Chapter 3

The Depository Relationship

As Justice William O. Douglas once observed, "The banking transactions of an individual give a fairly accurate account of his religion, ideology, opinion, and interest . . . ."[1] Moreover, the emergence of a checking account as an economic and social diary for many individuals is one reason why commercial banks are acutely aware of the need to keep their clients' financial affairs confidential. Yet, as noted in Chapter 1, the Supreme Court, in *U.S. v. Miller*,[2] recently rejected the notion that such expectations of confidentiality are either warranted or legally enforceable.

The Supreme Court decision comes at a time when electronic funds transfer services, and other developments in personal-data record keeping, promise far-reaching consequences for the type of individually identifiable documentation entrusted to depository institutions. For these among many reasons, the Commission felt compelled to examine the record-keeping practices of depository institutions and to reexamine the assumptions underlying depository practices.

DEPOSITORY INSTITUTIONS

Depository institutions—that is, commercial banks, savings and loan associations, mutual savings banks, and credit unions—are financial intermediaries[3] acting as go betweens for suppliers and borrowers of money and for payers and payees. In simplest terms, when an individual deposits his money with such an institution, the institution becomes his agent and the records resulting from the relationship exist primarily to document transactions. For example, when an individual writes a check, the bank pays on the basis of that order. The check is the individual's instruction to the bank and provides an accounting to protect both the individual and the depository institution.

Americans have long thought that the details of an individual's financial affairs are nobody's business but his own unless he chooses to reveal them. The record-keeping policies and practices of depository institutions visibly reflect this view. Depository institutions testified that

[1] *California Bankers Association v. Shultz*, 416 U.S. 21, 94 S. Ct. 1494, 39 L. Ed. 2d 812 (1974).

[2] *United States v. Miller*, 425 U.S. 435 (1976).

[3] Written statement of First National City Bank (Citibank), *Credit-Card Issuers and Reservations Systems*, Hearings before the Privacy Protection Study Commission, February 11, 1976, p. 13. (Hereinafter cited as "Credit-Card Issuers Hearings.")

they are cautious in responding to inquiries concerning even the mere existence of an account.[4] The number of institutions that have self-imposed policies for notifying individuals when government agencies are seeking account information further indicates their concern. Nonetheless, information about depositors is available for purposes other than accounting. New banking services, such as overdraft protection for checking accounts[5], and concern about fraud contribute to data availability. The demands of governmental agencies responsible for regulatory oversight, law enforcement, welfare administration, and other public-sector programs also affect the level of disclosure by depository institutions.

The proliferation of personal banking service records parallels the phenomenal growth of open-end consumer credit[6] over the past several decades. As a consequence, commercial banks keep a much broader range of transactions for a significantly larger population than they did only a few years ago. The combined increase in personal checking accounts and penetration of the open-end credit market described in Chapter 2 has made commercial banks major repositories of information about the activities and relationships of millions of people.

Commercial banks have begun to market services that guarantee the availability of funds to the recipient of a check. Such authorization, or "check-guarantee," services protect the depositor against having his personal checks refused by retailers, and protect the retailer against loss from forged checks and from checks returned because there are not sufficient funds in an otherwise legitimate account. These services create a new type of economic risk for depository institutions, making them more selective—and more inquisitive—about applicants for checking accounts. For the individual, the process of applying for these new types of depository services, in some instances, resembles the process of applying for open-end consumer credit,[7] and applications for ordinary checking accounts are now being declined at times on the basis of information provided by independent check-guarantee services and credit bureaus.

In response to the increasing frequency of fraudulent and overdraft checks written during the past decade, other types of institutions have also developed services for guaranteeing checks. They are functionally similar to the independent credit-card authorization services discussed in the preceding chapter and basically maintain information on individuals who have fraudulently used checks or have outstanding unpaid checks. Such institutions also may keep a log of check-writing activity for a brief period to be

[4] Written statement of Continental Illinois National Bank and Trust Company of Chicago, *Depository and Lending Institutions*, Hearings before the Privacy Protection Study Commission, April 21, 1976, p. 5 (hereinafter cited as "Depository and Lending Institutions Hearings"); also, written statement of Bayview Federal Savings and Loan Association, Depository and Lending Institutions Hearings, April 22, 1976, pp. 5-6; and, written statement of Credit Union National Association, Depository and Lending Institutions Hearings, April 21, 1976, p. 8.

[5] "Overdraft protection" is a pre-established line of credit to assure that a checking account does not get overdrawn.

[6] For a discussion of this growth, see Chapter 2.

[7] See Chapter 2.

able to report to subscribers the total number and amount of checks written by an individual on whom an inquiry is made.

An independent check-guarantee service may verify that an individual does not have any outstanding checks for which payment was refused by the individual's bank; or the service may guarantee, or insure, that the check will be honored. If the individual's bank refuses payment, the service will meet the obligation and then collect the funds directly from the individual.

It should be noted that a check-guarantee service can combine in one organizational framework functions normally associated with depository institutions, insurers, credit bureaus, collection agencies, and credit-card authorization systems.[8] The development of these multifaceted services illustrates how traditional relationships between individuals and institutions can blur in the coming decades. Although it may be premature to address such matters, the Commission believes that the President and the Congress should be attentive to the long-term effects they may have on individuals. At the very least, future framers of protective legislation will be faced with a new set of definitional problems.

The Bank Secrecy Act of 1970

The Currency and Foreign Transactions Reporting Act of 1970, the so-called "Bank Secrecy Act,"[9] requires depository institutions to retain certain records on individuals and to report certain types of financial transactions to the Federal Government. The law was enacted largely in response to a concern over the use of secret foreign bank accounts to evade American laws. At the same time, however, Congress also recognized that the required records could be helpful to many law enforcement, regulatory, and tax administration authorities. Government agencies came to view the Bank Secrecy Act as a kind of insurance policy, guaranteeing that copies of checks and certain other documentation would be available if needed.

Bankers and civil libertarians have challenged the Act on the grounds that it raises fundamental questions about the confidential relationship between depository institutions and their customers and the relationship between government and citizens in a free society.[10] While the Commission addresses these concerns in Chapter 9, the Act is discussed here only as it affects the record-keeping practices of depository institutions.

---

[8] See written statement of Telecredit, Inc., *Credit Reporting and Payment Authorization Services*, Hearings before the Privacy Protection Study Commission, August 5, 1976. (Hereinafter cited as "Credit Reporting Hearings.")

