Role and Security of Payment Systems in an Electronic Age

Remarks Prepared for

IMF Institute Seminar on

"Current Developments in Monetary and Financial Law"

June 1, 2004

by

Mark Fajfar*

Fried, Frank, Harris, Shriver & Jacobson LLP

In the past decade, methods of effecting banking and other financial transactions via the Internet in the United States have quickly become more and more sophisticated. This paper will examine, from the viewpoint of a U.S. legal practitioner, the implications of this trend towards conducting financial transactions electronically. The focus of this paper is not on legal theories, but rather on the interesting and novel practical issues that arise in the legal implementation of new electronic payment systems that are now more prevalent or are appearing on the horizon. This paper discusses consumer, as opposed to business-to-business, transactions and concentrates on how the particular characteristics of the new electronic payment systems (contrasted to the "traditional systems") affect the consideration of two issues: information security and efforts against money laundering and terrorist financing.

A "silent revolution" in the payment systems in the U.S. has occurred over the past decade or so. Payment systems are moving from paper towards real-time, electronic execution and settlement. "Real-time" means that payments are settled or cleared not

* This paper reflects only the author's own views, not the views of Fried Frank or any of its clients. The author recognizes Fried Frank's Financial Institutions and Electronic Commerce Transactions Group, headed by Thomas P. Vartanian and including Robert H. Ledig and David L. Ansell, for their contributions to this paper.

only in a few days or even overnight, but on a continuous basis, 24 hours a day. Consumers have generally been willing to adopt these new electronic systems because they have confidence in the financial system in general and in electronic operations in particular. But this is a silent revolution because these extensive changes have occurred slowly, and not necessarily in ways that are obvious or dramatic. The traditional, trusted and convenient means of effecting payments still have a strong attraction to consumers, who therefore change their economic behavior slowly because of their emotional relationship to money and the payment mechanisms they trust.

Overview of New Electronic Payment Systems

Before talking about the security and law enforcement implications of the new payment systems, this paper will briefly describe the new systems themselves. As a preliminary aside, the reader should note that this paper does not discuss the credit and debit card systems in detail, for two reasons. First, credit and debit cards are so pervasive a means of effecting electronic transactions in the U.S. that a discussion of them would at least double the length of this paper. Second, this paper aims to address recent changes in the electronic payment systems and the implications of those changes on the issues of information security, money laundering and terrorist financing. While they are important, the credit and debit card systems are not especially changing at this time (and to the extent they are, this paper will discuss them). Nonetheless, the credit and debit card payment systems are a crucial part of the overall U.S. consumer finance structure, and much of this paper's discussion of information security and other concerns does apply to credit and debit cards.

Transformation of the Paper Check

The silent revolution in payment systems in the U.S. is most apparent in the ongoing transformation of the paper bank check, which has been for decades the mainstay of the consumer payment system. The demise of the paper check has been predicted since at least the 1960s, but its familiarity, simplicity and consumer protections

have fostered its continued use, and a very large percentage of payments are effected today by paper checks.

Electronic processing of check transactions has accelerated, however – the primary change being the increasing use of the automated clearing house ("ACH") system for direct deposits and direct payments. Common uses are the direct deposit of payroll checks and consumer payment of recurring bills by direct payments to utilities, for example. Furthermore, these systems are evolving into a comprehensive system of electronic bill presentment and payment, which permit a consumer to register (typically through a bank, but also through third-party service providers) to receive bills from a variety of merchants by electronic mail, rather than postal mail. Then, instead of using checks, the consumer uses the Internet to initiate direct electronic payments to those merchants.

The important lesson from the transformation of the paper check is that it reflects a gradual expansion of an electronic system. In the early stages, the ACH system was used for only repetitive payments to specific merchants. Today, this electronic system encompasses the billing process and payments to a variety of merchants.

