Making Payments on the Internet

*James J. McAndrews**

The Internet has begun to make the idealized marketplace discussed in economic textbooks seem more plausible. It allows low-cost, speedy, convenient, and informative communication across the world. However, to become an active market in goods and services the Internet must overcome a fundamental hurdle: a way must be devised for buyers and sellers to securely and conveniently exchange payment over the Internet. Software companies and financial institutions are now developing methods that will allow people to pay on the Internet. A review of these efforts reveals the importance of security, authenticity, and privacy, which are often overlooked or taken for granted in other instances of making a payment.

Money is an ancient human artifice. For approximately 3000 years coins have been minted in India and Greece. Minting coins for use as media of exchange was a significant improvement over the alternative: exchange of metals by weight for purchases. Coins made a particular amount and quality of metal easily recognizable and hard to counterfeit. Milling the edges of coins made the practice of removing small amounts of metal from the coins very easy to detect. The creation of banks of deposit and their vaults made safeguarding coins easier.

*James McAndrews is a senior economist and research advisor in the Banking and Financial Markets section of the Philadelphia Fed's Research Department.

Hence, coins became readily identifiable and transferable, attributes that raw metals did not possess. These attributes made trade easier.

Our society is grappling with ways to create, once again, a way to make payments in a new medium: the Internet. The designers of Internet means of payment have the same concerns that occupied mints centuries ago: how to make the proposed means of exchange easy to recognize and authenticate, but hard to counterfeit and steal. Today's designers work with powerful mathematical means of encryption, which can serve the same roles for Internet payments that minting coins served for earlier payment systems.

Several attributes of a successful medium of exchange—one of money's primary roles—have emerged over the centuries. Money should be identifiable, divisible, easy to transfer (both technologically and in the sense of there being widespread acceptance), and easy to protect against theft. The attempts to create successful media of exchange over the Internet reveal the importance of these attributes as well as the difficulties of successfully designing a system with those attributes.

THE INTERNET

The Internet, a network of computers that use a common method of communication, has experienced rapid growth in recent years. While estimates of Internet size and usage are imprecise, one estimate shows that the number of computers linked to the Internet increased from 213 in August 1981 to 3,864,000 in October 1994 and to 9,472,000 in January 1996. The amount of message traffic across one part of the Internet is estimated to have grown from 85 million packets in January 1988 (a *packet* is approximately 200 bytes; a byte holds one alphabetic character) to more than 60 billion packets in January 1995.[1] The Internet is used to send mail, to transfer files, and—using the World Wide Web—to transmit graphics and sound.[2]

The impressive growth of the Internet has been facilitated to some extent by the steadily declining cost of computers. Furthermore, in many cases, individual users of the Internet (or their employers or sponsoring organizations) pay a fixed fee, or a fee that does not vary with the number of sites from which they gather information, and there is no marginal fee for the use of the network facilities in sending or receiving information. This zero marginal cost of usage makes sending a message across the country essentially free for many users.

The Internet differs from telephone networks in that each message does not have a *circuit* dedicated to it. Instead, a message on the Internet is divided into packets, each with the address of the message attached to it, and the individual packets are sent through computers (known as routers) to their destinations. This *packet switching* method allows many packets to simultaneously share the physical telecommunication lines across which the packets travel. This greatly economizes on the use, and therefore the costs, of telephone lines, relative to telephone calls, which use a *circuit switching* method that dedicates a circuit to a particular call.[3]

This inexpensive and increasingly ubiquitous form of communication and information transmission has made it possible to imagine continuous, worldwide electronic commerce. On the Internet, one can comparison-shop, read

[1]The first of the two estimates was made by network analyst Mark Lottor, and the second refers to message traffic across the NSFNET backbone—that part of the transmission lines funded by the National Science Foundation. These estimates are reported by the Merit Network, Inc., a nonprofit corporation providing a number of Internet services.

[2]The World Wide Web is a communications protocol developed for graphical content and sound.

[3]A good discussion of the Internet is given by Jeffrey K. MacKie-Mason and Hal Varian in "Economic FAQs About the Internet," *Journal of Economic Perspectives,* Volume 8, Number 3, Summer 1994, pp. 75-96.

warranties, establish accounts, view images of products, and order goods and services from companies located anywhere in the world. Home shopping on the Internet could reduce the transaction costs of shopping significantly; many believe that it is the "killer app" of the Internet.[4] To flourish as a marketplace, however, the Internet needs a means of payment, but payment over the Internet faces some unique barriers. In particular, the challenge is to devise ways to protect against theft while conveying payment information that is recognized as authentic.

