion, for the purposes of this paper we define established payments to include paper checks, recurring transactions transferred through the automated clearing house (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 will 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. Three notable examples of emerging payments include:

**Proprietary online balance-transfer systems** – like PayPal, these are online arrangements to transfer balances of funds between accounts. Customers establish an account with a service provider and use e-mail messages to initiate payments. 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/micro businesses and individuals) involved in online transactions, usually at an auction site. Outside of the U.S., Nettlell is frequently used, among other purposes, to settle gambling transactions. These services are also used by small online companies and by individual

## Keeping the bad guys out: risk management and retail payment innovation

customers who value the ability to transfer funds from person to person.

**ACH e-checks** – over the last decade, the National Automated Clearing House Association (NACHA), which sets rules for ACH transactions, has developed rules and formats for a variety of new electronic debit transactions. These e-checks allow banks and their clients to convert checks or information from checks into ACH debits. Telephone-initiated transactions (TEL) are debits to consumers' accounts authorized by the account holder via telephone to a merchant, vendor, or service provider. To help control risk, NACHA rules restrict TEL transactions to where there is a preexisting relationship between merchant and consumer or when the consumer initiates the call. These transactions make one-time ACH payments available when written authorizations are not feasible.

**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. The cards are marketed widely and distributed directly to consumers by nonbank third parties. They provide tremendous flexibility, opening up access to electronic transactions at physical and remote points of sale to individuals without credit or debit cards [McGrath (2005), Worthington (2008)].

Third, 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 transactions or used 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.

Illicit use risk is the risk that a payment method may be used for illegal purposes such as money laundering, terrorism financing, or the purchase of illegal goods and services such as illegal drugs or child pornography. The ease with which criminals can launder stolen funds or terrorists can be financed with legitimately earned funds affects the victims of the crimes that give rise to the 'dirty' funds, and also affects society as a whole. Unfortunately, many of the features of emerging payments that provide value for legitimate transactors, such as speed of value transfer, transportability, intermediation, anonymity, quantity limits, network connectivity, and ease of interface, can also make them susceptible to misuse by individuals engaging in money laundering and terrorism financing.

The high degree of similarity between the needs of legitimate and illegitimate users of payments 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 paper.

### Examples of fraud using payment innovations

- In 2003, the Federal Trade Commission (FTC) brought charges against the Assail Telemarketing Network and its affiliates. The FTC alleged that the Assail companies had deceptively persuaded consumers to provide the bank and account information from their checks and then withdrew funds from consumers' bank accounts [FTC (2005)]. To consummate these transactions, Assail used an electronic debit through the automated clearinghouse (ACH). Although similar frauds could have been perpetrated without the ACH debits, paper-based techniques do not offer the speed and scale these fraudsters achieved using automation.
- In 2002, the U.S. Department of Justice won convictions against two Russian men, who, in 2000, had gained unauthorized access to Internet service providers in the U.S. to misappropriate credit card, bank account, and other personal financial information from more than 50,000 individuals [U.S. Department of Justice (2002)]. They allegedly hijacked computer networks and then used the compromised processors to commit fraud through PayPal and the online auction company eBay. The fraudsters hacked into databases, stole payment-related and other information, used stolen identities to create fictitious accounts, manipulated online auctions, and used machine-based tools to proliferate their thefts and confound the transaction/audit trail.
- More recently, in early 2007, the TJX Companies, which operate retail stores in the U.S., Canada, Ireland, and the U.K., reported that data security breaches from mid-2005 or earlier until late 2006 might have compromised more than 45 million customer records. The Wall Street Journal reported that hackers tapped into data transmissions, used stolen data to crack encryption codes which enabled them to steal employees' user names and passwords, and, ultimately, credit and debit card numbers [Pereira (2007)]. Stolen card numbers were then allegedly sold on the Internet, with losses traced to banks across the country. The thieves or their customers also purchased prepaid cards, which were in turn used to purchase goods and services.

