

# ECONOMIC COMMENTARY

Federal Reserve Bank of Cleveland

## Making Payments in Cyberspace

by Paul W. Bauer

Cyberspace is loosely defined as the collection of computer communication networks that has evolved since the early 1970s. Although it is most often associated with the Internet, a myriad of bulletin board providers and commercial services are also included.

Vendors are attracted to cyberspace for several reasons. First, millions of people throughout the world have at least some access to the "Net," and their ranks are swelling. These users tend to be young, educated, and wealthier than average — characteristics that marketers find very attractive.<sup>1</sup> Second, by building a presence in cyberspace, a business can offer its goods and services relatively cheaply, worldwide, and 24 hours a day. Finally, a cyberpresence, by distributing detailed information to potential consumers, may also boost sales through conventional channels.

What makes the emerging cybermarket particularly exciting is that the technology will allow many new products to be developed and markets to be tapped. With communications and computing costs plunging, cyberservices will be available to anyone with a telephone and a personal computer.

Unfortunately, a number of problems will have to be overcome as the electronic marketplace evolves. Currently, not everyone has access, and many users lack the high-speed equipment required to take full advantage of the graphic interfaces. A number of procedural and legal challenges will also have to be

addressed, such as who — if anyone — will control the content of the material sold in cyberspace and how copyright issues will be handled. But one of the most vexing problems is how to pay for cybergoods and services.<sup>2</sup>

### ■ Why New Payment Instruments Are Needed

Traditional means of making payments (cash, check, credit card, automated clearinghouse, wire transfer) conflict with the characteristics of many cybermarkets. In particular, many transactions are likely to encounter problems of trust, security, or size. To illustrate, consider the following. After browsing the Web, you decide that you'd like to download a photo of Lance Armstrong winning a stage in the 1995 Tour de France bike race.<sup>3</sup> If you find the image in one of the many noncommercial sites on the Net, you can simply download the picture, since no payment is required. Volunteers throughout the world have made a vast quantity of useful information available free of charge. But professionals — photographers included — are unlikely to allow much of their work to be distributed widely without receiving some sort of compensation.

A second possibility is that access to the image will be available only to those who subscribe to a particular on-line service. On-line services bill their subscribers per minute of connection time and share some of that revenue with the content provider (in this case, the photographer). This system works well when you have established a prior, continuing

According to one market-research firm, there will be more than 22 million World Wide Web users by the turn of the century, and two-thirds of them will come from the consumer ranks rather than from academia or corporate America. As electronic communications expand, cybermarkets are expected to burgeon. But one issue that will have to be resolved before the on-line marketplace can truly compete with traditional markets is how to pay for the goods and services sold in cyberspace.

relationship with an on-line service provider, but does not fit the standard pattern of marketing.

A number of general payment problems can arise when this prior relationship is lacking. Suppose that a professional photographer having only a "home page" presence on the Internet wants to market pictures directly to individual buyers.<sup>4</sup> As a customer, you could mail the photographer cash (not advisable) or a check (better), but "snail mail" is unlikely to be a satisfactory solution. The necessary trust probably doesn't exist between two strangers in cyberspace. On one hand, if the photographer provides the picture immediately and has to trust a customer to send the check, how many payments might never be mailed? On the other hand, if you as the customer can't download the picture until your check clears, should you get your money back if the procedure doesn't work or if the product is not as advertised?

Credit and debit cards seem somewhat better suited to dealing with a lack of trust among electronic strangers. The seller could rely on the same verification system used in filling phone orders from catalogue shoppers. Purchasers would be protected by Federal Reserve Regulation E, which enumerates the rights, liabilities, and responsibilities of participants in electronic funds transfers. Ultimately, however, cardholders as a group would have to make up any loss.

Solving the matter of trust between buyers and sellers would not eliminate all of the problems. The Internet is an "open" system that also raises questions of security. Information travels over the Net in packets that may pass through many intermediate nodes before reaching their final destination. At any point along the way, someone with only a little technological expertise could set up a "packet sniffer" to look for information resembling credit card numbers. The odds are slight that any given transaction would be intercepted, but with millions of transactions poised to occur in cyberspace, the potential for credit and debit card fraud is huge.

These cards have another problem: They are not well suited to those transactions for which coin and currency are used in ordinary markets. The photographer may want only 50 cents for his digital picture, but the average cost of a credit card transaction is at least 88 cents, making this an uneconomical means of paying for small-value items.<sup>5</sup> In addition, the cost of becoming a credit card merchant is not insignificant and could further hinder the spread of the electronic cottage industries that some have envisioned. Credit card payments also lack the anonymity that cash provides and that many people prize.