[9] 31 U.S.C. 1051-1122

[10] *Amend the Bank Secrecy Act*, Hearings before the Subcommittee on Financial Institutions of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 92d Congress, 2d Session, 1972; *The Effect of the Bank Secrecy Act on State Laws*, Hearings before the Subcommittee on Financial Institutions of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 93d Congress, 2d Session, 1974; *Bank Failures, Regulatory Reform, and Financial Privacy*, Hearings before the Subcommittee on Financial Institutions of the Committee on Banking, Currency, and Housing, U.S. House of Representatives, 94th Congress, 1st Session, 1975.

The regulations issued by the Treasury Department[11] pursuant to the Bank Secrecy Act can be divided into four categories: (1) those pertaining to the record-keeping practices of banks and other financial institutions; (2) those requiring reports of currency transactions, foreign financial accounts, and the international transportation of monetary instruments; (3) those requiring financial institutions to verify the identity of their customers; and (4) those requiring persons having foreign financial accounts to report them to the government and to maintain records on them.

The first category requires banks, savings and loan associations, securities brokers, dealers in foreign currency, agents of foreign banks, and certain other financial institutions to retain the original or a copy of a record of each extension of credit in excess of $5,000 (except for credit secured by real estate), and the original or a copy of a record of each instruction given or received concerning the transmission out of the United States of more than $10,000 in credit, funds, currency, or other monetary instruments, checks, or securities. *[31 C.F.R. 103.33]*

A bank or other similar institution, such as a savings and loan association, credit union, or agent of a foreign bank must also retain a copy of the following: (1) documents granting signature authority over each deposit or share account; (2) account statements; (3) checks and other charges in excess of $100 that are posted to accounts (only checks drawn on certain high-volume accounts are exempt); (4) each check or other item in excess of $10,000 transmitted outside the United States; (5) each check or draft in excess of $10,000 drawn on or issued by a foreign bank which is paid by the domestic bank; (6) each check in excess of $10,000 received directly from a foreign financial institution; (7) records of each receipt of currency, other monetary instrument, securities, checks, or credit received from a foreign financial institution; and (8) records necessary to reconstruct a checking account and to furnish an audit trail for each transaction over $100. *[31 C.F.R. 103.34(b)]*

The Securities and Exchange Commission regulated the record keeping of securities brokers long before the Treasury Department issued its regulations implementing the Bank Secrecy Act. The Treasury regulations, however, added the requirement that the brokers obtain a signature card or similar document establishing trading authority over an account, and that they make a reasonable effort to obtain a Social Security number for each account. *[31 C.F.R. 103.35]*

One of the reporting requirements that affects the record-keeping practices of private financial institutions is only a modification of the longstanding requirement, in effect for more than 25 years, that financial institutions report to the Internal Revenue Service (IRS) any unusual domestic currency transaction involving more than $2,500. The new regulation raises the threshold amount from $2,500 to $10,000, and adds a penalty for willful failure to report. *[31 C.F.R. 103.32, .25(a), .47, .49]*

A new reporting requirement mandates reports on the international transportation of currency and certain monetary instruments in excess of

[11] 31 C.F.R. 103.

$5,000. A traveller carrying that amount with him must file a report with the U.S. Customs Service when he enters or leaves the United States. If the amount is transported in some other manner, a report must be filed with Customs before the monetary instrument enters or leaves the country. Conversely, a United States resident who receives $5,000 or more from overseas must file a report within 30 days after the money arrives. *[31 C.F.R. 103.23, .24(b)]*

Another reporting requirement of interest actually went into effect before Treasury issued its regulations. On the 1970 Federal income tax return, the IRS included a question concerning the ownership or control of foreign financial accounts and required any person who had such an account to file a separate schedule describing it. Under Treasury's regulation, such persons are also required to retain certain specified records of the account.

The precept "know your customer" is widely accepted in financial circles. The Treasury regulations reinforce it by requiring financial institutions to verify and record the identity of any person for whom they handle a reportable transaction, and by specifying minimum identification procedures. The identity of someone who is not a depositor may be verified by examining a driver's license, passport, or other document normally accepted as positive identification, but financial institutions must also make a reasonable effort to obtain a Social Security number or other taxpayer identification number for each entity identified with a deposit account.

Checks and other charges in excess of $100 must be microfilmed and retained for five years. The $100 minimum was supposed to exempt the vast majority of checks written by individuals, but selecting out checks in excess of $99 has proved so expensive that most banks microfilm all checks.[12]

The Service Role of Federal Financial Regulators

The fact that some financial regulatory agencies provide information-processing services for those they regulate distinguishes the depository area from other spheres of government regulation. The Federal Communications Commission, for example, does not provide the common-carrier facilities through which broadcasting networks distribute their programs, nor do State Insurance Commissioners operate computers for processing insurance companies' claims. In banking, however, Federal Reserve District Banks and Federal Home Loan Banks both provide important, though fundamentally different, record-keeping services for commercial banks and savings and loan associations.[13]

Since 1913, the Federal Reserve District Banks have cleared checks among the nation's commercial banks. Although they do not clear all checks, their services play a significant role in the movement of money from

[12] Written statement of American Bankers Association, Depository and Lending Institutions Hearings, April 22, 1976.

[13] Written statement of Board of Governors of the Federal Reserve System Staff, Depository and Lending Institutions Hearings, April 22, 1976; written statement of Federal Home Loan Bank Board Staff, Depository and Lending Institutions Hearings, April 22, 1976.

one part of the country to another. For years, this payments mechanism has depended on the physical movement of paper, with millions of individually documented transactions flowing through it every day. Concern over confidentiality was seldom expressed, since the paper glut alone was expected to protect an individual depositor's anonymity. However, changes in the form of such transfers to include electronically recorded entries, as discussed later in this chapter, have begun to undermine confidence in the continued preservation of confidential transactions as they pass through the Federal Reserve System.

Because savings and loan associations lack the payment powers of commercial banks, their record keeping does not usually cover transfers of funds among institutions, and thus is significantly less complicated than that of the commercial banks. Certain Federal Home Loan Banks, however, operate data-processing facilities as a service to savings and loan associations that are too small to support a data-processing facility of their own or are inconveniently far from a commercial data-processing service bureau.

The Commission has paid particular attention to the service role of these Federal financial regulators because of its concern with a continued public presence in the development and operation of electronic funds transfer services. The basis for this concern and the Commission's recommendation with respect to it is set forth in a later section of this chapter. First, however, the specific problems posed by the record-keeping practices of depository institutions today must be considered along with the Commission's recommendations with respect to them.