### Some insights from economic theory

#### Risk containment as a good

Economic theory offers some useful concepts for managing risks in payment systems and establishing the integrity of emerging payments networks. First, we note that information stored and transmitted by a payment system meets the definition of an economic good: all payment systems are systems for managing information

## Keeping the bad guys out: risk management and retail payment innovation

– that is, keeping records of transactions and communicating transactions data – and these records and data have value.

More specifically, Varian (1998) described a digital good as a good that can be stored and transferred in digital form. Thanks to modern information technology, emerging payment methods can offer tremendous efficiency gains over traditional methods of making payments, in part because electronic data can be easily stored at a few locations and then shared among payment system participants at a very low cost. Varian further explains that digital goods are different from standard, physical goods (cornflakes, sneakers, 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: my consumption of a TV show does not diminish the quantity available for consumption by another individual. Other examples are recorded music, video, and computer software. The data managed by modern payment systems is another example: 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.)

Central to maintaining the value of any digital good is data integrity – garbled music or video is useless, for example. The usefulness of payments data can be diminished by fraud and security breaches or by operational disruptions that interfere with data transmission. Consequently, the integrity of payments data is also a nonrival good. If a payment system participant secures a facility against operational disruptions and fraud it creates an environment that is conducive to smooth operation of the payment 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 for which consumption can be limited to specific groups or individuals and, therefore, others can be stopped from consuming. For example, cable television firms exclude nonsubscribers from their service by encoding their signals and only giving decoders 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 risk in emerging payments, the club good description is perhaps the most appropriate. Successful private-sector payment providers (for example, credit card, debit card, ATM networks, and other payments providers) have by and large managed to contain fraud. They also maintain operating procedures and auditable controls to limit operational risk. Participation in these systems is limited by mem-

bership rules, and participants (individuals, merchants, banks, processors) associated with high levels of fraud or operational snafus can be expelled. For example, in 2005, shortly after CardSystems Solutions, Inc., a transaction processor, disclosed a significant security breach in which records of 263,000 transactions were stolen – including account holders' names, account numbers, expiration dates, and security codes – two major credit card companies announced that they would stop permitting the firm to process their transactions. Thus, CardSystems was closed out of the club and shortly thereafter went out of business [Perry (2005) and Pay by Touch (2005)].

There are natural limits to the power of exclusion, however. Since every payment system is a type of communications network, excluding too many network participants lowers the network's value for those parties who remain. There will always be a tradeoff between security and inclusivity.

We now turn to how risk mitigation efforts within the club might pose a challenge.

### Why containing fraud and operational risk is difficult

Hirshleifer (1983) describes a model of a nonrival good that is particularly applicable to data integrity over electronic payment systems. Hirshleifer considers the problem of people living in a 'polder,' a low-lying patch of land that is 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 height of the lowest portion 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 payment 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.

There are obvious parallels between flood protection in Hirshleifer's 'polder model' and the mitigation of fraud and operational risk over payment systems. The CardSystems Solutions data breach, for example, resulted in problems not only for CardSystems, but numerous other users of card payment systems – cardholders, merchants, banks, and processors. A data breach or operational disruption in one portion of a payment 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.

## Keeping the bad guys out: risk management and retail payment innovation

Varian (2004) has pointed out some difficulties in the provision of such nonrival goods. Because the amount of mitigation depends crucially on the participant who 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 that which those with lower net benefits are willing to support. However, because overall protection depends on the participant who exerts the least effort – the weakest link – the latter group determines the overall level of risk mitigation.

Many different providers of services are integral in the processing of electronic payments. These providers include encryption firms, processors that route transactional data, and Internet service providers, among others. But because minimizing fraud and operational risk 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 payment systems have learned to keep fraud and operational risks at fairly low levels. Competition among payment systems provides important incentives for payment method providers to mitigate these risks. Systems that fail to contain risks do not survive in the payments marketplace.

