# An Introduction to Electronic Money Issues

prepared for the
United States Department of the Treasury Conference

## Toward Electronic Money and Banking: The Role of Government

September 19-20, 1996
Washington, DC

[Graphics are not included]

---

This paper was written by staff from the U.S. Department of the Treasury offices to provide an introduction and background for this conference. Nothing in this paper should be interpreted as a statement of the policy of the U.S. Department of the Treasury or any of its bureaus.

Primary contributors to the paper include: David G. Hayes, Office of the Comptroller of the Currency; James F. E. Gillespie, Office of the Comptroller of the Currency; Peter H. Daly, Office of the Assistant Secretary for Management/CFO; Gary Grippo, Financial Management Service; Pamela J. Johnson, Financial Crimes Enforcement Network.

# Contents

## Executive summary

Today, electronic money and electronic payments systems for retail transactions are on the top-ten list of issues for those with significant interests in financial services. Technological breakthroughs promise consumers and retail businesses a wide range of financial services and products in an electronic or digital format.

The decline in cost and increases in capacity of computers, as well as advances in communications technology, have altered not only the way information is communicated but also the cost of processing and storing information. These changes, in turn, have led to the emergence of two new forms of retail payment systems: electronic cash and banking from home by personal computer. Among the many challenges these emerging developments create, is determining the appropriate role for government in the new digital world of financial services.

Many argue that the private sector should resolve most policy issues and that government should only act when there is clear evidence of market failure. There are others who want the government to play an active role, going so far as being the exclusive issuer of electronic cash. Still others recommend some intermediate approach.

A review of the role of government in the traditional world of money and finance could be helpful in understanding the competing interests in this debate. In the traditional world of finance, industry has been the source of product innovation and solved many problems on its own. The public has looked to government to set and enforce basic rules that provide a foundation for, among other things, consumer rights and responsibilities (in such areas as protections against loss and invasions of privacy); law enforcement tools and techniques to combat financial crimes; the issuance of legal tender; and the management of the money supply and the payments system.

With respect to electronic cash and banking, the need for and application of many of those laws is less clear, and the resulting ambiguity creates issues for the private and public sectors. Determining where to begin and what clarifications to make is a complex undertaking. Understanding the pace of change may help put this issue into perspective. If it takes time before consumers make widespread use of these products, there will be a lot of room for markets to engage in experimentation and for providers to solve consumer and governmental concerns.

Although relatively common in several European countries, electronic cash in the United States is still in an early stage of development. Relatively few people use electronic cash, or do business on the Internet. Estimates of future growth are clouded by competing forces.

The potential benefits of electronic cash will likely stimulate its wider use. These benefits include lower costs, reductions in check and credit card fraud, reduced risk of theft and vandalism in retail outlets, and increased convenience for consumers. As old forms of money crimes decline, however, new ones are almost certain to arise. Electronic payments systems offer new opportunities for various violations of law and new challenges to government agencies that combat financial crimes.

There are also obstacles to the widespread use of electronic money. Industry experts will have to develop standards for interoperability among the hardware and software systems merchants must use when accepting various forms of electronic cash. Experience will have to support widespread trust in the safety of electronic cash and a mutual trust between Internet consumers and merchants. Consumers will seek assurance that electronic-based purchases are free from unauthorized prying eyes, financial crimes, and many of the legal ambiguities surrounding electronic cash.

Moreover, the onset of change raises questions for policy-makers in such key areas as consumer protection, law enforcement tools and techniques, government payments, and international cooperation. It seems clear that some questions such as financial stability, monetary policy, and seigniorage will not be ripe for government action until products are much more robust. Even then, it might be that only limited new measures are warranted.

Further, in many of the arenas where government may play a role it will take time to address questions because solutions are both complex and unclear. Efforts to combat financial crimes can pose tradeoffs between law enforcement needs for information, and the privacy interests of consumers and merchants. Plans for increasing the efficiency of government payments could have an impact on private-sector plans for achieving interoperability.

In sum, there will be many areas in which markets will develop well on their own, but in some areas government participation and involvement may be helpful. Clearly, there is much to learn, and government must combine aggressive fact-finding with patience. Premature and uncoordinated action among government agencies or decisions based upon incomplete analysis could thwart innovation and its ensuing benefits, including, perhaps, the ability of U.S. firms to compete effectively in global markets.

# I. Introduction

Electronic money and electronic payments systems for retail transactions are commanding widespread attention. These systems, wherein neither legal tender, nor paper checks, nor credit-card numbers change hands at the time of purchase, have already started to spread across the globe (see map). They offer significant and profitable opportunities for changing the way consumers pay for the widest possible range of goods and services. Hardly a month seems to pass without some announcement of another alliance of computer and financial services firms. Organizers' plans invariably envision a broad array of retail financial services and products available in an electronic or digital format.

The electronic transfer of funds is not a new phenomenon in the United States or, indeed, most of the developed world. Large scale and wholesale payment transactions in the United States and other nations have been conducted electronically for some time. What is new today is the expansion of electronic money technology in financial transactions conducted by consumers and smaller, nonfinancial organizations.

Electronic wholesale payments in the United States account for a much larger dollar volume of transactions than all retail transactions, but they take place among relatively few parties that have worked long, hard, and successfully at making these transactions secure. Retail transactions, the vast bulk of the number of transactions in the United States, take place among parties who are concerned about both the security and the privacy of those transactions. Developing systems that meet the variety of consumer and merchant needs during a period of evolving technology will be a challenge.

Electronic money and the technology that makes it possible raise important questions about the continuing effectiveness of existing government tools and methods used to carry out traditional responsibilities in such areas as consumer protection and law enforcement. Further, in the United States, the operability of much electronic money technology and many electronic money systems for retail payments is largely untested, except in pilot projects and limited experiments.

At the same time, electronic money raises the possibility of actually reducing crime and increasing access for low and moderate income households. It is also quite possible that for competitive reasons private sector purveyors of this new technology will effectively address consumer, criminal, and other issues raised by the development and use of electronic money.

This paper provides background material for the United States Department of the Treasury Conference Toward Electronic Money and Banking: The Role of Government. Section II offers a brief description of electronic money developments, including the incentives for and the obstacles to further growth. The material in Section II provides a context for understanding the issues before all conference panels. It especially addresses themes that the panel on Payment System Issues and the panel on Security and Authentication will explore.

Section III offers a discussion on the role of government in a world of retail electronic payments. Topics cover the themes of conference panels devoted to issues concerning consumers (including privacy concerns), law enforcement, issuers of electronic money, and international cooperation. The discussion of issuers offers additional thoughts on some payment system issues. Section III closes with some observations on the potential impact of electronic money developments on Treasury payment operations.

Section IV summarizes major themes.

Four appendixes accompany the paper to provide brief overviews of the law relating to central aspects of electronic money. The first appendix discusses the commercial rules–particularly transactional and disclosure rules–that may apply to electronic money products. Appendix 2 discusses the anti-money laundering rules that may apply to electronic money transactions. Appendix 3 discusses laws that control the types of firms (e.g., banks and nonbanks) that may issue or offer electronic money products. The last appendix discusses the supervisory and regulatory systems that address the financial risks presented by certain electronic money products.

