
James V. Vergari
LATENT LEGAL REPERCUSSIONS IN ELECTRONIC FINANCIAL SERVICES AND TRANSACTIONS†

by JAMES V. VERGARI∗

TABLE OF CONTENTS

I. LEGAL STRUCTURE ....................................... 185
   A. FEDERAL LAW CONCERNING ELECTRONIC FINANCIAL
      TRANSACTIONS ........................................... 185
      1. Electronic Funds Transfer Act ...................... 185
      2. Truth-in-Lending Act ................................ 187
      3. Fair Credit Billing Act .............................. 188
   B. PROPOSED UNIFORM NEW PAYMENTS CODE .......... 188
   C. STATE STATUTES REGULATING ELECTRONIC FINANCIAL
      SERVICES AND TRANSACTIONS ........................... 188
   D. DOMESTIC AND INTERNATIONAL TRANSFER OF FUNDS ...
      1. Domestic Transfers .................................. 191
      2. International Transfers ............................. 191

II. POTENTIAL PROBLEMS .................................. 193
   A. COMPUTER-RELATED CRIME AND ABUSE ..................... 193
      1. Violent Crimes Against the Computer System .... 194
      2. Robbery or Assault of Users ........................ 194
      3. Insider Crime ........................................ 195
      4. Unauthorized Use .................................... 195
      5. Theft of Valuable Computer-Store\ed Assets .... 196
   B. COMPUTER FRAUD AND ABUSE .......................... 196
      1. Credit Card Fraud .................................. 196
      2. Electronic Thefts .................................... 197
      3. In-House Embezzlement ............................ 197
   C. COMPUTER ERROR OR FAILURE ......................... 198

† © James V. Vergari 1984.
* Adjunct Professor of Law, University of San Diego School of Law. Retired Senior Vice President and General Counsel, Federal Reserve Bank of Philadelphia. Attended Wharton School, University of Pennsylvania 1929; B.S. University of Scranton 1937; J.D. Temple University School of Law 1942. Life member of the American Law Institute.
The main force driving the economy in the next ten years will be information-based technology, including computers, factory automation, and communication systems for home and business. Electronic Funds Transfer (EFT) and Paperless Entry Payment (PEP) systems will become increasingly prevalent. Those systems can transfer data and information relating to financial transactions through a series of communication networks. For example, a transaction may begin with the entry of data at the point-of-sale or transfer and culminate in computerized bookkeeping at a depository financial institution many miles away. Unlike the present paper-based system, transfers or payments under an EFT/PEP system will be electronic. Electronic or electromagnetic impulses will be transmitted from terminal to terminal, computer to computer, utilizing thousands of miles of wire, microwave carriers and satellite transmitters. These transmission systems will be used to enhance the financial services products and to relay data and information regarding funds transfers and payment transactions.

Electronic financial services also may be provided by non-financial enterprises. Large brokerage firms offer “customer financial management accounts” against which checks may be written or credit card purchases charged. Further, several large retailing organizations and private money-order companies offer payment and

transfer of funds services. The trend is toward homogenization of financial institutions, with depository institutions becoming increasingly similar in transfer of funds, payment powers, and in the rules by which they compete. Conversely, financial institutions are also offering new kinds of financial services (e.g., discount brokerage and insurance). The line between the financial and nonfinancial sector is blurring.

Financial services and payment systems entered the electronic age in the 1960s. Third generation computer systems and advanced telecommunication systems made large data-bases readily available to users at remote locations. Costs of data conversion and storage dropped rapidly and software became more sophisticated and reliable. The result was a transformation in the handling of financial data for both individuals and organizations. New technology is causing a revolutionary change in the processing of financial transactions and in the communication of information, spawning a myriad of new financial service products. Among these are certificateless securities and "book entry" electronic systems for their handling, cash management and financial planning services, and Videotex.

Advancing electronic technology and rapid development of new financial products and services increase the exposure of service-providers to risk and monetary losses. Total computer fraud losses are estimated to average between $3 billion and $5 billion a year. In electronic funds transfers, loss may occur from unauthorized access to funds, internal theft, external eavesdropping, fraud from intruders and electronic interceptors, and errors and omissions caused by employees or agents. Figures suggest losses from fraud at automated cash withdrawal machines are currently nowhere near that experienced by credit card issuers. This is due in part to personal identification numbers, daily cash withdrawal limits, and the limited

---

2. The "book entry" system is a method of storage and representation of financial assets (e.g., bonds and other debt securities) through electronic data processing systems that record everything from bank account balances to investment securities. No physical security is ever issued; transfer, settlement and delivery for buying and selling purposes is done electronically.

3. Videotex is an embryonic application of new technology promising a new medium for transmitting information from a host computer to a television set or personal computer, giving the consumer/user home access to shopping, library services, banking and other financial transaction services, and a wide variety of electronic services (e.g., business statistics, commercial information, news, stock prices), from distant computer information data bases.

number of automated cash withdrawals.\textsuperscript{5}

Litigation involving electronic financial transactions is frequently based on contract-related disputes (e.g., scope of service, warranties, disclaimers, and limitations or remedies), common law fraud (e.g., misrepresentation), negligence (failure to act reasonably so as not to damage others), and other torts. Although these areas of the law have old and well established roots, the law with regard to computer service products has developed only recently. The litigation generally concerns the computer product resulting from the capability of computer systems to access, analyze, process, summarize, and report data and information. As always, when old legal principles are used to meet new needs, problems and ambiguities arise. The resulting patchwork of statutes and case law lags far behind the new and developing needs of society.

