Chapter 1
Summary

Chapter 1

Summary

Introduction

Electronic funds transfer (EFT) provides an alternative method of paying for goods and services and making a wide range of financial transactions that will increasingly challenge currency and checks as a dominant payment system, EFT is a cluster of technologies that allow the execution of financial transactions by electronic messages without the necessity of a paper instrument of exchange. The messages substitute for an exchange of currency or a signed check. The term EFT has also come to include electronic transfer of information critical to such transactions without an immediate transfer of funds; for example, credit authorization or check validation by telecommunication.

Some EFT systems are used for transfers between large organizations or institutions. For instance, automated clearinghouses (ACHSs receive, sort, and redistribute financial information that instructs participating banks to debit and credit accounts at a specified time. ACH services are used by some organizations for direct deposit of wages to employee accounts in many different banks.

Other EFT systems provide services to and for individual consumers. Automated teller machines (ATMs) are now widely available in many communities for making deposits or withdrawing funds 24 hours a day. Other consumer-oriented EFT technologies include point-of-sale terminals and telephone bill payer systems. Most EFT systems involve computers, telecommunication links, and automated data files. (See ch. 2 for detailed discussion of EFT technologies and services.)

Since EFT is a new and evolving technology, whose full impacts are unknown, it has given rise to a number of concerns. This paper focuses on the issues of user privacy, system security, and consumer equity in the use of EFT systems and services. Other EFT-related issues, such as competitive implications of electronic interstate banking and shared EFT networks, vulnerability of EFT to national security threats, impacts of EFT on employment, and the Federal Government role in EFT, are outside the scope of this preliminary analysis but are discussed briefly in appendix A.*

One major incentive for financial institutions in the move to EFT is the desire to reduce the growing burden of check handling and processing. The cost of processing checks is estimated at approximately $7.5 billion annually and is increasing rapidly because of rising labor costs and postage fees and the expanding volume of checks (about 5 percent more checks each year). The push for EFT is also a response to the dynamic interaction of the recent economic environment, increasing consumer sophistication, and deregulation of the banking and thrift industries. (See ch. 3 for a discussion of the competitive and regulatory environment of EFT,)

A number of factors appear to be accelerating the rate of EFT development. As a result of deregulation, the distinctions between the services offered by banks, thrift institutions, and other financial institutions are breaking down. Moreover, competing services are being marketed by nondepository institutions (e.g., securities brokers, credit card companies, and retailers). EFT makes it easier for firms to compete in financial services markets that were previously protected

*See also, the OTA report *Computer-Based National Information Systems: Technology and Public Policy Issues,* OTA-('1T-146 (Washington, D. C.: Government Printing Office, September 1981).

by regulatory boundaries. As in other areas of our economy, advancing EFT technology is contributing to de facto deregulation of markets.

In addition, financial institutions are no longer able to readily subsidize the cost of the paper-based payments system. Historically, financial institutions could more than cover the cost from earnings accruing as a result of the margin between regulated interest rates paid on deposits and market interest rates. Higher interest rates and the increasing demand by consumers to earn market rates of interest have reduced the availability of low-cost funds to subsidize paper-based transactions. Furthermore, the Federal Reserve is now required to explicitly charge for check-clearing services. Thus, EFT is used by firms in part to help offset these cost pressures as well as to counter general inflationary pressures.

In sum, EFT is increasingly viewed as an important part of the competitive and cost-containment strategies of institutions competing (or planning to compete) in the financial services markets. Projections of EFT deployment are still very rough at best, and have been badly off the mark in the past. But recent developments suggest that within the next two decades, EFT will transform the way many Americans carry out their day-to-day commercial activities and personal monetary transactions.

Privacy

Three principal concerns about EFT privacy have arisen: 1) the extent to which personal data in EFT systems are or might be disclosed to third parties by financial institutions; 2) the possibility of Government or private surveillance through EFT systems and data files; and 3) the right of consumers to see, challenge, and correct personal data in EFT systems that might be used, for example, to refuse them credit or in other disadvantageous ways.

With increased use of EFT there will be a large number of points at which traditional norms of privacy could be violated. More EFT terminals will be online, making electronic surveillance a more credible possibility. Single statement reporting of all kinds of financial transactions will become common; more data will be aggregated and thus easier to access. There could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information.