## II. The dimensions of change

The basis of retail payments evolved gradually from physical coins to paper currency and checks and, more recently and rapidly, from there to debit and credit cards. In large-scale wholesale transactions, money has for decades been transactional information transmitted electronically over closed, wire transfer systems. Now, money in retail transactions is becoming electronic, transformed into information stored on a computer chip in a plastic card or on a personal computer so that it can be transmitted over open information systems, such as the Internet.

## Two underlying developments

Two forces in particular are responsible for pushing advanced economies around the globe into this next phase in the evolution of money. The first is the steep drop in the cost of computing power. The second is the continuing advance in the application of computer technologies to communications systems. Together, these forces are fundamentally changing the character of traditional money and related financial activities and are setting the stage for even greater changes in the years ahead.

- Decline in the cost of computing power

The declining price of personal computers over the past decade has been dramatic. Despite reportedly thinning profit margins, that trend continues, while falling prices and enhanced performance also increasingly characterize computer peripherals such as hard drives, modems, and CD ROM drives.

- Advances in communication technologies

The trend lines for consumer usage of electronic communication innovations are strongly upward. At the end of last year, 8.8 million Americans were connected to their offices by computer, an increase of almost 16 percent over 1994. In the last six years, host computers on the Internet increased by a staggering 4,700 percent. Some analysts have predicted that, by 1997, about six million Americans will be using some form of wireless communication–triple the number for 1995.[1] At the same time, the capacity of communication channels is growing sharply, reducing the time needed to transmit text and graphics.

Those improvements in communication technologies are changing fundamentally the economics of conducting information-related business.[2] As traditional barriers and costs to information-sharing fall, banks and others in the financial information business are better able to achieve economies of scale in storing and moving data. They can more comprehensively assimilate large quantities of financial data on their

---

[1] Richard Shaffer, High-level Computing , Forbes Magazine, October 9, 1995, p. 116.

[2] It is worth noting that, while these phenomena are largely attributable to the dynamism of the free market, government actions laid the groundwork for some of the technological infrastructure necessary to develop electronic money and commerce. For example, as of December 1995, 28 federal programs provide development funding for rural telecommunications projects, thereby ensuring rural access to worldwide telecommunications networks and to the Internet. The Internet itself grew out of two government computer networks, ARPANET (created by the Advanced Research Projects Agency in the Department of Defense) and NSFNET (created by the National Science Foundation). Although both were designed originally for communication, research, and development purposes, they became important building blocks in the creation of the Internet system.

operations at a lower cost and in less time. They and their customers can have more direct and immediate access to each other, at lower cost.

Most strikingly, perhaps, changes in communication and computer technologies also mean that banks and their customers no longer have to conduct their business face-to-face, and, consequently, no longer have to reside in the same country, state, county, or town. As the need for geographic proximity between financial institution and customer fades, so generally does the importance of geography-based procedures, practices, and rules that govern much of the financial services industry today.

## New retail payments systems

Advances in computers and communications technology have led to a change of some significance to policy-makers–the development and growth of new retail payments systems. The most noteworthy developments are electronic cash and engaging in financial transactions from home or elsewhere by personal computers.

- ### Electronic cash

  Electronic cash is a claim on a party, most commonly, the issuer, stored in the form of computer code on a card about the size of a credit card or on the hard drive of a computer. Consumers purchase the claim with traditional money. Consumers exchange the claims for goods and services with merchants who are willing to accept the claim as payment.

  Cards representing such claims often go by the name "stored value cards" (SVCs). The technology for storing claims with which to make payments, and other information, on cards ranges from the magnetic strip common to all credit cards to computer chips that store and process information. Cards containing computer chips are called "smart cards."

  One convenient way to understand SVCs is to classify them as representing either "closed" or "open" systems.[3] SVCs that are limited to just a few merchants regardless of location or to many merchants in a relatively small

[3] The ensuing descriptions and accompanying diagrams are only illustrative; there may be many other ways to establish and operate closed and open systems.

geographic area would represent a closed system. SVCs that consumers could use at many different businesses over a large geographic area would represent an open system. The distinction between closed and open, however, is largely one of degree.

Closed-system SVCs. One example of a closed-system SVC is the system in which the card issuer and the seller of the goods and services are one and the same (the "merchant-issuer" model). Examples of such cards include: the farecard used by riders of the subway system in Washington, D.C.; cards issued by a number of colleges and universities in the U.S. to students and perhaps employees that holders may use to purchase a variety of goods and services supplied by the college or university; cards issued by public bodies;[4] and cards issued by certain telephone companies to pay for telephone calls.

In these systems, the user buys a claim on the merchant-issuer with traditional money and receives electronic cash in return. When the user buys goods or services from the merchant-issuer, special point of sale (POS) devices record the transactions with the merchant, reducing the value of the electronic cash recorded on the card by the amount of the purchase. Although consumers make purchases in this system with electronic cash, the system is linked to the current payment system by the merchant-issuer's relationship with its bank. (See Diagram 1.)

Campus cards, and other such limited distribution cards, are examples of closed-system cards where the issuer and merchant are different parties. One such example is the 1995 Jacksonville Jaguar stadium card. In this case, one bank issued cards that fans could use at the stadium to buy food, drink, and souvenirs at football games. The transactions with these stored value cards work much the same as with the merchant-issuer. The special POS devices record the transaction for the merchant, altering the purchaser's stored value card to reflect the decreased value. The merchant later presents the electronic cash to the bank-issuer by downloading the payment information from the POS, receiving traditional funds in exchange, typically in the form of a deposit balance at the bank. The merchant's bank would then send the electronic cash through the traditional payment system in much the same manner as presenting a check. As with the merchant-issuer systems described above, bank-issued electronic cash in this somewhat more complex "closed" system would

[4] For an extensive discussion of stored value cards used in the public sector, see Financial Management Services, Government Application of Computer Card Technology , U.S. Department of the Treasury, May 1996.

commonly be closely linked to the traditional payments system. (See Diagram 2.)

Open-system SVCs. Examples of open-system SVCs exist today in several countries in Europe and the Far East, and to a more limited extent, in the U.S. They work essentially in the same manner as bank-issued SVCs in closed-systems, with the important exception that a greater variety of businesses over a relatively larger geographic area accept them. (See Diagram 2.)

Technology, however, can support electronic cash regimes that could operate independently of banks and thus outside traditional payments systems. In these systems, users would buy electronic cash from issuers using traditional money. Users would "spend" the electronic cash at a merchant, just as in the case of bank-issued electronic cash. Merchants would then send the electronic cash to the issuer who would redeem it with some form of traditional money such as a check on a bank balance. In this system, the electronic cash would not "clear" through the traditional payments system, but could circulate outside it. (See Diagram 3.)

In expansive versions of either bank-issued or nonbank-issued electronic cash, such cash could circulate among users before presentment to merchants, in much the same manner as traditional cash. Users would have their own special computer equipment enabling them to transfer electronic cash from one user's card to another. Such a transfer often goes by the name "peer-to-peer" and can be accomplished with some electronic cash systems today. Peer-to-peer transfers of electronic cash would not clear through the traditional payments system, in contrast to peer-to-peer transfers involving paper checks. (See Diagram 4.) With such regimes, the only point of contact between the traditional payments system and electronic cash would be the initial purchase of electronic cash from the issuer with the use of traditional money and redemption of electronic cash by merchants.