CAN I PAY WITH A CREDIT CARD OVER THE INTERNET?

When I make a phone call to my favorite mail-order catalog to order a pair of shoes, the only parties to the call are the order taker and me. If I were to send an e-mail over the Internet to the catalog company instead, the information may be routed through many computers not party to the transaction before it reaches the merchant, allowing others to intercept my message. If my credit card number is included, others can steal it. Furthermore, if a hacker has infiltrated either the merchant's computer network or the one of my Internet access provider, the hacker could intercept, read, and alter messages. Because of that, I can't be sure that my messages haven't been read or altered after I've sent them. The activity of intercepting and reading others' messages is known as snooping.

While telephone fraud is a big problem, the ease with which criminals can fake e-mail messages of others—someone with sufficient knowledge of computer systems can connect to the victim's mailserver on the Internet and send the fake message from it (an activity known as spoofing)—makes enhanced security a necessity. It is also much easier for criminals to establish untraceable computer accounts to fraudulently collect credit card numbers (if they were unencrypted). It is much more difficult to do so with telephone mail-order operations.

The real possibility of theft of the information has precluded the widespread use of unencrypted credit card numbers over the Internet. Furthermore, the ease with which criminals can adopt fraudulent identities and untraceable addresses on the Internet deters people from attempting to purchase items over the Internet. Therefore, new means of making payment must be devised.

Designing a method of Internet payments, therefore, requires attention to two features of money that are necessary to securely convey payment information. Authentication of messages is important for both parties to a transaction. Finding a means to prevent eavesdropping is important, so that criminals cannot steal payment-related information, such as credit card numbers, as they are transmitted over the Internet. It may be that secret coding of information can solve both of these problems.

ENCRYPTION

As with all types of money, identification and recognition are necessary before a seller will accept a payment. Payment systems today use various means to identify a payer. In credit card transactions conducted in person, possession of the card and a signature matching the one on its back suffice. For point-of-sale transactions with a debit card, possession of the card and a password identify the account holder. When paying by check, a signature (and often a photo identification card) is necessary. For cash transactions, the currency is examined to authenticate it.

On the Internet this means that correctly identifying the customer and maintaining the integrity of the information are vital. A password—even one that has been encoded by some encryption device—is not enough to identify a person if it is used more than once (because of

[4] A killer app is an application of a particular technology that many potential users find irresistible.

the possibility of theft of the password). If an encoded message is used more than once, it could be duplicated and sent by some other person posing as the original sender.

None of the measures used to authenticate the means of payment today are foolproof. Counterfeit currency and check and credit card fraud are significant problems. But the ease with which snoopers can intercept unencrypted messages has led security experts to believe that encryption of financial information is necessary to approach the levels of security that people now enjoy with cash, checks, and routine credit card payments.

Privacy. Securing the integrity of a message sent on the Internet poses a difficult problem. Even when a message is encoded, if criminals were to decode the message, or steal the "key" by which the original message was encoded, the integrity of the message would be lost. With traditional encryption methods the sender and receiver have to share the key to successfully encrypt and decrypt a message. Therefore, the sender has to give the key to the receiver in some way. This makes the management of the secret key extremely difficult because it is much more likely to be stolen as it is shared with many parties (for example, all the merchants that accept a type of credit card) and as it is being communicated to all the parties to a message. Furthermore, with traditional methods of encryption, once someone has stolen the key, messages can be both decoded and encoded. Hence, a criminal, armed with the key, can pose as a legitimate party to the encryption system, and no one could detect the deception.

A new type of encryption was discovered in the 1970s by Whitfield Diffie and Martin Hellman, two American mathematicians. Their contribution to encryption theory was to recognize that systems of encryption can be created that use a pair of keys, one to encrypt the message and another to decrypt it. One type of these "asymmetric" cipher systems is a "public key/private key"cipher (commonly referred to simply as a public key cipher) in which the encrypting key need not be kept secret to ensure a private message.[5] The decrypting key (the "private key") need never be shared with anyone else and, therefore, is much less susceptible to theft. (See *Keys to Establishing Trust in Cyberspace.*)

Under public key cryptography, if two people wish to exchange private messages, they each create a pair of public and private keys. Alice obtains Bob's public encryption key, uses it to encrypt a message to Bob, and sends it to him. Bob can then decrypt it using his private key. Only someone who has Bob's private key can decrypt messages encoded with his public key. To reply, Bob obtains Alice's public key, encrypts a message, and sends it to Alice. She deciphers the message using her private key. This system of encryption offers a great deal of security in managing the private keys because they never have to be shared with anyone. Clever applications of this type of cryptography can be used to verify identity (using a "digital signature"), authenticate messages, and provide a record of when a transaction occurred—all vital aspects of a trustworthy means of payment on the Internet.

