Catholic University Law Review

Volume 25
Issue 4 *Summer 1976*

Article 7

1976

A Survey of Fraud and Privacy Obstacles to the Development of an Electronic Funds Transfer System

August Bequai

A SURVEY OF FRAUD AND PRIVACY OBSTACLES TO THE DEVELOPMENT OF AN ELECTRONIC FUNDS TRANSFER SYSTEM

*August Bequai**

The oldest form of financial exchange is probably the barter system, which can still be found today in many areas. This system gave way to the Age of Metal Coinage[1] which later yielded to a check system that made its appearance in this country in 1861.[2] Although the check system was long considered to represent one of the most sophisticated forms of payment, it is now being replaced by computerized payment mechanisms.[3] In 1970, a private study concluded that the present check collection system will be adequate only until the 1980's.[4]

In 1971, a committee of the American Bankers' Association called for the establishment of regional automated clearing houses to deal with the large

---

* Private Practitioner, Washington, D.C. B.A., 1967, New York University; J.D., 1972, American University; LL.M., 1976, George Washington University.

1. The development of the payments system can be broken down into five stages: the period of commodity money or the barter system; the age of metal coinage; the period in which written receipts became the dominant medium of ownership; the age of paper money; and, in the 19th century, the checking system. One knowledgeable source now foresees electronic transfer systems displacing, at least initially, half of the present volume of checks without the concomitant problems of check "bouncing," inflated deposit totals, and other defects that add to the cost of the check system. Address by George W. Mitchell, Member, Board of Governors of the Federal Reserve System, at the American Management Association, New York City, Mar. 24, 1971.

2. *See* Duffy, *Automation and Checkbook Money Outlook*, BANKING, May 1966, at 30; *Soon You'll Never See Money at All*, CHANGING TIMES, Oct., 1967, at 7, 8.

3. FEDERAL RESERVE BANK OF BOSTON, REPORT ON ELECTRONIC MONEY AND THE PAYMENTS MECHANISM 3 (1968).

4. ARTHUR D. LITTLE, INC., THE OUTLOOK FOR THE NATION'S PAYMENTS SYSTEM: 1970-1980, Dec., 1970, at 7. As an indication of the decreasing manageability of the checking system, experts estimate that if all the checks written in 1967 had been processed by hand, it would have taken every female in the United States between the ages of 18 and 60 to accomplish it. Reynolds, *The Checkless Society*, DUNS REVIEW, May 1968, at 13.

volume of paperwork created by our checking society,[5] and the Federal Reserve has joined the call for some way to improve the present mode of payment.[6] These groups maintain that the automated checkless society, because it will greatly reduce the amount of paper money in circulation, will help lower this country's high crime rate.[7]

An automated payments system, however, will face a number of serious problems. These may be categorized under four headings: (1) the problem of electronic fraud; (2) the problem of computer-generated litigation; (3) the problem of privacy; and (4) the problem of the McFadden Act[8] and bank branching. It may well be that an automated payments system will create more crime, albeit of a different nature, than it will solve.[9] Commenting on computer (electronic) fraud, one source has said, "[b]usiness has probably never been so vulnerable to theft."[10] Since computer-generated information is difficult to have admitted as evidence in court, the prosecution of electronic frauds will likely prove to be an immense problem. In addition, an automated payments system will include the storage of large amounts of personal data about millions of persons, thus raising important questions regarding privacy. Serious issues concerning bank branching and the McFadden Act will also develop as thousands of terminals are installed throughout the country. The implementation of an automated payments system, or electronic funds transfer system (EFTS), may indeed never become a reality unless these problems can be dealt with effectively. Even if the difficulties can

---

5. *See* Homrighausen, *One Large Step Toward Less-Check: The California Automated Clearing House System*, 28 BUS. LAW. 1143, 1158-59 (1973).

6. Board of Governors of the Federal Reserve System, *State of Policy on Payments Mechanism*, 57 FED. RES. BULL. 546 (1971). *See generally Evolution of the Payments Mechanism*, 58 FED. RES. BULL. 1009 (1972).

7. Stuart M. Speiser has stated that "[p]aper currency is the lifeblood of crime and corruption in the United States. Without paper money, it would be virtually impossible for criminals and corrupt officials to profit from illegal activities. If all substantial transfers of money were recorded in bank transactions, no one could conduct profitable illegal activities without creating highly visible permanent evidence of the illegal activities . . . . With the chances for profit from illegal activities so slim, it is difficult to visualize large numbers of persons running the risks of imprisonment." Speiser, *Abolish Paper Money and Eliminate Most Crime*, 61 A.B.A.J. 47, 47 (1975). See *Time Bomb in EFTS Security*, AMERICAN BANKER, Apr. 4, 1975, at 4, for a critique of the system and some of its possible weaknesses.

8. 12 U.S.C. § 36 (1970).

9. A study of 12 cases of computerized bank embezzlement that occurred in the late 1960's and early 1970's revealed that the losses averaged $1,090,000, or about 10 times the average loss from all other types of embezzlement. Porter, *Computer Raped by Telephone*, N.Y. Times, Sept. 8, 1974, § 6 (Magazine), at 40.

10. CHAMBER OF COMMERCE OF THE UNITED STATES, A HANDBOOK ON WHITE COLLAR CRIME 20 (1974).

be resolved, however, the cost of doing so may well be too high relative to the benefits which would be derived from an automated payments system.

I. The Electronic Funds Transfer System

EFTS may be defined as the transmission of information regarding fund transfers over communication networks, starting with input from a terminal at the point of sale and culminating in a computerized bookkeeping transaction at some central funds transfer computer station, which in most cases would be a banking institution.[11] The transfer may involve movement of funds from the account of a consumer to the account of a merchant, from a buyer to a seller, or from an employer to an employee.[12] Under an advanced EFTS, for example, a consumer could pay for his purchases by handing a plastic identification card to a store clerk who would insert the card into an apparatus located behind the counter. The consumer would then enter an identification code into a small input terminal which would be connected through the store's telephone lines to a computer system located at a bank. The signal from the store terminal would activate the computer to check the consumer's credit rating, compute the credit, and notify the store by means of a signal. If the account had sufficient funds to cover the purchase, the clerk would be so informed by the computer and could then conclude the transaction. The amount purchased would be deducted from the client's account and added to that of the store.

An employer's payroll could also be totally integrated within an EFTS. Salaries to employees would be encoded on tape that would be run through the employer's computer, which in turn would be connected to one or several bank computers. The employer's computer would instruct the bank computers to deposit an employee's pay in his account. The funds would be transferred electronically, thereby eliminating the need for a paper exchange between the employer and the banks.

It is the computer which represents the heart of this system, and makes an EFTS a real possibility. At present, the technology to build an EFTS exists. Computers with high processing speed, multiprocessing capability,

11. The development of an EFTS is fundamentally rooted in, and dependent upon, the development of appropriate technology and hardware. National chains and affiliated stores are expected, within the next several years, to have electronic cash registers which could easily serve as payment terminals. One such chain has a credit program larger than either of the two national bank charge card systems. C. Christophe, Competition In Financial Services 5 (1974).

12. The essence of the projected electronic payments system is simultaneous crediting of a payee's account and debiting of a payor's account. 58 Fed. Res. Bull. 1009 (1972).

high speed mass memory, on-line terminals systems,[13] voice recognition devices, and sophisticated computer languages are currently in operation. Third generation computers[14] capable of vast memory storage permitting instantaneous access from a large number of terminals also exist. Taking advantage of this technology, several automated clearing houses (ACHs) made their appearance in early 1972. Under the present clearing house system, banks maintain clearing balances on one another or on a common bank. The Federal Reserve serves the same function, but the ACH adjusts balances electronically and with much greater speed. The ACHs are presently used for the distribution of payroll payments. Employee salaries are put on magnetic tapes or punched cards and delivered to the city's Federal Reserve Bank or branch. The employer's bank then pays the employee's bank by interbank settlement at the Federal Reserve Bank. Although this system falls short of a sophisticated EFTS, it is a strong starting point for the development of a more advanced system.

Recently, a federally chartered savings and loan association devised a remote deposit and withdrawal system with the transaction terminal located in a supermarket.[15] In order to deposit or withdraw funds, an association account holder gives a plastic card to a store employee who places it into a reading device which extracts information contained in a magnetic stripe located on the back of the card. The supermarket clerk then enters the amount and type of transaction into a communications device linked by telephone lines to a central computer at the association. The computer processes the information and effects a transfer of funds in the amount indicated. If a customer wants to withdraw funds, his account at the association is debited and he receives cash from the supermarket after the computer indicates that the transaction may continue. The supermarket, in turn, receives credit in

13. Activated by specially encoded customer identification or bank credit cards, these terminals can be used to withdraw cash from or make deposits to, a checking or savings account, to authorize payments to third parties, or to obtain cash under prearranged lines of credit. The equipment can be either "on-line," that is, directly linked to the bank's computer, or "off-line." If it is off-line, each transaction must be recorded on tape and brought to the bank periodically. The terminals can be customer-operated, or operated by an employee of the store or other business in which the terminal is located. A customer-operated terminal dispenses cash and receives deposits directly. A store-operated terminal communicates information and initiates transfers of funds.

14. Third generation computers are characterized by modularity and compatibility. These computers are sufficiently adaptable so that new equipment may be added to them when needed, rather than having to build an entirely new system. They can easily provide the basis for an EFTS.