- PC financial transactions

The continued development of the personal computer (PC) has given many households the opportunity to conduct financial transactions from their homes, or indeed from any location where they can connect their portable computers to telephone networks. Through the use of special software and a modem, they can connect to the system used by their financial institution to examine accounts, issue orders to transfer funds among their own accounts, issue orders to transfer

funds to the accounts of other parties (e.g., to pay bills or send funds to others), and apply for loans.

In some cases, households dial a number that connects them directly with their financial institution. In other cases, households connect to their banks by using the Internet.[5] After gaining access to the World Wide Web portion of the Internet through their Internet service provider, households go to the Web page sponsored by their bank and conduct their business.[6]

Currently, most retail electronic banking involves transmission of information over relatively protected telephone networks or limited access networks of computers called intranets. To date, such systems have not given rise to significant security breaches. Even so, the widespread availability of powerful home computers poses the risk of financial crime, creating incentives for maintaining tight controls and security systems. Strong security systems will be especially important for successful banking and commerce over the more open Internet, where packets of information can pass through a number of computers, each one accessible to a large number of people, before reaching their final destination.

PC-based electronic cash. Technology permits the transmission of electronic cash over networks that link personal computers and the storage of electronic cash on the hard drives of personal computers.[7] PC-based electronic cash is thus one means of paying for goods purchased over the Internet.[8]

The possible points of contact between PC-based electronic cash and the traditional payment system are functionally identical to those between SVCs and the payment system. So long as merchants regularly redeem such cash for traditional forms of money and there is little, if any, peer-to-peer transfers, PC-based electronic cash will be a simple adjunct to, not separate from the existing payments system.

---

[5] Consumers are also using PC-based systems to make purchases over the Internet. As discussed later in this paper, many observers have raised questions about the security of Internet transactions and have cited security-related issues as one of the causes of the small level of Internet commerce.

[6] Other forms of remote access to banking services include telephone banking and automated teller machines (ATMs).

[7] In the U.S., Mark Twain Bank offers its customers an electronic cash program developed by DigiCash, a Netherlands-based corporation.

[8] Other means of paying for Internet purchases include credit cards.

Regimes with peer-to peer transfers and little, if any, redemption of electronic cash for traditional money would offer the possibility of separate payments systems. As in the case of stored value cards, the popularity of such systems remains somewhat unclear for the immediate future.

## Developments: slower than some believe

Understanding the speed with which electronic money develops, and the actual systems that will be marketed and by whom, is key to the formulation of government policy. Notwithstanding a considerable amount of excitement over the development of electronic money in the press, the pace of moving from the analog world of retail payments to the digital world of electronic money is likely to be slower that many may think. Today, electronic banking is just beginning to become popular, electronic commerce and payments over the Internet are in their infancy, and principal use of SVCs in this country is in a relatively few closed systems. Nevertheless, financial and nonfinancial firms are spending billions of dollars to ensure the success of this market, and there is a clear public interest in these new products.

As electronic money and banking products mature it may well turn out that many of the policy issues raised by these new technologies–money laundering, counterfeiting, fraud, consumer disclosure, access for low and moderate income households–will be resolved by the private sector. Beyond this, some policy issues–the loss of seignorage and the impact on monetary policy–only become important when there is widespread use of electronic cash. Innovators will have ample incentive to introduce new products that will help solve many of the potential problems associated with electronic money.[9] Inappropriate government intervention could delay, deny, or limit the quality of such improvements. Government will have to take care not to act in a manner that stifles innovation.

At the same time, it is incumbent upon government to follow these developments carefully, in particular monitoring the pace of change, so that where there are emerging issues that can only be dealt with by government, they are in fact addressed. E-money participants may find that some regulation is necessary to assure consumer confidence and an acceptable environment for commerce develop.

- Smart-card usage in the United States

---

[9] When left to its own devices, the private sector has provided, without government help, new financial products that responded effectively and efficiently to consumer needs. These include travelers' checks, NOW accounts, telephone banking, and wholesale electronic banking.

Compared with several other countries, the United States has been slower to take up multi-user smart-card activity, although some usage has developed. The stadium card noted earlier is one example and the experiment conducted by VISA International during the 1996 Olympic Games in Atlanta, Georgia is another.

The slow adoption of these systems in the United States may be explained by the abundance and convenience of other payment options. Many U.S. consumers have access to cash, credit cards, checks, and debit cards, and for any purchase can select the payment option that best meets their needs. Another contributing factor may be the sheer size of the United States as compared to countries such as Belgium, Denmark, Finland, and Portugal where smart-card usage is more advanced.

How long, then, will it take for U.S. consumers to ultimately decide to embrace electronic money to any significant degree? Widespread electronic money use in the United States, particularly over open systems such as the Internet, seems to be at least two years away. The forces for change, however, are strong. There is considerable commercial interest in developing these new means of payment in the United States for both closed and open systems. As noted earlier there are growing applications of electronic cash technology to such arenas as transportation systems, college and university campuses, and even sports complexes. Several firms such as VISA International, MasterCard, Mondex, and Proton in various alliances with banks are investing large sums of money into projects that will develop into open systems.

Such ventures may need more than a few years to prove their merit. If consumer acceptance of electronic money parallels the history of automated teller machines (ATMs), direct deposit, the credit card, and banking by personal computer, growth in electronic money usage will be slow and limited for the first five years, but increasing dramatically thereafter.

- Internet commerce

Although the subject of much discussion, the actual level of Internet commerce remains modest by any standards. Scattered, unofficial estimates, the only ones available, suggest a level in the range of $100 million to $200 million in annual transactions.

The growth of Internet commerce may increase the volume of Internet financial transactions, but will not necessarily guarantee the growth of

electronic money. Some observers believe that efforts to reduce the cost of credit card transactions will be successful and that credit cards, one of the most ubiquitous substitutes for money payments in the United States, will become the dominant Internet payment vehicle. They cite the existence of a huge, familiar, and successful infrastructure currently supporting credit card purchases and clearings.[10]

## Forces for growth

Despite the current level of electronic money activity in the United States, the forces stimulating faster growth in electronic money and commerce here are strong, and the pace of change could quicken. These forces include:

- Expanding electronic-based government payments

  The need for greater efficiency in government operations is perhaps stronger today than ever before. The question here is, "How should the government use electronic money in its drive for greater efficiency?" Government has already begun to formulate its answer. The Debt Collection Act of 1996 and the electronic benefit transfer (EBT) initiative are but two examples of recent efforts to achieve greater efficiency. The implications of these and related measures on Treasury operations are substantial.

  Debt Collection Act. The Debt Collection Act of 1996 mandates government use of electronic funds transfers (EFT) for all government payments, except tax refunds, by 1999. This includes the payment of government benefits. The act has two effective dates. After July 26, 1996, every new recipient of government payments must accept them electronically, unless the recipient certifies that he or she does not have an account at a financial institution. After January 1, 1999, all payments made to individuals and businesses–including those to persons without accounts at a financial institution–must be made electronically.