Encryption of electronic financial information traveling across the Internet offers a safeguard against theft of information, and the digital signature offers a way to authenticate the message. Hence, these sophisticated mathematical devices play the roles that other devices that prevent the theft of money—such as vaults, wallets, and commonsense security precautions—and devices that authenticate money—such as watermarks, specially printed paper, passwords, telephone authorization, and signatures—play in other forms of money.

[5]A good discussion of public key cryptography is contained in Bruce Schneier's book *Applied Cryptography,* John Wiley and Sons, Inc., second edition, 1996.

APPROACHES TO INTERNET PAYMENTS

There are currently several approaches to offering payment services on the Internet: credit-card-based systems (which represent an extension of credit by the issuer of the credit card to the holder); payment orders (much like a check is an order to one's bank to make payment); or a new form of payment, digital cash.[6] Most use some form of the public key/private key encryption system, but others safeguard financial information in other ways.

Trusted Third Party. At least one firm offers a trusted-third-party method of payment: a customer authorizes the trusted third party to make payments on her behalf. In such a system the customer supplies (over the phone or through the mail) the trusted third party with her credit card number or a voided check and written authorization to effect payment on her behalf. The customer is supplied with a password. As the customer orders a product over the Internet, she supplies the seller with her password; the seller reports this to the trusted third party; and it, in turn, sends to the customer a report of the transaction and asks the customer to confirm it. Once confirmed, the trusted third party conveys the payment information through the automated clearing house system (the electronic interbank system that banks use to exchange small-value payments). This system avoids the problem of eavesdropping, which is a concern in transmitting payment information across the Internet.

The trusted-third-party method offers the benefit of securing credit card or checking account information against theft. It requires, however, sellers as well as buyers to accept payment by the trusted third party; therefore, widespread acceptability is a potentially difficult hurdle for the system. As in all the systems we discuss, the security of the system itself is vital. Such security requires electronic firewalls that cannot be breached by a hacker.

Digital Cash. At least one firm is offering customers the ability to make payments in "electronic," or digital, cash, and others plan to do so.[7] Digital cash consists of messages that use a sophisticated set of variants on the public key/private key encryption system. It is stored on a computer's hard disk and is electronically transferred to a payee. It may also be electronically replenished by transfer from one's account at a participating bank. A digital cash system employs software held by the participating financial institutions, their customers, and merchants. Using that software, the customer creates digital messages that are authenticated by the issuing institution in a way that third parties can recognize. The issuer's authenticated message is returned to the customer and acts as a substitute for cash. A merchant that receives the digital cash can send it on to its bank and have its account credited or it can spend the digital cash.

Digital cash systems typically propose to prevent counterfeiting by virtue of the issuer's digital signature on the digital cash, which verifies its authenticity. Issuers intend to prevent double spending of the cash by "reissuing" or replacing digital cash each time it is spent; participating financial institutions will not accept cash with serial numbers that indicate it has already been spent.

Digital cash has the potential for a feature many believe is increasingly important in an electronic information age: anonymity. In principle, the merchant need not know who is spending the digital cash it receives: the cash is

[6] An extensive list of such approaches is maintained by Michael Pierce on the Internet; the address is http://ganges.cs.tcd.ie/mepierce/Project/oninterest.html. There are links at this site to many firms offering some of the services described in this article; those sites typically provide descriptions of the services and plans of the firms.

[7] See "Banks Get the Green Light to Hit the Internet," *Bank Network News,* July 12, 1995.

Keys to Establishing Trust in Cyberspace

Cryptography is the science of hiding the contents of messages from eavesdroppers by means of "secret writing." It has been explored and developed spectacularly in the last quarter of a century—a happy coincidence given the security needs of the world's ever-expanding communication networks. Cryptography can assist in providing the necessary identifiability and protection against theft that a digital or electronic means of exchange requires. But, first, some definitions are needed.