RECOMMENDATIONS

In contrast to the consumer-credit relationship, the depository relationship is not regulated with respect to determining eligibility for services and to use of third parties for information to make decisions about such eligibility. However, the introduction of new depository services involving economic risk for depository institutions, coupled with the *Miller* decision's effect on the confidential status of depository records, have persuaded the Commission that this lack of clear rights and responsibilities is undesirable for both depository institutions and their customers; the recommendations that follow reflect this conclusion.

The Commission's recommendations are presented in terms of its three recommended public-policy objectives: (1) to minimize intrusiveness; (2) to maximize fairness; and (3) to create a legitimate, enforceable, expectation of confidentiality.

Governmental Mechanisms

Because of the greater risk banks assume when they offer check-guarantee services and append lines of credit to depository accounts, individuals can no longer count on getting a bank's depository services even if they apply with cash in hand. Although the evaluation of an individual

who applies for a depository service does not appear to be as complex or as extensive as it is when he applies for consumer credit, there are parallels.

The Equal Credit Opportunity Act, as amended,[14] curbs the collection of some information about individuals by consumer-credit grantors, but depository institutions are under no such constraint. However, the Commission found no evidence that depository institutions collect items of information which could be considered excessively intrusive, and for this reason finds it unnecessary to recommend that governmental mechanisms should exist for individuals to question the propriety of information collected or used by depository institutions, or to bring such objections to the attention of bodies responsible for public policy. The need for such mechanisms may arise in the future, and the Commission suggests continued attention to developments bearing on the intrusiveness issue.

Reasonable Care in the Use of Support Organizations

Because of the similarity between applying for some new types of depository services and for open-end consumer credit, and because, as noted earlier, an independent check-guarantee service can combine functions normally associated with insurers, credit bureaus, collection agencies, credit-card authorization systems, as well as depository institutions, the Commission believes that implementation of its recommendations regarding depository institutions will be enhanced considerably if depository institutions have a strong incentive to assure that the activities of their support organizations are proper. Hence, the Commission recommends:

Recommendation (1):

That the Federal Fair Credit Reporting Act be amended to provide that a depository institution must exercise reasonable care in the selection and use of credit bureaus, independent check-guarantee services, and other support organizations, so as to assure that the collection, maintenance, use, and disclosure practices of such organizations comply with the Commission's recommendations.

If it could be shown that a depository institution contracted for or used the services of a support organization with knowledge, actual or constructive, that the organization had been engaging in illegal practices, an individual, the Federal Trade Commission, or other appropriate enforcement agency could initiate action against both the depository institution and the support organization and hold them jointly liable for the support organization's actions.

[14] 15 U.S.C. 1691 *et seq.*

Fairness

Fairness in Collection

Notice Regarding Collection from Third Parties

Although the Commission believes that there is currently no need for governmental mechanisms to question the propriety of information collected or used by depository institutions, the individual's participation in striking a balance between the amount of information he must divulge about himself and the service he expects in return does need to be strengthened. Thus, the Commission recommends:

Recommendation (2):

That Federal law be enacted or amended to provide that when an individual applies for a depository service, a depository institution must notify the individual of:

(a) the types of information expected to be collected about him from third parties and that are not collected on the application; and

(b) the types of institutional sources that are expected to be asked to provide information about him.

The recommended measure, like the parallel measure recommended for consumer credit, ensures that the individual will be told the scope of an inquiry before agreeing to it. The usual institutional sources to be queried are the individual's employer and the depository institutions with which he has or once had a relationship. The emergence of independent check-guarantee services and the new reliance on credit bureaus introduce additional institutional sources, and this recommendation also applies to them.

The Commission believes that this recommendation can best be implemented by giving additional authority to the Federal Reserve Board to supplement similar regulatory authority it now has under the Truth-in-Lending, Equal Credit Opportunity, and Fair Credit Billing Acts. The resulting Federal Reserve Board regulations could then be enforced both by the enforcement agencies with authority over particular depository institutions, and by the individual as currently provided in the Truth-in-Lending Act which allows an individual to seek damages for violation of standards promulgated by the Board either on his own behalf, or on behalf of a class.

Notice as the Collection Limitation

The Commission is concerned that a depository institution's practices and those of its support organizations conform with the individual's expectations pursuant to *Recommendation (2).* Therefore, the Commission recommends:

Recommendation (3):

That Federal law be enacted or amended to provide that a depository institution must limit:

(a) its own information collection practices in connection with an application for a depository service to those specified in the notice called for in *Recommendation (2)*; and

(b) its request to any organization it asks to collect information on its behalf to information and sources specified in the notice called for in *Recommendation (2).*

Recommendation (3) should be implemented in conjunction with *Recommendations (1)* and *(2).* Its purpose is to make clear that both the depository institution and any organization the depository institution utilizes to collect information on its behalf are equally subject to to the limitations implicit in the notice called for in *Recommendation (2).*

Fairness in Use

Access to Depository Records

An individual needs a right of access to records about himself compiled for the purpose of making depository decisions just as he needs it for other decisions about him. The need grows more urgent as depository institutions depend on information from third parties, such as independent check-guarantee services. Without such access, the individual has no control over the accuracy and completeness of the information that is used, and has no way of discovering errors or other inaccuracies in the information another institution has provided. Thus, the Commission recommends:

Recommendation (4):

That Federal law be enacted or amended to provide that an individual shall have a right to see and copy, upon request, all recorded information concerning him that a depository institution has used to make an adverse depository decision about him.

The recommendation recognizes the individual's right of access only to the records about himself which enter into an adverse decision. In the adverse decision situation, the individual is affected by information that does not stem from transactions directly related to the depository account. The Commission recognizes that an individual presently receives copies of records with respect to his depository account on a periodic basis, usually in the form of monthly statements and cancelled checks or receipts for deposits and withdrawals. The implementation of this recommendation is discussed under *Recommendation (5)* below.