  The Financial Management Service (FMS), a U.S. Department of the Treasury bureau, has adopted an interim rule as part of its plan for implementing the new law.[11] The interim rule implements the requirements of the new law that became effective July 26, 1996, and establishes the responsibilities of federal agencies and federal payment recipients.

---

[10] Cybercash and First Virtual Holdings are two firms that offer security in the use of credit cards for Internet purchases.

[11] 61 Fed. Reg. 39254, (July 26, 1996).

Agency responsibilities. The interim rule requires all federal agencies to make payments electronically to individuals who, on or after July 26, 1996:

(1) apply for federal benefit payments;
(2) begin employment with a federal agency;
(3) apply for retirement benefits;
(4) enter into a contract or purchase order with the federal government; or
(5) file or renew a grant application.

Recipient responsibilities. The interim rule requires each recipient of a federal payment to designate a financial institution or authorized payment agent through which a federal payment may be made. If the individual does not have an account with a financial institution or an authorized payment agent, the individual must certify that in writing to the agency.

Implementation of the new requirements by those paying and receiving benefits could help provide those without bank accounts better access to mainstream financial services.

EBT programs. Even before passage of the Debt Collection Improvement Act, the federal government had taken some initial steps toward realizing the efficiencies promised by electronic money. One such step was the formation of a federal task force that would coordinate the development of EBT programs.[12] Such programs substitute for benefit delivery systems (checks, food stamp coupons, and payment vouchers) used by both federal and state agencies.[13] In one type of EBT program, the value of food stamps to an individual, and codes indicating the acceptable purchases that the individual could make with the electronic funds, would be encoded in the computer chip embedded in a stored value card. Benefit recipients use these cards in lieu coupons or vouchers to pay for goods and services at merchants and others equipped to receive this form of electronic payment.

Impact on Treasury operations. Conversion of Treasury payments, now running at about 800 million a year, to an all electronic format will bring changes permitting, for example, a consolidation of disbursing operations that currently produce checks. With regard to retail payments, the complete displacement of traditional cash is unlikely. About 18 billion in currency

---

[12] See Federal Electronics Benefits Transfer Task Force, Creating a Benefit Delivery System That Works Better & Costs Less: An Implementation Plan for Nationwide EBT , Washington DC, 1994.

[13] At last count 42 states had formed six alliances for purposes of developing and implementing their own EBT programs.

notes valued at approximately $400 billion circulate world wide, despite the growth in checks and wire transfers. Demand is especially strong outside the United States where about $270 billion circulates. There, among the less technologically advanced countries, cash is the principal means of payment, the dollar seems to be one of the currencies of choice, and the infrastructure that will support widespread use of electronic money seems many years away.

Impact on electronic money. The U.S. government is the largest receiver and disburser of payments in the world, and as it makes ever increasing use of electronic payments it is likely to have an influence on operating standards for electronic payments systems. That is because it must ensure any system it uses meets its requirements for security, reliability, and accuracy. To the extent it adopts stored value technology, it will greatly affect interoperability standards. Thus, the pace at which the public sector seeks to implement electronic payments could have a significant effect on private-sector planning and related activity.

- Greater efficiencies for businesses

Lower costs. Electronic money eliminates the costs of handling coin and currency. The estimated cash handling cost for U.S. retailers and banks is over $60 billion annually, which includes costs associated with the processing and accounting of money, as well as storage, transport, and security. Electronic money brings greater efficiency to those tasks, offering substantial cost savings.

According to the National Automated Clearing House Association (NACHA), the cost savings to the banking industry alone flowing from the new requirement for federal EFT payments could be sizeable. For example, NACHA reports: "Studies have shown that a financial institution saves between $.75 and $1.25 for each payment converted from a deposit made with a teller to Direct Deposit," and consequently, "annual costs savings to the banking industry as a result of these new electronic payments should run between $350 million and $500 million."[14]

Electronic money potentially provides merchants with cost savings resulting from: reduced collection and deposit float associated with coin, currency, and checks, and faster funds availability; increased sales due to faster throughput at checkout counters and consumer tendencies to spend more with stored value cards; and increased self-serve transactions. Acceptance of electronic

[14] Http://www.nacha.org/newlaw.htm.

money would allow merchants to move more commerce from the physical world to the Internet, which offers access to global markets at low cost. The continuing rapid decline in the cost of technology will increase the extent of these cost savings, enhance innovation, and further increase the attraction of electronic money and finance.

Reductions in some forms of fraud. While magnetic strip debit and credit cards can be overwritten or copied, smart cards are fitted with tamper-resistant chips and strong cryptographic protocols. Additionally, smart cards could be tied to biometric identification mechanisms, such as voice, hand, or retinal prints, to verify the identity of the user. To the extent electronic money displaces checks, moreover, check fraud may be reduced. The new systems will be, however, targets of criminal activity.

Greater safety and security. Another benefit electronic money offers merchants is increasing safety and security by eliminating some opportunities for theft. Electronic money could help curtail vandalism of vending machines, public phones, and the like, because there would be no coin or currency to steal. Similarly, owners and employees of retail establishments and other service providers who handle cash, such as taxicab drivers, could be much less vulnerable to robbery.

More value-added services. Electronic money technology–particularly smart card applications–could help sharpen merchants' offers of value-added services, strengthening customer relationships. For example, retailers could track customer activities (to an even greater extent than they currently do with credit cards) to discern buying patterns and offer buyer-specific discounts and loyalty programs. These targeted promotions, also known as "micro-marketing," are generally viewed as more efficient than the mass-marketing techniques currently used.

Some hard-pressed communities may benefit. If merchants did not need to collect and store cash, they might be willing to locate in areas that they now see as unacceptably risky.

- New choices for consumers

One of the biggest advantages of electronic money is that it is more convenient than other payment mechanisms for small-value purchases. It is faster and easier than exchanging cash and making change, writing a check, or getting a credit card authorization. For all micro-payments, including those on the Internet, sending a 10 cent digital coin for a small purchase of

information could prove to be more convenient and less costly than using a credit card.

## Obstacles to growth

Despite those benefits, uncertainties on the part of consumers and merchants about the underlying technology could slow widespread use and acceptance of electronic money systems. Some of these uncertainties focus on how well the technology secures personal transactions information over the Internet from theft and related forms of abuse such as false or non-authentic commitments. Other uncertainties arise from concerns about whether or not competing forms of electronic-money for use outside the Internet will require idiosyncratic computer hardware and software. Still others arise from the fact that innovation is often fast-paced, creating doubts about how long any particular technology will be at hand.

- ### Internet security and authentication

  Security. Many analysts believe that the use of electronic payments on the Internet will depend on the development of widely available systems that guarantee the security of credit card numbers and the various forms of electronic money. There are numerous mathematical formulas to code or encrypt such numbers, as well as electronic cash, in a way that seriously complicates the task of stealing them or interfering with the intended use. Experts tend to evaluate methods of encryption in terms of the difficulty knowledgeable parties would face in decoding or decrypting the information. There can be differences of opinion among experts on the strength of any particular form of encryption and such differences could contribute to consumer, and merchant, unease.

