1978

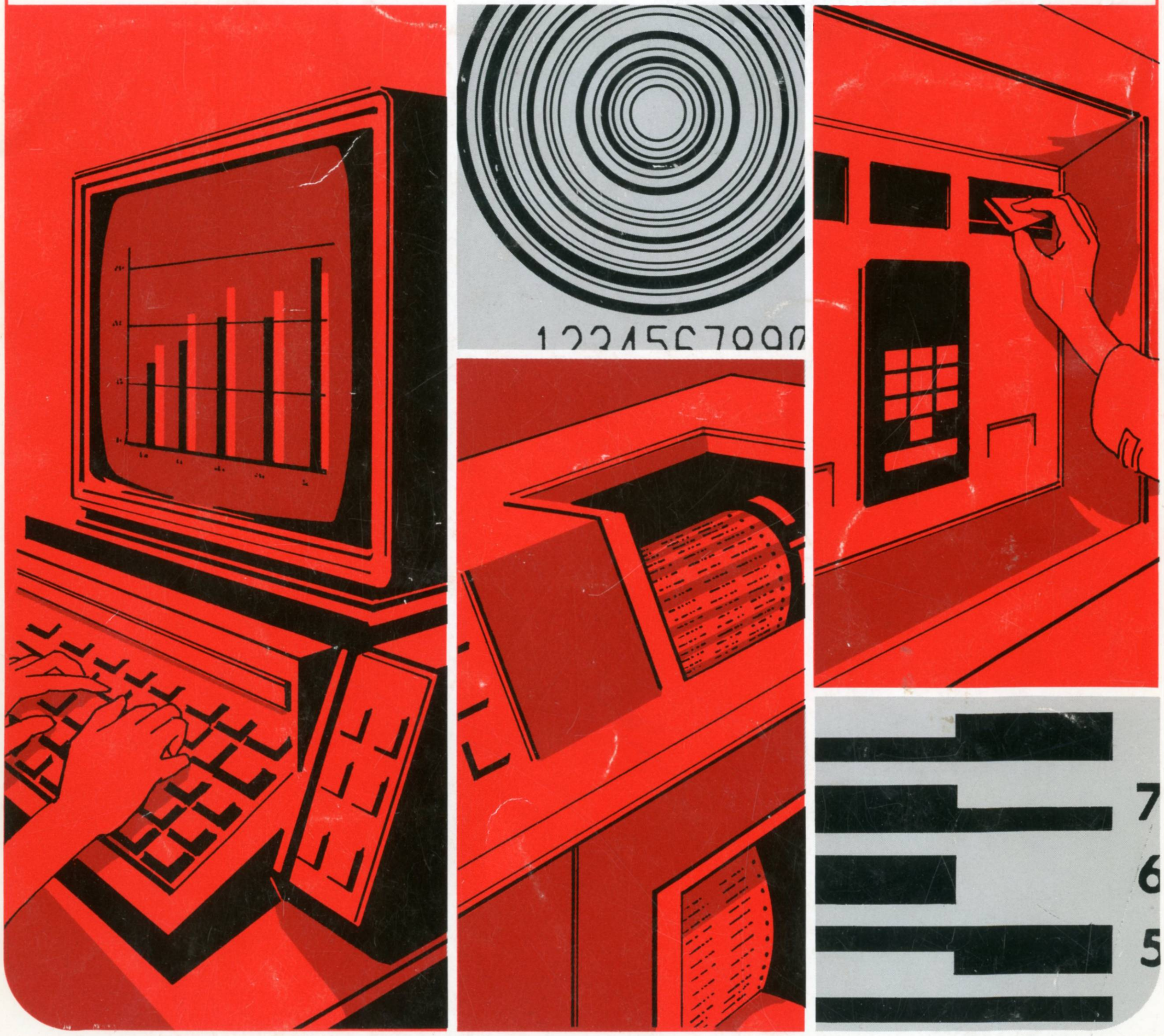
Audit considerations in electronic funds transfer systems; Computer services guidelines

Dana R. Richardson

COMPUTER SERVICES GUIDELINES

Audit Considerations in Electronic Funds Transfer Systems

American Institute of Certified Public Accountants AICPA



Notice to Readers

Computer services guidelines are published to assist members in understanding and utilizing various aspects of data processing. These guidelines represent the recommendations of the computer services executive committee on the various topics covered.

Prepared by

Auditing Electronic Funds Transfer Systems Task Force

Dana R. Richardson,
Chairman
Edward Arnold
John F. Kelly
John F. Lehman
James Loud
Ernst L. Schaefer, Jr.
Don L. Sneary

Carol Schaller, *Manager, Computer Services*

Approved by

Computer Services Executive Committee (1977–78)

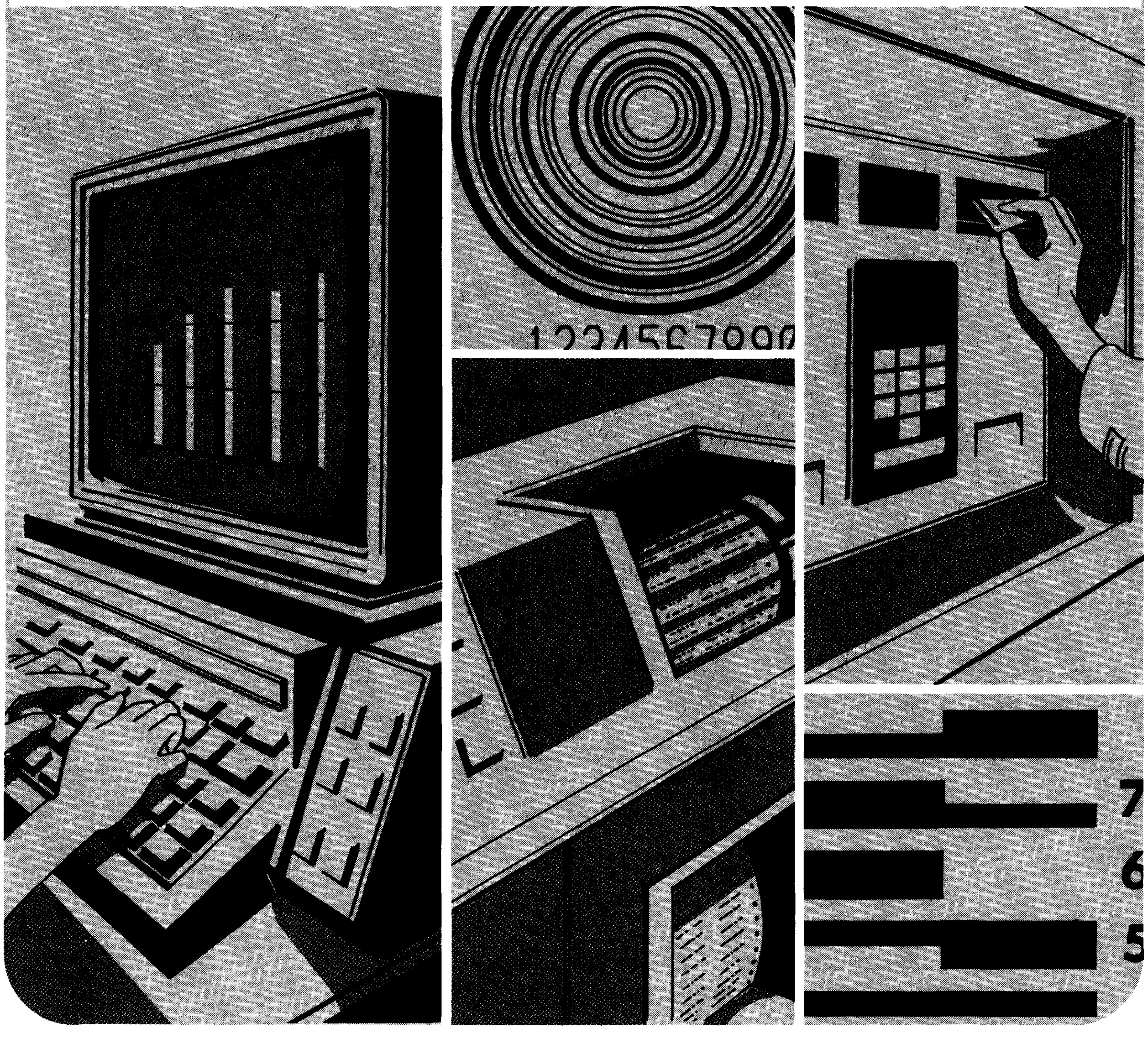
Richard J. Guiltinan,
Chairman
Lois L. Cohn
John P. Harrison
Karl G. King, III
Albert A. Koch
Richard F. Maginn
John W. Nuxall
Phillip A. Parker
William E. Perry
Walter D. Pugh
Joseph D. Wesselkamper

Donald L. Adams, *Managing Director*
Administrative Services, AICPA
Paul H. Levine, *Manager, Computer Services*

COMPUTER SERVICES GUIDELINES

Audit Considerations in Electronic Funds Transfer Systems

American Institute of Certified Public Accountants AICPA



1211 Avenue of the Americas, New York, N.Y. 10036
First Impression 1978

Contents

PREFACE **v**

THE NATURE OF EFTS

Definition **1**

Impact of EFTS **1**

Types of EFT Systems **2**

THE CURRENT STATUS OF EFTS REGULATIONS

Current Guidelines for National Banks **8**

Current Guidelines for Federal Savings and Loan Associations **10**

Current Legislation for State Financial Institutions **11**

Summary **12**

EFTS AND THE LEGAL ENVIRONMENT

Are Remote-Banking Terminals Branches? **13**

What Are the Antitrust Implications of Shared EFT Networks and Terminals? **14**

How Will Consumer Privacy Be Protected? **15**

Who Will Be Liable for EFTS Errors or Irregularities? **16**

Summary **16**

INTERNAL CONTROL CONSIDERATIONS IN EFT SYSTEMS

The Extent of the Client's System **17**

Controls in EFT Systems **19**

Physical Security **21**

Application Controls **21**

Study and Evaluation of Internal Control in EFT Systems **23**

Summary **24**

Preface

Almost 37 billion checks will be written per year by 1980 to pay personal, commercial, and governmental obligations. During recent years, financial institutions have been experimenting with and, in many cases, implementing new systems designed to reduce the need for "paper based" payments. Through the application of computer and communications technologies, these institutions are developing systems that transfer funds electronically rather than physically—electronic funds transfer systems (EFTS).