Cipher. A cipher is a mathematical function used for encrypting (or coding) and decrypting (or decoding) a message. One example is the Caesar cipher, in which each letter in a message is replaced by the third letter following it in the alphabet: a is replaced by d, b by e, and so on, with x replaced by a, y by b, and z by c. Modern ciphers use a key, which can take on many values (and are usually very large numbers). The value of the key affects the cipher; for example, the Caesar cipher is a simple substitution of one letter of the alphabet for another, with a key value of 3. If we change the key value to 5, then a is replaced by f, b by g, and so on.

Key. There are two types of key-based ciphers: secret key ciphers, in which the same key is used for encryption and decryption, and public key ciphers, in which a pair of keys is created, one for encryption and one for decryption. In a secret key system, a group that wishes to exchange messages must share the key to communicate but keep it secret from third parties. Secret key, or symmetric, cryptography is most useful for long messages. In a public key system, one of the keys (typically the one used for encryption) can be made public, but the private key (typically the one used for decryption) need not be shared with anyone else. Furthermore, if the keys are chosen well, it is practically impossible to determine the private key even with knowledge of the public key.* Public key systems make *key management*, which refers to the way keys are created, stored, and maintained, much simpler and less susceptible to attack.

Public key systems have many useful features that can aid in authenticating a message, uniquely identifying a person, confirming receipt of a message, and enhancing the privacy of the message. They have the drawback of being costly in terms of computing time and effort, relative to secret key systems, for encrypting and decrypting large amounts of text.

Authenticating a Message. A public key system can assist in authenticating a message by incorporating a "digital signature" in the message. A digital signature is a clever double use of a pair of public key ciphers. Alice, in sending a message to Bob, appends her signature to the message, and she encrypts her signature by means of her private key (usually used for decrypting a message). She then uses Bob's public key to encrypt this "signature" and sends it on to Bob. Bob uses his private key to decrypt the

message and, seeing a potential signature of Alice, uses her public key to decrypt it. Upon successful decryption, Bob realizes that only Alice could have sent the message because only she has the private key counterpart to her public key. Hence, the digital signature has authenticated the message Alice sent to Bob.

Identifying a Person. But how does Bob know that Alice is in possession of her private key? It's possible that an impostor, claiming to be Alice, sent out the public key in Alice's name simply to intercept messages intended for Alice. How then to verify that the person who claims a public key in Alice's name is Alice? A "digital certificate" can serve to verify the identity of the person holding a particular key because it contains that person's name and public key, a digital signature, the name of a trusted *certificate authority*, a serial number, and a set of dates for which the certificate is valid. The certificate authority thereby verifies that the public key in the certificate belongs to the person whose name is attached to it. The process of obtaining a certificate for one's public key requires a high degree of trust and may involve visiting the authority in person and showing proof of identity.

DIAGRAM 1
Alice's Digital Certificate

Alice's Identifying Information: Name, Organization, Address
Alice's Public Key
Certificate Serial Number
Certificate Validity Dates
Issuing Authority's Digital Signature and I.D. Information
Message with Time-Stamp

Confirming a Message. Alice can cheat in this system. First, she purchases an item using her credit card and a digital signature and certificate. After she receives the item, she publishes her private key. She then reports that her private key has been compromised, and she did not authorize the purchase. One way to lessen the possibility of this type of cheating is for the receiver, Bob, to have the message *time-stamped* by an authority upon receipt. The time-stamp would be similar to the digital signature of the time-stamping authority and cannot be altered. Alice would have had to declare her private key compromised before the purchase, making it possible for the certificate authority to repudiate its certificate for Alice before Bob receives the message. Diagram 1 shows a digital certificate with a time-stamped message.

Enhancing Privacy. Using public key cryptography for sending a long message would be costly in terms of computing time; therefore, secret key, or symmetric, cipher is preferred. The difficulty lies in how to communicate the secret key, which cannot be revealed publicly without compromising the encryption. Public key cryptography can solve the problem by encrypting the secret key using the public key. Then the secret key would be hidden from everyone except the holder of the associated private key. This encryption of the secret key is called a digital envelope (Diagram 2). Digital envelopes are useful when sending a long message. Most payment messages would not be long enough to require the use of secret key cryptography. The public key cipher could be used directly to encrypt the message.