  The availability and strength of encryption seems to be on the minds of some consumers. In informal surveys, consumers cite lack of security as the primary reason they are reluctant to purchase goods and services online. At the same time, consumers routinely send credit cards and credit card numbers through the postal system and over the phone to catalog merchants and offer them to anonymous clerks at retail counters. Such different results suggest that security per se may not be crucial to the success of electronic money on the Internet.

  Encryption is not the only form of security of concern to consumers. Traditional cash and credit card transactions suggest that some consumers seem to value written verification of the basic facts of a retail transaction–the name of the seller, a description of the goods or services purchased, and the

cost. The seller ordinarily offers the buyer a piece of paper containing those details. Consumers may want their use of electronic money, especially electronic cash, to create similar information. How issuers meet that need may determine the pace of electronic money growth.

Authentication. If consumers are to use electronic money over the Internet they must have confidence in the issuers of the electronic money and the merchants who accept it. Consumers may demand that a trusted third party certify or authenticate the legitimacy of both those parties. Confidence is particularly important for the development of Internet commerce with its virtual shopkeepers that consumers cannot see and evaluate in the traditional way.

Confidence is a two-way street. Merchants will want assurances that the consumers from whom they receive orders for goods and services are the consumers who really want them and that verified consumers will not refuse to meet their responsibilities as defined by law.

A trustworthy and reliable system of authentication can provide comfort to merchants on both fronts. Merchants could require customers to sign orders with encrypted digital signatures that can be authenticated by trusted and reliable third parties. Such authentication would unambiguously identify the consumer and provide proof that the consumer requested the goods or service.

Trustworthy authentication can also boost electronic communication among businesses, ranging from merchandise orders to contracts that bind all manner of business contracts. Authenticated digital signatures could, for example, substitute for the notary public of the analog world.

There is a growing concern among policy makers and consumer groups in Europe and the United States that individual privacy is greatly compromised by electronic commerce and electronic payments. Such concerns are of course not limited to recent developments regarding electronic money or payments, inasmuch as they apply to current use of credit cards. However, electronic money and payments are likely to materially increase the intensity of debate over these issues for several reasons. SVCs raise the possibility of tracking and recording virtually every payment an individual makes. Such extensive tracking and recording raise issues of extensive target-marketing, government surveillance, and even personal safety as patterns of behavior are mined from this potentially rich data. In addition, the Internet raises serious concerns about the data being examined by unauthorized persons.

Balanced against this is the potential for data created and stored in an electronic money environment to aid law enforcement authorities in preventing crimes and tracking criminals (and, indeed, some of the data may be essential for effective law enforcement efforts). As well, legitimate use of such data could help firms to be more efficient in their marketing efforts.

- Other technological issues

  Interoperability. Most observers agree that electronic money will not find widespread use until technical experts solve the problem of interoperability. In the context of electronic money, the term interoperability captures the extent to which debit cards and stored value cards from different issuers use a common set of standards. These standards govern such issues as the size of the cards (length, thickness, and width) the location and size of the magnetic strip or computer chip, and the coding technology manufacturers use to store information on the magnetic strip or computer chip. They also cover other matters such as the design and workings of devices that "read" the cards. The greater the acceptance of common standards, the greater the degree of interoperability.

  Large-scale interoperability would help promote acceptance of electronic money. Merchants generally would be more inclined to invest in card readers if one reader could service a variety of debit and stored value cards. Similarly, with large-scale interoperability consumers could be reasonably confident that many merchants would accept many forms of electronic money. In sum, the greater the number of merchants accepting electronic money the greater the inclination among consumers to use it; the greater the number of consumers using electronic money, the greater the number of merchants willing to accept. Interoperability made possible the success of credit cards and ATMs.

  Technological change. Another potential problem is technical change itself. The march of technological innovation seems unending, offering opportunities for improving communications and computer capabilities. Such "progress" can be disconcerting for consumers and merchants. It clouds, rather than clarifies, the future, creating incentives to wait for the next round of improvements, if not for the emergence of a technology that seems to be on its way toward winning widespread acceptance.[15]

---

[15] This is by no means a complete list of consumer, or merchant, concerns. Section IV contains a discussion of selected consumer concerns that raise issues about a government role .

## III. The role of government

There is considerable debate about what role government should play in the transition to a digital world. Some argue that the government should play little, if any role and allow the private sector to resolve most of the issues. Others advise the government to go so far as to set all the standards for issuing and using electronic cash, if not be the exclusive issuer of electronic cash. Still others recommend approaches that fall between those two extremes.

A look at the role of government in the analog world is helpful in considering the role of government in the digital world. In the analog world of finance, the private sector, through innovation and adjustments in practices, has solved many concerns government might have raised. At the same time, both industry and the public have looked to government to set and enforce rules that provide a foundation for, among other things, consumer rights and responsibilities, law enforcement protections against financial crimes, and the conduct of money issuers. Given the increasing globalization of finance, international agreements also come into play.

At the same time, there are important differences between the development of electronic money, banking, and commerce today, and the development of other financial services products in the past that make it a bit less clear what the appropriate response of government should be. As noted earlier, there is reason to believe that the private sector will work hard to resolve a number of potential policy issues that may emerge as the development of E-money proceeds, and use of E-money becomes more widespread. Moreover, developments are likely to unfold at a pace that allows careful study of potential issues.

Accordingly, government must be careful not to overreact to, or stifle, new innovations that can greatly benefit the consumer and the American economy. Government should take advantage of marketplace solutions to issues where appropriate. To do this, and at the same time to be in a position to act appropriately, it is important for government to maintain expertise in electronic money and payments developments, and to consider carefully major questions presented by these developments. Those questions include the following: Will consumers enjoy adequate protections? Will laws and regulations be sufficient to combat electronic-money crimes effectively? What questions about electronic money should the United States raise in international forums?

Finding the best answers to those questions will be challenging. Underlying questions about the applicability of the existing legal and regulatory framework will need answers. As discussed in this report and its appendixes, many federal laws have not anticipated electronic money, particularly electronic cash, and the

application of some laws to electronic money systems is uncertain and unclear. In some areas, such as the issuance of electronic money, additional federal interpretations, rules or, perhaps, laws may be needed to provide an appropriate legal foundation for electronic money systems. In others, we may find existing requirements are no longer relevant and need to be eliminated.

## Consumer Issues

One important area of ambiguity in the law involves the rules (including mandatory disclosures) governing many of the financial transactions that are commonplace between consumers and financial firms. Transactional rules for electronic debit systems are relatively well-established, but those for electronic cash are not.[16] The government must decide whether it is best that electronic cash transactional rules evolve by contract, whether it should apply rules and precedents developed for related areas to electronic cash (e.g., those applicable to travelers checks and money orders), or if that is not appropriate, whether to develop new rules.[17] A key consideration should be the ability of consumers and merchants to protect adequately their interests by negotiation.

The issue of protecting consumer interests has four parts: To what extent should consumers be liable for electronic cash that is lost, stolen or compromised by the insolvency of the issuer? How much information should an issuer of electronic money disclose to consumers? Will the privacy of electronic-money users be adequately protected? Should the government take steps to ensure that all consumers, including the poor, gain access to electronic money and banking services?