This Article examines the legal repercussions of electronic financial services and transactions and the effect of the movement by society into an environment where financial service products will be provided without paper. The treatment of the problems is not exhaustive. The conclusions offered are tentative, an appropriate posture since so many facets of electronic financial transaction services are as yet undeveloped. Nevertheless, the legal problems presented by paperless entry or fund transfer systems and electronic banking are of some immediacy, because these systems will fundamentally alter current patterns of business practice. Electronic financial services will change the way in which financial institutions deal with their customers, and will change the existing competitive balance among financial and nonfinancial providers of services. Important and difficult regulatory and legal questions are presented. Also, because EFT and PEP will generate an expanded and more easily accessible data-base of information regarding the behavior of citizens, significant constitutional questions will arise.

EFT and PEP systems exploiting data processing and communications technology for electronic transfer of funds and other financial transactions emerged in the early 1970s. EFT and PEP are mechanisms for processing value exchanges (debit or credit orders) using properly instructed electronic equipment, interfaced to various institutions through switching centers and facilitators. Bank check processing and collection is the keystone of paper-based payments and transfer of funds and remains one of the most important routine services of commercial banks.\textsuperscript{6} Spurred by the mounting

\textsuperscript{5} Tyson, On-Line Discount Broker Expects A Rush of Competition From Banks, Am. Banker, Feb. 21, 1984, at 1, col. 2.

\textsuperscript{6} During 1982, 37.7 billion checks for $29.3 trillion were processed by the bank-
problems of transporting, processing, accounting, and storing the paper generated in the check payment system, financial institutions have increasingly utilized electronic computer technology to process checks and deposits and to increase customer accessibility to money transaction information. The computer has thus fundamentally altered the delivery and processing of financial services by making possible electronic funds transfers and paperless entry transactions. This has created legal issues and transitional relationships among the participants (e.g., consumer and other customers, institutional providers of financial services, vendors of goods and services, telecommunication utilities, facilitators and switches).

EFT and PEP are properly viewed not only as systems for delivery of a new variety of electronic financial services, but also as alternatives to paper-based means of transferring funds and making payments. The introduction of debit cards, "In-Home" banking services, and electronic shopping will eventually slow check usage, but check usage will continue to expand at a fairly steady rate throughout the next decade. The "cashless/less-checks" society that futurists predicted in the 1960's is still a few decades away.

Existing microcomputer, data processing, and telecommunication technology is more than adequate to support a vast array of electronic financial service products for quasi-self-service banking. This technology has given rise to delivery innovations for providing financial transaction services. Among these are: (1) Automated Teller Machines (ATMs); (2) point-of-sale (POS) terminals;

---

7. In a pure paperless entry payments (PEP) and electronic funds transfer (EFT) environment, physical deposit and collection processing of checks would be replaced by a series of electrical impulses communicated between computers that would read and process the information and instructions, and transfer the funds from institution to institution and from the drawer/remitter to the authorized recipient while performing the necessary transmission and deposit accounting functions. Payment and debit/credit entries would be almost instantaneous, and no paper would need to be produced. Plastic access cards and paperless payment entries are not cash nor its equivalent. They are simply substitutes for checks and cash in payment transactions: a form of "electronic" or "computer" money. The computer cannot verify the drawer's signature or the authorized user of the plastic access card, unless the related personal characteristics are pre-stored in the related data base and communicated at the time of use.

8. Unattended facilities consisting of intelligent terminals (ATMs or other remote service/transaction units), installed either on the premises or elsewhere, give a financial institution the means through which its customers with authorized access
devices and valid user identification can withdraw cash, make deposits, inquire about account balances, move funds from one account to another, and make payments on loans or credit card accounts, all without human intervention. Shared ATM networks permit authorized customers to withdraw money at other ATMs or POS terminals on the network in which their account institution is a member. NATIONAL COMMISSION ON ELECTRONIC FUNDS TRANSFERS FINAL REPORT, Appendix C at 345 (hereinafter cited as NCEFT).

9. POS terminals are designed to receive information concerning payment or transfer of funds and transmit that information from the unattended terminal, usually located in a retail establishment, to the financial institution's main computer. Thus, with the proper plastic access card (e.g., credit card, debit card) and the required (secret) customer/user identification, data entered at the POS can be recorded at the account institution, debiting the customer's account and crediting the retailer's account for the transaction. The purchase effected through the POS terminal is completed with the finality of a cash transaction. The POS facility may also be used by the retailer to retrieve data concerning the related transaction for the operational needs of the business enterprise where the terminal is situated. It may also be used for cash withdrawals from the user's account at the issuer institution. POS terminals can also be used for processing check authorization or verification cards and for credit card charges or inquiries. POS terminals provide many convenient ways for the customer to buy goods and services. Functionally, the POS terminal replaces the cash register. A POS debit card transaction results in a direct debit to the demand deposit or transaction account at the buyer/user's financial institution, similar to a check or ATM transaction. Id. at 341.

10. Banking-by-phone service includes bill paying and other financial transactions performed using the telephone. A customer, generally a consumer, by prearrangement with a financial institution offering a telephone bill-paying service, uses a telephone and an appropriate identification code to instruct the financial institution to transfer funds from his or her account to the account of the designated creditors. In most cases, the customer communicates directly with the institution's computer, utilizing the various frequencies produced by a push-button telephone. Id. at 345.

11. The electronic debit card is the electronic heir apparent to the personal check, and the next step in the evolution of an electronic payment mechanism. Debit cards ("computer money") are required to access ATMs, POS terminals, and other EFT mechanisms in order to withdraw cash or transfer immediately available funds. The parties involved in an electronic debit card transaction are: the customer/user; recipient (e.g., vendor, service or professional groups) who accepts the debit card as a cash payment for the transaction; the facilitator (the service unit or switch involved in the telecommunication process); and the payor financial institution which issued the debit card.