15. *See* Ege, *Electronic Funds Transfer: A Survey of Problems and Prospects in 1975*, 35 MD. L. REV. 1, 6 (1975).

an account it maintains at the association. Several other banks are also planning to offer this service.[16]

Automated cash dispensers and teller machines are another form of electronic financial service currently offered by banks. These units, which are installed in the wall of a financial institution or its branch, may receive deposits in the form of cash or check, dispense cash, and transfer funds between accounts of the same individual. These machines, however, are not as versatile as the ACH and are more costly to operate than the simple supermarket system discussed above.[17]

The point-of-sale system, still in the planning stage, represents a more highly developed and sophisticated EFTS. This system can effectuate payments without the intervention of currency.[18] The customer, upon making his purchase, initiates the process by making a withdrawal from his account at the bank; a credit is then made to the account of the store. If the store does not maintain an account at that bank, then an ACH may be used. Of the three systems discussed above, this is the only one regarded as being a true EFTS,[19] although it is rather simplistic when compared with the complex and highly sophisticated EFTS of the future, which will involve more than 50 million subscribers and over 70 million terminals.[20]

A study conducted by a New York bank several years ago indicated that many of its clients were happy with the present system of payment.[21] In

16. *Id.*
17. *Id.* at 7.
18. *Id.*
19. *Id.* at 8.
20. A truly national and widely used EFTS, to be successfully implemented, will need a secure communications system linking every place of business. More than 150 million people must change their outlook toward credit, money and purchasing, and over 11 million business accounting and control systems must be modified. In addition, more than 50 million people must be positively identified so as to permit verification over a communication system, and over 70 million new terminals must be installed. Household units must also be included if maximum reduction of checks is to be achieved. *See* Long, *Checkless Society*, AUDITGRAM, Jun., 1967, at 7.
21. A random sample of some 2000 customers was surveyed and some 1,069 questionnaires were returned. Only 20.6 percent said they would definitely use the system if it were offered; 26.4 percent felt they would use it, but with some reservations; 32.2 percent were not sure; and 20.8 percent said they would not use the system. This is one of the few studies which has measured customer response to an EFTS. *See* Jablon, *Marketing an Electronic Fund Transfer System*, BANK MARKETING MANAGEMENT, Dec., 1970, at 18-19. A study of some 300 bank executives conducted by San Diego State College indicated that 68 percent believed checks would never be completely eliminated; 93 percent believed cash will not be eliminated; and 58 percent believed that some form of checkless society will eventually become a reality, but only by the end of this century. SAN DIEGO STATE COLLEGE, SCHOOL OF BUS. ADMIN., SUMMARY BANK SURVEY REPORT 1-2 (1968).

fact, the majority of those polled said they would be reluctant to comply with a change.[22] A threshold question, then, is whether an EFTS should be developed when consumers are satisfied with the current check system. The response is that, even with all its advantages, the check system is an inefficient and expensive mode of payment. At present, some 13,693 commercial banks, with their 17,690 branches and 248 clearing houses, and 12 Federal Reserve Banks with their 24 branches, are the processing points for the entire check payment system.[23] In 1945, the annual check volume was 5.3 billion. It went up to 8.9 billion in 1955, 18.0 billion in 1966,[24] and 22.0 billion in 1970.[25] This continued expansion places increasing pressure on the banking industry's ability to process check transactions.[26] In addition, there is serious concern with the industry as to whether it can adequately cope with the future volume of paper money.[27] The current strain on the postal service and brokerage houses is an example of what may happen to banks in the future.[28] The introduction of computers, and their continued refinement in both hardware and software,[29] offers the banking industry an escape from the mounting paper flow, and makes the checkless society an attractive alternative.

II. The Problem of Electronic Fraud

Although an EFTS would be impossible without computers, the computer is also the major obstacle to the development of such a system. This is so because computers are subject to electronic fraud. Under an EFTS, payments would be made instantaneously and independent of the use of paper. Bills could be paid by telephone from one's home or office, and one would be able to shop anywhere without carrying cash. All of these transactions

22. Jablon, *supra* note 21, at 18-19.

23. Bank Administration Institute, The Check Collection System—A Quantitative Description 12 (1969). For a discussion of the disadvantages of the present check system, see Dunne, *Variation on a Theme by Parkinson or Some Proposals for the Uniform Commercial Code and the Checkless Society*, 75 Yale L.J. 788, 790, 792, (1966).

24. Bank Administration Institute, *supra* note 23, at 3.

25. *A Cashless Society Isn't Here*, Business Week, Jun. 21, 1971, at 21, 22.

26. Clarke, *The Payments System: Problems, Fantasies, and Realities*, Federal Reserve Bank of New York Monthly Rev., May, 1970, at 109. The Postal System and the brokerage houses on Wall Street are presently struggling to handle an avalanche of paper work. *See Banks: Left at the Line?*, The Magazine of Bank Administration, Mar., 1969, at 1.

27. The Magazine of Bank Administration, *supra* note 26, at 1-2.

28. *Id.*

29. "Software" refers to the programs and routines used to extend the capabilities of computers.

would be recorded by computers and stored in their memory banks. Although traditional types of crime may decrease, more sophisticated forms of theft will probably evolve.[30] A system with millions of subscribers, and the bulk of this country's economy dependent on it, could easily prove a nightmare for law enforcement agencies—computer experts estimate that the crippling of 100 key computers in the United States would paralyze the American economy.[31] Consequently, unless preventive steps are taken, EFTS may displace the bank robber but introduce the saboteur and manipulator who will ransom the bank's computer, or create fictitious accounts and nonexistent money.[32]

A. Computer Crimes

Computer crimes take several forms: embezzlement, misappropriation of computer time, theft of programs, and illegal acquisition of information.[33] The dollar loss per incident of computer crime has been as high as $5 mil-

30. Proponents of EFTS predict that every business establishment, including taxicabs, would be equipped with terminals in which payment cards could be inserted. The terminal would replace the need for paper money, and thereby discourage criminals. *See* Speiser, *supra* note 7, at 47. However, one study concluded that credit card frauds at present cost the public an estimated $100 million annually. *See* CHAMBER OF COMMERCE OF THE UNITED STATES, *supra* note 10, at 33. Another study concluded that organized criminals will, in fact, accept credit cards in lieu of cash, and that some criminal groups have actually established special units concentrating on such operations as stolen credit cards. *See* CHAMBER OF COMMERCE OF THE UNITED STATES, DESKBOOK ON ORGANIZED CRIME 52 (1972). It is doubtful whether an EFTS will reduce crime. It may, in terms of economic harm, give rise to more sophisticated and much more dangerous forms of crime.

31. This figure is based on an estimate by the Honeywell Corporation. *See* G. MCKNIGHT, COMPUTER CRIME 204 (1973). It is believed that in Britain as few as 20 key people in its computer industry "could hold the nation to ransom." *Id.*

32. *Id.* Computers are also open to attack from extremist groups. It is not inconceivable that such a group might destroy computers or hold them in ransom for political objectives. The entire economic and monetary fibre of this country could easily be damaged, perhaps beyond repair. The amazing storage power of computers makes this possible; for example, the information contained in a 300,000 volume library can easily fit into a computer the size of a six foot cube. *See* Garland, *Computers and the Legal Profession*, 1 HOFSTRA L. REV. 43, 44 (1973), *citing* THE CONFERENCE BOARD, REP. NO. 537, at 24 (1972). *See also Computers: A New Wave*, NEWSWEEK, Feb. 23, 1976, at 73, 74.

33. Computer frauds generally fall within one of the following five categories. First, frauds involving "programs and programming" which may involve thefts or alterations of programs. Second, thefts of "computer time" which in some ways resemble misuse of copying machines. Third, manipulation and distortion of "input data." Fourth, thefts of "output data," such as printouts of mailing lists and other confidential information. Last, interception of "data communication." *See* CHAMBER OF COMMERCE OF THE UNITED STATES, *supra* note 10, at 21-22.

lion;[34] in one instance, the case of Equity Funding Life Insurance Co. in New York, computer fraud was employed to place $2 billion worth of phony insurance policies on company records.[35] In 1973, the chief teller at the Union Dime Savings Bank in New York City was charged with stealing in excess of $1.5 million; the teller was able to transfer electronic money from legitimate accounts in computer files to fraudulent accounts and then withdraw real money.[36] He then redeposited these electronic funds at quarterly interest payment times to make all accounts balance correctly.[37] This type of crime is common in systems where the computer is used for financial processing, including payrolls, accounts payable and receivable, and storage and maintenance of financial data.[38] A related case, involving another major New York bank, lends further support to the fears of many who saw the computerization of finances as a two-edged sword.[39] A bank teller instructed the computer to issue dividend checks in the names of former shareholders who had sold their stock to companies for which the bank acted as transfer agent.[40] After the issuance of the checks, the computer was instructed to erase all records of the payments.[41]

---

34. *Id.* at 20.

35. Of the approximately $3 billion worth of insurance shown on the books of the company, approximately $2 billion was fictional. Of the 90,000,000 policies allegedly in force, 60,000 were nonexistent. The computer served as a very useful tool in the perpetration of this fraud. *See* Payne, *Equity Funding Life Insurance Company*, 10 THE FORUM 1120, 1127 (1975). The scandal finally surfaced when a discharged officer contacted an expert in insurance stocks, who in turn "blew the whistle." *See* Porter, *supra* note 9, at 36.

36. Porter, *supra* note 9, at 33. It should be borne in mind, however, that given the present tools of law enforcement, the chances of uncovering a computer-related fraud are 1 in 100. *Id.* at 34.

37. *Id.* at 33.

38. *Id.*

39. *Id.*

40. *Id.* The computer criminal has been described as being highly motivated, bright, energetic and between 18 and 30 years of age. He has access to all the relevant information he needs. The organization's claims about the security of the system have not dissuaded him, but rather have encouraged him to "pit his mind against" that of the computer. *Id.* at 36. Moreover, the individuals employed at the key "input data" stage are generally low-paid clerical employees, who tend to have a high turnover rate and low motivation. They can be easily manipulated by the "ringleader" in any such conspiracy.

41. The first federal criminal case involving a computer occurred in 1966 when a 21 year old programmer put a "patch" (a program change which is very difficult to detect even by a trained specialist) in a program used to process bank checks and to detect overdraft accounts. The "patch" caused the computer to ignore overdrafts on the programmer's account if his "invisible" bank account on magnetic tape was in overdraft. The "patch" was in for three months before the programmer's activities were detected due to a computer breakdown. *Id.* at 35.

Given the history of electronic frauds,[42] there is little reason to be optimistic that electronic funds transfer systems will be any less susceptible to this kind of crime. EFTS will offer sophisticated and organized criminal elements an entirely new means for counterfeiting money. It will also offer extremists the opportunity to cripple the financial system of this country. Add to this the fact that victims of computer crimes seldom want to advertise their losses,[43] and one has the elements of a dangerous situation.