Initially, these new systems were limited in terms of the services provided and restricted in geographical area and so did not figure clearly in the future of electronic banking. Today, however, these systems are growing rapidly and are impacting far larger numbers of consumers and businesses, as the following examples illustrate. A large New York bank recently installed approximately five hundred remote-banking terminals throughout its branch network, and an additional 3,500 terminals in retail stores. In California, a new centralized switching network is being installed on a cooperative basis by a group of ninety-two savings and loan associations to allow the transfer of funds between participating merchants' and customers' savings accounts. Similar networks have been formed in several other states. And, as a final example, thirty-two separate automated clearing houses currently are clearing funds transactions electronically rather than through the physical movement of paper payment instruments.

EFT systems do not employ totally new technology, but rather, adapt existing technology to provide a new method for exchanges of value. This adaptation does not represent a revolutionary, but rather an evolutionary, change in auditing requirements or procedures.

These and other current developments as well as the potential for changes in the near future have led to the development of this paper. The computer services executive committee of the AICPA requested it to ascertain the state of the art in electronic funds transfer systems and to determine the impact these systems will have on the audits of business entities involved in EFTS.

This guide is divided into four chapters. The first chapter addresses the nature of EFT systems and provides background information on EFTS; chapters 2 and 3 cover the current status of EFTS in government and the legal community, respectively; and the final chapter discusses the task force's initial assessment of the audit impacts of EFT systems and is designed to present comments and suggestions for further research and professional deliberation.

Chapter 1

The Nature of EFTS

A key to any economy's success is the proper functioning of one or more payment systems to provide the means for conducting exchanges of value. In most modern societies, these involve exchanges of goods and services for money. In recent years, substitutes for money, such as checks or other promissory obligations in the form of credit, have become popular. Travelers' checks, money orders, telegraph transfers, and letters of credit all have special characteristics as payment mechanisms. The unique characteristics of payment mechanisms and their various levels of acceptance impact their use.

Definition

Electronic funds transfer systems are another, potentially more complex, payment mechanism. Broadly speaking, electronic funds transfer systems are payment systems in which the processing and communications to effect economic exchange, and the processing and communications for the production and distribution of services incidental or related to economic exchange, are both dependent wholly or in large part on the use of electronics. At a more technical level, an EFT system can be defined as a computer-based network that enables payment-system transactions to be initiated, approved, executed, and recorded with electronic impulses and machine-sensible data, rather than with paper.

Impact of EFTS

In most electronic payment systems, the goal is to reduce the number of paper-based transactions and thereby reduce the overall cost of handling all transactions. This move toward electronically based transactions will have major impacts on the business community, financial institutions, consumers, and, certainly, the certified public accountant.

The *business community* will find that the new technology in the payment process will provide not only the potential for decreased costs of processing but also a potential risk of misappropriation of funds through the electronic network.

Industry will likely find a reduction in bad debt expense. Certainly, many members of the banking community are looking at the new electronic payment systems for their potential to reduce the float currently provided to checking account customers. However, *financial institutions* will have to consider the significant cost to develop the EFT systems.

The *consumer* is an important link in most EFT systems because customer acceptance of EFTS is crucial to success. Such acceptance can come only through increased awareness and an understanding of the potential advantages and disadvantages inherent in such systems. Disadvantages center around consumers' perceived loss of control over the payment process and the potential for lost privacy with respect to personal financial information. EFT does, however, provide several advantages: Convenience and lower costs are important positive considerations as are the reduced need to carry large amounts of cash, the elimination of personal bank reconciliations, and fewer "bills" to pay by check each month. The consumers' costs associated with the payment process can be reduced with EFT systems. Fewer bills mean less postage and a potential reduction in checking account charges and check printing costs.

Finally, the *CPA* providing audit services to a client who either uses or maintains an electronic payment system will find significant impacts in the nature of auditing procedures currently performed within paper-based payment systems. Often no "visible" audit trail will be provided by management to the auditor. Tomorrow's auditor will have to bring new and creative auditing techniques and concepts to an EFTS environment.

Types of EFT Systems

Electronic funds transfer systems can be grouped into three major functional areas:

- Remote-banking services
- Retail point-of-sale services
- Direct-deposit and preauthorized payment services

All three types of systems involve computer technology to perform part or all of the payment and/or funds transfer functions. In both remote-banking and point-of-sale systems, remote computer terminal devices are connected to one or more computer systems through a leased-line and/or direct-dial telephone communications network. Direct-deposit and preauthorized payment systems closely resemble traditional batch processing systems with one exception: Once the transactions have been processed by the originating financial institution, they are cleared and settled electronically through an automated clearing house (ACH) rather than through the traditional paper-based clearing house. Each of three types of EFT systems is discussed in more detail below.

Remote-Banking Services. These services are provided through the use of remote-banking terminals or touch-tone telephones. Remote-banking terminals are called *automated teller machines* (ATMs), *customer/bank communications terminals* (CBCTs) or *remote service units* (RSUs). The functions that are normally performed by remote-banking EFT systems can be divided into five categories, depending on whether the system uses terminal devices (terminal systems) or touch-tone telephones (automated telephone payment systems). See table below.

Terminal systems can provide twenty-four-hour banking services in a variety of locations. The customer inserts a plastic card into the terminal and enters data for a specific transaction. Usually, the first piece of data entered is a *personal identification number* (PIN). The EFT system uses this number to assure that the holder of the plastic card is its authorized user. After the PIN number, the customer enters an amount and depresses a function key (specifying the type of function to be performed—deposit, withdrawal, and so forth).

Once all the appropriate validation procedures for the transaction have been completed, the terminal either issues cash (in the case of a cash withdrawal) or a receipt (in the case of a deposit, transfer, or other function), and then returns the plastic card to the customer.

At various points in the transaction, the terminal can communicate with a central computer system. If the central computer services a specific financial institution, the system is called a *proprietary EFT system;* see exhibit 1-1 for a graphic illustration. If the central computer is a service center that switches messages and/or settles accounts for several financial institutions, the system is called a *switch system* (exhibit 1-2). The communications between the terminal and the central computer are usually over a leased-line telephone network. In most systems, the communication between the terminal and the central computer is scrambled or "encrypted" so that anyone trying to tap the telephone network will not be able to enter false transactions or obtain valid card numbers and their associated PIN numbers. In some systems, the terminal is not continuously connected to a central computer system but operates "off-line"; at the end of the day, it sends the day's data to the central facility via a communications network or other means.

Automated telephone payment systems allow the transfer of funds by telephone between a customer and a merchant through a financial institution. These systems also allow a customer to inquire about the status of an account with a financial institution. Some systems require voice communication with a teller; but, in others, the customer uses a touch-tone telephone to enter the data necessary to accomplish the desired transaction. The account number is entered along with the customer's PIN number. Participating merchants in the telephone payment system are identified by a special number, which is also entered. Finally, the amount of the transfer is entered. At several points during the transaction, the central computer system communicates with the customer.

Function	*Terminal Systems*	*Automated Telephone Payment Systems*
Deposits	X	
Withdrawals	X	
Transfers between accounts	X	X
Bill paying	X	X
Inquiry on account status	X	X

EXHIBIT 1-1
REMOTE BANKING–PROPRIETARY SYSTEM

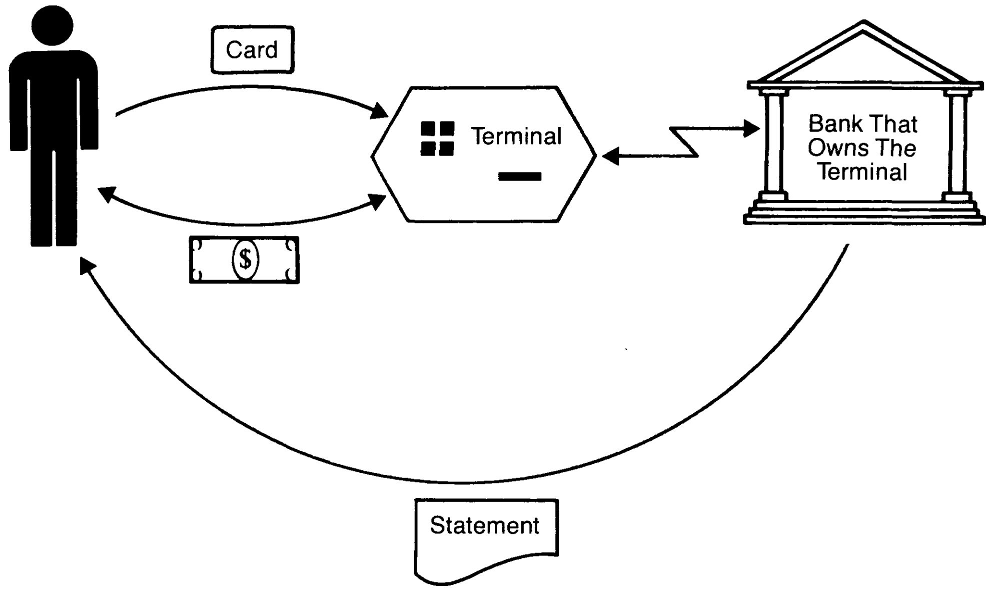
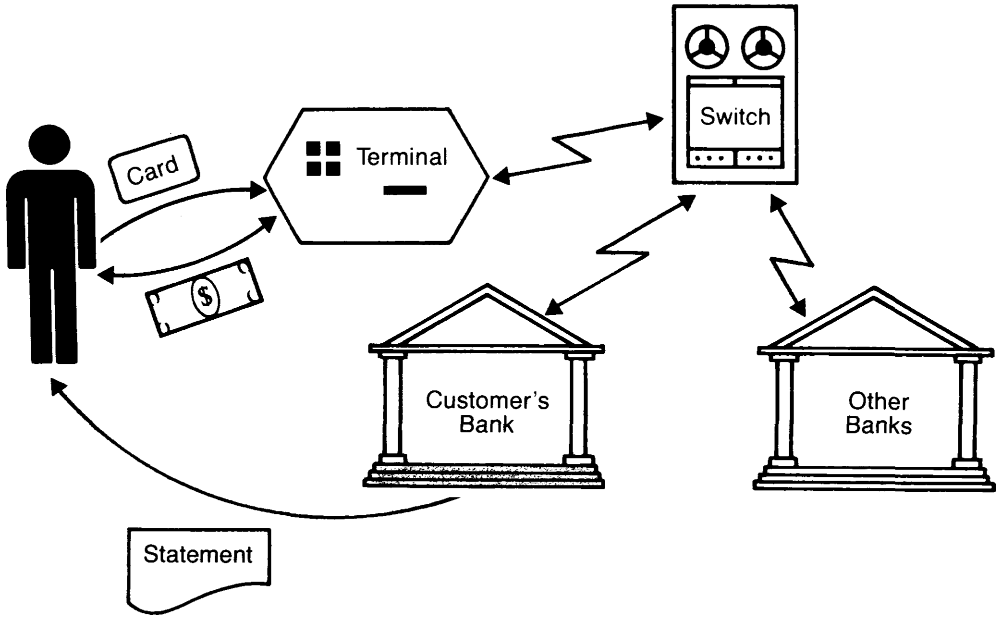


EXHIBIT 1-2
REMOTE BANKING–SWITCH SYSTEM



This is done with a *voice-response system,* which groups prerecorded words into meaningful phrases to confirm to the customer the data that has been entered into the system.