At present, many debit card transactions are not entirely electronic: a paper charge or debit order is produced and used as input to complete the transaction. Electronic debit cards access the cardholder's demand deposit account rather than a line of credit as with a credit card. Thus more care should be taken with debit card transactions than with credit card transactions. Error as to one's credit is less serious than error as to amounts in one's bank accounts. Garson, Debit Cards Spur MasterCard Push on Payments Network, Am. Banker, May 4, 1983, at 14, col. 1. A debit card is similar in nature to a check as a funds transfer or payment device. The confidential code or personal identification number (PIN) for use with the debit card to
financial services;\textsuperscript{12} (6) domestic and international transfer of funds;\textsuperscript{13} (7) automatic clearing house (ACH) facilities for exchange and clearance of paperless-entry debits and credits;\textsuperscript{14} \textsuperscript{8} telecom-

access the demand deposit account to transfer funds or make payments is analogous to the drawer's signature on a check.

An evolving type of electronic debit card is the "smart card," a plastic card with a computer microchip imbedded in it, which offers a different set of advantages and protections than one without a microchip. The main advantage is security. The smart card draws its power from the imbedded microprocessor chip that can be read by an intelligent terminal when the card is inserted in the reader device. In effect, the smart card is a small computer that can remember balances or purchases and can store and update information such as financial and medical history. French banks originally developed the smart card as a replacement for checkbooks. At present, it is being used as the payment medium for pay telephones in France, and at POS terminals as a substitute for cash payments. Trigaux, International Standards Drafted for 'Smart' Card, Am. Banker, May 31, 1984, at 1, col. 2; Young, What's Happening With Smart Cards?, MAG. OF BANK AD., Jan. 1984, at 28-30.

12. In-home financial services (e.g., "Home Banking," Videotex) usually are performed over cable television facilities as an interactive service in which the user's financial account information is accessed as well as a variety of commercial data bases. Among the services usually offered in addition to home banking are shopping-at-home, news and weather reports, restaurant listings, library research, and financial statistics. A microchip access card coded with the user's signature characteristic may be a way to solve the problem of personal identification for Home Banking Services. Tyson, Chip Card Might Solve Home Banking's Id, Am. Banker, May 17, 1984, at 3, col. 2. Home banking could increase significantly if the number of home computers grows as rapidly as predicted. Computer-based home financial services are the next step in electronic financial service products. Further, the Federal Reserve Board stated that home banking terminals did not have to produce a terminal receipt under the Electronic Funds Transfer Act. This will spur the growth of home banking. Still, it is generally agreed that it will be years before home banking or videotex will be a significant factor in the payments or transfer of funds area. Garson, Consortium Will Test Home Banking, Am. Banker, May 19, 1983, at 3, col. 1, NCR Universal Credit Union Claims a First with Home Banking Services, Am. Banker, Aug. 24, 1983, at 10, col. 1.

13. Transfers of funds over domestic and international "wire" systems (e.g., FEDWIRE, BANKWIRE, CHIPS, SWIFT) are generally interbank or corporate transfers of high dollar amounts for the bank's own account or that of third parties, and are now effected electronically by means of debits or credits to the demand deposit accounts of the parties at the participating financial institutions. See S.E.C. v. Miller, 495 F. Supp. 465 (S.D.N.Y. 1980).

14. An automated clearing house (ACH) is an association of financial institutions whose operations functionally parallel check clearinghouse operations, except that in an ACH the payment data is processed and exchanged electronically. ACH computerized facilities receive, process and distribute magnetic tape or other machine-readable data. This data is received from participating financial institutions in groups of paperless entries (debits and credits). These entries can be used for electronic exchange, clearance, transfer of funds, and settlement of the total debits and credits of each institution at a designated financial institution such as a Federal Reserve Bank.

An ACH is designed to facilitate the electronic processing of recurring payment credits (e.g., social security payments and other government disbursements, payrolls,
munication of information and data from check truncation,\textsuperscript{15} electronic Giro and other recurring transactions,\textsuperscript{16} (9) check guarantee plans; and (10) the electronic processing of paper entries from credit card transactions and from electronic credit cards.

The development and use of national standards are of great importance to efficient and secure processing of electronic financial transactions, but use of these standards is voluntary in the United States. The American National Standards Institute (ANSI) is the clearinghouse and coordinating body for standards activity on the national level. It also represents U.S. interests in international standards development which is coordinated by the International Organization for Standardization (ISO). EFT systems encompass data processing, communications, banking, and retailing. Universal standards in these areas will allow consistency in record formats, physical specifications and characteristics, location of fields, numbering systems, and data elements. Standards and record formats are vital to critical areas in the EFT/PEP design, communication and processing.\textsuperscript{17}

Some legal disputes arising from electronic financial services and transactions may involve:

corporate transfers), preauthorized debits from a demand deposit account (e.g., insurance premium remittances, periodic mortgage payments, utility bill payments, business trade payments), and other paperless direct debits and credits. NCEFT, Appendix C, supra note 8, at 339.

15. The cumbersome processing and shipment of checks, with the related paper-listing of data and information, eventually may be replaced by "check truncation" [i.e., the interception and retention of the actual checks or other items (defined in U.C.C. § 4-104(1)(g))] at some point in the check collection process. The data and information needed for interbank clearing and settlement, presentment, payment or dishonor, and accounting at the payor bank will be captured, processed, and telecommunicated to the designated destination of the check or other item. The paperless entries for the truncated items may be cleared and exchanged through an ACH or ACH network. See Vergari, Articles 3 and 4 of the Uniform Commercial Code in an Electronic Fund Transfer Environment, 17 SAN DIEGO L. REV. 287, 288 (1980).