There is also much discussion today of the Check Clearing for the 21st Century Act, Pub. L. No. 108-100, 117 Stat. 1177 (2003) ("Check 21 Act"), which will permit "electronic check truncation." That is, banks will be permitted to convert paper checks to electronic entries, and process the check transaction electronically, without the physical delivery of checks from place to place.

Electronic Payment of Government Benefits

Another new application of electronic payment systems is their use to provide government benefits. Already, federal, state and local governments favor the ACH direct deposit system for payments to individuals – such as tax refunds, social security benefits and cash assistance. While that system is relatively straightforward, difficult issues arise

when governments seek to make electronic payments to people who do not have bank accounts (which constitute a significant number of lower-income individuals). For them, the existing, paper check-based system imposes costs on both the government-payor and the recipient. The government has to pay for the printing and mailing of checks, and the individual recipient has to pay the cost of a check cashing service.

For this reason, governments have started to pay benefits in the form of debit cards known as electronic benefits cards. These are similar to cards used at automated teller machines ("ATMs"). The electronic benefits cards are periodically "loaded" with additional funds by the government (i.e., the government deposits funds into a bank account tied to the cards). Individuals use the cards to make purchases in stores or to withdraw cash from ATMs.

The interesting point here is that the large volume of government payments is likely to hasten the acceptance of debit cards as a means of transferring funds to individuals. Similar systems are sometimes used for payroll, especially the payment of wages to transient or temporary workers. The issue discussed later in this paper is whether, as the use of debit cards to transfer funds to individuals becomes more common, they could also be used for money laundering or terrorist financing.

Person-to-Person Electronic Payment Systems

The previous two examples are illustrations of the evolution of an existing system into a new, electronic format. In addition, other electronic payment systems have introduced entirely new ways to transfer funds between individuals.

For example, person-to-person electronic payment systems, such as PayPal, are used to transfer funds electronically among individuals without using cash or checks. Basically, these systems require that each user designate a bank account or a credit card account. Then, when an individual initiates an electronic transfer to another, PayPal's

electronic system causes a debit in the account of the payor and a credit in the account of the payee.

Many similar systems were introduced during the technology boom of the late 1990s. Those that remain viable found success in niche markets, such as facilitating purchases between individuals on Internet auction sites like eBay. The advantages of these systems are that they clear payments faster than check processing systems, do not impose the high fees of credit cards, and do not impose merchant-qualification requirements. Instead, anyone with a bank account or credit card can use a PayPal account to receive money electronically from other individuals.

"Closed-System" Stored Value Cards

A wide variety of new electronic stored value cards which defy easy classification under traditional rules and regulations have recently appeared. For example, electronic gift cards issued for a particular value by a particular merchant have become very popular. The card can be given as a gift, or just used as a convenient way to make purchases at the merchant later on. Ease of use and convenience are the primary attraction of these cards to consumers, while merchants favor them because customers tend to spend more freely when using a gift card (probably because of the disconnection between the payment of money and the use of the card).

Similar cards are issued by the larger urban mass transit systems, universities and other "campus-based" organizations to permit users to make payments within the issuing system. Typically, the consumer loads a certain amount of money onto the stored value card (using cash or a credit or debit card) and then spends that amount over time. The Washington area Metro uses an electronic stored-value card, for example, and the EZ-Pass and other systems for toll roads are prevalent in large cities throughout the U.S. All of these systems are primarily for relatively low value transactions. They are called "closed-system" stored value cards because their use is usually limited to a single merchant or organization.

"Open" or "Universal" Stored Value Cards

"Open" or universal electronic stored value cards – that is, those that can be used at a large number of locations of diverse types – have so far failed to succeed in the U.S. because there simply does not appear to be demand for a new electronic alternative to cash. The existing credit card, debit card and ATM systems already meet this demand, since they are convenient, inexpensive and widely available.