Clearly, one issue common to those four questions is whether a given electronic money system is an electronic debit system that transfers value among deposit accounts or an electronic cash system. Since only chartered depositories can accept deposits, and since those firms are highly regulated, the existing statutory regime presents a ready framework within which to address issues raised by electronic debit systems. Electronic cash systems, however, may present significant challenges to policymakers. While most issuers of electronic cash, in all likelihood, will continue to be subject to some form of regulation, the application of existing laws to E-cash instruments is less clear.[18]

---

[16] See Appendix 1.

[17] The Federal Reserve Board has proposed amendments to Regulation E that address stored value cards. See, 86 Federal Register (Fed. Reg.) 19696 May 2, 1996.

[18] Several states regulate money transmitters; see Appendix 4.

For some, the answer to these problems might be to restrict the issuance of electronic money to banks.[19] Such a policy at the very beginnings of electronic money development could place unnecessary barriers in the way of competition and innovation, possibly delaying or denying public benefits.

- Liability for losses

  Most electronic cash holdings will not be insulated against certain kinds of losses, such as misplacement by the holder, theft, and insolvency of the issuer. Misplacement and theft are risks holders of traditional cash incur, but not loss due to the insolvency of the issuer.

  Some electronic cash issued by banks may have the protection of FDIC insurance, and some issuers may elect to provide holders with protections against loss and theft. Barring substantive changes in law, some electronic cash issued by nonbanks will not be insured by the government against a loss due to issuer insolvency, although state statutes governing money transmitters may reduce the risk of issuer insolvency.

  Electronic cash issued by banks, however, won't necessarily offer holders insurance against issuer insolvency,[20] and the absence of such insurance would mark a sharp distinction between insured deposits and bank-issued electronic cash. Consumers may, therefore, be confused by the existence of visually indistinguishable electronic cash systems, and policymakers must decide whether this concern warrants legislative or regulatory action.

- Disclosure

  Existing federal rules governing transactions and disclosure may not extend to some electronic money activities. While the Electronic Fund Transfer Act and Regulation E, which is issued by the Federal Reserve, will apply to consumer electronic debit transactions, no comprehensive body of transactional rules

---

[19] The European Monetary Institute proposed this approach for European Union members.

[20] See, FDIC General Counsel's Opinion No. 8, 61 Fed. Reg. 40490 (August 2,1996).

defines the rights and obligations arising from electronic cash transactions.[21] Similarly, detailed consumer disclosures for EFT transactions apply to debit systems, but not necessarily to electronic cash systems. There is likely to be some pressure from consumer groups and some market participants to extend current law to electronic cash systems, as those systems become more commonplace. The Federal Reserve is working to resolve some aspects of this issue through revisions to Regulation E.

- Privacy

  As noted previously, electronic commerce and finance creates new opportunities for unauthorized access to and manipulation of private information. Although the European Parliament has moved to address some of those issues, few federal laws address them.[22] The extension of electronic debit and electronic cash systems to the Internet presents additional risks. Data traveling through the open network of the Internet is more susceptible to interception and can be copied or modified. The extent of the risk to privacy will depend on the design of the systems and the types of information traveling over the Internet.

  Protecting individual privacy in the digital world will be at least as complex as it is in the analog world. Finding the right balance between governmental needs for information to combat crime and individual needs for anonymity will be challenging. That is not the only hurdle. Consumer data derived from financial transactions covers a broad spectrum of information, and consumers may be more concerned about the confidentiality of some types of information than others. For example, consumers may object strongly to the public release of data describing their income and net worth, but allow some information describing their spending patterns to be used by direct marketers.

- Access

  Judging the impact of electronic money on groups of consumers, especially the poor, is difficult. On the one hand, the application of advanced technology to finance and commerce could exacerbate current inequities in the access to financial services. The poor are much less able than others to afford computers or to have access to educational opportunities facilitating computer use. As the cost of computers and associated technologies

---

[21] See Appendix 1.

[22] The significant European interest in this issue is indicated by Directive 95/46/EC of the European Parliament, described later in this paper.

continues to fall, the availability of financial services from traditional outlets such as branches, and perhaps even ATMs, will decline. That trend could also disadvantage those in rural areas where the infrastructure necessary for electronic money and banking is not now in place.

On the other hand, not all PC developments need to disadvantage the poor. PC-based systems for banking services offer the potential for a community group or church to work as partners with a bank or other financial-services firm for the delivery of financial services at convenient and safe locations.

Additionally, the technological revolution holds the potential to enhance greatly the ability of the poor to have convenient access to financial services because of the advantages that are inherent to high-tech payments systems. The cost of low-value transactions–transactions most common to the poor–can be much lower in high-tech systems than in traditional payments systems centered, for example, on brick-and-mortar branches. High-tech systems have more flexibility than traditional systems in the delivery of financial services virtually. Evidence of this flexibility is available today in the form of electronic benefit transfer (EBT) systems, banking over the telephone, and to some degree in high-tech branches in supermarkets and convenience stores. Such flexibility provides added convenience, in that services can be available on virtually a 24-hour basis, and added safety, in that funds are less subject to theft. In the not-to-distant future, additional evidence may include the use of home television sets hooked up to cable systems that give access to banking and other services.

## Law enforcement

As noted earlier, electronic cash could, depending on how it is developed, share an important attribute with traditional cash. Like cash, it could lead to anonymous transactions that do not leave a "paper trail." While those attributes give ordinary citizens privacy, they also make possible the commission of large-scale financial crimes with relatively low risk of apprehension. Should the use of electronic cash become pervasive, government may question the effectiveness of its regulatory provisions and investigative strategies and techniques in combating financial crimes.

Evaluations of those issues will necessarily depend on the particulars of electronic money and electronic cash product. For example, many smart-card systems abroad generate audit trails and limit the maximum "value" that a card may hold at any time. Reports from countries with such cards suggest that criminal interest in the cards is low.

For the most part, the crimes in a world of electronic cash and digital commerce will be familiar: theft, fraud, counterfeiting, tax evasion, and money laundering. To ensure that law enforcement agencies have the necessary tools to combat financial crimes, government will have to determine the impact of electronic money systems on regulations and policies designed to control financial crime, and investigative strategies and techniques.

Traditionally, law-enforcement agencies have relied on rules and regulations allowing them to see documents, hear information exchanges, and track or interdict goods in clearly defined jurisdictions in their fight against financial crimes. Such tangible evidence and the certainty of geography will erode in the digital world of electronic money. Moreover, the applicability of existing laws to electronic money and related activities is not certain.

- The Bank Secrecy Act

  Certain laws, such as the Bank Secrecy Act (BSA) and its implementing regulations, require consumers and businesses to provide information that enables the government to combat certain financial crimes. How such laws apply to new electronic payment systems is not clear.[23] Historically, law enforcement and regulatory officials have relied upon banks and other types of financial institutions to provide data "chokepoints" through which funds from criminal activities must pass.

  The BSA, by requiring these institutions to keep records and file reports on certain types of financial transactions, provides a paper trail that enables law-enforcement officials to deter, detect, investigate, and prosecute illicit activity. Electronic money systems that allow large, unaccountable transactions have the potential, however, to undermine the effectiveness of the BSA. If such electronic money systems are not covered by BSA requirements, there is reasonable certainty that criminals will use them to evade the BSA "chokepoints." Electronic cash could lend itself to totally anonymous transactions without a paper trail, increasing the investigative hurdles faced by law-enforcement officials. The application of the BSA requirements to electronic money systems will depend upon whether the participants and products involved in those systems fall within certain definitions of the BSA.[24]

---

[23] See Appendix 2.