16. In electronic Giro transactions the payment instructions and funds move from the remitter to the recipient by electronic telecommunication. The Giro entry is a credit transfer, moving funds from the remitter's financial institution on the specified payment date to the recipient's designated financial institution. To receive a Giro remittance, the recipient must designate the financial institution and account data to which the remittance/payment is to be transferred. Electronic Giro will be useful in making recurring types of remittances or payments on consumer utility bills, insurance premiums, periodic mortgage payments, or business trade payments, where the remitter wants to retain control over the time when the payment or transfer of funds is initiated. For further discussion, see Vergari, Electronic Giro for the United States, 2 COMPUTER L.J. 101, 102-04 (1980).

I. LEGAL STRUCTURE

The legal structure for electronic financial services and transactions presently is based on private contracts and federal statutes, including agreements among financial institutions and/or service providers, ACH operation rules, Federal Reserve Regulation J (Wire Transfers), and Regulation E (Electronic Transfers) issued pursuant to the Electronic Funds Transfer Act of 1978 (EFTA) and authorization agreements or standing orders between customers and creditors or employers and employees. These contracts and rules allocate risk for events that may occur in a given transaction, such as fraud, mistake, negligence, malfunction, or error. There are also rules regarding the payment and settlement of various electronic financial transactions.

A. FEDERAL LAW CONCERNING ELECTRONIC FINANCIAL TRANSACTIONS

1. Electronic Funds Transfer Act

The Congressional purpose of the Electronic Funds Transfer Act (EFTA) was "to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems." This goal was achieved only to the extent

18. NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION OPERATING RULES (REV. ED. 1979).
of providing consumers with protection and rights in EFT transactions analogous to those available in similar circumstances under existing consumer protection laws. EFTA relies heavily upon the principle of comprehensive disclosure. It also allocates risks and liabilities between the consumer and the institutional provider of EFT services, in such matters as the institution's failure to respond correctly to the consumer's instruction, losses caused by an unauthorized access to a consumer's account, and procedures for resolving disputes concerning alleged errors.

Exemptions include: transactions originated by check, draft, or similar paper instrument; check guarantee or authorization that does not result directly in a debit or credit to a consumer's account; transactions through FEDWIRE, BANKWIRE, or any similar network servicing financial institutions and businesses; and telephonic transfer of funds initiated by a conversation between a consumer and a financial institution. Check truncation is not covered as the transfer is initiated by a check.

The EFTA requires EFT providers to disclose to consumers key information about their rights and liabilities; to provide consumers with paper documentation of transfers and error correction procedures; and to limit a consumer's liability for losses resulting from computer fraud and unauthorized access to the consumer's account (generally $50). For example, under EFTA, a customer's potential liability for unauthorized electronic transfers may not exceed $50 if the financial institution is notified within two business days of the discovery of the loss or theft of an EFT access card. After two days, the customer's liability limit increases to $500. Failure to notify the financial institution within 60 days after an account statement is sent removes the ceiling on liability for unauthorized transactions. The financial institution has the burden of proving either that the transfer was authorized or that the customer failed to notify on time.

The Federal Reserve Board was authorized to promulgate regulations to implement EFTA (i.e., Regulation E—Electronic Funds Transfer). Administrative enforcement responsibilities are allocated among the federal regulatory agencies that normally oversee

the operations of the regulated parties.\textsuperscript{31}

EFTA preempts state law only to the extent that protection provided to the consumer is greater than that afforded by state law.\textsuperscript{32} The Federal Reserve Board has been delegated the responsibility of evaluating whether federal or state law applies in such situations.\textsuperscript{33} If no specific determination is made, the state provision remains in force.

Under EFTA and Federal Reserve Regulation E—Electronic Transfers, the telephone is not deemed an electronic device. By analogy, "Home Banking" transfers may be exempt, raising questions as to duties and obligations concerning transfer of funds or payment orders executed on home equipment via telecommunication media (e.g., cable TV lines), and as to the rules when home banking transactions are made by means of computers interacting over cable TV lines. These questions will be compounded when a computer user operates an "In-Home" financial service apparatus to access both personal and business accounts. Until recently, "In-Home" financial services were deemed "electronic terminals," which under EFTA must generate and deliver a receipt to the customer.\textsuperscript{34} Customers considering "In-Home" banking would have been required to buy an expensive printer to produce a receipt for the transaction. However, the Federal Reserve Board staff has interpreted EFTA to exempt home terminals from the rule, reasoning that using a home terminal is like using a telephone, which does not require a receipt.\textsuperscript{35}

2. Truth-in-Lending Act

The Truth-in-Lending Act (TILA)\textsuperscript{36} requires creditors to disclose in writing to the debtor in a consumer credit transaction information concerning the "annual percentage rate" and "finance charge";\textsuperscript{37} a periodic statement of the credit transactions, including written notice of any change in terms;\textsuperscript{38} and two copies of the notice of the right to rescind certain consumer credit transactions.\textsuperscript{39} TILA applies even in electronically executed consumer credit transactions.

\begin{itemize}
\item 32. 15 U.S.C. §§ 1693q, 1693r (1982).
\item 35. 12 C.F.R. § 205, Supp. II ¶ 2-23 (1982).
\item 37. 12 C.F.R. § 226.6 (1982).
\item 38. 12 C.F.R. § 226.7 (1982).
\item 39. 12 C.F.R. § 226.9 (1982).
\end{itemize}
3. *Fair Credit Billing Act*

The Fair Credit Billing Act (FCBA)\(^4^0\) imposes a duty on creditors, if certain specified conditions exist, to correct billing errors on customer statements. This includes statements of credit cardholders and errors as to extensions of credit.\(^4^1\) Most creditors, including credit card issuers, provide customers with a disclosure form showing the consumer's billing rights and procedures to be followed in the event a customer thinks the billing is wrong, together with the creditor's responsibility under the FCBA.\(^4^2\) These requirements also apply to electronic financial transactions.