DIAGRAM 2
A Digital Envelope
Created by Alice

Secret Key Used for Encrypting and Decrypting a Message, Encrypted with Alice's Public Key
Message Encrypted with Secret Key

* Decrypting a message in a secret key system requires finding the inverse of the key; for example, in the Caesar cipher one substitutes a letter three places to the left of the encrypted letter to decrypt a message. Finding the inverse of a public key is practically impossible for large keys because it would require extraordinarily large amounts of computing.

authenticated by the bank, not the customer. The merchant might sell an item and be directed to send it to a computer account (if it is a piece of information that can be sent over computer networks) or to a post office box, not knowing who requested it. If the merchant is paid in digital cash and does not know the identity of the holder of the computer account, there is no way the merchant can find out the identity of the buyer.[8]

The concern for privacy is increased today because of the greater ease of compiling information electronically. Many firms sell information on their customers to other organizations for marketing purposes. The enhanced privacy that is possible in a digital cash system comes at a cost of more complex software to run the system.

Credit Card Methods. Visa International and MasterCard announced on February 1, 1996, that they have agreed to jointly develop a standard to solve the problems of snooping and spoofing. American Express later joined the effort as well. The standard is called secure electronic transactions (SET), and it is based on public key cryptography. The developers of the standard will attempt to ensure the integrity of credit card numbers that a cardholder sends to a merchant by encrypting the numbers. Prior to any transaction, however, the developers of SET propose to verify the identity of both merchant and cardholder by having either the bank that issues the card (in the case of the cardholder) or the merchant's bank that processes the transaction (in the case of the merchant) provide both parties with "digital certificates." These certificates may bear the digital signature of Visa or MasterCard or some certifying authority (see *Keys to Establishing Trust in Cyberspace*). Verifying that the digital certificate does indeed bear the digital signature of the expected certifying authority should help to assure the cardholder that the merchant has a legitimate relationship with a bank and is therefore not attempting to fraudulently collect credit card information for later criminal use. Furthermore, the proposed design for SET seeks to ensure that the merchant will not be able to decrypt the holder's card number; rather authorization from the merchant's bank will ensure payment, and the consumer's number will remain unreadable to the merchant.

Prior to their February announcement, Visa and MasterCard had embarked on creating separate standards for securing credit card transactions on the Internet. The subsequent decision to join forces to create and adopt a single standard will simplify the process of using the software that will operate the standard. With a single standard a merchant will be able to identify itself and secure its payment information using only one system. The decision to jointly develop the system avoided a potentially costly duplication of effort on the part of the card associations, banks, and merchants.

Internet Banking. At least one bank exists primarily for banking on the Internet: it has only a small physical office, but a "virtual branch" on the Internet. While this bank does not offer a direct method of payment on the Internet, it allows its customers to pay bills by writing checks or making an electronic payment through the automated clearing house. This method is a variant of trusted-third-party payments because information flows through private interbank networks.

Other banks and technology companies have created the Financial Services Technology Consortium. This group is sponsoring research into electronic commerce over open networks, such as the Internet. One of their ventures is the electronic check project, an attempt to create a pay-

[8]If the merchant were to find that the cash had previously been spent, it would seem to have no recourse, given the cloak of buyer anonymity. However, David Chaum, an expert in cryptography, ingeniously devised a system in which the buyer's identity is revealed only if the buyer attempts to spend the cash twice.

ment method that will be accepted much as a paper check is today. It, too, proposes to rely on encryption to secure account numbers and digital signatures to verify identities, but it will provide access to one's bank account, rather than create digital cash.

ACCEPTANCE OF THE NEW MEANS OF PAYMENT

There are many approaches to payment over the Internet. Will they all survive? It is too early to determine whether the different means of payment are useful and cost-effective, but as in non-Internet-based payments, it may be that different forms of payment may survive for different uses and for different users.

Many competing and complementary means of payment exist today. For example, while credit cards are useful for international and many retail and mail-order transactions, only some merchants are able to accept credit cards (that is, they are "signed-up" customers of banks' credit card services). Nor do all consumers have sufficiently high credit ratings to obtain a credit card. Credit card payments are relatively costly to make because they involve an extension of credit by the issuing bank. Furthermore, credit cards typically are not useful for paying a friend. Checks, while convenient for payments to individuals, are not as useful for international transactions. Checks are also fairly costly because of the care that must be taken in routing the paper check through the banking system and back to the one who wrote the check. Cash is convenient for low-value purchases and can be used anonymously in some circumstances, but it is costly to hold in inventory.