[24] See Appendix 2.

- Regulatory policy

  Law enforcement and regulatory officials have mechanisms in place for tracking the flow of money derived from illegal activities based on laws and regulations applied to the financial system.[25] With an open system such as the Internet or with electronic "peer-to-peer" transactions, however, exchanges of financial value may occur that are not technically subject to the BSA. As electronic systems develop and government gains a greater understanding of the transactions conducted over these systems, government must identify what additional regulatory measures, if any, law-enforcement officials need to combat financial crimes.

- Investigative techniques

  With the advent of home banking and the development of new retail electronic payments systems, there will be fewer and fewer face-to-face financial transactions. Law enforcement agencies are particularly concerned about the ability of financial institutions to "know their customers" in a potentially anonymous payment system. Further, government is concerned that paperless payment systems with anonymous users will present fewer opportunities to use traditional techniques such as analyses of financial documents, and surveillance of those suspected of financial crimes.

- Decryption

  As noted earlier, decryption is the reverse process of encryption. It refers to the decoding of messages that the sender altered–encrypted–in an attempt to keep the message secret from all parties except the one who was to receive it. There are many different encryption techniques, but they all revolve around a process of substituting a number, letter, or some other symbol for the true letter or number or symbol. Each process has its own rule for substituting a false symbol for the true one. Sometimes observers call this rule a "key," since knowledge of the rule or key will enable an interested party to "unlock" or decode the encrypted message.

  Encryption provides the potential for security in the digital world, and in the minds of those with large financial stakes in the development of electronic commerce and money "security is to the Internet what safety is to the

---

[25] See Appendix 2.

airlines."[26] Within the last several years, the private sector has made significant strides in strengthening the commercially applicable encryption processes. These advances respond to consumer and business concerns about the authenticity, reliability, and security of buyers and sellers and of purchases and payments, whether transactions are conducted over the Internet or in the shop of a retail merchant. For the private sector, the stronger the encryption, the smaller the cause for concern.

Because of its law-enforcement responsibilities, government has as strong interest in its ability to decrypt encrypted messages and in the advances in encryption technologies. For the government, powerful, private-sector encryption technology can pose challenging issues. Undecipherable encryption could facilitate criminal activities and, potentially, expose the United States to national security risks. To manage those risks, the Administration has proposed development of a Key Management Infrastructure (KMI) that would, with court permission, give selected federal officials access to the "keys" that would unlock messages encrypted using private-sector technology. The debate on the advantages and disadvantages of this proposal is continuing.

## Issuers of electronic money

The question of who may issue electronic money cuts across a wide spectrum of interest. Answers to the question have the potential to affect such activities as the regulation and supervision of issuers; and the management of both the payments system and monetary policy.

For that reason they deserve discussion. By any measure, electronic money plays a minor role in the U.S. economy and, as noted elsewhere, that role is not likely to increase any time soon. According to some estimates, "80 percent of all retail purchases in the United States are settled in cash, the vast majority of them for less than $20."[27] Debit cards, the biggest form of electronic money, accounts for about two percent of retail transactions, and credit cards, the most popular electronic payment option, accounts for only 5 percent.[28]

---

[26] Some observers have attributed this quote to James Barksdale, CEO of Netscape.

[27] A Payments Revolution in the Making , 1995 Annual Report, Federal Reserve Bank of St. Louis, p.10.

[28] Financial Crimes Enforcement Network, Exploring the World of Cyberpayments, An Introductory Survey, U.S. Department of the Treasury, September 1995, p. 5.

- The law

  If the government should find that the issuance of electronic cash involves the receipt of "deposits," federal laws precluding or restricting deposit-taking by nonbanks might be applied to nonbanks issuing electronic cash (e.g., 12 U.S.C. 1831t and Section 21 of the Glass Steagall Act). The states could also limit the types of firms that can offer electronic money services.[29]

- Regulating issuers

  In Europe, government officials favor banks as issuers of electronic money, reflecting, in part, the availability of a well-structured regulatory regime. In this country, there is a belief among a number of policy makers and knowledgeable private-sector parties that limiting the issuance of electronic cash to banks could stifle competition an innovation. Many also believe that appropriate regulation of the nonbank issuers can effectively resolve the problems they may pose.

  Designing the appropriate response will be a challenge. Some of the nondepositories may be affiliated with depositories and others may not be affiliated. Subjecting all nonbank electronic money issuers to the full panoply of depository regulation may not be appropriate.[30] Although some requirements may well be appropriate, nonbank issuers, be they affiliated with depositories or not, may not warrant the same regulations regarding capital, asset diversification, and asset quality, for example, that now apply to depositories.

  If and when the time for government action arrives, attention should focus on determining how different regulatory structures for depositories and nonaffiliated nondepositories will affect the competition between those two groups, including how consumers may value the regulatory structures. For example, depending upon whether electronic cash is found to be a "deposit" under certain Federal Reserve rules, banks may incur costs of deposit reserve requirements that are not imposed on nonbank issuers. The government will also need to decide whether providing holders of electronic cash issued by both depositories and nondepositories with the kinds of protection available, for example, from the FDIC would be appropriate.[31]

---

[29] See Appendix 3.

[30] See Appendix 4.

[31] See Appendix 4

Payments system stability. Significant electronic money issuance, especially by those outside the traditional banking system, could also pose challenging problems. The operational failure or insolvency of a key issuer could create a widespread loss of confidence in other forms of electronic money, leading, perhaps, to additional insolvencies and a flight to legal tender. Conceivably, the orderly flow of the inter-bank clearing system could be at risk, to the extent that the ability of banks to meet their inter-bank payments depended upon the ability of electronic money issuers to redeem their obligations in traditional bank deposits. This would be of great concern to the Federal Reserve.

Monetary management. Electronic money, if successful, could gradually lead to shifts among different forms of money held by consumers, and thus potentially affect the behavior of the monetary aggregates. However, electronic money may be only one of a number of changes in financial markets in the years ahead. Some of these may require modifications in the details of how monetary policy is implemented, just as other financial innovations have required adjustments in the past. The Federal Reserve believes that it has the capability to adjust to these changing circumstances while continuing to meet its traditional responsibilities. In order to monitor the monetary aggregates, however, the Federal Reserve may need to obtain data on outstanding amounts of electronic money from issuers, similar to the situation with nonbank-issued travelers checks.

- Government revenues

The government, as the exclusive issuer of currency, stands to lose revenue if privately issued electronic money significantly displaces the use of legal tender. Legal tender provides revenues in two ways. The first is seignorage, the difference between the face value of coins and the cost of making them (by about $773 million in 1994).[32] Second, government interest payments are reduced to the extent that people hold currency instead of interest-bearing debt. Some estimates suggest that the reduction in interest payments could be as much as $3.5 billion annually.[33] As noted in the discussion of electronic money and Treasury operations, the likelihood that the adoption of E-money

[32] This is the precise definition of seignorage, though in public discussions of the issue of E-money and seignorage, the reduction in interest payments that accrues to the Treasury as a result of the public holding currency instead of government securities is sometimes also included.