**B. Proposed Uniform New Payments Code (NPC)**

Electronic funds transfers, paperless entry payments, and other paperless financial transactions provide a modern and convenient method to conduct business. They are not subsumed by existing law governing older, more traditional, paper-based methods such as checks.\(^4^3\) As a result, a payment or transfer of funds transaction might have very different legal consequences depending upon the method chosen: paper, paperless, or electronic. To combat this discrepancy, the Permanent Editorial Board for the Uniform Commercial Code is drafting a Uniform New Payments Code (NPC). The latest draft\(^4^4\) indicates that the NPC would apply to all forms of payment and transfer of funds except cash. All forms of payments including credit cards, check guarantee plans, and "In-Home" banking transactions would have the same legal effect and bear the same legal consequences.\(^4^5\) The relevant legal issues include not only the specific rights and obligations of the parties for computer and telecommunication of transfers of funds and payment orders, but also the broader issues of privacy, security, theft, and unauthorized use of access devices and illegal entry in the telecommunication media.

**C. State Statutes Regulating Electronic Financial Services and Transactions**

Thirty-two states have enacted laws that expressly regulate the

---

\(^4^1\) 12 C.F.R. § 226.13 (1982).
\(^4^2\) 12 C.F.R. § 226.6(d) (1982).
establishment and use of EFT systems. The statutes permit limited area (e.g., city, or one or more counties), or statewide offering of EFT services. Three other states, without statutes framed to directly regulate EFT, are likely to have regulations governing electronic financial transactions issued by the state's financial institutions regulatory agency under its general regulatory powers. Some state laws have provisions regarding the sharing of ATM/POS terminals within the state, ranging from the extreme of mandatory sharing in Connecticut and Nebraska to permissive sharing in New York. A state's sharing law may have an impact on a financial institution's participation in a network, especially since some states have outright prohibition of an out-of-state financial institution's use of ATMs within its borders.

Some state laws permit: (a) customers of out-of-state banks access to EFT services; (b) out-of-state banks to offer EFT services


48. Conference of State Bank Supervisors (CSBS) survey, noted in Telephone Interview with Glenn L. Allen Jr., Director of Automation and Public Interest, CSBS (January 22, 1984).

49. Those states are Alabama, Arkansas, California, Delaware, Florida, Illinois, Iowa, Minnesota (at retail locations), Montana, Nebraska, Oregon, South Dakota, Texas (cash and purchases at retail locations), Utah, Virginia, Washington and Wisconsin. See supra notes 46 and 47.
or place EFT facilities in that state;⁵⁰ and (c) banks chartered by that state to provide EFT services out of state.⁵¹ Eleven states include consumer protection provisions in their EFT statutes.⁵² In June 1983, Texas adopted a law allowing Texas financial institutions to debit customers' accounts from the use of debit cards at point-of-sale terminals.⁵³

D. Domestic and International Transfer of Funds

Only a fragmentary body of common law governs transfers of funds by wire or electronic means.⁵⁴ Generally, wire or electronic

⁵⁰ Those states are Alabama, Florida, Illinois (point of sale), Maryland, Minnesota (at retail locations), Montana, Oregon, Utah, Virginia, Washington and Wisconsin. See supra notes 46-47.

⁵¹ Those states are Alabama, Arkansas, Illinois (point of sale), Minnesota (at retail locations), Oregon, Utah, Virginia and Washington. See supra, notes 46 and 47. Only Iowa specifically prohibits this activity.


⁵³ Stearns, Point of Sale Bill to Governor, Am. Banker, June 1, 1983, at 2, col. 1.

⁵⁴ There are four interbank electronic “wire” transfer networks:

(1) FEDWIRE: a telecommunication and settlement network linking Federal Reserve offices and banks nationwide since 1918, FEDWIRE facilitates the transfer of money throughout the United States by debits and credits to financial institutions' accounts at Federal Reserve banks. A number of banks have established direct online terminals for moving and monitoring the transfer of funds (“federal funds”) from the sender financial institution’s reserve account to the receiving institution's reserve account. FEDWIRE is also used to execute the net settlements for paperless entries processed through ACHs. See S.E.C. v. Miller, 495 F. Supp. 465 (S.D.N.Y. 1980).

(2) BANKWIRE(II) or CASHWIRE: BANKWIRE is a private communications system serving about 200 banks in the United States and Canada through a membership cooperative payment and administrative communications corporation. Its payment and communication services meet most of the needs of both bank management and customers. BANKWIRE cannot make interbank settlements directly, but such settlements are now effected on a net basis through debits and credits to the reserve accounts of the respective institutions at the Federal Reserve banks. The principal advantage of BANKWIRE is its ability to transmit free-form interbank communications and repayment instructions, confirm securities transactions, and transfer funds directly among members. NCEFT, Appendix C, supra note 8, at 338-39. BANKWIRE may also be used in connection with nationwide ACH operations.