Retail Point-of-Sale Services. Retail EFT facilitates financial transactions in supermarkets and other retail outlets, through the use of electronics. Retail EFT services are provided through the use of *point-of-sale* (POS) terminals. These POS terminals can vary widely in their capabilities. The simplest of these devices verify or guarantee checks or perform credit card authorizations. The more sophisticated units will be used not only to capture sales and inventory data but also to transfer funds directly from a customer's account to the merchant's account without the use of paper-based means of exchange. (These systems will continue to issue a customer's receipt.) POS services can be grouped into three functions:

- Check verification/guarantee
- Funds transfer
- Data capture

Remote banking as described above may also take place in a retail environment.

Check Verification/Guarantee. This service (though not truly an EFT service) has been implemented in various forms for several years. In most early systems, the retail clerk used the customer's driver's license number and possibly one or more other sources of identification to verify a check. As check guarantee and check verification systems grew, this data was submitted to a central system by telephone and an oral authorization was obtained. In newer systems, a plastic card is entered into a POS terminal for direct communication with a central computer system. The central computer system transmits a simple electronic response back to the POS terminal, for example, to light a green signal of valid authorization or a red signal of "not approved." Some check-guarantee systems also transmit to the POS terminal an authorization code, which the retail clerk writes on the check.

Funds Transfer. Some retail POS systems can perform funds-transfer functions similar to remote-banking systems. These POS systems use a *debit card* to facilitate the transfer of funds from the customer's account to that of a merchant. The debit card, in essence, provides for a charge to a depository account (rather than extending credit, as *credit cards* do). The customer presents the debit card to the retail clerk, who enters the card into the POS terminal. On the customer's side of the terminal is an enclosed numeric-key pad, which the customer uses to enter the PIN number associated with the debit card. At this point, the transaction is handled just as it is by the remote-banking terminal for a funds-transfer transaction. The POS terminals are connected to the central computer through a leased-line telephone network. As with remote-banking services, the central computer can be either a proprietary EFT system or a switch system. Exhibit 1-3 contrasts the present method of paying for a purchase using a check with an EFT system using a central switch.

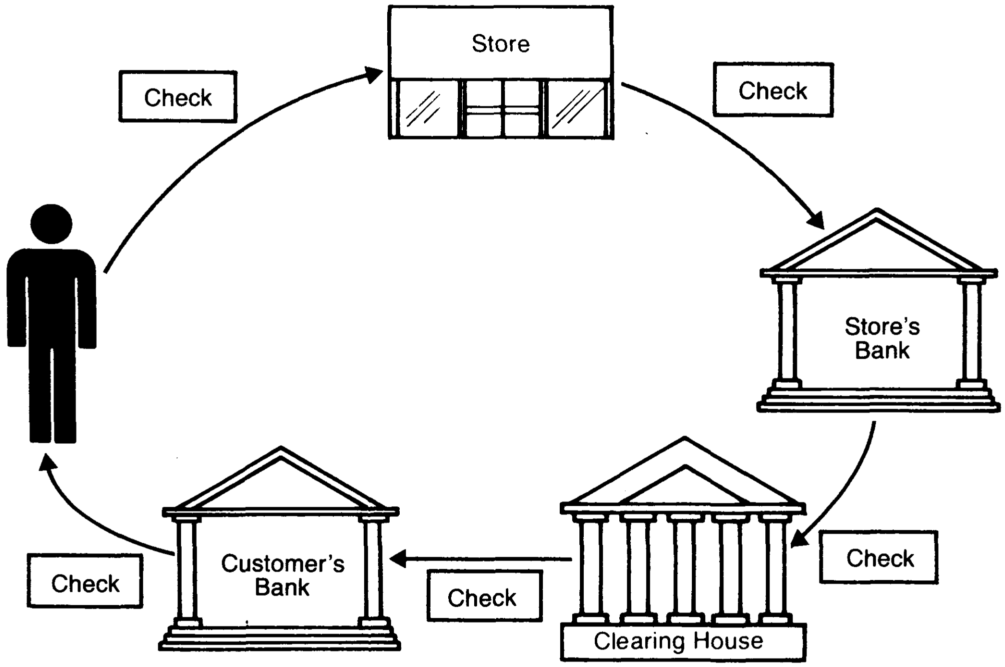
Data Capture. Several in-store retail computer systems have developed capabilities to enter product data through an electronic cash register. They capture inventory data as well as pricing and discount information. Most of these systems use a minicomputer located in the retail store. They can provide a natural extension of EFT services by incorporating POS terminal functions in existing electronic cash registers. These systems can use the independent minicomputer as a communications controller for the out-going and in-coming EFT transmissions.

Direct-Deposit and Preauthorized Payment Services. Direct-deposit and preauthorized payment systems are used to initiate and process recurring payments to and from customers electronically without manual intervention. These EFT systems, as mentioned earlier, closely resemble traditional batch processing systems. The difference in'these systems results from the substitution of electronic impulses for paper-payment mechanisms. Thus, instead of transporting a batch of paper documents to a conventional clearing house, electronic data are batched and forwarded to *automated clearing houses* (ACHs) for clearing and electronic settlement. Each system is described in more detail below.

Direct-Deposit. A direct-deposit system can be defined as a process in which payments are made directly to the recipient's depository account at a financial institution.

The direct-deposit process begins when the recipient issues a standing authorization to the paying organization ("payer"). Subsequently, as payment is due, the payer's system produces a machine-sensible credit, which is then forwarded to its financial institution. The payer's financial institution debits the payer's account, posts credits of recipients with accounts in that bank, and forwards the remaining credits to a clearing house for distribution to the other appropriate recipient's financial institution. The

EXHIBIT 1-3
PRESENT POINT-OF-SALE CHECK CYCLE



EFT POINT-OF-SALE FUNDS TRANSFER SYSTEM USING A CENTRAL SWITCH

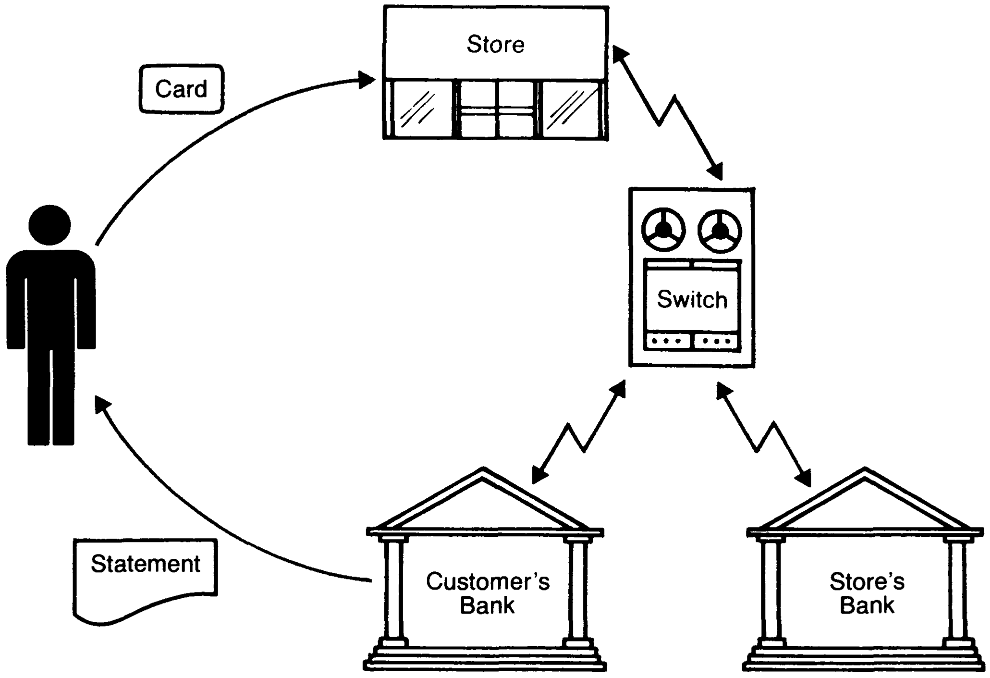
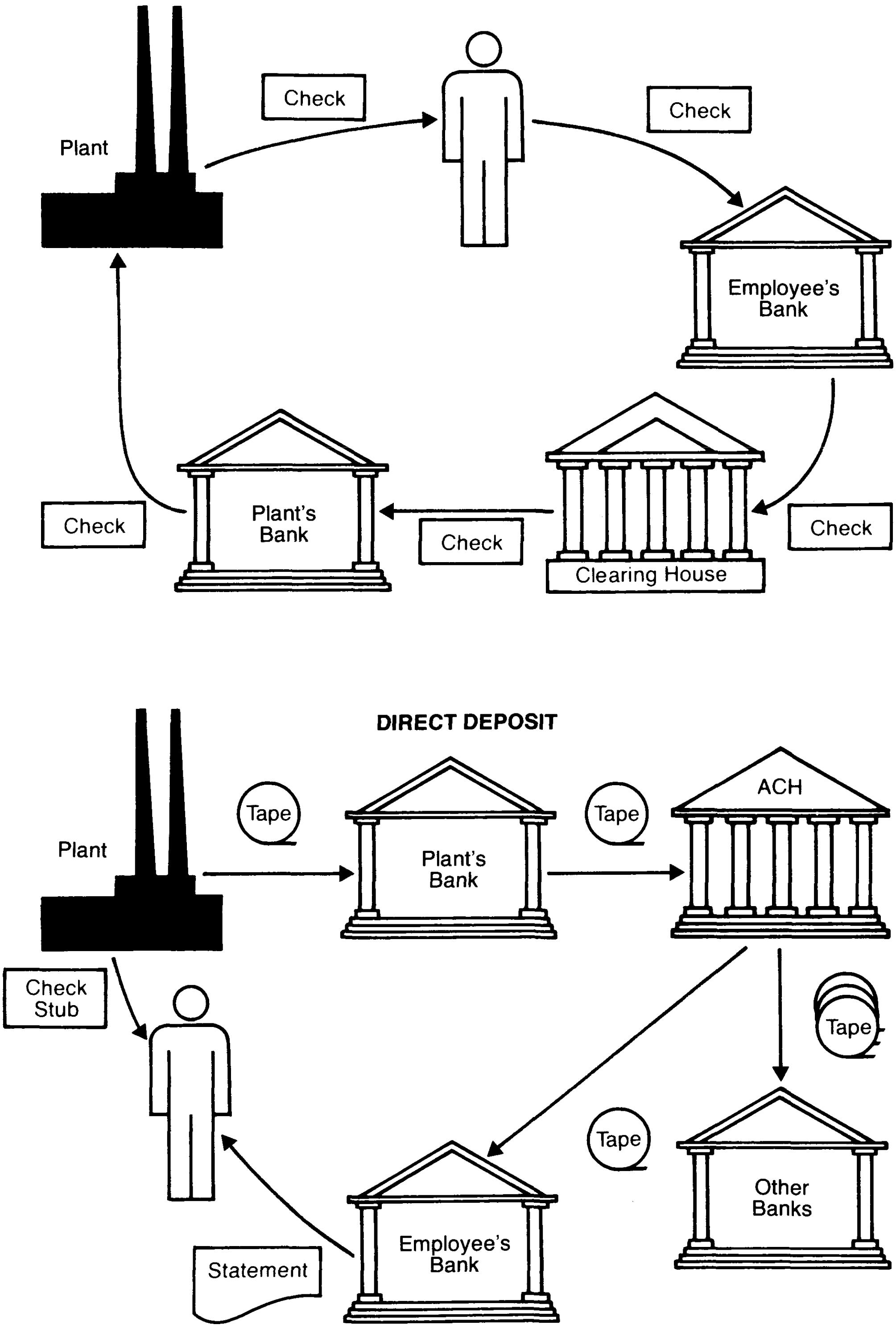