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

- **Pricing** means that a party who 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 and higher annual fees for cards, to sub-prime 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 by issuing banks compensates for the greater risks they take on.
- **Insurance** is an agreement between two parties about who will bear a loss when the loss occurs. Thus, for instance, a merchant who 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.

**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. However, when the payee and payer are anonymous to each other, the payee cannot know if the payer 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 (i.e., over the Internet or telephone), adverse selection undermines incentives to play by the rules. So called '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 payment processor might fail to spend the resources to maintain sufficient back-up facilities in the case of 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 are spread across thousands of other individuals and businesses. Card networks impose back-up and resiliency standards to offset incomplete private incentives and contain this particular risk.

Thus, pricing and insurance are not individually 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 provide unknown buyers and sellers with guarantees against loss.

### Containment techniques: monitoring → penalties → exclusion

Containment of fraud and operational risk requires cooperation among payment system participants. All players need to have incentives to undertake actions that will keep fraud and operational risk 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 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

## Keeping the bad guys out: risk management and retail payment innovation

establish performance standards and impose penalties when not met. Varian's (2004) theoretical analysis of the polder model suggests that relatively severe penalties, beyond the economic cost of a security lapse, may be necessary to ensure compliance.

In practice, penalties can significantly motivate behavior but even they cannot do the whole job. As a result, the threat of the ultimate penalty, exclusion, may be the most effective deterrent. Payment system participants that fail to maintain adequate operational standards or fraud controls may not be allowed into or may be expelled from the system entirely. 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 particularly useful for creating deterrence tools.

### Special concerns for emerging payments

Any viable payment system must find ways to maintain the integrity of payments data, but there are certain concerns that are unique to emerging payments. First, there is a newness factor. The novelty of emerging payment methods implies that various problems may not be anticipated and 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 provides important incentives for payment method providers to mitigate many of these risks. Users can choose from many payment methods, and their choices reflect the extent to which payment methods best facilitate smooth, low-risk transactions. In competition with payment methods that are less susceptible to fraud or operational failures providers of new payment methods have clear incentives to address those risks. A failure to do so jeopardizes a payment 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 non-bank service providers – to exchange payments data in ways that were not previously possible. The value of these technologies hinges, of course, on data integrity. Successful payment systems will find ways of coordinating the behavior of diverse parties to facilitate data exchange that serves their mutual best interest.

### Lessons learned from recent payment innovations

We have looked at several examples of recent payment innovations as informal case studies and found many examples that illustrate the economic principles discussed above. The lessons learned from these experiences can be organized into three basic messages.

#### Lesson 1 – Recognize the problem

The very features that contribute to the efficiency of new forms of payment – scalability, speed, and relative anonymity – can also enable the rapid proliferation of various types of payment risk. As information moves more easily among payment 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.

To date, most innovative payments still have relatively low volumes of transactions, so that even if risks are not well controlled the overall risk of loss is limited. But as demonstrated by the Russian PayPal scam, even interruptions of low-value payments can result in large losses and disruption of business for many participants. And some emerging payments can grow very rapidly from their onset. For example, 'TEL' transactions grew fairly rapidly after introduction, but also experienced a large rate of fraud. Investigation showed that most of these unauthorized transactions came from telemarketers, such as the Assail Telemarketing Network. Similar to the PayPal experience, NACHA adapted to the unanticipated risk in TEL transactions. It recognized the problem early on and manually intervened to stop the worst abuses and brought fraud rate down to manageable levels [Wells Fargo (2008)].

#### Lesson 2: Maintain a perimeter

All legitimate payment 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 participants operate behind the same common protective perimeter of security and reliability. Successful payment systems find ways to encourage an appropriate buy-in of all participants, in terms of contributing to this shared resource. Wrongdoers need to be kept outside this perimeter, even in the most inclusive payment systems. PayPal offers a nice illustration of this principle. A key aspect of PayPal's market positioning is its openness, inclusivity, and ease of use. It claims that all one needs to participate in PayPal is an e-mail address. However, as PayPal has become more sophisticated it has placed increased value on avoiding fraud and operational losses. It has, so to speak, tightened its perimeter and imposed participation standards. Today, PayPal screens participants, requiring some identifying information as well as credit card, debit card, or bank account information (all of which can be independently verified) in addition to an e-mail address, before a participant is permitted to send funds.