Many foresee demand for a way to make very low-value payments over the Internet. For example, a person may wish to purchase a photograph of a movie star for $0.50. For such small payments it is costly to write a check or to use a credit card (which usually requires a minimum payment of about $20 because of relatively high cost per use). Typically, one uses cash for such a small payment. Hence, digital cash, if it proves sufficiently convenient and low cost, would be much in demand for low-value payments. The cost of a digital cash system is not yet known. Until such a system is operating on a fairly large scale, it is not certain that it can be operated at a sufficiently low cost to make payments for, say, less than a dollar economical.

Credit card methods may prove useful for larger dollar amounts on the Internet. People may be discouraged from using digital cash for large-value payments because they enjoy less float when using digital cash—a debit method of payment—than when using a credit card. Furthermore, many credit-card holders already use their cards to make payments by phone and may therefore be more willing to make the leap to using them over the Internet.

Privacy and security concerns may induce some people to use the trusted-third-party method of payment as well as digital cash. Both of these methods avoid sending credit card information over the Internet, even in a highly secure encryption scheme. In addition, a consumer may wish to withhold his identity from a merchant to avoid having the information used either for marketing purposes or by law enforcement agencies if he is engaging in illegal activities.

PUBLIC POLICY CONSIDERATIONS

The ways that payments are made in the United States today are governed and supported by law and public policy. For example, the laws, policies, and contracts that govern the rights of the various parties involved in a check transaction are well established. These policies help to make checks a reliable and predictable method for making a payment for all the parties involved in the checking system.

For the proposed Internet payment systems, issues such as consumer protection, disclosure and assignment of participant liability, and privacy are being addressed by regulators and law-

makers. The resolution of these policy issues will affect the development and acceptance of the proposed systems.

In particular, questions about the degree to which disclosure requirements, account statements, and some form of electronic receipt would be useful and appropriate for Internet payment systems remain largely unanswered. Required disclosure of liability can help inform parties to a system about their responsibilities and thereby improve decision-making, although such disclosures impose an administrative cost on the system's operator, which, if the system is to succeed, will be collected in some way from the consumers of the service. Account statements and electronic receipts would assist users of payment systems in reconstructing their activities in case there were questions about unauthorized use of their accounts or unauthorized payments—again, at a cost of record-keeping for the system and its users. Resolution of these issues will clarify the obligations of the parties and, with a careful balancing of the costs and benefits involved, will advance the development of acceptable forms of payment systems on the Internet.

Recently, for example, the Federal Reserve suggested modifying some provisions of its Regulation E, which governs many (conventional) electronic methods of payment, as it applies to stored-value cards.[9] The Board's proposal suggested that cards that can store no more than $100 be exempted from the provisions of the regulation, and it makes further exceptions for various specific types of cards. For example, under the proposal, a merchant would not be required to issue paper receipts when certain types of stored-value cards are used for payment. Furthermore, in the proposal the Board also recognized that stored-value systems (such as various digital cash systems) are being developed for the Internet: "Systems are being proposed, for example, for making payments over computer networks, such as the Internet"; it also requested comments on the extent to which the Board should consider applying Regulation E to "various types of network payment products."

Another legal and contract issue is that, on the Internet today, the merchant (and the system operator and the consumer, for that matter) has no standardized or generally accepted and enforceable way to verify the signature or password of the other party to the transaction. As a result, the liabilities of the parties are unclear in the event of a repudiation of a transaction by a customer when the transaction was authorized using the customer's digital signature. In contrast, the assignment of liability in a credit card or (off-line) debit-card transaction is well established. The credit card associations were instrumental in standardizing the form of the contracts used today in the credit card industry. If Internet payment systems not based on credit cards are to succeed, such an association may be helpful in organizing contracts and standards that would form the basis for widespread merchant and bank acceptance of the systems.

A widespread acceptance of contractual standards that make the digital signature of the customer binding may be desirable to address the issue of how liability is to be assigned in the case of a repudiated payment.[10] This issue is complicated by the fact that the federal gov-

[9]See the proposed rule of the Federal Reserve System, 12 CFR Part 205, Regulation E; Docket No. R-0919, April 3, 1996.