EXHIBIT 1-4
PRESENT PAYROLL CYCLE



DIRECT DEPOSIT

process is complete when the recipient's financial institution posts the credit to the recipient's deposit account. Exhibit 1-4 shows the present payroll cycle contrasted with the direct-deposit cycle.

Preauthorized Payments. A preauthorized payment system is a process in which recurring payments are paid directly by the payer's financial institution to the recipient's financial institution, without a negotiable paper document.

In a preauthorized payment system, the payer provides its financial institution with written authorization to pay one or more specific recurring bills. When the financial institution receives a bill, it verifies it using authorization master files that contain all the preauthorizations currently in effect. After validation and editing are complete, the bill payer's account is charged for the amount and a machine-sensible credit is generated and forwarded, if necessary, to an ACH for settlement.

A memorandum bill is usually sent to the bill payer showing the amount due and the date that it will be charged to the account. Various regulatory authorities have recommended that this notice be mailed one week before payment. The bill payer is responsible for ensuring that enough funds are available to the account to carry out the payment.

If bill payers question the amount of the memo bill, they can notify the financial institution to prevent any payment until the matter is settled. An individual is usually allowed the option to terminate participation in the program with relatively short notice. A record of payment is included in the bill payer's periodic account statement, which serves as a receipt.

A preauthorized payment plan, in addition to saving time and postage costs, also guarantees that the bill payer does not pay late charges in the event that the payment goes astray.

Chapter 2

The Current Status of EFTS Regulations

Government regulation of EFTS can be divided into several areas: national bank regulations, federal savings and loan regulations and examination guidelines, and state regulations for financial institutions. In addition, the National Credit Union Administration has recently proposed regulations in this area and Congress has been considering a number of bills addressing certain consumer issues.[1]

Current EFTS guidelines for national bank examiners are set forth in Banking Circular no. 66, issued April 16, 1976.[2] The circular emphasizes that the guidelines do not represent regulations, but merely the "current thinking" offered for the consideration of bank examiners reviewing EFT systems. The guidelines are primarily concerned with consumer safeguards and the security and systems integrity of terminal-network operations.

The current guidelines for federal savings and loan examiners are found in the Code of Federal Regulations, 12 C.F.R. 545.4-2, and the Federal Home Loan Bank Board Office of Examinations and Supervision's *Examination Objectives and Procedures (EOP) Manual,* section EOP-011. Section 545.4-2 deals primarily with consumer issues and physical security of remote facilities. The EOP manual sets forth guidelines and related review procedures for examiners reviewing EFT systems. The guidelines are concerned with evaluating the operating system and related physical security and accounting controls and with the planning and development process for the investment in the EFT system.

State legislation for EFTS facilities deals primarily with consumer protection and with competitive balance between federal and state chartered financial institutions, between large and small financial institutions, and between commercial and noncommercial banking institutions.

Current Guidelines for National Banks

The primary reference source for EFTS guidelines for national banks used in this discussion is Banking Circular no. 66, issued April 16, 1976. In the circular's cover letter addressed to the presidents of all national banks, James E. Smith, former comptroller of the currency, stated, in part:

> These guidelines are by no means regulations, nor are they to be interpreted as operating standards nor as static and timeless thoughts. They are simply representative of our current thinking and offered for your consideration as new systems are developed or existing systems reviewed.

The circular expresses two basic sets of concerns. The first represents the concerns expressed by consumer advocates, individuals, and various research groups and deals primarily with consumer rights and liabilities in EFTS. The second focuses attention on safeguarding the security and systems integrity of terminal-network operations. The following recommendations are those presented in the circular.

Consumer Guidelines. The circular discusses several major consumer guidelines. It states that the bank should assure its customers that it will use the personal and financial information collected by the EFT system only for banking purposes. The bank should not sell or divulge such information without the customers' written instructions unless it is legally required to do so or the situation is within accepted banking practices. When a national bank uses the services or computer systems

[1] Also, the Federal Reserve Board has promulgated regulation J, which governs the respective rights and liabilities of member banks using the Fed. Wire.

[2] *EFTS Guidelines,* Banking Circular no. 66 (Washington, D.C.: Comptroller of the Currency, 1976).

of another firm, a contract between the bank and such firm should indicate that any information compiled by the servicer must be treated with the same degree of confidentiality as transactions handled entirely within the bank.

Customers should be provided with the name and telephone number of the banking department to notify if they lose the card, find a statement error, or have complaints. At each terminal location, the bank should provide customer instructions in the event a transaction is denied at the point of sale. This will encourage the customer to determine the cause of the problem immediately when a transaction is denied and will reduce the potential for mistakes or adverse customer reaction. No account balance, specific overdraft information, or similar specific dollar amount information should be transmitted to a remote terminal operator other than a duly authorized bank employee or the customer. However, administrative information such as customer identification and instructions should be permitted.

Customers should be notified seven calendar days before processing any preauthorized debit transactions. This guideline allows the customer time to stop payment on otherwise preauthorized transactions.

The circular states that banks should develop reasonable procedures to prevent unauthorized withdrawals from customer accounts. Liability for such losses should be clearly stated in the contractual relationship between the bank and the customer. Although the circular states that the bank will bear the liability for such losses except in cases of customer fraud or negligence, federal law limits the liability of *credit card holders* to $50 regardless of whether or not the cardholder has been negligent.[3]

Card transactions should provide for adequate customer identification and authentication. The circular uses the example of personal identification numbers as an acceptable technique. Such a system should avoid use of numbers such as social security numbers or birth dates. The customer should be cautioned against writing the identification number on the card itself or giving it verbally to a terminal operator.

Security Guidelines. The circular discusses several important security guidelines. It recommends protection of data transmissions between terminals and the computer facility from external threats such as tapping, surveillance, and message insertion by security techniques such as message encryption.

Terminal and operator authentication codes should be used. If a retail electronic cash register is used as a terminal, the contract with the retailer should stipulate that an adequate audit trail will exist and that transactions can be adequately identified through an audit or edit routine within the retailer's system.

The circular has several guidelines regarding physical control over the use of personal identification numbers. They are primarily concerned with preventing unauthorized association of the identification number with the customer account number. Accordingly, the circular enumerates specific procedures, including retention cycles for tapes and print-outs used in the encoding of identification and account numbers, physical controls over the supply of blank cards and encoding equipment, and suggested procedures and policies for mailing and physical distribution of cards.

Automated teller machines that operate in an off-line mode should have files adequate to accommodate the "bad card" identification information for a period of two years or a period that reasonably exceeds the card expiration/reissue cycle, whichever is shorter. These files should be updated daily. The circular recommends conversion of off-line terminals to on-line as soon as is economically and operationally feasible.

Although specific guidelines are not set forth, the circular recommends that the physical controls over the computer room be at least as stringent as those provided for the terminal network. Segregation of functions should be enforced, and the systems should be fully documented and audited.

When a bank contemplates installation and operation of a banking facility in a non-bank commercial establishment, whether operated by the merchant or bank personnel, bank management should review the security devices and procedures in effect in the location before installation. Even though retail POS devices are not covered by the Bank Protection Act, the availability and accessibility of an alarm system should be considered. In case a POS system fails, the merchant should be aware of the backup procedures, applicable credit limits, and provisions for restoring service.

Although the circular does not discuss specific guidelines to detect fraud or criminal abuse, sufficient controls should be established over data flow in a multibank switching environment. The circular identifies message encryption as a recognized technique for this purpose; however, alternative techniques may become

[3] Note that federal law deals solely with individual consumers, rather than corporate users of EFTS.

available as a result of technological or systems innovation.

The bank should review its Bankers Blanket Bond coverage with its insurance carrier to determine whether and to what extent EFT systems are covered. Bank management and the board of directors should be fully aware of the potential liability assumed by the bank if it elects to self-insure.