Adverse Depository Decisions

The Commission has concluded that a depository institution should be

obligated to explain its adverse decisions to the affected individuals. Unlike credit grantors, depository institutions have no procedures for fulfilling this obligation, and neither the Fair Credit Reporting Act nor the Equal Credit Opportunity Act applies to decisions denying an individual a depository service. Therefore, the Commission recommends:

Recommendation (5):

That Federal law be enacted or amended to provide that a depository institution must:

(a) disclose in writing to an individual who is the subject of an adverse depository decision:
- **(i) the specific reason(s) for the adverse decision;**
- **(ii) the specific item(s) of information, in plain language, that supports the reason(s) given pursuant to (a)(i);**
- **(iii) the name(s) and address(es) of the institutional source(s) of the item(s) given pursuant to (a)(ii); and**
- **(iv) the individual's right to see and copy, upon request, all recorded information pertaining to him used to make the adverse decision; and**

(b) inform the individual of his rights provided by the Fair Credit Reporting Act, when the decision is based in whole or in part on information obtained from a credit bureau or independent check-guarantee service.

The value of *Recommendation (5)* will be more apparent as depository institutions become more selective in opening depository accounts. Inequities stemming from the fact that no law now allows an individual easily to learn the reasons for an adverse decision, the information items behind those reasons, or the identity and whereabouts of institutional sources are discussed extensively in the preceding chapter. The inclusion of independent check-guarantee services in subparagraph (b) assumes the adoption of *Recommendation (6)*, below.

Recommendations (4) and *(5)* could be implemented either through amendment of the Fair Credit Reporting Act or the banking laws. An individual should be able to sue in Federal court or another court of competent jurisdiction if the depository institution fails to perform. This right should include the right to sue for failure to state specific reason(s) for a specific decision where the individual has cause to believe that the reason is other than the one(s) stated by the depository institution. The court should have the power to order the depository institution to comply and to award attorney's fees and court costs to any plaintiff who substantially prevails. If it could be shown that the credit grantor willfully or intentionally denied the individual any of the rights *Recommendations (4)* and *(5)* would give him, the court should have the power to award up to $1,000 to the individual.

Systematic denials of access by depository institutions could be subject to enforcement by the Federal Trade Commission and other agencies[15] that currently have enforcement authority under the Fair Credit Reporting and Equal Credit Opportunity Acts. The remedy would be an order directing a depository institution to disclose records upon request. Once the FTC or other agency issued such an order, the depository institution would then be subject to the usual statutes available to enforce such orders.

The burden should be on the individual to reasonably describe the documents sought and the depository institution should be able to defend itself on the basis that it could not reasonably locate or identify them. For example, an individual could sue for disclosure to him of any document developed as a result of an application for a depository service if the individual could reasonably identify the date and nature of the application. If, however, an individual requested any information that relates to him in a file, and could not identify, with some specificity, the circumstances pursuant to which such a file was developed, the depository institution would not be under any affirmative obligation to search every record to locate a possible passing reference to the individual.

Regulation of Independent Check-Guarantee Services

Independent check-guarantee services are arguably excluded from the Fair Credit Reporting Act because they do not influence credit or other decisions, such as employment and insurance. The Commission finds, however, that independent check-guarantee services affect individuals in the same way as do credit bureaus and inspection bureaus. The Federal Trade Commission staff has advised independent check-guarantee services that they *are* subject to the provisions of the FCRA, but this interpretation lacks the force of law. The Commission believes that the law should explicitly cover independent check-guarantee services, exempting them only from those FCRA requirements that are not appropriate. Therefore, the Commission recommends:

Recommendation (6):

That the Federal Fair Credit Reporting Act be amended to provide that an independent check-guarantee service shall be subject to all requirements of the Act, except the requirement to disclose corrected information to prior recipients upon completion of a reinvestigation of disputed information.

The rationale for the exception in this recommendation is the same as the rationale for the exception in *Recommendation (9)(b)* in the previous chapter on credit grantors and independent authorization services—namely, that once an error in an independent check-guarantee service record is

[15] Under the pertinent provisions of the FCRA *[15 U.S.C. 1681s(b)]* and the ECOA *[15 U.S.C. 1691c(a) & (c)]*, twelve agencies have some administrative enforcement responsibility, ranging from traditional financial regulators such as the Federal Reserve Board to agencies such as the Civil Aeronautics Board and the Department of Agriculture.

discovered, the damage has already been done and usually cannot be remedied. Hence a requirement that previous recipients be notified of any corrections would, in most, cases, be gratuitous. If an independent check-guarantee service fails to meet the requirements called for in *Recommendation (6)*, it should be liable for actual damages in the event an individual is harmed by its failure.

Inaccurate Reports to Independent Check Guarantee Services

The subscribers of an independent check-guarantee service are its principal sources of information. The subscriber list of Telecredit, Inc., the nation's largest check-guarantee service, includes automobile dealers, airlines, hotels, gasoline stations, commercial banks, department stores, car-rental agencies, and other retailers across the country. Other fruitful sources of information, less frequent but not less significant, are law enforcement agencies that track down stolen and forged checks.[16] Thus, an independent check-guarantee service's sources of information can be as diverse as those of credit bureaus.

The consequences of having one's name and identification adversely reported to an independent check-guarantee service are clear and certain; a subscriber to the service will not honor your check. The Commission is concerned about errors that may occur and the unfairly preemptive actions that they can cause. Accordingly, the Commission recommends:

Recommendation (7):

That the Federal Fair Credit Reporting Act be amended to provide that if a contributor learns it has incorrectly reported an individual to an independent check-guarantee service, it must notify the check-guarantee service within a reasonable period of time so that the service can correct its files.

As with *Recommendation (6)*, a contributor that incorrectly reports an individual to an independent check-guarantee service and fails to correct the error after it is discovered should be liable for actual damages in the event that an individual is harmed by its failure to do so.

Expectation of Confidentiality

Confidentiality of Depository Records

As with other confidential relationships, an individual's expectation of confidentiality in his depository relationship can be at best impressionistic unless a depository institution apprises him of its disclosure policies. Further, it must again be emphasized that an individual currently has no legally recognized interest in the records maintained about him by a depository institution and therefore cannot prevent a disclosure of them that may be inimical to him. Thus, the Commission recommends:

[16] Written statement of Telecredit, Inc., Credit Reporting Hearings, August 5, 1976.

Recommendation (8):

That Federal law be enacted to provide:

(a) that a depository institution must notify an individual with whom it has or proposes to have a depository relationship of the uses and disclosures which are expected to be made of the types of information it collects or maintains about him; and that with respect to routine disclosures to third parties which are necessary for servicing the depository relationship, the notification must include the specific types of information to be disclosed and the types of recipients;

(b) that information concerning an individual which a depository institution collects to establish or service a depository relationship, as stated in the notification to the individual called for in (a), must be treated as confidential by the depository institution; and thus any disclosures to third parties other than those necessary to service the depository relationship must be specifically directed or authorized by the individual, or in the case of marketing information, specifically described in the notification;

(c) that an individual must be considered to have a continuing interest in the use and disclosure of information a depository institution maintains about him, and must be allowed to participate in any use or disclosure that would not be consistent with the original notification, except when a depository institution discloses information about an individual in order to prevent or protect against the possible occurrence of fraud; and

(d) that any material changes or modifications in the use or disclosure policies of a depository institution must be preceded by a notification that describes the change to an individual with whom the depository institution has an established relationship.