## Keeping the bad guys out: risk management and retail payment innovation

NACHA similarly sets requirements for access to the ACH system. Banks are the primary gatekeepers because ACH transactions must be processed, collected, and paid through participating banks. The bank that provided ACH services to Assail failed to perform due diligence on the activities and legitimacy of this customer and later paid U.S.\$200,000 to Iowa, South Dakota, and Minnesota and agreed to vigorously engage in know-your-customer practices and ongoing monitoring of customer activities [Iowa Attorney General (2005)].

Recent and proposed NACHA rule changes are meant to encourage banks to control this problem. They do so by imposing monitoring of problematic originators, and under some proposed rules by imposing penalties on violators. There now seems to be increasing acceptance of the idea that stringent rules, including exclusion, are required to keep fraud rates down to manageable levels.<sup>2</sup>

Prepaid cards are something of an intermediate case, being neither purely proprietary like PayPal nor as decentralized as the ACH. 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. 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. Prepaid cards facilitate nearly anonymous transactions, which makes them attractive to illegal enterprises. The illicit use risk associated with this 'flexibility' was illustrated by the TJMaxx story of stolen credit card data being used to purchase prepaid cards and, thus, launder funds.

The governance of prepaid cards has both centralized and decentralized features. On the one hand, entry to the market is relatively easy so that nonbank issuers proliferate. Issuers have differing abilities to manage risk and varying policies concerning consumer protections. 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. Issuing banks, in turn, screen and monitor the merchants that sell the cards for a variety of risks, including security, to prevent wholesale theft. Finally, the card associations impose contractual and monitoring provisions on merchants that accept their cards.

Two structural issues that characterize emerging payment methods also complicate risk management: lengthening supply chains and repositioning of third-party service providers. The CardSystems case highlights difficulties posed by lengthening supply chains in the payment industry. Again, tensions arise between efficiency and security. Specialization along the payments supply chain represents a source of efficiency, but the heavy involvement of non-bank or third-party participants means that the defensive perimeter for data integrity cannot be monitored by the banking system alone

[Sullivan (2007)]. And, historically, the role of third-party processors was limited to back-office services. In conjunction with emerging payment methods, some third-party entities have moved into the more prominent position of maintaining primary relationships with customers. Conversely, banks have moved from maintaining primary relationships to being back-office service providers.

### Lesson 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, to give 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. This principle also applies to electronic payment services, including the security and reliability components of these services. New payments products are immediately subjected to the forces of the invisible hand, including exposure to operational, fraud, and data security risk. Operators are, as a result, 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 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 promptly and thoroughly addressed.

As payment systems grow and flourish, however, so too does the potential for disruption. Recent developments in the payments 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. From January 2005 to April 2007, nearly 154 million records were compromised in 541 publicly reported data breaches [Sullivan (2007)]. Nonbank payment processors accounted for only 3 percent of all data breaches but 27 percent of compromised records. Banks and other financial service companies accounted for 9 percent of incidents and 4 percent of records compromised over the entire period. A large number of data breaches have occurred in education, retail, health care, and government sectors. These four sectors together account for 77 percent of data breaches and 67 percent of records compromised in this particular period. Increasing volume and a more diffuse supply chain have posed new difficulties. The card networks have responded by beefing up efforts to force merchants to comply with data security standards, but this remains a work in progress [Sidel (2006)].

The vitality of the market for payment services does not rule out a role for public policy. Well-designed regulations can help to coor-

<sup>2</sup> NACHA 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." [McEntee (2006)].

# Keeping the bad guys out: risk management and retail payment innovation

dinate industry efforts, and to maintain industry standards. Laws and criminal penalties can serve as deterrents to activities such as fraud. And, the importance of the public good of confidence in the overall payment system should not be underestimated. Policymakers will always have an interest in ensuring that disruptions in one method of payment, however unlikely, will not spill over into other segments of the payment system.