Supervisory Action. The circular states that the examining staff of the office of the comptroller of the currency (OCC) will review bank-customer agreements and the underlying rights and liabilities of all parties in such contractual arrangements. Furthermore, security safeguards and operator procedures for terminal-network EFT systems will be reviewed in the same manner as other operating systems. The OCC will initiate corrective action where the examining staff detects consumer abuse of the system or imprudent procedures by the bank.

Current Emphasis of OCC. In two separate speeches in October and November of 1976, an official of the OCC emphasized current areas of concern over the control and planning functions of EFT systems. The OCC indicated that the circular was issued primarily in response to numerous requests for such guidelines from banks interested in developing EFT systems and to provide guidance in the development and improvement of EFT systems without the negative effects of additional regulations.

Major concerns of the OCC in EFT development are consumer acceptance and controls to protect consumers from fraud and abuse. The OCC official emphasized controls over custody and distribution of cards to prevent counterfeiting and unauthorized association of personal identification numbers with account numbers. Controls mentioned included dual control over the supply of cards, separate mailing of personal identification numbers and related cards, and encryption of identification numbers on plastic cards.

Also of major concern are the physical controls over computer hardware and software to detect and prevent unauthorized access to information or disruption due to sabotage or catastrophe. Controls in this area included encryption of messages from terminals to CPU, backup hardware facilities (including disaster plans), and adequate insurance coverage of EFTS transactions.

Current Guidelines for Federal Savings and Loan Associations

To date, federally chartered savings and loan associations have operated EFTS units as pilot projects under the authority of temporary regulations of the Federal Home Loan Bank Board (FHLBB). The FHLBB's official position regarding EFT systems has been set forth in the following:

- Code of Federal Regulations (the temporary EFTS regulations), section 545.4-2.
- The FHLBB office of examinations and supervision's *Examination Objectives and Procedures Manual,* section EOP-011.

In addition, part 563*a* of the C.F.R. insurance regulations, which deals with physical security in savings and loan offices, is incorporated by reference in section 545.4-2. A permanent regulation has replaced the temporary provisions of section 545.4-2 as of July 1, 1978. Certain of its provisions differ from those of the temporary EFTS regulation.

Section 545.4-2. The board's EFTS regulation, in both its temporary and permanent forms, authorizes the use of remote-banking terminals and describes minimum standards for physical security of these facilities. It also authorizes the FHLBB to require a financial institution to provide EFT services to other financial institutions under certain conditions. Although the FHLBB does not consider remote terminals to be branches or satellite facilities, as a matter of policy it has not permitted federally chartered financial institutions to establish facilities on an interstate basis. In addition, the FHLBB position on the "branch" issue is currently being litigated.

The physical controls over remote terminals are incorporated by reference to section 563*a* of the insurance regulations. Minimum physical security standards are presented in an appendix to section 563*a* and provide specific guidelines for the weight of the unit, thickness of the exterior walls of the unit, and tensile strength of the steel used in the unit. According to the section, the terminal "should also be designed so as to be protected against actuation by unauthorized persons, should be protected by a burglar alarm, and should be located in a well-lighted area."

EOP-011. This section of the EOP manual provides guidance to examiners reviewing EFT systems. The guidelines are primarily concerned with two phases of EFT systems:

- The propriety and reasonableness of the development process and investment in the system.
- The functional system and related physical security and accounting and control procedures.

The guidelines describe several considerations for the evaluation of an association's operating policies and practices:

- A feasibility and marketing study should be performed. Such a study should include a cost/benefit analysis, which should be updated on an on-going basis.
- The integrity, business history, and financial stability of hardware and software suppliers should be investigated.
- Safeguards should be built into the system to protect against over-withdrawals, provide adequate security over personal identification numbers, protect the main EDP system from penetration by taps into communication lines, and provide physically safe operating conditions for users and servicers of remote terminals.
- Written customer agreements outlining the terms of plastic card use, liability for unauthorized use, and conditions under which account information may be released to third parties should be developed.[4]
- Internal and procedural controls should be sufficient to provide an audit trail for transactions processed through the EFT system.

The guidelines also list examination objectives and procedures that are designed primarily to ensure that EFT systems follow FHLBB policies and regulations. Such procedures rely largely on the individual examiner's experience and judgment to evaluate the adequacy of the procedures and controls of the EFT system.

Recent Emphasis of FHLBB. As indicated above, on July 1, 1978, a permanent EFTS regulation has replaced the temporary provisions of section 545.4-2. The new regulation will include consumer protection provisions, clarify application procedures, and require federally chartered associations to take reasonable measures to secure adequate bonding and security. Both the temporary and permanent EFTS regulations contain a number of conditions for approving individual applications to operate remote terminals. However, as a matter of policy, the board will not approve an application for a remote terminal unless—

> before the applicant begins to operate its remote service unit system, it [has], to the satisfaction of the Board's staff, fulfill[ed] the following requirements:
>
> (1) Design[ed] the remote service unit system to provide for on-line real-time operation at all times that the remote service units at the merchant locations are operational, or otherwise provide[d] that financial transactions at a remote service unit result in instantaneous debits and credits to all affected accounts at the time the transaction occurs.
>
> (2) Design[ed] a settlement procedure with the merchants so that at no time will a merchant be the recipient of funds from the applicant which constitutes unsecured lending; and
>
> (3) Submit[ted] executed copies of all agreements between the applicant and each of the respective merchants concerning the remote service units.

Current Legislation for State Financial Institutions

The primary reference source used in this discussion of current legislation for state banks is a summary developed by the director for education and research of the Conference of State Bank Supervisors. The summary was issued in April, 1976, but the information contained in it is still reasonably accurate.

It appears that there is no uniform approach to EFTS legislation by the various states. The states take different positions with respect to such issues as (1) whether all or certain EFTS units are branches and subject to state restrictions on branching, (2) whether EFTS units may be manned by nonbank personnel, (3) whether all

[4] Effective July 1, 1978, this will be part of section 545.4-2, as well as the guidelines.

institutions must be allowed to share remote-banking terminals, and (4) whether additional regulation is required to protect the consumer.

Thirty-two states (as of May, 1978) have enacted legislation or have had regulatory interpretations that (1) allow electronic off-premise facilities and (2) do not consider such facilities branch banks. Of these thirty-two states, nineteen require some form of mandatory sharing of such facilities under specified conditions, eight states permit sharing facilities but do not require it, and five do not mention the sharing issue.[5]

Of the remaining eighteen states, seventeen view electronic off-premise facilities as branch banks under existing statute. One state, Nevada, has not taken any statutory or regulatory action regarding such facilities.

A review of examples of specific EFT legislation enacted by several states indicates some of the legislators' concerns: (1) enabling legislation for EFT systems for state chartered financial institutions allows such institutions to remain competitive with federally chartered financial institutions located within the state and with financial institutions in other states that allow EFT systems; (2) EFTS legislation can affect the competitive balance between commercial and noncommercial financial institutions; (3) the consumer's liability for fraud, theft, or unauthorized use of cards should have specific limits; (4) information gathered by EFT systems should be protected to the same degree of confidentiality as transactions handled entirely within the financial institution; (5) the competitive balance between large and small financial institutions should be maintained by allowing smaller institutions to share the EFT facilities of larger institutions, or by removing geographical limitations and/or capital requirements which otherwise apply to branches.

Summary

EFTS regulations enacted to date principally address consumer safeguards, competition among financial institutions, and system security and control. Most jurisdictions require regulatory approval for remote-banking terminals.

[5] *Analysis of Enacted EFTS State Legislation* (Washington, D.C.: American Bankers Association, May 1978).

Chapter 3

EFTS and the Legal Environment

Currently, several major legal issues involving EFTS remain to be resolved. These issues are being addressed by the courts, various regulatory authorities, and individual state legislatures. Overlapping responsibilities, and in some instances, conflicting decisions have contributed to the uncertainty. At the same time, the development of EFT systems has continued.

Congress realized that large EFT systems were in development and was aware of the potential problems; it, therefore, established the National Commission on Electronic Fund Transfers (NCEFT). The purpose of this commission was to develop recommendations for legislative action that would resolve the confusion and provide for consumer protection. On March 7, 1977, the commission published its preliminary recommendations and on October 28, 1977, it issued its final report. The NCEFT recommendations will have a significant impact on action taken by Congress as well as by other legal and regulatory authorities.

In this chapter, three of the major legal issues are discussed. Each has a brief explanation, followed by some of the related court cases and the recommendations of the NCEFT.

Are Remote-Banking Terminals Branches?

This issue is most significant in states that either (1) have more liberal branching provisions for one type of financial institution than for other institutions or (2) limit bank branching. The more liberal the branching laws, the less significant this issue. Consider a state, for example, which limits the number or the locations of a financial institution's branches (or which requires a high level of capital for each branch). If a remote-banking terminal is deemed not to be a branch, the financial institution may place terminals throughout the state, thus expanding their market area free of those restrictions or requirements.[6]

One aspect of the branching issue concerns the types of transactions terminals may handle without being considered branches. In several unit-banking states, a terminal can dispense cash, transfer money, and provide account balance information. However, the terminals are not permitted to accept deposits. Until recently, the comptroller had taken the position that remote banking terminals were not branches, but, in the cases described below, his position was challenged and ultimately rejected.

Terminals authorized by the FHLBB may perform deposit services, withdrawals, and transfers between accounts but may not be used to open new accounts. The regulations governing the terminals expressly state that the terminals are not to be deemed branches. As indicated below, this issue is being litigated. An additional issue exists with respect to federal savings and loan associations—namely, whether state EFTS legislation can supersede or supplement the FHLBB regulations.

The court cases to date have been primarily in unit-banking states and have primarily involved a challenge to the comptroller's definition of "branch" under the McFadden Act.[7] The McFadden Act applies only to commercial banks; thus, savings and loan associations and

[6] If a remote-banking terminal established by a national bank is deemed a branch, the comptroller must, under the McFadden Act, impose the same requirements for the establishment of the terminal as the state in which the financial institution is located imposes on its state chartered institutions.

[7] The McFadden Act is an amendment to the National Bank Act that describes a "branch" as including any additional office or branch or place of business where deposits are received, or checks paid, or money lent.

credit unions have had little legal restriction, at the federal level, on their remote terminals.