In addition to enacting the recommendation, the statute should give the Federal Reserve Board regulatory authority similar to the regulatory authority it now has under the Truth-in-Lending, Equal Credit Opportunity, and Fair Credit Billing Acts. The resulting Federal Reserve regulations could then be enforced both by the enforcement agencies having authority over particular depository institutions, and by the individual, as currently provided in the Truth-in-Lending Act, which allows an individual to seek damages for violation of standards promulgated by the Board, either on his own behalf or on behalf of a class.

ELECTRONIC FUNDS TRANSFER SERVICES

The phrase Electronic Funds Transfer (EFT) includes several related techniques for processing and documenting deposits, withdrawals, and transfers of money with the aid of computers and telecommunications. Point-of-sale services and Automated Clearing House (ACH) Services are

currently prominent examples. Variations in EFT services depend largely on the size and type of depository institution, the regularity of the payments to be processed, the purpose and complexity of the financial transaction, regulatory and other legal restraints, and the willingness of consumers to indulge business and governmental institutions in their search for new financial services.

Point-of-sale services are probably the form of EFT most visible to the individual. They offer the individual a convenient way to use the funds he has on deposit without having to visit the depository institution or draw a check or draft on his account. Some point-of-sale services simply allow the withdrawal of funds, as for example, when an individual receives cash at a supermarket and purchases his groceries with the cash. More sophisticated services allow the individual, at the location and time of purchase, to move funds electronically from his account to the merchant's account in exchange for goods or services that he would otherwise pay for with cash, check, or credit.

The information-processing technology necessary for providing point-of-sale services is similar in many respects to that used extensively by credit-card issuers. The ubiquitous plastic card has been borrowed from the credit-card world and enhanced with a *personal identification number,* a unique number known only to the account holder and his financial institution and intended to safeguard against unauthorized transfers of funds. Point-of-sale services depend on telecommunications and computer systems in the same manner as credit-card issuers use them for authorizing transactions, transmitting information among various institutions, and keeping track of credits and debits.[17] If a point-of-sale service involves many combinations of merchants and financial institutions, switches route each transaction to the appropriate financial institution, a technology also employed successfully by the two national bank-card associations.[18] In light of many existing credit-card systems, it seems that the novelty of most point-of-sale services for the individual will be a new way to make withdrawals of deposited funds. Point-of-sale services may eventually involve all types of depository institutions, i.e., commercial banks, savings and loan associations, mutual savings banks, and credit unions. However, to understand how these services work, one need only look at their impact on commercial banks and savings and loan associations.

Commercial banks have long offered their customers convenient access to deposits by means of checking accounts.[19] Checking accounts,

[17] Written statement of Dee W. Hock, President, National BankAmericard, Inc., and John H. Reynolds, President, Interbank Card Association, Credit-Card Issuers Hearings, February 11, 1976.

[18] As the following passage emphasizes, the techniques that make electronic exchange possible have been utilized quite successfully for bank-card operations: "EFT is emerging and coming fast . . . . Much has been learned in processing credit cards that will be useful in electronic funds transfer systems. Pre-authorized credits, sales authorization and interchange will be necessary." Western States Bankcard Association, *Annual Report 1975,* p. 1.

[19] Uniform Commercial Code § 3-108. See *Independent Bankers' Association of America, et al. v. Smith,* Doc. No. 75-0089 (D.C. Cir., March 23, 1976).

however, have two main drawbacks. For the banks, there is the cost of processing a glut of paper;[20] and for the individual, there is the reluctance of merchants to accept personal checks, a reluctance which has been rising with the number of fraudulent and overdraft checks.[21] Point-of-sale services promise to reduce both drawbacks. For some commercial banks, check-authorization services are a first step toward developing the computer and telecommunications capability necessary for a mature point-of-sale service.[22] Consumer acceptance will, however, determine how far such services can go in eliminating personal checks.[23]

Savings and loan associations and other thrift institutions ordinarily lack the payment powers necessary to offer their customers the convenience of checking accounts.[24] Point-of-sale services give them a way of overcoming this obstacle. One observer of EFT developments summarized this transformation of savings and loan accounts as follows:

> Electronic technology confuses payment powers limitations as well as doing away with the necessity of creating a negotiable instrument for purposes of conveying payment orders from account holder to financial institution. As a result, the technologies present two intriguing options to users. The account holder can turn any account into a "payment account" by dealing in cash if machines are strategically and conveniently located, or the account holder could, by electronically ordering the institution to do the paying for him by appropriate debits and credits to accounts, eliminate the use of cash or paper . . . .[25]

Automated Clearing House services also transfer funds electronically. Their principal purpose as presently constituted is to effect debits and credits of a recurring nature between institutions; for example, payrolls, insurance premiums, social security benefits, and payments for utilities and mortgages. The main differences between point-of-sale services and ACH services, now and for the foreseeable future, are in the type of transactions processed, details of processing, and institutional control over the systems.

---

[20] In 1970, an estimated 21.5 billion checks were written on demand deposit accounts in commercial banks in the United States. Approximately one billion additional checks were written by the Federal government. It has been estimated that the total cost to society of the check payment system is $10 billion annually. See Arthur D. Little, *The Consequences of Electronic Funds Transfer: A Technology Assessment of Movement Toward a Less Cash/Less Check Society*, Chapter 4, June 1975.

[21] Written statement of Telecredit, Inc., Credit Reporting Hearings, August 5, 1976, p. 1.

[22] Written statement of First National City Bank (Citibank), Credit-Card Issuers Hearings, February 11, 1976, p. 2; also, written statement of Continental Illinois Bank and Trust Company of Chicago, Depository and Lending Institutions Hearings, April 21, 1976, pp. 2-5.

[23] For some thoughtful comments concerning EFT from the consumer's perspective, see Peter H. Shuck, "Electronic Funds Transfer: A Technology in Search of a Market," *Maryland Law Review*, Volume 35, Number 1, 1975.