In 1977, both the Privacy Protection Study Commission and the National Commission on Electronic Funds Transfer (NCEFT) recognized that EFT privacy concerns could be especially strong. NCEFT devoted 19 recommendations to means of protecting privacy.

Only a few of the NCEFT recommendations are reflected in the two EFT-related laws enacted since 1977—the Electronic Funds Transfer Act of 1978 (and Federal Reserve Regulation E) and the Right to Financial Privacy Act of 1978. For example, the use of EFT systems for surveillance purposes is not covered by existing legislation, but would be tightly restricted by the proposed privacy of EFT bill introduced in the 96th Congress, Disclosure of EFT information to third parties is addressed only minimally by the EFT Act of 1978. The proposed privacy of EFT and fair financial information practices bills would provide more detailed conditions and restrictions on third party disclosure. Even so, these proposed conditions are not as restrictive as some customers would prefer, and neither of these bills was enacted by the 96th Congress.

Thus, the needs identified by NCEFT for more comprehensive EFT privacy protection, whether through new legislation, modification of existing law, administrative procedures and regulations, industry standards, or some combination, are still largely unmet.

Security

Security means the protection of the integrity of EFT systems and their information from illegal or unauthorized access and use. Although the loss per theft appears to be greater than for paper-based payment systems, there is no real evidence that EFT systems to date have resulted in a higher than average crime rate. Why, then, is the security of EFT systems an important public concern and potentially a major policy issue? In comparison with other payment systems, EFT appears to have some additional vulnerabilities. For example:

- EFT systems have many points of access where transactions can be affected in unauthorized ways because of direct customer involvement with the dynamics of the systems, the use of telecommunication lines, and the ways in which data are aggregated and transmitted among and between sites and institutions.
- EFT crime is often difficult to detect because funds/data can be removed or manipulated by instructions hidden in complex computer software; the dynamics of the criminal action may be understood by only a few experts within the institution.
- EFT crime offers a sporting element, or intellectual challenge, that perhaps is as enticing to some as the opportunity for financial gain.
- It is possible, in theory, for large banks of data to be destroyed by remote agents, creating the opportunity for maliciousness, extortion, blackmail, or terrorism.
- EFT systems reduce the effectiveness of—or eliminate altogether—some of the traditional methods of controlling and auditing access to financial accounts.

The level of EFT security violations is difficult to assess at present because there is underreporting of EFT crime, a paucity of information about EFT security, and a lack of informed public discussion. While there is a danger that giving these problems higher visibility through public discussion may at first exacerbate them, the public is entitled to know what risks they are exposed to in using EFT services. Furthermore, both law enforcement agents and financial institutions would benefit by sharing information about vulnerabilities, defense strategies, and security-enhancing technologies.

Some believe that effective technology and sound management procedures exist to adequately assure EFT security, though even present technology and procedures are not all widely used. Their use varies among institutions. There is as yet no clear and consistent set of industrywide security standards for protecting computer systems.

Better information about EFT security would allow Congress and State legislatures to assess more effectively the possible need for new legislation and/or regulations.

Equity

The concept of equity includes the principles that individuals, groups, and organizations should be afforded access to necessary financial services; that the range of financial choice, rights, and benefits that consumers now enjoy should not be arbitrarily reduced; and that the rules and procedures for access to and choice of financial services should not be differentially reduced for certain population subgroups.

As long as EFT is one of an array of alternative payment systems or sets of financial services, it does not appear that its use will result in a necessary or significant loss of equity to any group in society. EFT delivers benefits to many customers, and these could be increased if technology designers and financial service managers were attentive to diverse human needs. For example, dispersed EFT devices could be tailored to the needs of the handicapped, and located to meet the needs of those whose mobility is limited. EFT offers important and obvious benefits in terms of customer convenience

and reduced costs and increased productivity for financial institutions (presumably for customers as well), and perhaps greater personal security for the user against crimes of violence and some kinds of privacy abuse.

However, to the extent that some forms of participation in EFT become mandatory or inescapable, or to the extent that EFT significantly displaces, reduces, or raises the costs of alternatives, some population subgroups could experience a loss of equity. Some people who choose not to deal with banks and other financial institutions could be forced to do so. People who for various reasons are poorly equipped to use EFT systems could have their access to financial services reduced. Some communities or neighborhoods could suffer a reduction in available financial services. Explicit public policies may need to be considered to preserve some level of conventional financial services if market and other forces move EFT to a dominant role,