B. Why Computers Lend Themselves to Fraud

The storage capacity and operational complexity of computers has increased immensely.[44] Basically, the computer system[45] consists of five operations. The first of these involves the "input device."[46] It translates data into signals that the computer understands. The different types of input devices include card readers, magnetic tape units, paper tape readers, optical scanners, and remote terminals. It is at the input stage that the criminal can introduce false data into the computer, and thereby manipulate it.[47]

---

42. Experts estimate that the ratio of undiscovered to discovered computer crimes may be as high as 100 to 1. *Id.* at 34. Computer crimes were seldom discovered through normal security precautions or accounting controls, and nearly all of them were uncovered by chance. *Id.*

43. Victims of computer crime seldom want to talk. In part, this is due to the sensitivity of corporate officials who want to protect their company's good name and image. Such corporate indifference means that a large number of computer crimes are ignored every year. There is fear of what competitors, shareholders, and lenders might do if they discovered that the company's costly computer had been criminally manipulated. *See* McKnight, *supra* note 31, at 47-48. To admit publicly that one has been robbed by a trusted officer would create a disastrous lack of confidence in the corporate leadership. All of this results in a great hesitancy to bring formal charges. *Id.* at 52-53, 61. In one case, a company's unwillingness to prosecute, for fear of harming its good name, led the directors to go so far as to provide the computer criminal with "good references" for another job. *Id.* at 62.

44. As an example, the storage capacity of the IBM 370, representative of the current generation of business computers, is 700 times that of the Univac I—the first commercial computer. The IBM 370 also executes additions 4300 times faster, multiplications 3100 times faster, and divisions 2000 times faster than the Univac I. Technological advances have increased the cycle speed of main memory devices by a factor of 1000, and the data transfer rate of current tape drives is more than 40 times that of the earliest tape drive used in the Univac I. For an excellent discussion of the developments in computer technology, see Garland, *supra* note 32, at 44; *see also Computers: A New Wave, supra* note 32, at 73-74.

45. The term "computer system" as used herein includes all mechanical and electrical devices used for processing the data ("hardware"), as well as the programs ("software") used to instruct these devices.

46. An "input device" may be defined as any device used to enter data into the computer system.

47. As the amount of human intervention required in the input process increases, the

Many acts of fraud depend on the undetected manipulation of input data.[48] At this stage, fraudulent records may be introduced,[49] current data may be altered, and key input documents may be removed.[50] In an advanced and complex EFTS, false accounts can easily be created, fictitious deposits and withdrawals entered, and, if the past is indicative, such electronic bank robbery may amount to billions of dollars.[51]

The second operation consists of "programming."[52] This operation consists of supplying the computer with a logical sequence of step-by-step operations relating to the solution of a particular problem. The computer can use only that data which the program instructs it to use, and can perform only those operations which the program directs it to perform. Computers, therefore, are subject to abuse since programs can easily be altered by criminal

---

probability of the introduction of error increases. Input devices, and the procedures employed in utilizing them, can be designed to detect errors in the raw data and prevent the introduction of error into the process.

48. As an illustration, an executive at a major manufacturing company inserted fraudulent data creating fictitious suppliers and truckers. Corporate checks, approximately $1 million worth, were issued to these fictitious accounts and pocketed by the executive and his six conspirators. Over the years, he received several awards from his company for the excellent condition of his records. *See* CHAMBER OF COMMERCE OF THE UNITED STATES, *supra* note 10, at 21-22.

49. One of the advantages of computerization is the ability to maintain records in compact form, thus doing away with bulky records. The data is fed directly into the computer and no paper record is ever generated. The original document, however, is usually destroyed, and external audit trails are lost as a result. Investigations involving computer frauds are thus frustrated because the compilation of evidence is difficult, if not impossible.

50. Several years ago, the computer operator of an engineering firm pocketed cash receipts and removed related input documents. He was able to steal about $200,000 before customers began to complain that their accounts were not being credited. In a similar scheme, customers who lodged this type of complaint were offered apologies and the explanation, "[w]e're having troubles with our computer. Your patience is appreciated." Customers accepted this explanation, and the fraud continued for months. *See* CHAMBER OF COMMERCE OF THE UNITED STATES, *supra* note 10, at 22.

51. A few years ago the Federal Reserve warned member banks that "[b]anks are being victimized by . . . bogus wire transfers of funds. . . ." and told of an instance when a $2 million wire transfer was fraudulently sent from a bank on the West Coast to a bank on the East Coast. *See* [1966-73 Transfer Binder] CCH FED. BANKING L. REP. ¶ 95,572 (1971).

52. Programs are written in a "program language," which is an intermediate step between the spoken language and the binary language recognized by the computer. Through "assembly" and "compiler" programs, the program is converted from its intermediary language to the language of the computer. The lowest level is "machine language," which is a binary language understandable by the machine but not by humans without a great deal of computation. The highest level is "problem oriented" language, which is used in the majority of business programs. English words and mathematical notations are used to describe the processing steps. As computers become more efficient, "higher level" language will increasingly approximate the English language.

elements.[53] Programs may also be stolen or destroyed, either at the computer installation itself or through remote terminals and telephone circuits.[54] Stolen EFT programs could easily be held for ransom or destroyed in a kind of advanced "industrial sabotage."[55] The program's safety devices could also be manipulated,[56] with changes easily continuing undetected for an extended period of time.[57]

The third basic operation in a computer system involves the "central processing unit" (CPU), which can be conceptualized as the brain of the computer. It guides the computer by following the instructions in the program. It retrieves the required data and directs the computer to perform the necessary functions with respect to that data. If the CPU were destroyed, all the records it contained would be destroyed with it. Experts estimate that in the case of a company with 90 percent of its records computerized, the continued operation of business would be virtually impossible after total destruction of the company's data bank. The dangers to the CPU arise from wiretapping,[58] electromagnetic pickups,[59] browsing,[60] and "piggyback entry."[61]

---

53. In one case, the manager of a company altered a computer program so that a few pennies were added to the cost of many purchase items. The altered program also enabled him to keep a double set of records. This, in turn, permitted him to steal amounts which did not overly distort the reported results. Over a period of five years he siphoned off about $1 million. To convert the bookkeeping entries into personal profit, he created fictitious suppliers and issued checks to them through bank accounts he had established. Under an alias, he drew out the funds as the checks cleared.

54. One such incident involved several million dollars worth of programs that an employee tried to sell to a customer of his employer.

55. In October 1971, a Los Angeles branch of the Bank of America was robbed. The bandits took more than $1 million in worthless checks and some computer reels. The robbers demanded ransom for the reels, but fortunately the bank had stored duplicates of the stolen data. It was apparent that the bandits had seen the value of "computer ransom." *See* MCKNIGHT, *supra* note 31, at 162-63.

56. That branch of programming known as systems programming, which deals with the operating system or software supplied by the manufacturers, provides for the automatic reporting of "halts" or "interrupts" as part of the computer security control system. *See* P. HAMILTON, COMPUTER SECURITY 28 (1973).

57. Program changes can continue undetected because of the suppression of entries in the computer log, which is maintained automatically. *Id.*

58. Wiretapping involves the connection of a "tap" directly to the telephone or teleprinter lines that transmit the data in order to intercept and record information.

59. Electromagnetic devices need not be connected directly to circuits. They are designed to intercept the radiation generated by the computer's central processing unit, telephone and teleprinter lines, or microwave communications.

60. This is done by tying an unauthorized terminal into a system that does not expose terminal entry. Through the unauthorized terminal, the "browser" can gain access to the computer for a variety of purposes.

61. "Piggyback entry" is achieved by selectively intercepting messages from the com-

The fourth operation involves what might be classified as the "output device." At this point, data is received from the CPU and translated into an intelligible form. Computer crimes during this stage typically have involved thefts of mailing lists, customer lists, and other confidential data.[62] The output stage, although not critical to forms of computer manipulation in itself, is a necessary step for the successful completion of such frauds.[63]

The final operation is that of "data communication." This involves the use of telephone circuits to transmit data back and forth between computers and terminals. The threat here comes from "telephonic penetration."[64] In addition, there is an added threat to privacy in that the ability to intercept data will provide information about the users of the system and their clients; this data may then also be fraudulently manipulated.[65]

An EFTS, with millions of subscribers, millions of terminals, and numerous computers will obviously be vulnerable to electronic criminal attacks. If an EFTS is to succeed, it must overcome this serious problem. Some experts suggest that protective measures be combined with detection mechanisms,

---

puter to the legal user, adding or deleting information, and releasing the modified message to the user.

62. Several years ago, the Encyclopedia Britannica Company accused three of its computer operators of copying nearly three million names from a computer file containing the company's "most valued" customer list. The employees then sold the list to a direct mail advertiser. The list was worth $3 million.

63. For example, a computer operator prepared a duplicate time card for a shipping department employee. He processed the card with the regular payroll data, except that he instructed the computer to omit listing certain details of the second checks, although the information was included in the totals. The checks were signed mechanically, and were totaled to prove that the amount disbursed corresponded with the total on the payroll register. After removing the computer-generated duplicate check, the operator forged the employee's signature and cashed the check by a second endorsement. This scheme was repeated many times. This activity, entailing the entry of false input data, alteration of the computer program, and check forgery, would have failed without the removal of the output data. *See* CHAMBER OF COMMERCE OF THE UNITED STATES, *supra* note 10, at 22.

64. In 1972, an engineering student at the University of California was arrested on charges of stealing $1 million worth of supplies from the Pacific Telephone and Telegraph Company over a two year period. He had found the entry code to the company's computerized ordering system in a trash can. Using a touch-tone telephone and the code, he entered item numbers obtained from the system manual and varied his orders by quantity and location. The manual he found indicated the quarterly loss for each location of the company. The computer informed him of what was being legitimately ordered from each location. Given this knowledge, he was able to keep his orders within the loss allowance. Finally, his activities were revealed by an associate.

65. The system may be entered through what is called a "between the lines entry." An unauthorized terminal is connected to a valid private line and enters the system whenever the legal user is inactive but still holds the communications channel. Sometimes the sign-off signal of the valid terminal is intercepted and canceled by the illegal user, who then continues with access to the computer.

and that some sort of code of behavior be promulgated.[66] Some of the safety measures suggested have been the following: (1) the computer room should be in an isolated site and only authorized personnel should have access to it;[67] (2) construction should provide high resistance to fire and physical impact;[68] (3) no individual should have access to all phases of the operation;[69] and (4) all waste should be shredded at the point of origin before being conveyed to the point of final destruction.[70] The question is whether these safeguards will be sufficient. The answer is unclear. In any event, the development of EFT must be accompanied by laws and regulations which provide for the strict prosecution of electronic felons.[71]

C. Present Legal Measures to Control Electronic Crimes

At present, white collar crime costs this country more than $40 billion annually; credit card frauds account for another $1.1 billion and computer frauds for $100 million each year.[72] These estimates do not include the amounts spent in combating white collar crime. It has been estimated that in the last 20 years, fraud has been a major contributing factor in the closing of 100 banks.[73]

If an EFTS is to function successfully, there are four major areas which will have to be regulated by criminal sanctions: (1) access by unauthorized

66. The British Computer Society has developed a model code of behavior to ensure that members accept and adhere to the highest standards of ethics. Among the tenets are that members will: accept full responsibility for any work undertaken; behave at all times with integrity; act with complete discretion when entrusted with confidential information; and act with strict impartiality when giving independent advice. The Code, however, has not been implemented by the industry as yet. It has also been suggested that both personnel and installations be licensed as a further means of preserving security. *See* HAMILTON, *supra* note 56, at 55-56.