This extended example illustrates several crucial points. In cyberspace, a vendor can reach highly specialized market niches quickly and effectively. In any one city, only a few hundred people may be interested in professional cycling, but nationwide there are hundreds of thousands of fans, and globally there are millions. Further, many payment instruments are likely to evolve in cyberspace — just as they have in the physical world — with each geared to different niches based on the dollar amounts involved and on whether there is a long-term relationship between the transacting parties. Once the security issue is resolved, these new methods of making payments will widen access to cybermarkets and stimulate the development of new products.

#### ■ Ensuring Secure Payments

Many companies both large and small are striving to develop secure methods of making payments in cyberspace.<sup>6</sup> The proposals vary tremendously in terms of the amount of privacy they retain for payors, how costly they are to use, and what parties are able to transact. Most rely on credit or debit cards to make payments over the Internet, but a few are much more ambitious, striving to create a cyberspace equivalent to cash known as "e-cash." There are two basic approaches to protecting the security of payment information — value-added networks and encryption — and they may be employed either separately or in tandem.

*Value-Added Networks.* The security weakness of using credit and debit cards

stems from sending plain text over a network that is open to anyone. The most straightforward solution is not to send information over the Internet at all. By using a relatively more secure value-added network (VAN) to handle confidential data, the risk of interception is greatly reduced. Information that flows from the open network must pass through "firewalls" (computers programmed to allow only authorized transmissions to penetrate) before reaching the VAN.

*Encryption.* The second general approach to providing secure transactions employs encryption, a method of scrambling information before it is sent out over a vulnerable open network. This way, anyone intercepting the data en route cannot make use of it. Encryption should be less expensive than the value-added approach, since the costs of an alternative, secure network are not incurred. Of course, encryption requires the party at the other end to have compatible software as well as the key to unscrambling the information.

The most straightforward use of encryption is to incorporate it into Web browsers, as several companies are seeking to do. This enables credit or debit card information to flow safely over open networks. Encryption also allows much more ambitious proposals.

Several companies are attempting to use encryption technology to replicate the features of finality and anonymity that coins and currency possess. Currency has finality because once you receive it, you can verify fairly confidently that it is genuine, and short of suing you, the payor has no legal way to reverse the transaction. Credit cards do not carry this feature. Currency is also anonymous. Merchants do not accept cash from you because you are you; they accept it because they can verify that the money is legal tender. In contrast, the validity of credit card transactions depends on you being who you say you are.

At least a few of these new approaches to providing secure electronic payments are likely to find profitable niches in cybermarkets, but it is far too soon to

predict which of the many specific proposals might acquire wide acceptance. The market may have room for only a few, given the large network economies present in using payment instruments. The value of participating in one particular network rises as the number of merchants and individuals with whom you can transact expands. This suggests that, eventually, a few dominant "brands" of electronic payments will develop, just as a few dominant ATM networks have come to prevail.

### ■ Policy Issues

New payment instruments raise new issues. Encryption is one, since non-mathematicians are likely to find it difficult to verify the degree of security it brings to a payment device. The stronger the encryption, the more secure the instrument (and the less likely that the government will allow the software to be exported).<sup>7</sup>

Even the best encryption may be vulnerable to breakthroughs in computer technology or mathematics. In August 1977, the inventors of RSA, the public key encryption system employed in many payment networks, offered a reward to anyone who could decipher a test phrase. At the time, they estimated that it would take 40 quadrillion years to break the code. They were a little off. Last fall, a team using 1,600 computers was able to decipher the phrase with a technique that allowed the problem to be broken up into many smaller tasks.<sup>8</sup> While RSA could employ much longer key lengths than the one used in its challenge (vastly increasing the difficulty of breaking the code), the lesson is clear: What is secure today may not be secure tomorrow.

Another set of issues involves the legal rights and protections of consumers, merchants, and issuers. It appears that Regulation E (covering credit, debit, and ATM cards) applies to credit and debit card purchases in cyberspace, but does it also apply to e-cash? As the regulation is written, the answer depends on the particular implementation. Its protections should hold whenever a transaction directly involves a financial institution, but probably would not apply otherwise.

This leads to the question of who should be permitted to issue e-cash. In most cases, e-cash is the liability of the issuer. Thus, while it circulates in cyberspace, to what uses can consumers' funds be put? Also, if the issuer is a depository financial institution, should deposit insurance and reserve requirements extend to e-cash holdings? All of these questions deserve careful consideration.