Related Court Cases. In *Independent Bankers Association of America (IBAA)* v. *James E. Smith, Comptroller of the Currency* (No. 75-0089, D.D.C. (Oct. 10, 1975)), the court of appeals upheld the district court's ban on remote-banking terminals. The comptroller was ordered to rescind a ruling that remote terminals were not branches and to consider them as branches subject under the McFadden Act to state branching restrictions. Other courts reached similar decisions, such as in *State of Missouri* v. *First National Bank of St. Louis* (No. 75-113, D. Mo. (Nov. '18, 1975)), and *State of Illinois* v. *Continental National Bank and State of Illinois* v. *First National Bank of Chicago* (409 F. Supp. 1167, N. D. Ill. (Dec. 10, 1975)).

In an Oklahoma case decided on December 23, 1975, however, the court upheld the comptroller of the currency's interpretive ruling that the terminals are not branches and thus can be deployed remotely and offer a full line of services including deposits.

On October 4, 1976, the Supreme Court refused to hear an appeal of *Independent Bankers Association* v. *James E. Smith, Comptroller of the Currency; State of Illinois* v. *Continental National Bank,* and *State of Illinois* v. *First National Bank of Chicago,* thereby permitting the lower court decisions to remain in place. The Illinois banks and eventually the First National Bank of St. Louis were required to discontinue use of their remote-banking terminals.

The FHLBB's regulations were challenged in *Bloomfield Federal Savings and Loan Association* v. *American Community Stores Corp.,* 396 F. Supp. 384 (D. Neb. 1975). In this case, a federal savings and loan association sued a retail store, the FHLBB, and the board members, challenging the validity of the FHLBB's temporary regulation governing remote-banking terminals. The plaintiffs contended that the board had exceeded its statutory authority in promulgating the regulation, and that the board did not obey its own office-location regulations in authorizing remote terminals. The Nebraska federal district court upheld the FHLBB, finding that its statutory authority was broad enough to encompass issuance of the regulations and that the office-location rules only applied to savings and loan branches, and, by the court's interpretation of previous regulations as well as according to the temporary regulation, remote-banking terminals are not branch offices.

The regulations have also been challenged in *Independent Bankers Association of America* v. *Federal Home Loan Bank Board,* No. 76-0105 (D.D.C., filed Jan. 19, 1976). The case is still pending.

Recommendations of the NCEFT. The NCEFT recommends allowing depository institutions to deploy their terminals for all typical banking transactions, including the acceptance of deposits, anywhere within a state. In addition, the terminals could also be deployed and provide the same services to contiguous states within the depository institution's natural market area.

Nondepository institutions, such as retailers and supermarkets who allow their customers to use terminals to communicate with depository institutions, should not be considered to be regulated depository institutions. Thus, they would not fall under the jurisdiction of the Federal Reserve Board, comptroller of the currency or other regulatory body.

What Are the Antitrust Implications of Shared EFT Networks and Terminals?

In many cases, remote-banking terminals and merchant point-of-sale terminals have been deployed on a shared basis. Essentially, there are two types of shared networks. In one case, a single financial institution develops the system and makes it available to other financial institutions for a "per transaction" fee. Another approach has been the joint development and operation by a group of financial institutions. Both approaches have caused some concern about the impact of a small number of shared EFT networks versus a larger number of competing networks. The major concern is that large shared or cooperative networks may not provide sufficient competition to ensure high quality services and the lowest possible prices to the consumer and merchant. An additional concern is that large financial institutions will establish EFT networks and not allow smaller institutions to join, thus diminishing their ability to compete.

Related Court Cases. Most of the legal activity concerning mandatory sharing has occurred within state legislatures and the Justice Department. The American Bankers Association noted in *Analysis of Enacted EFTS*

State Legislation that nineteen states have some form of mandatory sharing legislation.[8]

The Justice Department has urged both the Federal Reserve Board and the FHLBB to minimize their efforts in the area of POS to encourage competition among the financial institutions.

On March 7, 1977, the Justice Department outlined its antitrust objections to the Nebraska Electronic Transfer System (NETS). The primary objections were:

1. As of October, 1977, NETS membership represented 86 percent of all commercial deposits, and it was expected to approach 100 percent. The Justice Department's available evidence did not support the necessity of an all-encompassing joint venture.
2. The system was designed to retard individual member initiative by requiring that all services be designed collectively and that terminals bear no corporate identification of the installer.
3. All commercial banks were allowed to join and were required to share terminals; however, savings and loan associations and credit unions were precluded from participating.

The NETS board stated that they intended to continue the program and will determine how to comply.

Recommendations of the NCEFT. According to the NCEFT, shared EFT systems should be established on a pro-competitive basis that provides free choice within federal antitrust laws. Decisions whether or not the network is pro-competitive should be made individually, based upon—

1. The feasibility and likelihood that two or more competing networks could be developed in the same area.
2. The effect on actual or potential competition in the market.

How Will Consumer Privacy Be Protected?

The privacy of the individual is becoming an increasingly important issue. The major concern is unauthorized storage of and access to personal data gathered by banks, insurance companies, credit bureaus, government, and other institutions. Problems relate to the unauthorized access to data, provision of incorrect or out-of-date information, and the unauthorized sale of name lists and other personal data. The advent of EFT systems and expanded technological capabilities provide the potential for even greater problems. EFT systems will be able to capture most of an individual's financial transactions at the place and time they occur. Expanded technological capabilities will make possible the storage and rapid retrieval of this massive amount of data.

Related Court Cases. In the case of *California Bankers Association* v. *Shultz* (416 U.S. 21, 39 (1974)), the Supreme Court upheld the constitutionality of the Bank Secrecy Act and found that the act's recordkeeping provisions did not violate the individual's Fourth and Fifth Amendment rights. The Bank Secrecy Act requires substantial collection, storage, and reporting of individual financial data by financial institutions. The law was enacted to enable law enforcement agencies to summon the individual's financial information without notifying the subject of the inquiry.

In the case of *United States* v. *Miller* (425 U.S. 435 (1976)), the Supreme Court denied that an individual has a constitutionally protected interest in transaction information maintained by his depository institution, holding that the information was freely given and that it is the property of the financial institution.

Recommendations of the NCEFT. The NCEFT recommends enacting federal legislation to grant individuals the right to contest any government access to their financial information, and to provide prior notification to individuals of any subpoena or summons to access information. This legislation should consider law enforcement and other government requirements.

Additional legislation should be enacted to prevent third-party private sector use of information concerning a consumer's depository account without specific consent except for the information necessary to verify or complete a transaction.

[8] *Analysis of Enacted EFTS State Legislation* (Washington, D.C.: American Bankers Association, May 1978).

Who Will Be Liable for EFTS Errors or Irregularities?

Under the Uniform Commercial Code (UCC), which covers paper-based payment systems, there are specific rules governing the liability of the bank or consumer in the event of an error, irregularity, or fraud. The consumer assumes no liability for fraudulent checks, for example, unless there is proof of negligence and the negligence substantially contributed to the loss.

The UCC's application to the new electronic payment systems is unclear at best. As a result, the rights and liabilities of the respective parties of an EFTS transaction are unresolved in the absence of specific contractual agreement. In many instances, contracts between the providers and users of EFT services either absolve the provider of all liability or fail to address the issue at all. On the individual consumer level, however, existing or pending legislation allocates primary responsibility (and liability) for errors or irregularities to the financial institution providing the EFT service. The 1970 amendments to the Truth in Lending Act limited the consumer's liability on credit cards to $50. Although those provisions do not cover debit cards, pending legislation would extend them to debit cards.

Recommendations of the NCEFT. The NCEFT recommends that the depository institution should be liable for erroneous, unauthorized, or fraudulent use of an account unless the depository institution can demonstrate its use of reasonable care and that consumer negligence or fraud substantially contributed to the act.

The consumer who reports to the depository institution the loss of a card, compromise of an identification code, or unauthorized use, shall not be liable for unauthorized transactions from *the same source* occurring thereafter but may be liable without any ceiling for losses occurring before notification. The consumer has the responsibility to examine statements and to report errors or irregularities to the depository institution within a reasonable amount of time. Failure to report would make the consumer bear the loss if the depository institution had acted with due care. Contrary to the NCEFT's recommendation, the pending legislation would limit the consumer's liability to $50 for unauthorized transactions occurring before or after his notification to the depository institution.

Summary

Several legal issues related to electronic funds transfer systems have not been completely resolved. However, NCEFT recommendations will provide at least the starting point from which consistent legislation can be developed. The Justice Department and NCEFT emphasis on competition should insure that consumer acceptance or rejection will have a significant impact on the eventual design of the EFT products and their pricing.

Chapter 4

Internal Control Considerations in EFT Systems

The Extent of the Client's System

EFTS can connect many different organizations into one vast system. The auditor of each organization must consider what portions of EFT systems are a part of his client's system of internal accounting controls. Statement on Auditing Standards no. 3, paragraph 24, defines the extent of the client's system of internal control and auditor's review of that system as follows:

> An auditor's review of the client's system of accounting control should encompass all significant and relevant manual, mechanical, and EDP activities and the interrelationship between EDP and user departments. The review should comprehend both the control procedures related to transactions from origination or source to recording in the accounting records and the control procedures related to recorded accountability for assets.[9]

SAS no. 3 also states that "the preliminary phase of an auditor's review should be designed to provide an understanding of the flow of transactions through the accounting system. . . ." [10] The problem in EFT systems is determining where the "flow of transactions" for a particular organization starts and stops. SAS no. 1 states that—

> Transactions include exchange of assets or services with parties outside the business entity and transfers or use of assets or services within it. The primary functions involved in the flow of transactions and related assets include authorization, execution, and recording of transactions and the accountability for resulting assets.[11]

In EFT systems, the point at which authorization for the transaction occurs and assets or services are exchanged will determine the outer boundary of the client's flow of transactions. Therefore, the client's system would encompass all aspects of the system from the point of origination through recording in the books of account (including, if applicable, notification to the customer by statement or other means). This extent may vary based on the types of transactions processed by the EFT system.

The following discussion will address the potential impact on the extent of the client's system of internal control of each of the following categories of the EFT systems and their related transactions: remote-banking services, retail point-of-sale services, and direct-deposit/preauthorized payment services.