## Conclusion

Innovative payment mechanisms, such the ones described above, are making transactions cheaper and easier and they are opening new commercial venues for payment transactions. As with more traditional forms of payment, however, one key to the ultimate success of these inventive arrangements is the ability to control risk. For retail payments the predominant risks include operational risk, fraud risk, risk of illicit use, and data security risk. Providers mitigate these risks through techniques such as pricing, insurance, and containment. In the growing market of electronic transactions these techniques have shared values that do not decline with additional use and can be enhanced with additional contributions.

All payment processes have risks that need to 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. And, 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 payments methods that use electronic and networked technologies.

An important message of this study of risks in emerging payment methods is that 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, data breaches, and the techniques for mitigating them. This study provides a new structure for considering risk and mitigation strategies that can be used to analyze new and established payment methods. Containment programs are critical to payment risk management. These programs include coordinated industry efforts to develop and maintain risk mitigation standards, monitor compliance with standards, and enforce penalties for noncompliance. Limiting access to the payments system is an essential tool, with exclusion from the system serving as the ultimate penalty. Containment alone does not eliminate risk. However, a payments system can successfully manage risk if it recognizes problems quickly, encourages commitment from all participants to control risk, and uses an appropriate mix of market and public policy mechanisms to align risk management incentives.

## References

- Bank for International Settlements, 2000, "Clearing and settlement arrangements for retail payments in selected countries," Basel, Switzerland
- Braun, M., J. McAndrews, W. Roberds, and R. Sullivan, 2008, "Understanding risk management in emerging retail payments," Federal Reserve Bank of New York, FRBNY Economic Policy Review
- FTC, 2005, "International telemarketing network defendants banned from telemarketing," press release, January 24
- Hirshleifer, J., 1983. "From weakest link to best shot: the voluntary provision of public goods," *Public Choice*, 41:3, 371-86
- Iowa Attorney General, 2005, "First Premier Bank agrees to deny automatic withdrawal services to telemarketing scams," July 6, available at [www.iowa.gov/government/ag/latest\\_news\\_releases/july\\_2005/First\\_Premier.html](http://www.iowa.gov/government/ag/latest_news_releases/july_2005/First_Premier.html)
- McEntee, E. C., 2006, "Open letter," NACHA, April 13
- 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
- Pay by Touch, 2005, "Pay by Touch to acquire CardSystems Solutions, a leading provider of integrated payment solutions," press release, October 15
- Pereira, J., 2007, "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
- 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
- Sidel, R., 2006, "Credit firms push to thwart fraud," *The Wall Street Journal*, September 25
- Sullivan, R. J., 2007, "Risk management and nonbank participation in the U.S. retail payments system," *Federal Reserve Bank of Kansas City Economic Review* (second quarter), 5-40
- U.S. Department of Justice, 2002, "Russian computer hacker sentenced to three years in prison," press release, October 4
- Varian, H. R., 1998, "Markets for information goods." Remarks prepared for a Bank of Japan conference, June 18 and 19, Available at [www.sims.berkeley.edu/~hal/Papers/japan/](http://www.sims.berkeley.edu/~hal/Papers/japan/)
- Varian, H. R., 2004, "System reliability and free riding," Available at [www.ischool.berkeley.edu/~hal/people/hal/papers.html](http://www.ischool.berkeley.edu/~hal/people/hal/papers.html)
- Wells Fargo, 2008, "Waging war on ACH fraud," [www.nacha.org/ACHNetwork/ACH\\_Quality/WellsFargo\\_DB.doc](http://www.nacha.org/ACHNetwork/ACH_Quality/WellsFargo_DB.doc). Accessed July 2
- Worthington, S., 2008, "Financial services for the unbanked in the U.S. - why, who, and what?" *Journal of Financial Transformation*, 23, 101-105