67. The best possible site for a computer complex would be an isolated one allowing control over access. It should also be an area free from civil disturbance with flat open terrain and access only to authorized personnel.

68. HAMILTON, *supra* note 56, at 41.

69. Authorizations to enter should always state the hours and days when entrance is permitted. They should only be for a limited term, not to exceed several weeks. Authorized personnel arriving or leaving at unusual hours should be viewed with suspicion. Consent to search should be a condition of employment. Main entry points should be controlled. In order for no one individual to have access to all facets of the operation, labor should be divided.

70. HAMILTON, *supra* note 56, at 46.

71. In a case involving a computer fraud of some $1 million, the felon received 40 days in a minimum security facility in Malibu, California, and later opened a consulting firm to advise clients on how to prevent computer fraud.

72. CHAMBER OF COMMERCE OF THE UNITED STATES, *supra* note 10, at 6. In addition, consumer frauds annually account for over $20 billion, security thefts for $4 billion, and insurance frauds for $2 billion. *Id.*

73. *Id.* at 4.

individuals to communication links between terminals and the CPU;[74] (2) access to the CPU by unauthorized individuals;[75] (3) unauthorized access to an individual's account either through theft or reproduction of the access device;[76] and (4) unauthorized access to accounts by employees who operate the system.[77]

At present, one of the principal pieces of legislation in this area is the Bank Protection Act of 1968.[78] The Act requires that the federal financial supervisory agencies[79] promulgate rules establishing adequate security devices and procedures.[80] There is nothing in the Act, however, to suggest that it would apply to an EFTS. The Senate Report which accompanied the Act recites several reasons for its enactment, but these deal with burglaries, robberies, and deaths suffered by bank employees.[81] EFTS crimes, were they covered, would raise novel issues in the context of the Act. Electronic fraud would not result in injury or death to bank employees, nor would it involve violence. Although the robbery of a store containing EFTS terminals may be considered a bank robbery, and thereby fall within the Act, the question would arise as to what extent the regulatory bodies could require stores with EFTS terminals to establish security devices and procedures. In any event, an EFTS would not fit within the present distinction between retail financial transactions and federal banking agency controls. Consequently, more specific legislation will be required.

When bank officials or employees are involved in EFTS fraud, present law may be adequate to prosecute them. Sections 656 and 657 of Title 18 of the United States Code make theft, embezzlement, and the like federal of-

74. This can easily be achieved through wiretapping and electromagnetic pickup. *See* notes 58 and 59 *supra.*

75. *See* note 69 *supra.*

76. Some added mechanisms, such as fingerprints, signature verification, voice prints or body dimensions, may be used in conjunction with access security. Elaborate encrypting devices may also be used. *See* Popek & Kline, *Verifiable Secure Operating System Safeguards,* 43 AMERICAN FED. OF INFORMATION PROCESSING SOC. CONF. PROCEEDINGS, NATIONAL COMPUTER CONF. 145 (1974).

77. The computer will enable large amounts of data to be collected at substantially reduced costs. This will ultimately raise serious questions regarding violations of privacy. Unlike present systems, a highly computerized operation will contain more in-depth profiles of individuals. Such a system will also open avenues for governmental abuse of private rights. *See* Ross, *Credit Privacy Invaded,* Wash. Post, Feb. 12, 1976, at A1.

78. 12 U.S.C. §§ 1729, 1881-84 (1970).

79. These agencies are the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Federal Home Loan Bank Board. *Id.* § 1881.

80. *Id.* § 1882.

81. S. REP. No. 1263, 90th Cong., 2d Sess. (1968).

fenses when the offender is an officer, an employee or an agent of, or connected in any capacity with, federally regulated banks or savings and loan associations.[82] An EFTS involving stored information at locations remote from a bank may or may not find protection under these sections. To determine whether these provisions will apply to an EFTS, the statutory meaning of "money," "credits," and "funds" will have to be re-examined.[83]

Application of the bank robbery statute[84] will also pose a problem. This statute covers federally regulated banks, savings and loan associations, and credit unions. It applies to one who forcibly takes, or takes with intent to steal, money, property or anything of value from one of these institutions. Persons found forcibly taking anything of value may be prosecuted under this statute. However, electronic frauds usually involve insiders—people who are employed in key positions—in which case there is usually no forcible taking and intent is difficult to prove. An EFTS may also be open to attack by employees of a store where the bank has one of its terminal devices installed. It is questionable whether such thefts will be considered bank robberies.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968[85] makes it a federal crime to willfully intercept any wire or oral communication.[86] The Act defines "intercept" as the acquisition of the contents of any wire communication through the use of any electronic, mechanical or other device.[87] One of the major purposes of the Act was to protect the privacy of an individual's wire and oral communications, not to protect financial institutions.[88] Even if EFTS information is intercepted, it will be in the form of computer language. Since the Act prohibits illegal "aural acquisition,"[89] it is doubtful whether this section contemplates electronic interception of EFTS communications.

The Federal Consumer Credit Protection Act[90] makes criminal the use of any counterfeit, fictitious, altered, forged, lost, stolen or fraudulently obtained credit card. The objective of the Act is to prohibit the use of such a device to obtain goods or services on credit. The Act does not apply to noncredit transactions. Since an EFTS would involve a transaction which

82. 18 U.S.C. §§ 656-57 (1970).

83. As to the present interpretation of "credits" within 18 U.S.C. § 656, see Theobald v. United States, 3 F.2d 601 (8th Cir. 1925); as to "funds," see United States v. Smith, 152 F. Supp. 542 (W.D. Ky. 1907).

84. 18 U.S.C. § 2113 (1970).

85. *Id.* §§ 2510-20.

86. *Id.* § 2511(1)(a).

87. *Id.* § 2510(4).

88. *See generally* S. REP. No. 1097, 90th Cong., 2d Sess. (1968).

89. 18 U.S.C. § 2510(4) (1970).

90. 15 U.S.C. § 1644 (1970).

has as its objective the effecting of a payment, or the deposit or withdrawal from an account maintained at a financial institution, it would seem that the Act would not be applicable.

It is clear that electronic funds transfer systems will open numerous opportunities for criminal activity. Although some present federal sanctions may be applied, there is no federal legislation aimed specifically at abuses which will arise after the implementation of EFT systems. In order for these systems to be viable, laws providing for the prevention and vigorous prosecution of EFTS crimes must be promulgated.

III. Problems Arising From Computer-Related Litigation

Under an EFTS, disputes among cardholders, merchants and issuers would inevitably lead to litigation which would raise many evidentiary questions. It would be difficult to determine what records, if any, comprise the best evidence and what ones come within the scope of admissible business records. Since no written records are retained during the process by which a computer arrives at its final conclusions, evidence of the actions taken by a computer would be merely circumstantial. Attention will thus have to focus not only upon the admissibility of computer records as evidence and the weight to be accorded such evidence, but also upon matters of proof. A proper foundation will have to be laid in order to prove that the data is trustworthy and that the performance of the computer is reliable.

Since a computerized record consists of patterned punch cards and magnetic or paper tapes, it is unreadable as contained in the computer's storage device. Consequently, the record must be translated into a computer print-out, and may, as a result, be open to attack under the hearsay rule.[91] Another argument against admissibility is that a computer print-out, as the translation of a computer record, is a document created especially for trial, and therefore not within the business entries exception.[92] In addition, in a completely automated system, no one would obtain personal knowledge of the record or even of the sources of information, since data are received and recorded entirely by computer.[93]

---

91. *See* French, *New Jersey Court Disallows NCIC Data as Evidence*, 8 Law & Computer Technology 20 (1975).

92. *Cf.* Freed, *Substantive Law Aspects of Computers* in Computers and the Law 103 (R. Bigelow ed. 1966) (published by the A.B.A. Special Comm. on Electronic Data Retrieval).

93. In those states following the Uniform Business Records As Evidence Act, business records will be inadmissible if the testimony shows that the record was made by persons who were neither engaged in the regular course of business nor had any duty to know the facts reported. *See, e.g.*, Cox v. New York, 3 N.Y.2d 693, 171 N.Y.S.2d

A number of experts maintain, however, that the existing legal system and concepts will prove adequate to handle the increasing amount of computer-generated litigation.[94] The courts themselves have in the last several years begun to deal with issues raised by computer-generated litigation, but no specific evidentiary tools have yet been developed. Although it may be too soon to predict the outcome, some litigation which has already taken place in this area may serve as a guide for the future.

A. Statutory Problems

To be admissible in court, computer-generated evidence must come within an exception to the hearsay rule. Since the bulk of computer-generated evidence has involved business records, the development of the law in this area has centered around the business records exception to the hearsay rule.[95] Under the common law, regular business entries were admissible under the "shopbook rule";[96] the Federal Business Records Act[97] has significantly expanded the common law exception. Under the Act, computer-generated evidence taken from, or representing, business records is admissible. The Act requires the following criteria for admissibility: (1) the entry must have been made as the record of an act, transaction, occurrence or event in the regular course of business; and (2) it must have been in the regular course of that business to make the record at the time of the act, transaction, occurrence or event.[98] The Uniform Business Records as Evidence Act, adopted

---

818, 148 N.E.2d 879 (1958). The record is admissible if the person who supplied that record had the duty to do so in the regular course of business. Kardas v. New York, 44 Misc. 2d 243, 253 N.Y.S.2d 470 (1964).