[24] The major exception to this general rule is the negotiable order of withdrawal (NOW) account. The orders of withdrawal are negotiable instruments but draw on interest-bearing accounts rather than demand deposits. Some States, such as New York, have granted checking-account powers to State-chartered thrift institutions.

[25] Stephen M. Ege, "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," *Maryland Law Review*, Volume 35, Number 1, 1975.

Typical ACH transactions are recurring pre-authorized transfers between institutions, as when social security recipients have their benefits deposited directly into their bank accounts each month. Such services arguably offer the most efficient, cost-effective, and convenient method of processing the innumerable government and commercial transactions that must be repeated regularly on fixed schedules. Telecommunications have not been essential to ACH operations in their early stages of development because each debit and credit does not need an authorization, as in point-of-sale services, nor does it need to be posted instantaneously to an account. However, ACHs across the country are being linked together by telecommunications to facilitate interregional exchange.[26]

Institutional control over ACH services differs from institutional control over point-of-sale services in that Federal Reserve district banks operate the computer and communications facilities used by all but two of them. To a large extent, Federal Reserve district banks also determine pricing of ACH services and liability for errors. *Most significant from the personal privacy viewpoint, the Federal Reserve System, which acts as a fiscal agent of financial institutions and the Treasury Department in some respects, is not constrained by either its government or its commercial clients, much less by any individual bank client, from disclosing information about a bank customer's account to other government agencies.*[27]

Impact of Electronic Funds Transfer on Financial Records

Commercial banks and savings and loan associations presently stand at the threshold of a vast development in point-of-sale services. Significant effects of such development on institutional record keeping are clearly predictable based on experiences with credit cards. Expansion undoubtedly means that: (1) information about individuals recorded by financial institutions will include more details than otherwise required; (2) the records will become more centralized and the details will be more easily retrieved than they are now; and (3) financial records will expand to include items of information not ordinarily considered payment data.

It is important to note that the increased scope of the records generated by EFT may well include more than simply information necessary to transfer funds. Indeed, there are pressures which could eventually transform EFT systems into generalized information transfer systems. In the commercial environment, for example, accounting and administrative data will probably flow with various recurring payments; e.g., related benefit and tax withholding information could accompany wage

[26] "NACHA/Federal Reserve Set Plans for Nationwide ACH 'Pilot' Exchange, Action Expected to Stir Concern as Implications Unfold," *Payment Systems Action Report*, Volume 1, Number 6, July 26, 1976.

[27] Submission of Board of Governors of the Federal Reserve System Staff, Depository and Lending Institutions Hearings, April 22, 1976, p. 4. Part 261.6(b) of the Board's Rules regarding availability of information provides for the release of reports or examination of banks "to other agencies of the United States for use where necessary in the performance of their official duties." In Part 261.7 of its Rules, the Board has established procedures for responding to duly issued subpoenas.

payments. Consumer transactions are likely to relay information concerning the purpose of the transaction along with essential payment data to payee and payer alike. While such developments are not inevitable, the pressures to move in this direction are high. The economic incentives to combine payment and administrative information are great from both payer and payee point of view. It would eliminate the need for a great deal of paper documentation or the need for a duplicate information transfer system. Given the emergence of an increasingly competitive market for financial services and the potential cost savings for public and private institutions alike, there would seem to be little reason for providers of EFT services to refuse to accept the additional information flow.

For savings and loan associations, point-of-sale services also expand both the number and content of the records they keep and make the recorded information more readily available. The number grows because customers who no longer have to visit their savings and loan association in order to make a withdrawal or deposit will use their accounts more often, and each use generates a record. The content will grow because a point-of-sale transaction at, say, a supermarket requires that the record of that transaction be expanded to include at least the identity of the supermarket, and probably the time, date, and location of the transaction; the record may also expand further to include a description of items purchased. Finally, point-of-sale services will increase reliance on sophisticated information technologies, in many cases altering the form in which information is recorded and stored, and easing retrieval of it by those who control access to it. The great preponderance of savings and loan associations already have terminal-oriented computer systems, and point-of-sale services will simply further this trend. For savings and loan associations not currently automated, however, point-of-sale services will generate electronic records where none currently exist.[28]

With commercial banks, point-of-sale development is not likely to expand appreciably either the number of records they keep or the content of their records, since records of checking services contain much of the necessary point-of-sale information. Clearer descriptions of transactions may be needed for verification by the consumer, but the data base maintained for a checking account is probably adequate for point-of-sale purposes.

Commercial banks have already invested heavily in information technology for processing the volume of paper generated by checking accounts; the main difference made by adding point-of-sale services will be to increase substantially the uses commercial banks can make of them. New point-of-sale services will further decrease the banks' reliance on paper, as their permanent records come to include a higher fraction of electronic records of point-of-sale transactions and a lower one of microfilmed checks. Since it is far quicker and easier to search and retrieve information from electronic records than from voluminous paper documentation and microfilm, the utility of an information base that is already recognized as useful

[28] Written submission of the U.S. League of Savings Associations to the Privacy Protection Study Commission, June 2, 1976.

for many purposes apart from banking, from marketing to law enforcement, will be considerably enhanced.[29]

Expanding point-of-sale services will also have other less specialized effects. Even the most primitive point-of-sale services depend on accurate identification to assure that only authorized individuals have access to an account. Given the paramount importance of controlling access, providers of point-of-sale services will predictably demand more personal characteristics (e.g., fingerprints or characteristics of one's signature) to verify the identity of an account holder, giving financial record keepers additional information.

When banks and other financial institutions began issuing credit cards, the number of locations where their payment records originate and where copies of them must be kept multiplied.[30] Since most of the new makers and keepers of these records are not financial institutions, more and more of the records historically controlled by such institutions are now also retained and available for use by others. *This drift is significant insofar as one recognizes the existence of a confidential relationship between an individual and his bank and the obligation that flows to the record keeper as a result of the relationship. One public policy consequence is that identical records may be retained by different record keepers with whom an individual has different types of relationships and thus different expectations of confidentiality.*[31]

Very significant for personal privacy is that point-of-sale transactions must be monitored, and monitoring transactions could become an effective way of tracking an individual's movements.[32] Large-scale credit-card systems already monitor frequency of card use and point-of-sale services extend the range of potential surveillance.