"High Velocity" Payment systems

Looking to the future, however, the new systems we anticipate will likely succeed could be called "high velocity payment systems." Private or quasi-public electronic payment networks, such as highway toll pass and urban mass transit fare pass cards, are becoming more sophisticated and being used by more consumers. Similarly, some merchants are attempting to expand the use of stored value cards they issue. In some trials, these cards can be used at a wider variety of locations. That is, they are transforming from closed systems to open systems. Mobile telephone service providers are entering the field with nascent offerings which may yet overcome the lack of industry standards and other practical challenges.

These systems are designed to be transparent to the consumer, and their focus is on repetitive, low value payments where speed and convenience are the primary goal. The twist they add to the merchant-specific cards is that they hope to offer consumers the ability to make payments at a wide variety of locations. It is likely that in the near future these products will add more features and expanded functions in order to be more widely accepted. In doing so, they face the same challenges that faced Mondex, CyberCash, DigiCash, and other systems in the 1990's.

Acceptance of Electronic Payments in U.S. Financial System

The issue in all the new electronic payment systems described above – the problem they all face – is whether and how they will effectively replace all the functions

of the paper cash and check systems, including their familiarity and acceptance by consumers. In thinking about this issue, it is helpful to consider two particular characteristics of the U.S. financial system which have affected how electronic payment systems have been implemented and gained acceptance to date.

The first important characteristic of the U.S. payment systems is that they are, as a practical matter, regulated not only by government laws and regulations, but also by the internal rules of private organizations, which apply to the settlement of checks, credit cards and other payment devices. That is, banks and merchants agree on a voluntary basis to abide by the rules of, for example, the National Automated Clearing House Association ("NACHA"), which governs check processing, and the rules of Visa, MasterCard, American Express and Discover, the main credit card organizations. These rules are, in turn, imposed on consumers when they agree to the terms and conditions of a bank account or credit card account which is governed by the rules.

For example, the rules of these private organizations resolve disputes regarding which party is liable for unauthorized transactions, or for authorized transactions that are not completed due to some error. For the large part, these rules provide that the consumer is not liable for unauthorized or erroneous transactions, which of course makes these systems more attractive to the consumer. The widespread acceptance by all parties (consumers, merchants, financial institutions and regulators) of the compromises reflected in these rules is one of the strengths of the currently predominant systems.

The second important characteristic of the U.S. payment systems is that they have not experienced any large or systemic failure within the past generation. While there have been scandals such as the savings & loan failures in the 1980s and the recent corporate accounting and governance scandals, neither have involved large scale losses to consumers. Similarly, the financial system recently withstood the Y2K problem and the September 11th attacks. Therefore, it is safe to say that U.S. consumers generally have a

high degree of confidence in banks, credit cards and electronic payment systems, and therefore are willing to try new systems as they are offered.

Can New Systems Effectively Replace Paper Systems?

Because of these two characteristics of U.S. payment systems, the operational challenge for the new electronic payment systems is to develop and maintain a private system of rules which replicates all of the functions of the traditional payment systems and also provides advantages over them. Over the long run, we believe the new systems will reduce costs and increase efficiency, but the short-term price may be some confusion in the absence of ground rules which are well-understood by consumers, businesses, financial institutions and regulators. The competition between the different systems to develop fair and effective rules is likely to benefit all parties involved rather than being a race to the bottom. In any case, it is clear that wider acceptance of the new payment products will require the development of universal standards, technologies and rules, which has not occurred yet.

From a legal perspective, the fundamental issue that the appearance of new alternatives to the traditional payment systems has raised for governments and financial regulators is the question of whether it is feasible to allow a mix of divergent commercial organizations to each have an effect on the nation's payment system – i.e. its "money." Before the appearance of new and, to some extent, less regulated electronic payment systems in the 1990's, regulators did not have to ask themselves this question. To the extent they pay attention to this issue now, there is a possibility that laws will be changed to accommodate the new systems.

Information Security and Money Laundering and Terrorist Financing

The specific challenges the remainder of this paper will address are how the new payment systems will deal with the issues of information security and money laundering and terrorist financing.