94. *See, e.g.*, D&H Auto Parts, Inc. v. Ford Marketing Corp., 57 F.R.D. 548 (E.D.N.Y. 1973); Brown, *Electronic Brain and the Legal Mind: Computing the Data Computer's Collision Course With Law*, 71 YALE L.J. 239 (1961); Freed, *supra* note 92, at 103-04. Whether the Federal Rules of Civil Procedure are sufficiently broad and flexible enough to handle the discovery issues and document protection requirements arising in situations involving computer-generated evidence remains to be seen. *See* FED. R. CIV. P. 34 & 45. However, because discovery, pretrial exchange of information, and resolutions of differences regarding intended offers of evidence may be more important in the case of computer-generated evidence than in the usual evidentiary situation, such matters should be resolved long before the trial, and the opposing party should be allowed to review the material.

95. FED. R. EVID. 803(6).

96. This rule was developed in the 17th century as a narrow exception to the hearsay rule. It generally permitted the introduction of shop-books only to prove amounts due. The books, however, had to be properly authenticated, and the makers of the records had to be called as witnesses. *See* 5 WIGMORE, EVIDENCE § 1518 (3d ed. 1940).

97. 28 U.S.C. § 1732(a) (1970).

98. *Id.*; *see also* Williams v. Humble Oil & Ref. Co., 53 F.R.D. 694 (E.D. La. 1971).

by a majority of states, contains substantially the same requirements.[99] These laws would facilitate any further developments in the area of computer-generated evidence.

The federal courts have demonstrated a tendency in the last several years to liberalize the rules of evidence.[100] Rule 803(6) of the Federal Rules of Evidence, which deals with business records, reflects this liberal trend.[101] However, there are two possible problems inherent in the present trend: first, there is a danger that computer-generated evidence will be admitted too easily;[102] secondly, this in turn may result in a backlash, which may give rise to a stricter set of evidentiary requirements. Stringent requirements for the admission of computer-generated evidence may be so burdensome that much of it will be inadmissible or useless.[103] Since computer-generated evidence is open to error and fraud, a proper evaluation of the admissibility of such evidence requires that a careful scrutiny be made of the original source of the evidence and that the proponent make available at least one witness who can be cross-examined by the party opposing the admission of the material.

B. Litigation Involving Computer-Generated Evidence: The Case Law

The leading case on the admissibility of computer printouts as evidence is *Transport Indemnity Co. v. Seib*.[104] In *Seib*, the defendant, who operated a fleet of trucks, was sued by an insurer for premiums due under an insurance contract. In an effort to prove the amount of premiums due, the plaintiff sought to introduce into evidence an exhibit printed by electronic computing equipment and prepared by its director of accounting. The director's testimony indicated that, within his personal knowledge, the figures reported and the computations made were accurate. The plaintiff laid a proper foundation for the admission of the printouts by satisfying the statutory requirements

99. Uniform Business Records as Evidence Act § 2, 9A UNIF. LAWS ANN. 299 (1957).

100. *See* United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969). However, Sunset Motor Lines v. Lu-Tex Packing Co., 256 F.2d 495 (5th Cir. 1958), rejected computer-generated forms that were assumed to be within the business records exception because the certification required by Federal Rule of Civil Procedure 44(a) was lacking.

101. Rule 803(6) provides that the records of a regularly conducted activity are not excluded by the hearsay rule, even though the declarant is available as a witness.

102. The computer can package data in a very enticing manner, and since it might be difficult to look behind the package, there may be a tendency to simply admit the material.

103. As Judge Learned Hand said: "Unless [records] can be used in court without the task of calling those who at all stages had a part in the transaction recorded, nobody need ever pay a debt, if only his creditor does a large enough business." Massachusetts Bonding & Ins. Co. v. Norwich Pharmaceutical Co., 18 F.2d 934, 937 (2d Cir. 1927).

104. 178 Neb. 253, 132 N.W.2d 871 (1965).

that the witness be qualified to testify about the mode of preparation and the identity of the printouts, and that the computer records were made in the usual course of business and were an indispensable part of that business.[105] The court noted that the reliability of the computer was not a factor to be considered in determining the admissibility of the printouts. Rather, the establishment of the identity and the mode of preparation of the printouts was relevant only in determining the weight and credibility of that evidence.[106] According to *Seib*, therefore, the element of reliability, which is the basis of the business records exception to the hearsay rule,[107] would be satisfied so long as computers are used as part of a firm's everyday operations.

Two Arizona courts have followed the *Seib* rationale. In *State v. Veres*,[108] the prosecution sought to introduce a computerized statement of a bank account against a defendant charged with passing bad checks. The assistant cashier who testified had not prepared the bank records nor had any knowledge of the mode of preparation or operation of the bank's computer. Yet, on the basis of his testimony that checks are "encoded by machines" as a part of the normal course of business,[109] the court held the evidence admissible under Arizona's version of the Uniform Business Records as Evidence Act.[110] The court did not consider whether or not the assistant cashier was in fact a custodian of the records or an otherwise qualified witness.[111] In fact, the court acknowledged that the cashier's testimony did not conform to the standards ordinarily required to lay a proper evidentiary foundation.[112]

In *Merrick v. United States Rubber Co.*,[113] a suit based upon a verified open account, the plaintiff sought to introduce electronically reproduced records as evidence of the account. The plaintiff called as a witness an employee who, although familiar with the accounting records, had no personal knowledge of the actual operations of the computer. The court, while noting that a more meticulous foundation had been laid in *Seib*, held that a proper foundation was established for the admission of the records.[114] By accepting the employee as a "custodian or other qualified witness," the court broadly

105. *See* NEB. REV. STAT. § 25-12,109 (1964).
106. 178 Neb. at 258, 132 N.W.2d at 875.
107. *See id.* at 257-59, 132 N.W.2d at 875.
108. 7 Ariz. App. 117, 436 P.2d 629 (1968).
109. *Id.* at 125, 436 P.2d at 637.
110. 4 ARIZ. REV. STAT. ANN. § 12-2262 (1956).
111. 7 Ariz. App. at 126, 436 P.2d at 638.
112. *Id.*, 436 P.2d at 638.
113. 7 Ariz. App. 433, 440 P.2d 314 (1968).
114. *Id.* at 436, 440 P.2d at 317.

interpreted the applicable statute.[115] *Veres* and *Merrick* seem to manifest a judicial inclination to more readily accept computerized records into evidence as the reliability of computers increases.

The rationale of *Veres* and *Merrick* has also been applied in the federal system. In *Olympic Insurance Co. v. Harrison, Inc.*,[116] the Fifth Circuit found no merit in defendant's contention that computer printouts were unreliable. During trial, the printouts were shown to have been produced in the regular course of business. The circuit court determined that the discretion vested in the district court by the Federal Business Records as Evidence Act was not improperly exercised by the admission of the printouts into evidence.[117] The Ninth Circuit continued this liberal trend in *United States v. De Georgia*,[118] where the defendant was charged with interstate transportation of an automobile stolen from the Hertz Corporation. The prosecution attempted to show that, according to Hertz's master computer, the automobile had not been rented during the relevant period. A copy of the computer-generated data was not offered into evidence, but a Hertz employee testified about the contents of the data.[119] The testimony was introduced to show that Hertz relied on computer records in conducting its business.[120] The court, pointing to Rule 803(7) of the Federal Rules of Evidence,[121] concluded that the evidence was admissible under the Federal Business Records Act to prove that the automobile had not been rented.[122]

For those states adhering to the common law shop-book rule, *King v. State ex rel. Murdock Acceptance Corp.*[123] should provide valuable guidance. The

115. 4 ARIZ. REV. STAT. ANN. § 12-2262 (1956).

116. 418 F.2d 669 (5th Cir. 1969).

117. *Id.* at 669-70.

118. 420 F.2d 889 (9th Cir. 1969).

119. A Hertz security officer testified that after he received information indicating that the car may have been stolen, he checked the master computer control through a terminal in his office. He further testified that the auto in question had been returned to Hertz about a month earlier and records showed it had not been rented since then. *Id.* at 891.

120. *Id.* at 893 n.11.

121. Rule 803(7) provides in pertinent part:

> Evidence that a matter is not included in the memoranda, reports, records, or data compilations, in any form, [of a regularly conducted activity] to prove the nonoccurrence or nonexistence of the matter [is not excluded by the hearsay rule, even if the declarant is available as a witness], if the matter was of a kind of which a memorandum, report, record, or data compilation was regularly made and preserved, unless the sources of information or other circumstances indicate lack of trustworthiness.

122. 420 F.2d at 894. In a concurring opinion, Judge Ely cautioned that the Federal Business Records Act should not be construed as authorizing admission of any and all information that can be obtained from the records of businesses. *Id.* at 895.

123. 222 So. 2d 393 (Miss. 1969).

King court, acting without the benefit of a statutory business records rule, admitted into evidence computer sheets that purported to reflect the balance due on six conditional sales contracts. The plaintiff's accounting manager testified that the computer sheets were prepared under his supervision in the normal course of business. The court, citing *Seib*, decided to admit the sheets.[124] In doing so, the court maintained that it was not departing from the shop-book rule, but merely extending its application to electronic bookkeeping.[125]

The reported cases, however, are not clear about the type of testimony necessary to provide an adequate foundation for the admission of computer-generated data. In *Seib* and *King*, the individual directly responsible for the operation of the computer system testified and probably could have answered questions regarding the system. The witnesses in *Veres, Merrick*, and *De Georgia*, on the other hand, could, at the most, testify that they relied on the computer printouts to carry out their duties for the companies. From these cases it could be argued that the party offering the evidence need show only that the computer-generated data was used in the normal course of business, or was generated from computer-maintained data used in the normal course of business.

Some courts have applied a stricter test. In *Arnold D. Kamen & Co. v. Young*,[126] the plaintiff sought to introduce a computer-generated statement of accounts, purchases and sales. A witness testified that employees transferred information from written order blanks to keypunch cards which were then sent to a tabulating service that ran the cards through a computer and returned the printouts. Although the printouts were part of the business records of the company, the defendant argued that the data should not be admitted because the plaintiff had not shown that the original keypunch data was prepared by someone with personal knowledge of the act or event recorded. The court agreed, and held that the evidence was inadmissible.[127]

---

124. In sum, the court held that printout sheets of business records stored on electronic computing equipment are admissible in evidence if relevant and material, without the necessity of identifying, locating and producing as witnesses the individuals who made the entries in the regular course of business, if it is shown that: (1) the electronic computing equipment is recognized as standard equipment; (2) the entries are made in the regular course of business at or reasonably near the time of the happening of the event recorded; and (3) the foundation testimony satisfies the court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and justify its admission. *Id.* at 398-99.