[33] John Wenniger and David Kaster, The Electronic Purse , Current Issues in Economics and Finance, Federal Reserve Bank of New York, April 1995, p. 5.

will lead to a significant reduction in avoided interest expenses for the Treasury is small.

International cooperation

Electronic money systems operating over open systems such as the Internet can, for all intents and purposes, operate outside of clear geographic boundaries. Within the United States, this creates potential questions concerning the applicability of state laws to transactions that may be initiated by a consumer in one state who uses a financial institution headquartered in a second state to make payments to recipients located in still other states, by means of a computer at some unknown location.

Those challenges are even greater at the international level. Nation states may find unilateral enforcement of electronic money related rules difficult. Laws such as those involving protection of personal privacy and entities permitted to issue electronic money may raise especially difficult problems, as will those dealing with tax collections. Sales over the Internet, for example, raise questions about the location of a transaction and consequently about which tax laws apply. All of these considerations raise the larger question, "What steps should the federal government take to identify and coordinate responses among interested countries to those common problems in such areas as law enforcement, personal privacy and issuers of electronic money?"

- Law enforcement

  Because most electronic payments systems can operate internationally and in multiple currencies, resolving jurisdictional issues for financial crimes will be difficult. This erosion of national boundaries by retail electronic money and payments makes it even more critical for law enforcement and supervisory authorities in different countries to cooperate in their anti-crime activities and to adopt consistently strong law enforcement policies and standards.

  Currently, the Financial Action Task Force (FATF), an international enforcement group with representatives from 26 countries, coordinates approaches to financial crimes and related areas. Recently, FATF adopted several recommendations for strengthening the ability of member countries to manage their crime-fighting efforts.[34]

- Protecting personal privacy

---

[34] See, for example, Department of the Treasury, FATF Updates Anti-money Laundering Standards , Treasury News, RR-1152, June 28, 1996.

Electronic-money technology can generate and capture a great deal of payments information. This information has substantial value for both commercial and anti-crime purposes. Using such information for those purposes, however, can raise serious questions involving personal privacy. Recently, the European Union (EU) adopted a policy on personal privacy that provides protections that some believe may not be available in U.S. law.

The policy is set forth in Directive 95/46/EC, a set of guidelines for member states to follow in their efforts to protect the privacy of individuals. Although the guidelines are extensive, they generally try to ensure that data on individuals are: collected for lawful purposes as specified in the directive and processed fairly and lawfully for purposes specified in the directive. Individuals have the right to see the data that pertain to them. The directive also requires those who hold and process personal information to notify individuals of releases of their personal data and, under certain circumstances, to obtain their consent for such release. Chapter IV, Article 25, encourages member countries to prohibit the export of personal information to third countries if those third countries do not provide the same degree of privacy protection as the member country. The chapter states, "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

Under the terms of that provision, it might be possible for EU member states to prohibit export of computer processed data on individuals under investigation by the U.S. government. This could decrease the effectiveness of well-established working relationships between U.S. agencies fighting financial crimes and financial intelligence units in other countries.

- Electronic money issuers

Another subject with potential international implications deals with who may issue electronic money. As noted above, a 1994 European Union report concluded that there was a need to restrict electronic money issuance to "credit" institutions.[35] In Europe, issuers of electronic money are largely limited to banks. By contrast, several U.S. firms that are not associated with

[35] Working Group on EU Payments Systems, Report to the Council of the European Monetary Institute on Prepaid Cards, May 1994.

banks are actively engaged, although on a limited basis, in issuing a variety of stored value cards, precursors to more technologically advanced smart-cards.

- New initiatives

  Among the developed countries, there is recognition of the need for greater and sustained cooperation to explore these issues as the importance and pervasiveness of the digital world grows. Separate working groups involving the central bankers, finance ministers, and law enforcement agencies of these countries have already begun to define the scope of mutual problems in this area.

  At the G-7 Summit in June 1996, Heads of States and Governments[36] called for a review of the implications of recent technological advances that make possible the creation of sophisticated methods for retail electronic payments and how to ensure the full realization of their benefits. This research will build on work already underway at the Bank for International Settlements,[37] the Basle Committee,[38] and the Financial Action Task Force.

  The study will provide an exchange of views among supervisors of financial institutions, central bankers, and law enforcement officials. They will have the opportunity to develop a broad understanding of the international dimensions of the policy issues facing governments as a result of the implementation of retail electronic money and banking systems and to consider whether the resolution of these issues would benefit from further international cooperative efforts.

## IV. Summary and conclusions

Electronic money systems are still in the relatively early stages of development, and the timing of many future developments is likely to be slower than some people

---

[36] Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. A representative of the European Union also joins in G-7 meetings.

[37] The Bank for International Settlements (BIS) dates from 1930 and promotes cooperation among the central banks of leading countries. Countries participating on the BIS Board include Belgium, France, Germany, Italy, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.

[38] The Basle Committee dates from 1974 and provides a forum for ongoing cooperation on the supervision of depository institutions among member countries--Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.

expect, for there are many obstacles to growth. These include issues relating to interoperability, security and privacy, and transaction verification and authentication.

The prospect of measured growth does not mean that government can simply sit back and wait for problems to develop. This is an area where major developments are taking place that could greatly alter the payments systems domestically and internationally. Accordingly, industry, the public, and government should use the available breathing room to consider the fundamental questions: What is the appropriate role for government with respect to electronic money? What course should government follow to carry out its responsibilities without unnecessarily inhibiting market forces that are shaping the development of electronic money systems?

Answers to those questions lie in assessing how and when electronic money will affect the ability of government to carry out basic responsibilities. Policy makers will likely wrestle, sooner rather than later, with questions in four areas: (1) consumer issues–clarifying rights and responsibilities; (2) law enforcement–evaluating the effectiveness of traditional tools in combating financial crimes; (3) government payments–moving steadily toward the complete use of EFT technology; and (4) international coordination–reinforcing the foundations of cooperative action across a wide range of issues. Traditional government responsibility for areas such as payments system stability and monetary policy may require government action, if and when electronic money systems are more fully developed and commonplace, although the timing for that is likely to be well down the road.

In acting upon the nearer-term issues, government can have an effect upon the removal of barriers to growth, a process in which the private sector has a considerable financial interest. Electronic payments and EBT initiatives can affect standards for interoperability. Law enforcement needs for information can affect privacy interests of consumers and merchants, as well as the technical standards that provide the security, transaction verification, and authentication of computerized messages. Specification of consumer rights and responsibilities can affect consumer confidence and acceptance of electronic money products.

Consequently, in meeting its responsibilities, government must combine patience with aggressive fact-finding, study, and coordination among government units both nationally and internationally. Premature action among government agencies or decisions based upon incomplete analysis could thwart innovation and its ensuing benefits, including, perhaps, the ability of U.S. firms to compete effectively in global markets.

For electronic money and banking, progress is best achieved through innovation by industry, and by government acting when markets are clearly unable to address concerns on their own. Even then it is important that industry, consumers, and government work together to find constructive solutions to problems.