[10]Such a repudiation may be done fraudulently; that is, a consumer may make a purchase using a payment system based on digital signatures and then later fraudulently claim not to have made the purchase. Hence, the effort to make it difficult to repudiate one's digital signature will reduce fraud of this sort. (Alternatively, the consumer may have mismanaged his or her private key, thereby allowing someone else to make a purchase using his or her digital signature, and repudiated the transaction for that reason.)

ernment has chosen a standard for digital signatures that is different from the standard that has emerged in private industry. Neither has the force of law behind it. Recently, two states, Utah and California, have passed laws giving digital signatures the same validity as handwritten signatures. Similar legislation is pending in other states. These laws should reduce the possibility for repudiation and thereby advance the development of systems using digital signatures.

A second issue regarding digital signatures is who should be allowed to be a certifying authority for the public key used to create such signatures (see *Keys to Establishing Trust in Cyberspace* for a description of the role of a certifying authority for public keys). The certifying authority, in granting a certificate to a party, puts its stamp of approval on the certificate holder's management of the private key and provides the certificate holder a proof of identity. Such certification may carry an implicit guarantee of performance and hence may require the certifying authority to bear a considerable amount of risk. The authority may therefore require considerable oversight power for those to whom it grants a certificate.

Digital cash also entails policy considerations. The creators of digital cash envision individuals transferring it among themselves with no intermediary, which raises the issue of what kind of backing digital cash must have. For instance, must digital cash be backed by currency 100 percent? This would involve an issuer's holding $1 in currency in its vaults for every $1 of digital cash created. Alternatively, should the issuer buy short-term securities, such as U.S. Treasury bills, as backing for the digital cash? Under this system, the creation of digital cash could represent an increase in the money supply. Beyond this issue lies the possibility for "designer digital cash," which could be backed by gold or issued in foreign currencies or which could earn interest. There are few technological limitations on the backing and characteristics of digital cash.

Should digital cash be covered by deposit insurance? This question needs to be settled in part to determine who is liable in the event of the failure of an issuer of digital cash. The Federal Deposit Insurance Corporation (FDIC) recently issued a notice and request for public comment addressing stored-value cards and other electronic payment systems and their eligibility for deposit insurance.[11]

The proposed Internet payment systems require areas of expertise new to most banks. Such expertise is typically found in software companies. Banks and bank holding companies are allowed to engage only in activities that are "closely related" to banking. It is clear from our discussion that encryption systems, among other things, are vital to the success of Internet payment systems. But is developing an encryption system an activity "closely related" to banking? By approving the acquisition of a home-banking software company by a group of U.S. and Canadian banks, and by approving the acquisition of an Internet banking software company by a subsidiary of a bank holding company, the Federal Reserve System and the Office of the Comptroller of the Currency have shown a willingness to allow banks to provide services in this area.[12]

Encryption systems raise issues that go beyond banking. There is a tension between the security of financial messages traveling the Internet (by means of strong encryption systems) and the security of the nation and the ability of its law enforcement authorities to prevent illegal financial transactions. The United States closely regulates the use of strong levels

[11]See the notice of the FDIC in the *Federal Register,* August 2, 1996, pp. 40494-97.

[12]See the orders of the Board of Governors of the Federal Reserve System in the *Federal Reserve Bulletin*, April 1996, pp. 363-65, and in the issue of July 1996, pp. 674-76.

of encryption because of its important role in national security. Some commentators fear that denial of licenses to export software that includes strong levels of encryption may put U.S. firms at a competitive disadvantage. At least one firm, though, has won approval to export software based on strong levels of encryption; its software was for financial use only, and it was felt that the encryption system could not be removed from the software.[13]

The need for confidentiality of payment information on the Internet is great because of the greater ease of compiling histories of consumers' purchases. Enhancements to consumer privacy laws may be needed to preclude the misuse of consumer information by nonfinancial firms that may offer payment services or affiliated software. The question of how much confidentiality is needed in Internet commerce has spawned a debate about the merits of a *completely* anonymous payment system versus the merits of lower cost, more conventional systems of credit card and electronic checks that allow merchants, banks, and system operators to maintain data bases of user information.

CONCLUSION

Efforts to create a form of Internet money are attempts to put old wine in new bottles. Money must be easily identifiable, easy to protect from theft, widely acceptable, and easy to transfer. Providers of Internet payment systems are attempting to meet these requirements in various ways. Sophisticated methods of encrypting the financial information used in payments may prove to be the modern equivalent of vaults, signatures, and watermarks. Public policy will play a role in securing the legal foundations that can help pave the way to widely acceptable and secure ways to pay on the Internet.

[13]"Cybercash Gets Clearance to Sell Product Abroad," *Wall Street Journal*, May 8, 1995.