(3) CHIPS (Clearing House Interbank Payments System): CHIPS was one of the first electronic funds transfer systems within the commercial banking system, handling interbank transfers of funds for international customers of the New York Clearing House member banks since April 1970. CHIPS is owned and operated by
transfers are governed by private contractual arrangements between the participants, and the application of analogous provisions of Uniform Commercial Code, Article 4 (Bank Deposits and Collections). If the transfer (wire or electronic) is processed through FEDWIRE, it is subject to the provisions of Federal Reserve Regulation J (Wire Transfer of Funds).55

1. Domestic Transfers

Domestic transfers of funds give rise to problems such as forged instructions and funds credited to improper accounts. In Securities Fund Services, Inc. v. American National Bank and Trust Co. of Chicago,56 the relationship between the initiator of a wire transfer and the collecting bank along with the corresponding duty of care was at issue. In that case, the initiator brought suit against the collecting bank to recover funds paid pursuant to forged instructions and credited to the wrong account. The Court held that under the Uniform Commercial Code, the initiator was a “customer” of the collecting bank, establishing an agency relationship. The bank breached its duty of care by not acting in good faith and failing to use ordinary care.57

2. International Transfers

One of the banking problems in international funds transfers is the lack of uniform standards for checking the authenticity of the New York Clearing House Association. A member bank desiring to make payment on behalf of a customer involving an international transaction simply provides the CHIPS computer with relevant payment instructions, including assigned account identification numbers. The computer stores the information until an authorized person at the sending bank approves the release of the message to the receiving institution. The CHIPS computer also performs the basic accounting functions required for clearing and settlement.

(4) The Society for Worldwide Interbank Financial Telecommunication (SWIFT): This originated in Europe in 1970. Presently it is a nonprofit corporation established in Belgium and owned by 300 banks in the United States, Canada and 13 western European countries. It is an international interbank communications network, enabling its members to transmit international payments, statements and other messages associated with international banking. SWIFT is a message switching and payment transfer system and not a settlement of accounts system; debit and credit entries are made only on the books of the respective institutions, whereas in settlement systems like FEDWIRE and BANKWIRE the squaring or settling of accounts by the institutions is done through the reserve accounts of the participating institutions at the Federal Reserve banks.

57. Id. at 237.
money-moving instructions by bankers and brokers in the international money market.\textsuperscript{58} In a New York case, \( D \) had an account with \( M \) Trust Co., and authorized \( M \) (by Telex messages sent the day before the transfer was to be made) to make payments out of \( D \)'s account.\textsuperscript{59} On June 25, \( D \) sent a Telex message to \( M \) authorizing transfer of $12.5 million to \( C \) Bank on June 26, for the account of Herstat. Herstat was closed by German authorities on June 26, but the transfer was effected before the time of notice of the closing. The court held that the U.C.C. is not applicable to wire transfers, as they are not "items."\textsuperscript{60} But, "based on the nature of the CHIP system and the fact that its member banks viewed such transactions as irrevocable (as evidenced by the short-term change instituted after the Herstat failure), the CHIP's transfer was irrevocable when made."\textsuperscript{61} The court applied the concept of finality of payment of checks once accepted to the wire transfer.

In an Illinois case, plaintiff \( H \) telephoned its Illinois bank to make a wire transfer of funds ($27,000) from its account to Swiss Bank for the account of Shipowner at Banque de Paris, to cover a charter hire period that was due April 27.\textsuperscript{62} The telex reached the London office of the Illinois bank on the night of April 25. Its Telex operator, failing to reach Swiss Bank through Swiss's general Telex number for transmittal of transfer of funds messages, diverted the telex message to Swiss Bank's Foreign Exchange Department. Swiss Bank had no procedures in its Foreign Exchange Department for transferring or recording telex messages destined for other departments, and failed to record the message in any manner. As no funds reached the Shipowner by April 27, he cancelled the charter resulting in a loss to \( H \) of $2 million. The court held U.C.C. Article 4 inapplicable to the wire fund transfer situation and concluded that Swiss Bank as a corresponding bank was not liable. The court stated that Swiss Bank did not know when payment was due, what the charter terms were, or that these terms were extremely favorable to \( H \), so that neither Swiss Bank nor Continental was liable. The Court said, "Electronic funds transfers are not so unusual

\textsuperscript{59} Delbrueck \& Co. v. Manufacturers Hanover Trust Co., 609 F.2d 1047 (2d Cir. 1979).
\textsuperscript{60} "Item means any instrument for the payment of money even though it is not negotiable, but does not include money." U.C.C. \S 4-104(1)(g) (1977).
\textsuperscript{61} Delbrueck \& Co. v. Manufacturers Hanover Trust Co., 609 F.2d 1047 (2d Cir. 1979).
as to automatically place a bank on notice of extraordinary consequences if such transfer goes awry.\textsuperscript{63}

The banking industry now has a set of rules covering errors in international funds transfers, adopted by the Council on International Banking and the New York Clearing House on January 1, 1983; by the Mid-American and Western Councils on International Banking on February 1, 1983; and accepted by the California Clearinghouse in March 1983. Other large clearinghouses are favorably disposed. The new rules cover three types of errors: (a) erroneous or duplicate payments; (b) late payments; and (c) payments to a correct bank but incorrect beneficiary.\textsuperscript{64}

\section*{II. POTENTIAL PROBLEMS}

\subsection*{A. COMPUTER-RELATED CRIME AND ABUSE}

The United States Chamber of Commerce estimates losses from business, economic and white-collar crime may cost more than $40 billion a year. Many crimes may be committed through the use of computers.\textsuperscript{65} The use of computers to conduct financial transactions, especially electronic fund transfers, is expected to be a lucrative area for theft. Computer technology has almost completely displaced manual and mechanical transfers of funds between individuals, financial institutions, businesses and government. The technology now available makes EFT cost-effective but vulnerable to criminal exploitation.

Computer crime is very difficult to detect. Often there is little or no evidence that a crime has occurred. Indeed, in the vast majority of cases, detection has been a matter of sheer accident rather than the result of an ongoing security or auditing effort. Most computer-related crime may be unreported or undiscoverable.\textsuperscript{66} The problem is as limitless as the technology that spawned it.

Computer crimes involve the use of data and information processing systems in a manner which causes loss, damage or injury. Main categories of computer-related crimes include:

1. Introduction of fraudulent records or data into a computer system;
2. Unauthorized use of computer-related facilities;

\textsuperscript{63} Id. at 956.