Finally, there will be a significant impact if ACH services become a

---

[29] The Bank Secrecy Act was passed explicitly recognizing that financial records would be used for nonfinancial purposes. In particular, the findings statement for Section 21(a)(1) reads: "The Congress finds that adequate records maintained by insured banks have a high degree of usefulness in criminal, tax, and regulatory investigation proceedings. The Congress further finds that photocopies made by banks of checks, as well as records kept by banks of the identity of persons maintaining or authorized to act with respect to accounts therein, have been of particular value in this respect."

[30] Unlike checks, which are governed by Articles 3 and 4 of the Uniform Commercial Code, credit-card transactions are governed by the Federal and State laws discussed in Chapter 2, and by contracts among card issuers and merchants. To get payment for purchases made with credit cards and to protect themselves against errors, merchants retain copies of credit-card transaction records.

[31] The importance of recognizing an expectation of confidentiality as the touchstone for protecting the individual's interest in his records is discussed extensively in Chapter 1. Two recent California Supreme Court decisions, *Burrows v. Superior Court*, 13 Cal.3d 238 (1974) and *Valley Bank of Nevada v. Superior Court*, 15 Cal.3d 652 (1975) have upheld and clarified the theory that a bank customer has and should have a reasonable expectation of confidentiality and privacy in his bank records and, conversely, that a bank has a duty to take reasonable steps to preserve such confidentiality.

[32] See James B. Rule, *Value Choices in Electronic Funds Transfer Policy*, prepared for the Office of Telecommunications Policy, Executive Office of the President, October 1975; also footnote 8.

major vehicle for processing transactions that originate in point-of-sale services.[33] As point-of-sale services penetrate different regional markets, the need for interregional exchange of data will arise just as did the need for interregional clearance of checks. Thus, the scope of ACH services could expand considerably, not only functionally, but also geographically to include a much greater share of individual transactions. Since such transactions are the raw material for piecing together personal profiles of individuals, ACH expansion into point-of-sale services would intensify the threat to personal privacy.

It should not be assumed, however, that extension of ACH services to include point-of-sale transactions is necessary for them to pose a threat to privacy. Even in the limited use for recurring payments, such as social security benefits or wages, an ACH service poses all three privacy problems inherent in a fully developed EFT environment: (1) its records include more personal details than traditional systems of payment transfer; (2) the information in its records is more centralized; and (3) it transfers more information than would ordinarily be considered payment data.

The first step in linking ACH services across regions has been initiated by the Federal Reserve district banks. Because the Board of Governors of the Federal Reserve System has not yet decided how far it will expand its provision of EFT services,[34] point-of-sale services under Federal Reserve System auspices must be considered a possibility. Indeed, this possibility is a central concern of the Commission.

RECOMMENDATIONS

The use of electronically recorded transactions for marketing is a well established practice of a variety of organizations, including retailers and financial institutions. Current market practice is to draw upon the vast pool of credit-card transactions and credit-bureau files, and more generalized sources of demographic information, such as census tracts. Point-of-sale services will dramatically expand the base of electronically recorded transactions that marketers can tap. It will not, however, create a new demand for such information; that demand already exists.

The disclosure of financial records to government agencies is another well established practice of the institutions that will provide or use EFT services. For savings and loan associations, point-of-sale services will create a new source of information for government agencies. For commercial banks, point-of-sale services reduce a major incentive to resist inquiries by government authorities because of the cost of searching microfilmed check records. Simply by changing the means of information storage and retrieval, point-of-sale services exacerbate the government-access problem which has existed long before the introduction of EFT.

[33] Comments of the Office of Telecommunications Policy before the Board of Governors of the Federal Reserve System, in the matter of Proposed Amendment of Regulation J, March, 1976.

[34] Letter from Arthur F. Burns, Chairman of the Board of Governors of the Federal Reserve System to the Privacy Protection Study Commission, November 1, 1976.

The practice of using point-of-sale services to locate an individual is not yet widespread, but already at least one nationwide independent check-guarantee service is deriving revenue from it.[35] If, for example, the wanted individual offers to pay by check at a store that subscribes to this authorization service, he is asked for his current address, which is promptly reported to the client who wants to locate him.

Marketing, law enforcement, and locator services are only a few of the many collateral uses for EFT records. The Commission's general recommendations with respect to depository relationships are designed to give an individual both access to and some control over the disclosure of information that an EFT environment would accumulate about him. However, the Commission also urges the adoption of the three recommendations immediately below as part of the overall regulation of electronic funds transfer services now being considered by legislatures and regulatory bodies at both the Federal and State level.

Centralized Financial Information Flows

The Commission recognizes that electronic funds transfer services inevitably create and retain some records which cannot be controlled by the institutions from which the individual can reasonably expect confidentiality. Institutional arrangements already formed for automated clearinghouses and shared point-of-sale systems introduce new sources of electronically recorded information that centralize, if only briefly, information otherwise segregated among diverse depository institutions. The Commission is concerned about the far-reaching consequences of these centralized financial information flows because of the scope of the records that is expected to develop and the manner in which information about individuals or groups of individuals may be accumulated on a selective basis.

Beyond the fundamental problem of the accumulation and centralization of detailed information, there are two additional threats that such an EFT environment raises. First, there is the well perceived one of electronic eavesdropping, though not necessarily at the relatively unsophisticated and illegitimate level of wiretapping. It is technically possible through electronic means to monitor the flow of information through an EFT network, and to capture items of interest on a selective basis. While this would require a sophisticated technical approach, it is nonetheless possible and could lead to a rapid-response capability for locating an individual, or to a capability for building a comprehensive record on an individual's movements, buying habits, and so forth. Equally important, it could be accomplished without surreptitious entry into the system by anyone given access to the computer facilities that sort and direct the flow of information.

The second privacy threat also arises from the fact that EFT services will require an extensive data communications network. While the detailed implementation of such a network may vary from one EFT application to another, each one must accumulate certain items of information about the traffic that flows through it. For accounting and billing purposes, as well as

[35] Written statement of Telecredit, Inc., Credit Reporting Hearings, August 5, 1976.

for controlling and operating a network, some portion of the information flowing through it must be retained within it. To illustrate, the telephone company automatically captures for all long distance connections the calling and called numbers, the duration of the call, and the time and date. Technically, the telephone network could also capture the voice conversation, but does not need to do so and in fact is prohibited by law from capturing it. In an EFT environment, however, this might not be so; for technical convenience a particular network design might capture everything that flowed through it.