For the Federal Reserve, to the extent that cyberspace credit and debit card transactions displace similar physical transactions, there should be no effect on monetary policy. If checks and currency are used less often, this will simply continue a long trend away from these instruments' share of the payments system. E-cash could be more complicated, however, particularly if it bypasses depository institutions and allows direct transfers between individuals. In the foreseeable future, cyberspace payments of any type are likely to command a minor share of the payments stream, so the impact on monetary policy should be correspondingly small.

For the Treasury, any type of electronic payment that substitutes for currency is likely to be costly. If people hold less coin and currency, the Treasury will lose seigniorage from the coins it mints as well as the income associated with Federal Reserve Notes. This reduces a hidden tax on consumers who use cash, but unfortunately, it also removes one of the few ways of taxing the underground economy.<sup>9</sup> The Internal Revenue Service could more than make up for this loss if e-cash methods are designed to track each transaction (thereby ensuring greater tax code compliance), but anonymous approaches would inflict some severe headaches. One of the starkest questions posed by electronic payments (and the Internet in general) is how much privacy society is willing to forgo to make illegal activities more difficult.

Few of us would be pleased to find out that someone had been following us around 24 hours a day recording our every activity, but this is precisely the ability that some electronic payment instruments (or regular credit and debit card transactions, for that matter) may

give both authorized law enforcement officers and "crackers" — hackers with criminal intent. Purchasing information services electronically makes it potentially very easy to build up a digital profile of consumers. This profile could be employed in a variety of useful ways (by you or your authorized agent) or for insidious purposes (by anyone else).

Despite the best promises of payment providers to protect confidential transaction information, there are many ways it could be released. Although a great deal of attention is centered on hackers, employee fraud and error (either intentional or unintentional) will probably be a much bigger problem. If the information exists, there is always the potential that it will be obtained by someone lacking authorization.

### ■ Conclusion

Whatever difficulties these new forms of payment present, their advantages are clear: They will lower the cost of some existing goods and services and spur the development of many new products. The nuts and bolts issues can be resolved relatively easily. Striking a balance between individual privacy and the concerns of law enforcement will be much more difficult, however. Given the many challenges that the legal system faces in the digital age, privacy could become a scarce commodity if we do not choose wisely now.

## ■ Footnotes

1. See Gary Welz, "New Deals: A Ripening Internet Market, Secure Systems, and Digital Currency Are Reshaping Global Commerce," *Internet World*, June 1995, pp. 36-42.

2. Although this article concentrates on electronic payments over open networks like the Internet, much of the information applies equally well to "electronic purses," a form of electronic money being developed to handle small-dollar transactions in the physical world. For a more thorough treatment of this technology, see John Wenninger and David Laster, "The Electronic Purse," Federal Reserve Bank of New York, *Current Issues in Economics and Finance*, vol. 1, no. 1 (April 1995), pp. 1-5.

3. The World Wide Web (often referred to as "the Web") is a collection of linked files on the Internet that allows relatively easy navigation from one site to another using specialized software called a "browser" (Mosaic and Netscape are two of the most common). The information accessed is usually text and graphics, but can also be sound and motion pictures.

4. A home page is the start-up screen of a content provider's Web presence. Generally, it contains links to many other pages.


5. See David B. Humphrey and Allen N. Berger, "Market Failure and Resource Use: Economic Incentives to Use Different Payment Instruments," in David B. Humphrey, ed., *The U.S. Payment System: Efficiency, Risk, and the Role of the Federal Reserve*. Boston: Kluwer Academic Publishers, 1990, pp. 45-92.

6. To access a plethora of information, you can use your Web browser to search for terms like "electronic money" or "electronic payments."

7. One problem faced by every company seeking to provide secure transactions using encryption is that U.S. munitions laws, which date back to the Cold War, prohibit exporting encryption technology without explicit government approval. This makes it difficult to develop payment instruments that can be used worldwide.

8. See "Superhack: Forty Quadrillion Years Early, a 124-Digit Code Is Broken," *Scientific American*, vol. 271, no. 1 (July 1994), p. 17.

9. Of course, the Treasury or the Federal Reserve could issue its own form of digital cash and thus minimize any revenue loss.


  
Paul W. Bauer is an economic advisor in the Financial Services Research Group at the Federal Reserve Bank of Cleveland.

The views stated herein are those of the author and not necessarily those of the Federal Reserve Bank of Cleveland or of the Board of Governors of the Federal Reserve System.

  
Federal Reserve Bank of Cleveland  
Research Department  
P.O. Box 6387  
Cleveland, OH 44101

**Address Correction Requested:**  
Please send corrected mailing label to the above address.

Material may be reprinted provided that the source is credited. Please send copies of reprinted materials to the editor.

  
**BULK RATE**  
U.S. Postage Paid  
Cleveland, OH  
Permit No. 385  