We believe that information security aspects of the new electronic payment systems will, for the next few years at least, be an area of increasing concern to consumers, merchants, financial institutions and regulators. In this context, the term "information security" refers to efforts to protect electronic payment systems from the relevant threats.

On a basic level, what are the threats that are of concern?

- That an individual will break into an electronic system in order to initiate unauthorized transactions on another individual's legitimate account, thereby stealing money.
- That an individual will steal customers' personal data, enabling the wrongdoer to set up illegitimate credit card accounts, bank accounts and other accounts – this is called identity theft.
- That an individual will attack or corrupt the data in the electronic system, either as vandalism or to extort money from the sponsoring financial institutions.
- That an individual will take advantage of the convenience and speed of the electronic system to mask illegitimate or illegal transactions – i.e., money laundering.
- That a an individual will take advantage of the efficiency of the electronic system to facilitate funding of illegal activities, particularly terrorism

It is also useful to consider not only these specific threats, but also the underlying themes that are of particular concern in recent years. Three such themes are terrorism, identity theft and internal fraud (that is, fraud committed by employees or other "insiders" in the organization).

Systemic Measures to Secure Electronic Payment Systems

Obviously, sophisticated electronic systems and technical procedures exist which can be used to counter each of the threats mentioned above. But from a legal perspective, the primary area of concern is not the technical details, but instead the measures taken at a systemic level by financial institutions and other organizations to protect their electronic payment systems. Lawyers look at the security system as a whole in order to understand the framework in which these security measures will be evaluated. Lawyers focus on the fact that, at some point, a third party will examine the merchant or financial institution to determine whether its electronic payment systems are sufficiently secure. This third party could be a bank regulator conducting a periodic examination, or an independent auditor, or an adverse party in litigation, or an internal investigation conducted by the organization itself. The point is to consider, now, the factors which will be important in that examination, later, and to consider steps the organization should take, now, so that its systems will be in compliance, later. Lawyers cannot wait for a problem to occur in order to attempt to fix it.

Electronic Payment Systems Require Remote Interaction

The analysis of information security requires an understanding of the underlying characteristics of electronic payment systems which increase their vulnerability to security threats. For example, it is important to understand that remote interaction is crucial to electronic payment systems. At its core, any electronic payment system is based on an ability to query a database of financial information from a distance, and then cause that database to be modified (e.g., by making debit and credit entries) to reflect a transaction. But this remote interaction is also the characteristic which renders electronic payment systems vulnerable to fraud, hacking and other disruptions. This risk is becoming of greater concern as users demand continuous access to their funds and ever faster transaction completion.

Consider the practical implications of this remote interaction:

- In the traditional systems, financial transactions were initiated and completed by bank personnel, using proprietary systems located at the bank. Network connections to other banks occurred, but were the exception more than the rule. Many transactions were cleared based on paper documents (such as a check), with a higher degree of oversight by a human being.

- Currently, we are in the midst of rapid changes in these systems:

    - Financial transactions are initiated and completed by customers themselves, using computers that are connected to the bank's systems via the Internet. This can include very high value transactions.

    - Network connections between systems of different banks are pervasive and virtually constant. Moreover, the U.S. financial system as a whole is dependent on these connections.

    - Fewer and fewer transactions are cleared on a paper basis. And virtually no high-value transactions are paper-based.

    - There is less and less human oversight of computers which clear transactions. That is, such operations are becoming more and more automated as the computer hardware and software becomes more sophisticated and autonomous.

Steps to Information Security Compliance

What are some of the steps that are recommended to secure electronic payment systems, in light of these changes and the resulting threats to the system? We refer to these steps as "information security compliance."

- Security efforts must be "risk-based," meaning that the company or financial institution must evaluate the threats to its information assets and concentrate on counteracting those that involve the highest risk of severe adverse consequences.