125. In Brown v. Commonwealth, 440 S.W.2d 520, 524 (Ky. 1969), a Kentucky court also admitted computer records under the common law shop-book rule.

126. 466 S.W.2d 381 (Tex. Civ. App. 1971).

127. *Id.* at 387.

Confusion about the admissibility of computer-generated evidence is also created by uncertainty over the applicability of the Best Evidence Rule.[128] This rule, which requires introduction into evidence of the original document, raises questions about information that is stored in a computer or on punch cards or tape and is readable only by a machine. With such information, there is no record comparable to the conventional documentary original required by the Best Evidence Rule. The rule, however, does have a number of exceptions which might be applicable to computer printouts. One exception deals with original writings which are too numerous to produce or so complicated that their introduction would only confuse the jury. In such cases a summary or extract is admissible at the court's discretion.[129] A second exception excuses nonproduction of the original records when they have been lost or destroyed with no fraudulent intent on the part of the party introducing the evidence.[130] Computer printouts may be admissible under either of these two exceptions.

C. Unresolved Issues

The case law regarding computer-generated evidence leaves numerous questions unanswered. It is not clear from a reading of *King* whether the common law jurisdictions will admit evidence upon the less adequate foundations allowed in *Veres* and *Merrick*. Further, none of the cases have explored the difficulty of laying a proper foundation to demonstrate the reliability of a computer that arrives at a complex, independently contrived conclusion which is not necessarily verifiable by an examination of the input.[131] The cases discussed above have involved computer programs that simply store input and consolidate items at the time of output. In an EFTS, however, computers will be required to make interpretive evaluations in areas such as credit ratings and investment securities.[132] No case has specifically

128. FED. R. EVID. 1002. The Best Evidence Rule provides that in proving the material terms of a writing, the original writing must be produced unless, for an acceptable reason, it is unavailable. FED. R. EVID. 1004. For example, in *Harned v. Credit Bureau*, 513 P.2d 650 (Wyo. 1973), a computer printout was held inadmissible because the Best Evidence Rule was not satisfied since the original records had not been presented.

129. FED. R. EVID. 1006.

130. FED. R. EVID. 1004. *See* Comment, *Authentication and the Best Evidence Rule Under the Federal Rules of Evidence*, 16 WAYNE L. REV. 195, 228 (1969).

131. *See* Mills, Lincoln & Laughead, *Computer Output—Its Admissibility Into Evidence*, 3 LAW & COMPUTER TECH. 14, 16 (1970).

132. In a suit involving libel, the doctrine of qualified privilege has been applied where credit bureaus provide erroneous data regarding an individual to its subscribers. In an EFTS the burden of proving malice will be nearly impossible to meet and the qualified privilege nearly impossible to overcome, making the system virtually immune from libel suits.

eliminated the requirement of personal knowledge, which would not be present in a completely automated system, or judicially noticed the scientific reliability of computers. Nor has any criminal case decided whether or not the admission of printouts into evidence would violate a defendant's constitutional rights to confrontation or due process.[133]

Computer-generated evidence can prove dangerous in litigation because of the computer's ability to package hearsay and erroneous or misleading data in an extremely persuasive form. The means used to create the evidence must be carefully examined by trial courts to determine its admissibility, validity and probative value. Despite what appears to be a liberal construction of the rules of evidence by many courts, the reported case law in this area is superficial, and long-term developments are still speculative. An EFTS will certainly raise legal issues that will test both the common and statutory law of evidence—these will be novel issues for which both courts and lawyers must prepare.

IV. The Problem of Privacy

The implementation of credit card systems in the past two decades has fostered the creation of credit reporting agencies whose sole purpose is to collect data on an individual's financial status. In the process of compiling these records, a large amount of personal information is obtained. Formerly, once such information was provided, there was no assurance that it would not be used for purposes not consented to by the individual. In fact, a system of cooperation developed among the various credit bureaus whereby access to records was easily obtained by subscribers, bureau employees, police and federal investigators.[134] In many instances, individuals were denied credit and no reason was given for the rejection. The individual had no access to his records and could do little to remedy any inaccuracies.[135] As the use of computers increased, the collection, storage and use of personal and financial data grew.[136]

This new communications technology has given rise to serious concerns about whether privacy will be adequately safeguarded in an EFTS. The information provided by credit bureaus differs in quality and value from that

133. *See* Mills, Lincoln & Laughead, *supra* note 131, at 21.

134. *See* Ross, *supra* note 77.

135. *See Hearings on S. 823 Before the Subcomm. on Invasion of Privacy of the House Comm. On Government Operations*, 90th Cong., 2d Sess. 3 (1968).

136. *See* Campbell & Woods, *Computers and Freedom*, 2 Law & Computer Tech. 3 (1969).

which an EFTS can supply.[137] Unlike an EFTS, credit bureaus lack the ability to provide large amounts of in-depth information about individuals; the available data has been maintained by credit bureaus on a decentralized basis, and the highly mobile nature of our society has made it difficult to update credit information. Moreover, access to credit bureau data has not always been easy to secure and few people have the ability to interpret it.

An EFTS, however, will be different. It will be possible to secure much greater detail as to the time, place and character of an individual's financial transactions. Numerous persons will potentially have access to the totality of the individual's existence. EFTS will, therefore, raise two major questions: (1) can the individual's privacy be protected?; and (2) can the potential for governmental abuse be minimized?[138]

A. The Fair Credit Reporting Act

The inadequacy of common law remedies and the great potential for abuse allowed by computerized credit reporting led Congress in 1970 to pass the Fair Credit Reporting Act (FCRA).[139] The FCRA was designed to protect the consumer by requiring reporting agencies to adopt reasonable procedures to assure the confidentiality, accuracy and proper use of credit information.[140] The Act applies to information collected by banks, credit card companies and other credit reporting agencies and limits the release of consumer reports to third parties. These institutions are also required to keep current files,[141] and upon request, to provide the consumer with all the information contained therein, including the source of the information.[142] If the consumer disputes the truth of any material in his file, the agency is required to reinvestigate the information unless it believes the dispute to be frivolous or irrelevant.[143] The FCRA also denies access by government agencies to all but identifying data,[144] except when the governmental body seeks the data for one of the permissible purposes listed in the Act.[145] Also, whenever an adverse report is the basis for a denial of credit, the individual must be ad-

137. *See* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society*, 67 MICH. L. REV. 1108, 1109 (1969).

138. It certainly can be stated that a system which records every financial transaction of an individual is open to governmental abuse.

139. 15 U.S.C. § 1681 (1970).

140. *Id.*

141. *Id.* § 1681c.

142. *Id.* § 1681g.

143. *Id.* § 1681i.

144. *Id.* § 1681f.

145. *Id.* § 1681b.

vised of the nature and substance of the information;[146] he must also be told the identity of the source of the information, if it is a credit reporting agency.[147] In addition, reporting agencies must inform consumers of the existence of investigative reports secured from interviews with friends, neighbors and relatives;[148] and agencies must inform the consumer of his rights regarding the reports, and must comply with any request by him that the information be disclosed.[149] The FCRA also applies to the use of computers by these agencies:

> Consumer reporting agencies employing automatic data processing equipment, particularly agencies that transmit information over distances by any mechanical means, must exercise special care to assure that the data is accurately converted into a machine-readable format and that it is not distorted. . . . Procedures must also be adopted that will provide security for such systems in order to reduce the possibility that computerized consumer information will be stolen or altered. . . .[150]

The FCRA also imposes criminal sanctions against individuals who obtain information about an individual from a consumer reporting agency under false pretenses.[151] Civil remedies are available to a consumer against a credit agency that willfully or negligently fails to comply with the Act.[152]

The FCRA, however, does not limit the kind of information that can be gathered or reported; nor does it allow a consumer to have physical access to his file or to possess a copy of it. Even if this were not the case, however, in a completely automated EFTS it would probably be extremely difficult to gain access to or possession of credit records since under an EFTS, data will be more detailed and more centralized.

Problems of inaccuracy and abuse will still arise under an EFTS. Consequently, the consumer must be guaranteed access to the information stored on him. The highly centralized nature of the data will require greater limits on access since the potential for danger of release of information would be greater with such a system. The Fair Credit Reporting Act is a step in

---

146. *Id.* § 1681m.
147. *Id.*
148. *Id.* § 1681d.
149. *Id.*
150. FEDERAL TRADE COMMISSION, DIVISION OF SPECIAL PROJECTS, BUREAU OF CONSUMER PROTECTION, COMPLIANCE WITH THE FAIR CREDIT REPORTING ACT 8 (1970).
151. 15 U.S.C. § 1681r (1970).
152. *Id.* §§ 1681n, 1681o. The consumer, of course, bears the burden of proving such noncompliance. *See* Note, *Consumer Protection: Regulation and Liability of the Credit Reporting Industry*, 47 NOTRE DAME LAW. 1291 (1972).

the right direction, but more legislation with both criminal and civil liabilities will be needed.

B. The Bank Secrecy Act of 1970

The Bank Secrecy Act (BSA)[153] requires the maintenance of records and the reporting of financial transactions to the government by certain individuals and financial institutions.[154] Although Congress passed the Act in order to aid the Government in its law enforcement activities against organized crime and to prevent the maintenance of secret Swiss bank accounts, the BSA record keeping and recording requirements could be applied to an EFTS. The Government, pursuant to the BSA, could obtain access to a centralized data bank of financial transactions in order to aid a criminal, tax or regulatory investigation.[155] There can be no doubt that a future bureaucrat, under the pretext of conducting such an investigation, could gain access to an immense amount of data regarding an individual.[156] If an EFTS is to serve a legitimate function, rather than become a tool for governmental abuse, legislation is needed to prevent such access and to punish violators through both criminal and civil liabilities.

C. Privacy Problems Unique to an EFTS

While mistakes in input, storage or delivery of information appear to be covered by the laws of defamation and negligence, the doctrine of qualified privilege has been applied in libel suits where credit bureaus provide erroneous information to subscribers who had legitimate business interests.[157] The privilege can only be overcome by a showing of malice,[158] or by proving a

153. Pub. L. 91-508, 84 Stat. 114 (codified in scattered sections of 12, 31 U.S.C.).

154. 31 U.S.C. §§ 1082, 1101(a), 1121(a) (1970). The constitutionality of the Act was upheld in California Bankers Ass'n v. Schultz, 416 U.S. 30 (1974).