\textsuperscript{64} Preston, \textit{Banks Now Have Rules on International Transfer Errors}, \textit{Am. Banker}, April 6, 1983, at 14, cols. 2-4.

\textsuperscript{65} For an excellent comprehensive review of computer crime, see 2 \textit{Computer L.J.}, No. 2, Spring 1980.

alteration or destruction of information or files stored in the computer;

(4) theft of money, financial instruments, property or services through a computer system;

(5) theft of valuable computer data or information; and

(6) sabotage or vandalism of the computer system.\textsuperscript{67}

The Government Accounting Office (GAO) reported that the most common weaknesses exploited by computer criminals in the federal agency cases studied were separation of duties and physical control over facilities and supplies.\textsuperscript{68} Both of these weaknesses can be overcome. Effective solutions will require computer crime experts to inform the user community of the vulnerability of computers and to assist users in implementing safeguard techniques for detection, investigation, prosecution and prevention of computer crime.\textsuperscript{69}

For the purposes of this article, computer-related crime includes: (1) violent crimes against computer systems; (2) robbery or assault of users; (3) insider crime; (4) unauthorized use; and (5) theft of valuable computer-stored assets. Computer fraud includes credit card related fraud, electronic thefts and "in-house" embezzlements.

1. \textit{Violent Crimes Against the Computer System}

This category includes physical attacks on the system such as bombing, burglary, vandalism and sabotage. ATM burglaries are a new problem confronting bank security experts. Bombings of ATMs also have assumed a new dimension. Recent bombings have been reported in two cities. No injuries occurred, and not all explosions penetrated the machines, but property damage was heavy (the explosions also destroyed the money). Terrorists have blasted ATMs to finance radical causes.\textsuperscript{70}

2. \textit{Robbery or Assault of Users}

ATM users have been robbed after withdrawing cash from the

\textsuperscript{67} 125 CONG. REC. 31,167 (1979); A. BEQUAI, \textit{COMPUTER CRIME} 13-14 (1978).


machines. Users have also been kidnapped and forced to withdraw cash from the ATM. Victims of such robberies may bring civil suits against the institutions alleging lack of adequate security and lack of notice to the public of special risks involved in ATM use.71

The Bank Protection Act of 196872 sets standards for surveillance systems, burglar alarms and vault strength. These can also be applied to ATMs.

3. Insider Crime

Theft by an employee with access to the computer system is insider crime. To combat this problem, institutions have reviewed their internal controls, placing emphasis on enforcement of system controls and safeguards. Sufficient controls are necessary to insure accuracy and reliability in the data produced by the computer. Restrictions should be put on access to and ability to alter computer records and data. Audit trails should document transactions and identities of those making particular entries.73 Electronic record keeping systems are only as trustworthy as the people who use them.

4. Unauthorized Use

Unauthorized entry into a computer to make free use of its data processing capabilities is another common abuse of computers. In one case, a credit fraud ring employed a data clerk to alter credit records of several hundred persons with poor credit, enabling them to obtain credit at financial institutions and retail businesses.74

In United States v. Sampson,75 the defendant admitted unauthorized use of advanced PDP computers for an average of 6 hours per week for a period of 32 weeks. He also admitted taking for personal use computer printouts with a commercial value of $1,924. The court held that computer time is a thing of value76 and consumption of computer time and use of its capacity is inseparable from the

76. Id. at 880.
physical identity of the computer equipment.\textsuperscript{77}

5. \textit{Theft of Valuable Computer-Stored Assets}

Information is the target of computer crime. Computer crimes may include alteration, seizure or destruction of a computer program or its data files. For example, a thief may use a home computer to tap into a financial institution's computer system, causing a series of unauthorized transfers to a bogus account for subsequent transfer overseas.\textsuperscript{78}

Creation of new computer-stored financial assets (e.g., certificat- eless "book-entry" securities, data-only bank account balances, computer money) creates the potential for misuse and theft of those assets and related information. Those who develop and work with these computer assets can often alter or delete them or create totally new assets. Such financial assets are sent through wires, microwave carriers and satellite transmitters in the form of electronic or electromagnetic waves and magnetism.\textsuperscript{79}

B. \textbf{COMPUTER FRAUD AND ABUSE}

The increasing dependence on EFT/PEP systems by financial institutions and their customers, while increasing efficiency, increases the threat of computer fraud and abuse. This threat exists not only in the less established (but expanding) retail and wholesale EFT/PEP systems (e.g., ATMs and POS terminals where relatively small transactions occur), but also in wholesale EFT networks (e.g., FEDWIRE, CHIPS) which involve much larger transactions. EFT/PEP systems are subject to theft, error and malfunction. Unlike more traditional payment mechanisms, however, these systems are not yet governed by laws that assign rights and responsibilities between depository institutions and their customers. One exception is EFTA, which is limited to consumer relationships with depository institutions. EFTA limits the consumer's liability on unauthorized transfers.

1. \textit{Credit Card Fraud}

Security and fraud issues pervade electronic transfer and payment systems. The credit card and debit card are highly vulnerable to fraud. The electronic debit card\textsuperscript{80} is more vulnerable because it

\begin{itemize}
\item \textsuperscript{77} \textit{Id.}
\item \textsuperscript{78} Koehn, \textit{Information is Target for Today's Criminal}, Am. Banker, March 15, 1982, at 10, col. 1.
\item \textsuperscript{79} D. PARKER, CRIME BY COMPUTER 4 (1976).
\item \textsuperscript{80} See supra note 11.
\end{itemize}
can directly access cash and demand deposit account balances, merchandise and services. Bank credit card fraud losses cost the banking industry an estimated $150 million per year.\textsuperscript{81} Collusion by merchants who intentionally accept unauthorized, fraudulent or fictitious credit card charges, charges from false sales, or charges from credit card thieves facilitate credit card fraud. Increasing fraud losses, which have prompted new federal legislation and a host of computer system changes, result largely from counterfeiting techniques used by syndicated criminal enterprises working with corrupt merchants.