- Security efforts must be continuous. Compliance measures must be periodically tested, reevaluated and modified to maintain their effectiveness. For example, errors may arise when a company or institution hires new employees, opens a new branch or enters a new business without updating its security controls to account for the new activities. Similarly, when employees leave, branches close or businesses wind-up, the information systems devoted to those past activities must be properly cleansed.

- Security efforts must cover the entire organization. Specific practices and the compliance culture must be overseen by the board of directors and extend to the lowest level of employee with operational responsibility. In particular, the compliance program must take into account that "human error" (whether negligence or willful misconduct) is the greatest threat to information assets. There must be rigorous training of employees

- Information systems must permit later auditing in order to detect efforts to alter or compromise information. Just as the "black box" is crucial to the investigation of a plane accident, there must be some means of reviewing how the information systems have actually been used and what they have actually done. If not, the organization will be unable to determine whether information security breaches have occurred, let alone determine how to prevent them.

- Third-party service providers must be held to the high standards. Many information systems tasks are subcontracted (or "outsourced") to third party service providers which are able to perform these services more efficiently. But responsibility for information security cannot also be subcontracted. On the contrary, these arrangements require close attention to the subcontractor's performance. In particular, the subcontractor should be subject to a written obligation that it meet all of the information security compliance standards of the hiring company or financial institution.

Manage Information Security as Part of Overall Legal Compliance

Last, and most important, it must be understood that the goal is not to create a list of compliance steps, and then conclude that if each of those actions is completed, the electronic system will be sufficiently secure. Instead, electronic payment systems need to be made secure as part of the organization's overall legal compliance effort. For example, decisions about what specific hardware or software measures to take need to be made in a rational way and documented, so that when the security of the system is later examined by a regulator or third-party, the institution will be able to explain why it took the steps that it did, and did not take other steps. This cannot be haphazard. Similarly, it is important to maintain access controls and logs, so that it is possible to examine how the system is used – to understand, for example, how a security breach occurred, to what extent information was compromised, and so forth. Even the most up-to-date security systems are much less valuable if there is no record of how they were installed, how they have been operated, and how they may have failed.

Money Laundering and Terrorist Financing

Turning now to money laundering and terrorist financing concerns, and recognizing the difficulty of covering all facets of such a broad topic, this paper will instead consider how these concerns are implicated in the new electronic payment systems.

It is helpful to begin with a simple example.

- An individual in the United States can open a bank account over the Internet, generally by providing a name, social security number and address, without entering a bank office.

- The individual could then transfer any sum of money into the account electronically. Money could be transferred from the U.S. or from overseas.

- Using the account, the individual could purchase stored value cards offered by credit card systems and others, and mail those cards overseas.

- Persons in other countries, then, who let us assume would be prohibited from opening a bank account in the U.S., could use the cards to purchase goods and services using funds in a U.S. bank account. (The important question of whether use of the stored value cards would require the presentation of identification is a question of local regulation and practice.)

- Similarly, persons overseas could access cash in the U.S. bank account overseas by using an ATM card linked to the account, which typically does not require the presentation of identification.

What are the facets of this example that are unique to the new electronic payment systems?

  - The first point is that as stored value cards gradually become more prevalent, common and accepted, their use becomes routine and does not draw attention.

  - The second point is that none of the individuals involved in the example described above would have any interaction with a bank employee. So

there is no question of a bank employee "noticing anything suspicious" about them, the account or the transactions.

- The third point is that in this example, an electronic network is the crucial "choke point." That is, since there is no person-to-person interaction, we must rely on an electronic computer network to detect illegal activity. Presumably, the bank or credit card networks involved in the transactions would use software to flag the fact that an individual was repeatedly buying stored value cards that are being used overseas, or that ATM withdrawals are repeatedly being made overseas. This itself raises a number of interesting points:

    - First, this would be a proprietary, commercial system. At this point, law enforcement agencies are not involved and we depend on the competence of the financial institution to detect suspicious activity.

    - Second, the obvious issue is where to set the threshold – i.e., at what point is activity deemed suspicious. It is crucial that the threshold be set at an appropriate point to avoid missing illegal activity or raising the alarm too frequently.