155. *See* 12 U.S.C. § 1829b(a)(2) (1970).

156. Justice Douglas, in his dissent in California Bankers Ass'n v. Schultz, 416 U.S. 30, 85, observed that:

> A person is defined by the checks he writes. By examining them the [government] agents get to know his doctors, lawyers, creditors . . . and so on ad infinitum . . . . [T]hese . . . items will . . . make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.

157. *See* Wetherby v. Retail Credit Co., 235 Md. 237, 201 A.2d 344 (1964); Shore v. Retailers Commercial Agency, Inc., 342 Mass. 515, 174 N.E.2d 376 (1961); Barker v. Retail Credit Co., 8 Wis. 2d 664, 100 N.W.2d 391 (1960). Some state courts and English courts deny the privilege on the ground that credit bureaus are mere business ventures trading for profit in the characters of other people. *See, e.g.*, Pacific Packing Co. v. Bradstreet Co., 25 Idaho 696, 139 P. 1007 (1914).

158. *See, e.g.*, Hooper-Holmes Bureau v. Bunn, 161 F.2d 102 (5th Cir. 1947).

conscious indifference or reckless disregard for an individual's rights.[159] The privilege can also be vitiated by showing that the subscriber did not have a legitimate interest in the report or that it was released to the general public.[160] However, when applied in a case involving an EFTS, the qualified privilege doctrine could prove more difficult to overcome. As computers become more complex and sophisticated under an expanding EFTS, they will be able to make evaluative judgments as well as direct feedbacks based upon stored data. Testing a computer's judgment would place an inordinate burden on the consumer to prove liability, as he would have to establish that the computer was maliciously misguided in its evaluation by some individual. Moreover, in an EFTS, a retailer with an on-line connection with the financial institution through a clearinghouse would likely be considered a privileged individual.

The doctrine of negligent misstatement could impose liability on banks and other participants in the EFTS if erroneous information were fed into or printed out of the computer due to the financial institution's failure to exercise reasonable care. At present, however, many jurisdictions have not adopted this theory as a basis for imposing liability for inaccuracies in credit information.[161]

Although individual privacy must be protected in an EFTS, reasonable investigations of credit should be permitted. Consequently, some form of regulation that will properly balance the competing interests will be necessary.

V. The McFadden Act and Bank Branching Restrictions

A national EFTS would involve the widespread installation of terminals in shopping centers and retail stores. At present, the major federal agencies which regulate banking have determined that EFTS terminals are not bank "branches."[162] Many states, however, take the opposite position.[163] A debate is presently raging between the states and the federal government over which governmental authority will regulate EFTS development. No clear

159. *See, e.g.*, Mil-Hall Textile Co. v. Dun & Bradstreet, Inc., 160 F. Supp. 778 (S.D.N.Y. 1958); Dun & Bradstreet, Inc. v. Robinson, 233 Ark. 168, 345 S.W.2d 34 (1961).

160. *See, e.g.*, Watwood v. Stone's Mercantile Agency, 194 F.2d 160 (D.C. Cir. 1952); Galvin v. New York, N.H. & H. R.R., 341 Mass. 293, 168 N.E.2d 263 (1960); Mitchell v. Bradstreet Co., 116 Mo. 226, 22 S.W. 358 (1893).

161. *See* Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 Geo. L.J. 509, 517 (1969).

162. *See* 12 C.F.R. §§ 545.14-5 (1976).

163. Currently, 12 states prohibit branch banking altogether; 21 allow it within a limited geographical area; and 18 allow statewide branching.

basis for agreement has yet emerged, but since many states have strict branching restrictions,[164] the development of a national EFTS may well hinge on the outcome of this debate.

The McFadden Act[165] is of no value to national banks in this conflict. The Act provides that national banks are authorized to establish branches only to the extent that state banks are allowed under state law.[166] If EFTS terminals are held to be branches within the McFadden Act, state restrictions on branching may inhibit the development of such terminals within the national banking system and thereby prevent the establishment of a national EFTS. Even those states that allow bank branching generally impose certain restrictions.[167] Thus, even if all the states were to amend their laws and allow terminals to be set up in stores and shopping centers, the characterization of them as branches would still subject them to regulatory restrictions.

On the other hand, if EFTS terminals are held not to be branches under the McFadden Act, the national banks will be regulated solely by federal authorities,[168] and federal control would likely be more permissive. In December 1974, the Comptroller of the Currency stated that his office would allow national banks the widest latitude to experiment with and develop customer-bank communication terminals (CBCTs).[169] The Comptroller was

164. Arkansas, Iowa and North Dakota, for example, restrict branching functionally as well as geographically. *See* ARK. STAT. ANN. § 67-340 (Supp. 1973); IOWA CODE ANN. § 524-1201 (Supp. 1974); N.D. CENT. CODE § 6-03-14 (Supp. 1973). *See also* ALA. CODE tit. 5, § 125(1) (1960); GA. CODE ANN. § 13-203(1) (Supp. 1974); MASS. ANN. LAWS ch. 172A, § 12 (Supp. 1974); N.H. REV. STAT. ANN. § 384-B:2 (1968); OHIO REV. CODE § 1111.02-.03 (Supp. 1973). The case of Independent Bankers v. Camp, 357 F. Supp. 1352 (D. Ore. 1973), is a further illustration of the difficulty an EFTS could meet when state branching laws are applied. The Comptroller of the Currency authorized an Oregon national bank to install two customer operated terminals that were activated by specially coded BankAmericards. The state superintendent of banks argued that these terminals were not the type of branches authorized by the state statute. The court held the terminals in question to be improperly authorized because they did not meet the state's statutory test of serving the public convenience and advantage. Oregon has since amended its law to specifically allow customer operated communication terminals. ORE. REV. STAT. § 714 (1973).

165. 12 U.S.C. §§ 36, 332 (1970).

166. *Id.* § 36.

167. *See, e.g.*, Independent Bankers v. Camp, 357 F. Supp. 1352, 1354-55 (D. Ore. 1973).

168. *See* Ruling and Opinion of the Comptroller of the Currency, issued on December 12, 1974. 12 C.F.R. § 7.7491 (1975).

169. Recently, however, the Comptroller amended his December 12, 1974 ruling under state pressure. National bank CBCTs are now restricted to locations within 50 miles of the bank's headquarters or nearest office or branch, unless the terminals are shared with one or more local financial institutions. This amendment was designed to allay state fears that larger banks would increase their market share at the expense of small banks. *See* Wall Street Journal, May 12, 1975, at 12, col. 3.

obviously concerned that the competitive position of national banks might erode vis-à-vis competition from other federally chartered institutions.[170] Whether national banks will be able to develop an EFTS free of state restrictions will depend largely on whether the off-premises CBCTs will fall within the Act's definition of a "branch."

A. Statutory Definition of a "Branch" Bank

Section 36(f) of Title 12 of the United States Code, originally part of the McFadden Act, defines a "branch" as follows:

> [A]ny branch bank, branch office, branch agency, additional office, or any branch place of business located in any state or territory of the United States or in the District of Columbia at which deposits are received, or checks paid, or money lent.[171]

In applying this statutory definition, a CBCT can be analyzed in terms of three things: (1) the situs of the transaction; (2) the physical characteristics of the terminals; or (3) the functions performed by the terminals.

In the Comptroller's opinion, the CBCT is compared to a mailbox, serving as no more than a conduit.[172] Thus, opponents of state regulation argue that the transaction is actually consummated at the banking house, and not at the CBCT.[173] Supporters of state regulation argue that this view ignores the role of the customer, who can complete his own participation in these transactions at the site of the terminal. Both of these viewpoints are reasonable in light of the electronic transaction itself, which really involves two sites, that is, the computer at the bank and the terminal itself.[174] It would thus appear that any attempt to fix a single situs must ultimately fail. Therefore, the situs of a transaction will be of little help in defining a "branch."

---

170. The Comptroller's office is also concerned about competition from federal savings and loan associations. The Federal Home Loan Bank Board (FHLBB) issued a ruling in June 1974, allowing federally chartered savings and loan associations to establish remote service units that can transfer funds, accomplish cash withdrawals, and receive loan payments. 39 Fed. Reg. 23991 (1974). Federal savings and loan associations, unlike national banks, are not subject to state branching restrictions. 12 C.F.R. § 545.14 (1974). In August 1974 the National Credit Union Administration issued a ruling allowing credit unions to establish pilot programs involving the use of similar remote terminals. 39 Fed. Reg. 30107 (1974).

171. 12 U.S.C. § 36(f) (1970).

172. 39 Fed. Reg. 44418 (1974).

173. *See id.* at 44421.

174. The Attorney General of Kansas issued an opinion stating that an on-line terminal is not a branch because the transaction is performed in the bank's computer. KAN. OP. ATT'Y GEN. No. 74-196 (June 12, 1974). The opinion was criticized by the Assistant Bank Commissioner of Kansas, who argued that many banks in the state relied on the computers of correspondent banks to do their data processing, and thus no transactions took place on the bank's premises. American Banker, Jul. 8, 1974, at 1.

The Comptroller has also pointed out that the CBCT is not an additional office because it does not possess the physical characteristics of a teller window.[175] Opponents of state regulation note that a CBCT more closely resembles a vending machine than a banking office. Supporters, however, point out that the Act is directed at any form of an office at which banking functions are performed.[176] Thus immersed in controversy, physical characteristics also will not help to define a "branch."

The Comptroller also has pointed out that the store, rather than being an agent of the bank in performing CBCT-related functions, has a bona fide business purpose of its own.[177] Supporters of state regulation argue that the Act specifically includes within its definition of "branch" any office which receives deposits, pays checks, or lends money.[178] Store terminals would certainly perform some or all of these services; therefore, under this view, any store with bank-owned terminals that transfers information and funds could be defined as a branch. It thus appears that the question of when a CBCT is a branch cannot be resolved solely by an examination of the statutory language of the McFadden Act. An examination of the legislative background of the Act is, therefore, appropriate.

In 1923, the Attorney General of the United States determined that the incidental powers of national banks included a power to establish teller windows remote from the bank's main office.[179] The United States Supreme Court overturned this ruling in *First National Bank v. Missouri ex rel. Barrett*.[180] A month later Representative McFadden introduced a bill to allow national banks to establish branches within their own cities if state banks were allowed to do so by state law.[181] Opponents of branching by national

---

175. 39 Fed. Reg. 44418 (1974).