Remote-Banking Services. The most prevalent transactions in remote-banking EFT systems are deposits and withdrawals. In both cases, an exchange of assets occurs at the terminal. Because this exchange occurs at the terminal itself, all portions of the EFT system linking the terminal to the financial institution's computer would be considered part of the financial institution's overall system. Both bill payment transactions and transfers between accounts represent some combination of a deposit and withdrawal and therefore are accounting transactions that originate at the remote-banking terminal.

Remote-banking terminals do, in some cases, provide for customer inquiry about account status and/or balance. Technically, such activity is not an accounting transaction because it does not involve an exchange of assets or services. However, inquiries do represent a potential exposure to the financial institution because of possible misuse of the information obtained by such inquiries.

[9] *The Effects of EDP on the Auditor's Study and Evaluation of Internal Control,* SAS no. 3, in *Professional Standards,* vol. 1, AU sec. 321.24 (New York: AICPA, 1975).

[10] *Ibid,* AU sec. 321.25.

[11] *The Auditor's Study and Evaluation of Internal Control,* SAS no. 1, in *Professional Standards,* vol. 1, AU sec. 320.20 (New York: AICPA, 1974).

Retail Point-of-Sale Services. As mentioned earlier, retail POS services include check verification, check guarantee, and funds transfer for purchases and returns. Check verification activities are not accounting transactions between the customer and the financial institution because no exchange of assets or services occurs. Such activity is, in essence, an inquiry to some portion of an EFT system. The check guarantee process may or may not result in an accounting transaction. Those guarantee functions that do *not* encumber a customer's account for the amount of the check are inquiries, not accounting transactions between the customer and the financial institution. However, those POS systems that interact directly with a financial institution to encumber or place a hold on the customer's account for the amount of the check would, in fact, result in an accounting transaction. In theory, such transactions represent the transfer of funds between a customer's account and the financial institution's holding account. In such systems, the financial institution has covered its future liability to pay the paper instrument by assuring that funds available at the time of the guarantee are not subsequently withdrawn, transferred by the customer, or used for other purposes.

In either the check verification or check guarantee process, the agreement between the POS merchant and one or more other participants in the EFT system may require a fee for the process of check verification or guarantee. The extent of the financial institution's accounting system for these fee transactions would depend on the portions of the EFT system involved in generating both the revenue and receivable portions of the transaction.

Retail POS systems also allow direct funds transfer for the purchase and/or return of goods. Funds transfers are accounting transactions because they too involve an exchange of assets or services. These transactions differ slightly from those previously discussed in that more than one transaction within the EFT system is involved. For example, a purchase would generally involve three separate transactions:

- A transaction between the customer and his or her financial institution to remove payment funds from a depository account.
- A transaction between the merchant and the customer involving the receipt of goods or services for the corresponding payment.
- A transaction between the merchant and the merchant's financial institution for the deposit of the funds.

The boundaries of the retail merchant's system of internal accounting control have not changed with the introduction of the EFT system. The retailer has another means of payment but has not extended his system. The boundaries of the financial institution's system have been extended to the remote terminal where accounting transactions are initiated. Neither the financial institution portion nor the terminal portion of the system is part of the switch's system of internal accounting control because none of the transactions processed through the EFT system are recorded on the books of record for the switch.

Direct-Deposit/Preauthorized Payment Services. As discussed in chapter 1, direct deposits and preauthorized payments are processed through an automated clearing house (ACH). The ACH functions in the clearing process by receiving deposits or payments in machine-sensible form from a member financial institution. The information received is similar to the information magnetically encoded on a check. The computer at the ACH sorts the deposits and payments by bank number and forwards them to the appropriate financial institution, again in machine-sensible form. The function of the ACH is essentially the same as the function performed by the Federal Reserve System in the clearing of paper checks.

The financial institution's system of internal accounting control begins with the payments or deposits received from its customer and ends with the sending of machine-sensible deposits and payments to the ACH and the recording of the transaction in the books of record (including the amount due to or due from the ACH).

The customer's system of internal accounting control ends when deposits or payments in machine-sensible form are sent to the financial institution and the transaction has been recorded in the customer's books of record.

For both direct-deposit and preauthorized payment transactions, the EFT system does not change the extent of any client's system; rather, it provides a new mode of payment or deposit. In essence, a business entity presenting machine-sensible deposit or payment transactions to its financial institution is effecting an exchange of assets between itself and the financial institution. For example, a local utility company could collect cash or checks over the counter and transmit those payments to its financial institution as a deposit. Similarily, the utility company could present its financial institution with a file of machine-sensible preauthorized payment transactions which are, in effect, the same payments in a form other than cash or checks. The deposit is the same, regardless of the form.

The above discussion has described the most common activities and transactions involved in EFT systems today. Clearly,as EFT technology evolves, the auditor will need to consider the functions performed by the EFT system in which the client participates. These functions will determine the extent of the client's system and, thus, the nature and extent of the auditor's review.

Controls in EFT Systems

Although the objectives and essential characteristics of accounting control do not change with the method of data processing, the organization and control procedures used in EFT systems may differ from those used in manual systems or less complex EDP systems.

According to SAS no. 3, the two basic types of EDP accounting control procedures are (1) general controls, which relate to all EDP activities and (2) application controls, which relate to specific accounting tasks. The AICPA audit and accounting guide, *The Auditor's Study and Evaluation of Internal Control in EDP Systems* (1977) relates to batch-oriented systems and discusses these two control categories, listing basic controls. The guide provides an explanation of the purpose of each control, suggests audit procedures and compliance tests, and discusses the possible audit effects of a weakness in each control area. Although many of the control objectives and techniques are applicable to EFT systems, this chapter does not repeat that discussion. Rather, this chapter covers

1. Aspects of the controls that differ between batch-oriented systems and EFT systems.
2. Controls that change in significance in EFT systems.
3. New control elements not included in the audit and accounting guide.

General Controls. The guide classifies general controls as follows:

1. Organization and operation controls
2. Systems development and documentation controls
3. Hardware and systems software controls
4. Access controls
5. Data and procedural controls

Organization and Operation Controls. The controls in this category involve (1) segregation of functions between the EDP department and users, (2) provision for general authorization over the execution of transactions (for example, prohibiting the EDP department from initiating or authorizing transactions), and (3) segregation of functions within the EDP department. These controls have greater significance in an EFTS environment because the output of transactions is often cash or the distribution of goods or services.

Plastic cards and PIN numbers should not be issued by computer programmers or operators. Programmers and operators may be able to use their knowledge of the system to circumvent control procedures or programmed controls. Similarly, POS system personnel who are responsible for assisting merchants with authorization when the merchants' terminals are inoperative should not be computer programmers or operators.

Because of the sensitive nature of the information in an EFT system, segregation of functions should also be considered in systems development. Control is enhanced if no one individual has a complete, detailed knowledge of and access to an entire EFT application.

Systems Development and Documentation Controls. These general controls relate to (1) the review, test, and approval of new systems, (2) control over program changes, and (3) documentation procedures. Areas of particular importance in EFT systems include—

- Testing of new financial institution interfaces (for example, between the bank and the switch).
- Testing of new terminal interfaces to the switch.
- Testing of new application features at the switch that impact internal processing at the financial institution (that is, new transactions that require new control procedures).

In addition, there is an even greater need to monitor and control program changes in EFT systems.

Hardware and Systems Software Controls. The control features inherent in the computer hardware, operating system, and other supporting software should be used to the maximum possible extent to provide control over operations and to detect and report hardware malfunctions.[12] This control category has increased importance in systems involving data communications. Transmission error detection methods between financial institutions and remote terminals should be employed. In addition, transmission should include time and date coding, transaction sequence numbers, employee identification codes, and terminal and merchant authorization codes, if applicable.

Access Controls. Access controls provide safeguards over the use of documentation, data files and programs, and the computer hardware itself. Access limitations are important, not only to prevent unauthorized transactions, but also to meet privacy requirements. Customer account numbers, account balances, and account relationships should not be made available to merchants or other third parties, except as provided by law. Controls should be established to prevent one financial institution from accessing another's data, or one user from accessing another user's data.

Distribution and handling of plastic cards should be carefully controlled. User cards should be mailed only to existing customers. Supplies of blank cards and equipment used to personalize cards should be guarded and subject to restricted access. In systems where institutions share terminals, cards for all member institutions must be accepted by the same units. The card construction therefore should be nearly identical. Accordingly, each member institution should agree to procedures to exercise proper control over the manufacture, storage, and distribution of the cards.

Another consideration is access to the system through the use of unauthorized equipment. For example, telephone lines are the usual communication link between on-line remote-banking terminals and the financial institution's data processing facility; however, telephone lines are susceptible to wire taps. The system could be protected by disguising transmissions between the terminal and CPU and by positive identification of the transmitting terminal. The National Bureau of Standards and various terminal vendors have devised encryption algorithms. Such codes require a significant amount of time to decipher, unless an appropriate decoder is used. Positive terminal identification can be accomplished by the use of answerback code transmission.

Access control over both the PIN encoding algorithms and tables and the communication line encryption algorithms should be strictly enforced. They should be confidential, and, if possible, changed frequently.

Although physical security practices vary, many terminals are unguarded twenty-four hours a day. Accordingly, the units should be strong and secure enough to prevent physical penetration. Federal regulatory authorities have prescribed specific minimum physical standards for remote-banking terminals.

POS terminals, which are smaller and more portable than remote-banking terminals, require different security systems. In addition to other controls, physical access to POS devices should be controlled. When a POS terminal is installed in a store, the financial institution should establish procedures and training programs to make the merchant aware of the minimum security standards required by the financial institution.

Data and Procedural Controls. Controls to ensure prompt and accurate processing include (1) a control or balancing function, (2) written manuals in support of systems and procedures, and (3) capability to restore or replace lost, damaged, or incorrect files.[13]

Because the direct output of many EFTS applications includes disbursement of cash and payment for merchandise, a control group that is organizationally independent of EDP operations, systems, or programming is essential. The control group should be responsible for performing many of the application controls discussed below.

In shared EFT systems, an agreement between the concerned parties should be written before the system is implemented. This agreement should outline security and maintenance procedures, transaction fees (if applicable), liability in case of damage or errors or irregularities, and procedures for termination of the agreement. Institutions sharing remote-banking terminals should agree to the physical security over the units. The members should share responsibility for the safety and security of the units unless the system provides that the members own the terminals separately. In that case, each institution should assure the others that the terminals are properly maintained.