    - Third, it is important to bear in mind that financial institutions are primarily concerned with the detection of unauthorized transactions (for which they may be held responsible). Typically, the bank or credit card network will contact the account holder to find out if he or she authorized a suspicious transaction. If the account holder can verify the transaction, there is likely to be no further verification (until another threshold is crossed, presumably).

Which is the Greater Concern: Large-Value or Small-Value Transactions

The crucial question is (and this question is probably unanswerable): how long could a group of persons use the electronic payment systems in this way, and how much money could they launder, before being detected? The issue for regulators concerned with the prevention of money laundering and terrorist financing is: which is the greater risk – that a few large-value, illicit transactions will occur or that a series of many small-value, illicit transactions will occur? In this regard, the key aspect of the electronic payment systems is that while large-value transactions may be effected more quickly, they are also more likely to be detected. That being the case, is illicit use of electronic systems more likely to occur in the form of a series of smaller transactions which, while taking more time, would be less likely to be noticed?

Issues of Identity Verification

Considering the risk that electronic payment systems may be used to launder money also raises interesting questions about identity verification. First, it is important to note that identity verification serves different purposes in different contexts. For example, if an individual seeks to withdraw money from an account or to obtain credit, the financial institution is concerned with verifying that the person is who she says she is. Or, speaking more precisely, to verify that this individual is the same individual who controls the account or has a good credit record. On the other hand, if an individual seeks to open an account and deposit money, the bank has the opposite concern – that is, to establish that this individual is not one of the people listed on various watch-lists, with whom the bank is prohibited from doing business.

Upon reflection, it is clear that the second situation raises more difficult issues of identity verification, whether the transaction is electronic or effected in person. In the first case, the individual has the burden (and therefore has an interest in), proving that he or she is a particular person, in order to obtain the benefit of access to that persons

accounts. But in the second case, all the bank has is a name on a list, and perhaps a few other details. So we face the difficulty of a person who has access to more than one identity, as criminals often do. If a criminal presents herself to a bank, in person, with a passport or other identifying documents which match her own physical characteristics, the bank will have difficulty "proving the negative" – that is, establishing that the person does not have another identity which is an identity on a watch list – no matter how diligent the bank is.

Current security controls are more effective in preventing criminals from assuming the identity of some other legitimate person, in order to steal their money. That is, both the traditional, paper-based systems and the new electronic payment systems include means of preventing access to financial accounts by unauthorized persons. But in the second case – the money laundering and terrorist context – the person will assume a bogus identity and authorize transactions under that name, and the bank will never know that the person is actually someone who appears on a watch list.

For purposes of understanding the new electronic payment systems, the point is that they seem not to be any more vulnerable to the use of assumed identities for money laundering or other illegal activities than are the traditional systems. That is, it seems to be just as likely that bogus assumed identities could be used in the paper context as in the electronic context.

Last, just a few words on particular concerns that the threat of terrorism raises for electronic payment systems. First, it must be noted that the system itself can be a target of terrorist attacks, because it is a part of the critical information infrastructure upon which the international financial system depends. The vulnerability to such an attack arises primarily from the fact that the closed proprietary networks used by financial institutions have to be open to the Internet in order to conduct business. This provides an access point to terrorists. Since it is impossible to prevent terrorist attacks completely,

electronic payment systems must include measures to contain and remediate any security breaches.

Balancing Difficulties Arising in Electronic Payment systems

In conclusion, there are benefits and detriments in electronic payment systems in terms of the risk of money laundering and illegal activities. While it is true that electronic transactions can be effected more rapidly and from remote locations, it is also easier to maintain automatic records of such transactions or to put in place automated blockages of certain transactions. Similarly, while it is nearly impossible to verify the identity of someone who initiates a transaction remotely by electronic means, we must bear in mind that identity verification, in itself, raises a number of conceptual difficulties.