176. For a discussion of this point, see H.R. REP. No. 583, 68th Cong., 1st Sess. 3 (1924).

177. 39 Fed. Reg. 44422 (1974).

178. 12 U.S.C. § 36(f) (1970).

179. 34 OP. ATT'Y GEN. 1, 5 (1923). The legal basis for his opinion was the National Bank Act of 1864, ch. 106, § 8, 13 Stat. 101, *as amended*, 12 U.S.C. § 24 (1970), which permitted national banks to exercise "all such incidental powers as shall be necessary to carry on the business of banking."

180. 263 U.S. 640 (1924). The Supreme Court concluded that "the mere multiplication of places where the powers of a national bank may be exercised is not . . . a necessary incident of a banking business." *Id.* at 659. In response to the Attorney General's argument that the power to establish teller windows had become "necessary" because of competition with branch offices of state banks, the Court replied that Congress alone could remedy this situation. *Id.*

181. The original bill introduced was H.R. 8887, 68th Cong., 1st Sess. (1924). The bill failed to pass the Senate, however, and was reintroduced in the House as H.R. 2, 69th Cong., 1st Sess. (1926).

banks feared that if the Court someday overruled *Barrett*, national banks would set up numerous branches and take over the business of local banks. The Act's definition of a branch must be viewed in this context. In balancing the views of those for and those against branching, Congress in effect placed the responsibility for deciding whether branching was a sound public policy on the individual states. The states were to weigh the benefits of convenience against the threat of monopolization.[182] Congress, therefore, defined "branch" broadly enough to include teller windows, but, with no consideration of possible technological changes, failed to define the limits of branching. This task was left to the courts.

B. Judicial Definition of the Limits of Branching

The question left unanswered by the McFadden Act was the extent to which state policy would govern the manner in which national banks established branch offices. In the leading case of *First National Bank v. Walker Bank & Trust Co.*,[183] the Supreme Court held that the Comptroller was required to follow a Utah statute that permitted establishment of a branch bank only by acquisition of an existing bank that had been in operation for five years or more. The Court found untenable, in light of the McFadden Act, the Comptroller's argument that once a state authorized branching, federal standards determined the criteria for allowing national banks to branch in that state. The Court pointed out that the intent of Congress was to leave the question of desirability of branch banking to the states.[184] Under this view, the Comptroller must apply the state statutory provisions in their entirety when he is considering a national bank's application for a branch. The Court's concern was that since national and state banks compete on an individual basis, neither should have branching privileges unavailable to the other. *Walker Bank*, however, did not consider what activities would constitute the establishment of a branch bank.

Subsequent to *Walker Bank*, new types of banking facilities, such as drive-in teller windows, armored car messenger services, and deposit machines, have become increasingly common.

In 1966, the Comptroller issued a number of interpretive rulings authorizing national banks to operate mobile messenger services and off-premises deposit machines without regard to state branch banking restrictions.[185] The Comptroller took the position that the armored car messengers acted as

182. *See* Comment, *Federalism in Interpretation of Branch Banking Legislation*, 32 U. CHI. L. REV. 148, 160 (1964).

183. 385 U.S. 252 (1966).

184. *Id.* at 260.

185. 12 C.F.R. §§ 7.7490, 7.491 (1966).

agents of the customers in delivering bank deposits, and that transactions at the deposit machines were not completed until the verification and crediting of deposits at the main banking house. Pursuant to the Comptroller's authorization, the First National Bank in Plant City, Florida established an armored car messenger service and a stationary receptacle for deposits. Florida prohibited branching, and state officials protested. The bank then sued for declaratory and injunctive relief, and the district court upheld the Comptroller's ruling in *First National Bank v. Dickinson.*[186] The court found that since no deposits were received, and no checks paid or money lent at these off-premises facilities, they could not be considered as branches.[187]

The Fifth Circuit reversed this decision, concluding that state statutes and their interpretations by state bank supervisors and courts would control the definition of a "branch" for national banks, just as they did for state banks.[188] The Supreme Court affirmed the Fifth Circuit's judgment, holding that deposits had been received off-premises in violation of federal branch banking restrictions.[189] The Court found, however, that the definition of a "branch" was a matter of federal law,[190] and stated that "[t]he term 'branch bank' at the very least includes any place for receiving deposits or paying checks or lending money apart from the chartered premises; it may include more."[191]

Furthermore, the Court noted that the Comptroller had been unreasonable in ruling that the armored cars and deposit receptacles were not branches. According to the Court, the capacity to provide these services gave national banks an advantage over state banks,[192] and such an advantage would disrupt competitive equality, the keystone of the McFadden Act.

As construed in *Dickinson*, the federal definition of a "branch" in section 36(f) appears to be exceedingly broad. A national bank employing CBCTs would certainly enjoy a competitive advantage over state banks forbidden to do so. According to *Dickinson*, any inequality between state and federal banks could be sufficient to bring the branching prohibition into play, and thus limit development of an EFTS by national banks alone.

C. CBCTs and Branching

Whatever the merits of the various arguments, Congress chose in the McFadden Act to allow the states to adopt their own regulations on bank

186. 274 F. Supp. 449 (N.D. Fla. 1967).
187. *Id.* at 454.
188. Dickinson v. First Nat'l Bank, 400 F.2d 548, 557-58 (5th Cir. 1968).
189. First Nat'l Bank v. Dickinson, 396 U.S. 122 (1969).
190. *Id.* at 133-34.
191. *Id.* at 135.
192. *Id.* at 137.

branching. The courts have not upset this policy. In deciding whether the CBCT, or any other off-premises facility constitutes a branch, we ought first to examine in detail the rationale for the prohibition against branches.

Opponents of branching argue that a fully developed branch banking system will tend to concentrate resources in the hands of a few banks. Branch banks, unlike local banks, are seen as outsiders, which represent a concentration of capital in the hands of a few national banks that are mostly concerned about big business and will ignore the needs of the local community.[193] These critics fear that a market which includes nothing but a few branch systems may close out the small local businessman.[194]

CBCTs will be open to the same attacks. A computer terminal system, however, can be programmed to serve multiple banks with complete impartiality. Bank service corporations, which at present provide data processing services to a number of small banks, could expand their operations to include CBCTs. Large banks, owning the system, could allow smaller ones access to it. Even the current credit card system might provide a basis for such cooperation, and a clearing house could provide the communications link between the customer at his terminal and his own individual bank.[195] Such a system would provide first rate technology to all its members regardless of size. Thus, if the purpose of state branching restrictions is to protect small banks from the large national banks, this end could be accomplished without prohibiting CBCTs.

At present, however, CBCTs are most likely to be installed by large banks and operated by them for their own use.[196] This would obviously give these banks an added advantage over their competitors. It would also reinforce the fears of critics who see branching as a tool of national banks to destroy competitors. CBCTs could also enable large banks to control the money market.

The judicial attitude manifested in *Dickinson* would seem to support the states in a showdown with the national banks. Therefore, if EFT is to become a reality, CBCTs should be made available to both large and small banks. In order to be viable, an EFTS must make available to local banking

193. *Compare* 71 CONG. REC. 5011 (1929), *with Hearings on Conflict of State & Federal Banking Laws Before the House Comm. on Banking and Currency*, 88th Cong., 1st Sess., ser. 1, pt. 3, at 26 (1963) (statement of Dr. Robert Lanzillotti, Chairman, Department of Economics, Michigan State University).

194. *See Hearings on Conflict of Federal and State Banking Laws, supra* note 193.

195. *See generally* Homrighausen, *One Large Step Toward Less-Check: The California Automated Clearing House System*, 28 BUS. LAW. 1143 (1973).

196. Since CBCT equipment is expensive, sophisticated and intricate, large banks are likely to be the first users and may well monopolize or control it.

interests the advantages of technology in a spirit of cooperation. Some steps have already been taken to assure small banks an access right to essential components of this system.[197]

An EFTS which does not threaten the federal policy of allowing states to regulate branching as a means of protecting their local banks may be able to survive within the confines of the McFadden Act. Supporters of EFT even argue that it will spur rather than hinder competition by freeing banks from the enormous load of paperwork under which they presently find themselves.[198] Supporters also contend that the Federal Home Loan Bank Board's decision to allow federal savings and loan associations to establish off-premises CBCTs is a threat to the market balance between those institutions and commercial banks.[199] They point out that the McFadden Act had as its objective the strengthening of the national banking system, and that the Act should not now be used to thwart the development of a technology wholly unrelated to the original concerns about branch banking. The controversy over the branch banking aspects of CBCTs continues, and could easily hinder the development, and perhaps even the economic feasibility, of an EFTS.

VI. CONCLUSION

This survey has attempted to describe the forces leading toward a checkless society and several of the problems facing the development of an EFTS. The present check system has numerous flaws. As the volume of paper continues to increase, so does the incentive to develop a less expensive alternative system. The credit card system has facilitated the development of an EFTS because it has accustomed the public to computer finance, and has laid the groundwork for an electronic payment system.

The computer, however, has shown itself to be vulnerable to attack by both criminals and terrorists. An EFTS utilizing several hundred computers will provide unlimited opportunities for those who seek to either manipulate or destroy it. Our society may very well be opened to new forms of blackmail and robbery. As has been seen, a highly sophisticated EFTS may increase the vulnerability of technical societies to both internal and external attack. In a single attack, a small band of extremists could easily cripple, if not destroy, the monetary data banks of this country. A handful of sophisticated

197. *See* American Banker, May 20, 1974, at 1.

198. An EFTS, by eliminating costly paper checking, would reduce the costs of transfers to less than a penny per item. 59 FED. RES. BULL. 875 (1973).

199. *See* Brooke, *Problems in EFT Development Extend Beyond Considerations of Technology*, American Banker, Nov. 20, 1974, at 1.

criminals could easily steal millions of dollars and, given our present system of laws, could live to enjoy the money for many years.

The threat to our privacy would be seriously increased by the establishment of an EFTS, and the tendencies toward totalitarian control could be enhanced and reinforced. The moneys of the citizenry would be recorded for any governmental agency to obtain in minutes. All purchases, movements and contributions would be stored in computers, presenting great potential for abuse.

An EFTS, unless regulated, would also pose a threat to small businesses and further augment the accumulation of capital in the hands of a few banks, for they alone would have sufficient resources to develop and best utilize an expensive national EFTS. These are but some of the challenges that face such a system. Unless they can be met, at an acceptable cost, it may well be that the system will never develop.