Whether an EFT network captures all the information flowing through it or only certain items or even portions of items, there is a risk that the resulting pools of information will become attractive sources of personally identifiable information for use in ways inimical to personal privacy. Because the response time of present EFT systems is hours or days, the temptation to use them to surveil an individual's movements is minimal. A transaction-oriented EFT system, however, will be much more dynamic, and will have to respond in seconds if it is to fulfill its function. Thus, the temptation to surveil may increase markedly.

For these reasons, the Commission believes that protection must be afforded individually identifiable information flowing through an EFT data communications network. Accordingly, the Commission recommends:

Recommendation (9):

That individually identifiable account information generated in the provision of EFT services be retained only in the account records of the financial institutions and other parties to a transaction, except that it may be retained by the EFT service provider to the extent, and for the *limited period of time,* that such information is essential to fulfill the operational requirements of the service provider.

An EFT data network not only deals with the original details of a transaction, but also may add or derive additional items of information. For example, the time-of-day or a running transaction number may be added; patterns of credit-card usage or frequency of particular activity can be derived. The Commission intends that both primary transactional information and derivative information created by the operation of the data network be subject to the restrictions of *Recommendation (9).* In essence, the Commission has concluded that information generated by an EFT system, like information which is the product of check or credit-card transactions today, should be available only from the parties to the transaction and, subject to the restrictions of appropriate expectations of confidentiality, from the financial institutions which maintain accounts for those parties. Further, the Commission seeks, through the measure suggested above, to limit the potential for misuse or improper disclosure of information by the service provider by eliminating the presence of identifiable information in the system (at the "switch," "clearinghouse," or other exchange point, for example) to the extent practicable.

Accuracy of Electronic Transactions

How to assure the accuracy of recorded information and reduce untoward effects of inaccurately recorded transactions was discussed in Chapter 2. Individuals are legally protected by the Fair Credit Billing Act against some of the untoward consequences of credit-card errors. Although a point-of-sale service for making withdrawals is operationally similar to a credit-card system, the individual has no comparable legal protection when disputing the accuracy of an electronic transaction. Therefore, the Commission further recommends:

Recommendation (10):

That procedures be established so that an individual can promptly correct inaccuracies in transactions or account records generated by an EFT service.

Government Operation of EFT Services

EFT services will produce qualitative changes in the information base available to various institutions and, in turn, will affect the demands placed on those institutions for financial records. EFT therefore adds to the urgency of the need to strengthen protections for personal privacy in the manner advocated throughout this report. The Commission's concern with EFT as a threat to personal privacy goes beyond its effect on depository record keeping as dealt with in the preceding section of this chapter. The Commission sees governmental provision of EFT services as a dangerous direction.

The surveillance potential of an EFT system becomes much more formidable, in the Commission's estimation, if government operates the facilities than when the service is controlled by private parties. When any government entity processes financial records which document the private affairs of individuals, the likelihood and opportunities for other government agencies to obtain and possibly misuse those records increases. *Current problems with government access to bank records are minor compared with the potential threat to privacy posed by government operation of EFT facilities.* As such services become more sophisticated and documentation and surveillance capability increases, government operation of EFT systems will become, in the Commission's view, an unparalleled threat to personal privacy. The current paper-based clearing system, though largely operated by the Federal Reserve, is not a useful source of information for government agencies because the checks being cleared cannot easily be retrieved on a selective basis. The situation changes when the Federal Reserve uses telecommunications technology for processing private transactions. Commission staff learned in an interview with Federal Reserve officials that the Department of Justice, for example, has requested that the Federal Reserve supply it with information from records of transactions between private parties where the Federal Reserve employed telecommunications to effect the funds transfer. The IRS has a much more limited information resource

than the Federal Reserve would if it operated an EFT system; yet it has been abused for harassment and political advantage. While in our system of taxation there is a compelling need for government to manage the information flow on which the system depends, there seems to be no analogous rationale compelling government to provide EFT services for private parties.

A secondary problem focuses on the activities of the Federal Reserve Board of Governors and district banks. As mentioned above, the Federal Reserve has played a dominant role in the development of EFT, most notably by providing ACH services. For the Federal Reserve to continue, indeed increase, its control over facilities for EFT is unwise, in the Commission's view, particularly in view of the possible meshing of ACH services with point-of-sale services. Unless the Federal Reserve limits its EFT operations and begins divestment now, the inertia of economic circumstance may destroy the policy choice, leaving the Federal Reserve as the basic provider of services used by financial institutions to transfer funds and support point-of-sale services. Therefore, the Commission recommends:

Recommendation (11):

That no governmental entity be allowed to own, operate, or otherwise manage any part of an electronic payments mechanism that involves transactions among private parties.

The Commission's position does not suggest that there be no government regulation of EFT services. Without addressing such matters as the existing Federal regulatory structure for depository institutions, competition in the provision of EFT services, or the impact of an integrated national EFT system on capital markets, the Commission believes that regulation of the financial community should not be tied to government operation of an electronic payments system. If a monopolistic and thus closely regulated EFT system does emerge, the agencies which will have to provide oversight should not also operate its facilities.

Actual provision of services to a particular industry has often created unavoidable conflicts for the government agencies that act as that industry's watchmen or regulators. Too deep an involvement in day-to-day operation results either in a growing lack of responsiveness to consumer and public-policy concerns, or in a domination by the regulator which discourages efficiency and innovation, and fosters static patterns of response.[36] An example of the former problem can be found in the Interstate Commerce Commission's response to the congressional policy mandated by the Railroad Reform Act. The consequences of domination are reflected in the problems which recently spurred reform of the Atomic Energy Commission and the restructuring of U.S. nuclear research, development, and regulation.

In addition, given the communications aspect of EFT delivery systems, and the potential for them to evolve into more general information transfer services, the responsibility to regulate its development ought to be

[36] See Roger Noll, *Reforming Regulation*, (Washington, D.C.: Brookings Institution, 1972).

shared with the FCC or with a similar regulator who has communications as a principal mandate. From a privacy perspective, the traditional safeguards for individual messages transferred by way of electronic communications are the first step toward the protections needed in an EFT environment.

Finally, even if government operation of facilities for EFT services were determined to be desirable, the Federal Reserve Board and its related financial regulators are hardly the appropriate agencies to do it. Financial regulators such as the Federal Reserve are not as accountable to outside authorities as other governmental organizations; self-discipline is the only real restraint on their activities. An exception to the canons of governmental accountability to such external authorities as the Congress and the President may be justified insofar as Federal Reserve activities pertain to monetary policy and bank supervision, but hardly to activities which impinge on personal privacy.