Capability to restore or replace lost, damaged, or incorrect files gains importance in EFT systems because the nature of the application increases exposure, and the real-time environment makes recovery more complex. Recovery procedures provide a means of reproducing paperless transactions in the event

[12] *The Auditor's Study and Evaluation of Internal Control in EDP Systems* (New York: AICPA, 1977), p. 37.

[13] *The Auditor's Study and Evaluation of Internal Control in EDP Systems,* p. 43.

of equipment malfunction. Backup and restart procedures should minimize downtime and maintain the integrity of data while the system is down. In addition, manual procedures to originate transactions during periods of equipment downtime should be specified.

For example, an off-line remote-banking terminal's transaction file initially stands alone as the source document for a transaction. Were a terminal to malfunction while in use, the transaction occurring could be difficult to reconstruct. Therefore, two recording systems (hard copy and magnetic or paper tape) should be built into each off-line terminal. If one system should fail, the other would maintain the audit trail. A disadvantage of off-line terminals is the requisite daily removal and processing of the terminal's transaction file. Security should be maintained when the records are removed from the terminal and transported to the central computer facility. Alteration of these records before they are input into the central system would be difficult to detect.

For on-line terminals, transaction logs should be maintained both at the main computer and at the terminal. The main computer file would serve as the original record of the transaction and the terminal file would serve as support. The file should be organized by terminal code and list account numbers and amounts without revealing PIN numbers or other identification codes. If an unusual transaction is detected or otherwise selected for testing, the transaction can be traced to the terminal from which it originated and compared to the terminal file. Any discrepancy would indicate that an unauthorized entry into the EFT system may have occurred.

Physical Security

Physical security over the host computer should be effective because a catastrophe involving an EFT system would be more difficult to recover from than a similar disaster in a less comprehensive system. Emergency plans and backup should exist and be periodically tested.

Procedures should be established to assure that no one outside of the maintenance staff attempts to repair a malfunctioning terminal. Instructions about whom to contact in case of malfunction should be displayed prominently on each terminal. Unauthorized repair of a damaged terminal may destroy the reliability of the audit trail. Backup systems should be developed for the period when processing is interrupted or when units are undergoing regular maintenance.

Application Controls

Application controls relate to specific accounting tasks. SAS no. 3 categorizes application controls as—

- Input controls
- Processing controls
- Ouput controls

Input Controls

> Input controls are designed to provide reasonable assurance that data received for processing by EDP have been properly authorized, converted into machine-sensible form and identified, and that data (including data transmitted over communication lines) have not been lost, suppressed, added [to], duplicated, or otherwise improperly changed. Input controls include controls that relate to rejection, correction, and resubmission of data that were initially incorrect.[14]

The input controls listed in the audit and accounting guide include (1) authorized input, (2) code verification and input conversion, (3) data movement, and (4) error handling.

Authorized Input. In an EFTS environment, many people may have access to the system. Where applicable, input controls should ensure that a valid card was used by the valid cardholder from a terminal authorized to perform that transaction.

For example, one common method of user identification is the use of a magnetic-striped card combined with a unique PIN number known only to the user. (Other more advanced identification methods such as finger- or voice-print analysis are presently not cost effective.) To operate the terminal, the user inserts a card and enters the PIN number on the terminal's

[14] SAS no. 3, in *Professional Standards,* vol. 1, AU sec. 321.08*a*.

keyboard. If the user is unable to enter the PIN number correctly or if the terminal recognizes the card as being invalid (stolen, counterfeit) the user cannot enter the system. Some systems do not return the invalid card but store it within the terminal until removed by an authorized individual. To help assure that an invalid user will not obtain both the card and PIN number, they should be mailed to the user separately.

An on-line terminal has direct access to the central computer file of invalid cards while an off-line terminal should maintain its own file for such cards. Off-line files will not be as current and may require larger terminal storage capability than on-line terminals.

While the cost of a card-PIN system is less than other systems, physical security may not be as good as some alternative system. Customers frequently write their PIN number on the card or give the number to other customers. Coded messages on a plastic card's magnetic stripe can be duplicated. In some systems, a PIN number or portion of a PIN number can be obtained by observing the user entering the number at the terminal.

Several methods exist to make cards more secure. Most involve machine-sensible messages encased within a plastic card, or use of radioactive isotopes. Each card should contain a unique random factor so that no two would be alike. Another method to discourage counterfeits is the use of heat- or pressure-sensitive plastic, causing the card to be damaged by conventional duplicating techniques.

Another control to help assure authorized input is to restrict the types of transactions that can be made from certain terminals (for example, restrict the terminals from which adjustments may be made or high-value transactions may be initiated). A terminal that handles customer deposits and withdrawals should not be capable of obtaining information or accessing files other than those necessary to complete the specified transactions. The system can identify the terminal by use of an "answerback" feature.

Code Verification and Input Conversion. Data entry errors and the loss or dropping of data can be a major source of error in EFT systems. The system should be designed to verify each transaction before acceptance by the system. The user could then eliminate mistakes before the transaction is entered into the files. This edit/validation process of input transactions should involve validation of the transaction content, formatting of data, and writing a log record including the transaction serial number. The log should also maintain the date and time of the transaction. Further, it would be desirable to maintain control totals for each terminal by transaction type.

Data Movement. Assurance should be given that data are not lost, suppressed, added to, duplicated, or otherwise altered. In an on-line environment involving data communications networks, this is much more complex than in a batch environment. The auditor should consider evaluating the controls related to message transmission and data security. The auditor should determine that a satisfactory technique is used to validate the receipt and transmission of messages (transactions) originating through the terminal. A transaction identifier should include not only the terminal device identification but also other control information such as message type indicator (that is, debit, credit, high-value debit), message sequence number generated at the terminal, designation or routing indicator(s), and character count. The message sequence number can be used to trace the transaction along the complete data stream and, if necessary, back to the originating station and person. The system should also be designed to respond to the terminal device acknowledging receipt of the message. If there is a problem with validation of the message header or transaction, the computer system should request retransmission using the same sequence number.

Error Handling. The correction of errors and resubmission of the corrected transactions should be controlled. The errors should be corrected either by the person who caused them (for example, reentering a transaction that was improperly input at the terminal) or by an independent third party who reviews them with the originator. Terminals from which error correction transactions can be made should be limited in number and subject to strict access controls.

Processing Controls. Processing controls are designed to provide reasonable assurance that electronic data processing has been performed as intended for the particular application, that is, that all transactions are processed as authorized, that no authorized transactions are omitted, and that no unauthorized transactions are added.[15] Controls in this category include use of control totals, limit and reasonableness checks, and run-to-run controls.

The following are examples of some processing controls in an EFTS environment:

[15] SAS no. 3, in *Professional Standards,* vol. 1, AU sec. 321.08*b*.

- Comparison of daily batch totals from the main computer to corresponding totals maintained by the terminal device and/or switch.
- Balancing by account of terminal and/or switch transactions for total dollar amount and number of items.
- Monitoring activity logs to identify unusual transactions. The monitoring may include establishing limits based upon the number and dollar amount of transactions. These limits may be monitored by terminal, type of merchant, and financial institution. The objective is to identify potential errors or irregularities as they occur.

Output Controls. Output controls are designed (1) to assure the accuracy of the processing result and (2) to assure that only authorized persons receive the output.[16]

Accuracy of Processing Results. During the processing of EFTS transactions, it may be desirable to save the master file's "before" and "after" processing image on a log. Control totals over selected data elements could be developed and the "before" totals compared with the "after" and "transaction" totals.

The customer or user of the terminal can serve a valuable control function. Customers should be given printed evidence of the transaction when it is complete. They should also be given periodic statements and have the opportunity to challenge the charges recorded. Mailing of the statements, and handling and investigation of customer inquiries should be performed by the control group or other function that is independent of the processing of EFTS transactions.

Distribution Controls. Because the direct output of an EFT system can be cash or the distribution of goods or services, output control over these applications is essential. Control over output of information from EFTS files is also important because of the sensitive nature of the information and the privacy regulations governing its distribution. One example of this type of control would be to limit customer information inquiries, based upon the terminal and person performing the inquiry.

Study and Evaluation of Internal Control in EFT Systems

Once the auditor has determined the extent of the client's system, the auditor has a responsibility to obtain an understanding of the flow of transactions through the system, the extent to which EDP is used in each significant accounting application, and the basic structure of accounting control within that system.

In many EFT systems, third parties are responsible for some portion of the processing of transactions. For example, the third party may provide the switching data center, the telecommunications network, the terminals, or all of the foregoing. To the extent that the client's system of accounting control includes processing performed by a third party, the auditor should consider this processing during the preliminary phase of the review. SAS no. 3 indicates—

> When EDP is used in significant accounting applications, the auditor should consider the EDP activity in his review and evaluation of accounting control. This is true whether the use of EDP in accounting applications is limited or extensive and whether the EDP facilities are operated under the direction of the auditor's client or a third party.[17]

There are two types of switches used in remote-banking and point-of-sale services. They are referred to here as "message-passing" and "bank" switches. A message-passing switch performs only straightforward data communications between the financial institution and the terminals. A bank switch can route transactions between financial institutions and may provide some control or accounting functions. Both types of switches are within the financial institution's system.

Because of the limited function performed by message-passing switches, the auditor's review of the switch will normally be concerned only with (1) determining which type of switch it is and (2) reviewing the financial institution's controls to ensure that the switch only transmits the data and does not alter it.

[16] SAS no. 3, in *Professional Standards,* vol. 1, AU sec. 321.08c.
[17] SAS no. 3, in *Professional Standards,* vol. 1, AU sec. 321.03.

The auditor's review of bank switches, however, would be based on the functions they perform. As indicated above, a bank switch owned by a third party should be considered a service center.

Summary

This chapter has discussed two problems facing the auditor of EFT systems:

- How much of the EFT system linking many organizations is included in the client's system? What parts of the system should the auditor consider in the study and evaluation of internal control?
- What controls have increased importance in EFT systems? How can certain control objectives listed in the audit guide[18] be met in EFT systems?

This discussion is the task force's initial assessment of these questions. Further research and professional deliberation will be needed as auditors gain experience with these systems.

[18] *The Auditor's Study and Evaluation of Internal Control in EDP Systems.*