Until October, 1984, there were no\textsuperscript{82} federal statutes specifically addressing credit or debit card fraud. However, Congress has now passed a bill which would make criminal certain credit card fraud, including possession of counterfeit or stolen credit cards.\textsuperscript{83}

2. Electronic Thefts

Electronic thefts are becoming commonplace and result in great losses. For example, in New York, thieves posing as bank service employees attempting to repair broken ATMs made withdrawals from the accounts of 485 customers at Citibank. The New York Attorney General sued Citibank, alleging that its failure to treat the "lost" withdrawals as "unauthorized" electronic transfers violated the customers' rights under EFTA. The cases were settled without admission of any wrongdoing by Citibank.\textsuperscript{84}

3. In-House Embezzlement

The criminal who constitutes the greatest threat to computer security may be trusted employees authorized to operate in-house computers. Possible safeguards against this threat are automatic dial-back devices, frequent change of user-passwords, biometrical measurements, and the use of a network of informants.\textsuperscript{85}

Embezzlement by in-house computer users often constitutes fraud. For example, where a corporate employee causes a computer to prepare checks to existing payees based on nonexisting accounts

\textsuperscript{81} Weinskin, Secret Service to Help Fight Card Fraud, Am. Banker, Aug. 1, 1984, at 1, col. 4. Credit Card Fraud Topic For House Unit, Am. Banker, May 23, 1983, at 63, col. 2; Tyson, supra note 5.


\textsuperscript{84} Winter, Banking By Blip, 69 A.B.A.J. 263, 264 (1983).

payable (e.g., analogous to a “fictitious payee” situation under Uniform Commercial Code, Article 3—Commercial Paper), a genuine writing containing false statements of fact was created, and the crime of false pretenses or fraud had been committed.\(^8\)

In most fraud cases there is usually a breakdown of security controls which permits the unauthorized or illegal use. The Equity Funding case involved the manipulation of computer files and creation of data to conceal fraudulent insurance policies.\(^8\) Much of this was performed by personnel outside the EDP department, who were allowed access to computer equipment and files.\(^8\)

One of the most notorious cases of computer fraud was the $10.2 million swindle of the Security Pacific National Bank, in Los Angeles, California. This crime did not directly involve the use of a computer. Rifkin, a familiar figure at the bank, obtained the authentication code for wire and electronic transfer of funds on a particular day. Posing as a branch manager, he ordered $10.2 million transferred to a Swiss bank account.\(^8\) In another case, four men were indicted by a federal grand jury for participating in a successful embezzlement scheme that cost Citibank N.A. $3 million. An employee of the bank aided the thieves by sending a telex communication transferring $3 million to a numbered account in Curacao, Netherland Antilles.\(^9\) These cases demonstrate the growth of in-house computer crime, the high costs of this crime, and the need for greater control over access to and use of computers.

C. COMPUTER ERROR OR FAILURE

The legal system must come to grips with new problems and potential legal repercussions created by computer error and failure. “Fraudulent intent is not the only threat to financial operations security, nor even the greatest. In terms of actual loss, inadvertent errors provide the most exposure; without adequate security precautions, a bank is literally at the mercy of the collective attitude of its data entry operators.”\(^9\) Increased reliance on computers by financial institutions has created other legal problems. Accounting

\(^8\) United States v. Jones, 553 F.2d 351, 356 (4th Cir. 1977).
\(^8\) Id.
\(^9\) For a more complete discussion of this case, see Becker, Rifkin, A Documentary History, 2 COMPUTER L.J. 471 (1980).
functions are often performed automatically by computers with little or no human oversight. Consequently, errors in the computer's operational systems and programs may go undetected, and can be compounded with each accounting cycle. These errors can place significant burdens on unsuspecting debtors and account holders.

A computer system consists of three components: hardware, software, and humans. Each component suffers from its own particular weaknesses and the failure of any component may result in serious harm. For example, in a case concerning a delay in dishonoring checks which was caused by computer failure, the court held that the delay was excused under U.C.C. Article 4 (Bank Deposits and Collections) as beyond the control of the payor bank, which had used reasonable diligence under the circumstances. Yet another court held a bank liable for failure to meet the deadline for payment or dishonor of a check, even though the delay was caused by a computer malfunction and a subsequent brief power failure in the area which shut down the computer, requiring lengthy restart procedures. The court found that the payor bank had failed to act with requisite diligence by not having alternative processing systems given prior computer failures. The bank was also remiss for relying on a computer requiring several hours to restart in the event of electrical failure. It is evident from these examples that the legislature and courts must develop a policy to deal with this problem.

Computer malfunctions, including errors in data or information input and malfunctions caused by faulty software, may result in spectacular accidents such as airplane crashes or nuclear power plant failures, as well as such mundane problems as the loss of accounting records, double billing, and deposits or withdrawals entered into the wrong account. The legal characterization of computer services may influence how courts apply traditional common law negligence theories or concepts to computer malfunctions and error.

There is a common law duty imposed on those who use or supply computer services to exercise reasonable care to ascertain the accuracy of the information furnished by or to a computer system, before transmitting or relying on such data. Traditional negligence theory requires a plaintiff to prove by a preponderance of evidence that the defendant breached a duty and the breach proximately caused harm to the plaintiff. The nature of the computer system, however, makes proof of negligence, particularly proximate cause,

difficult. Because computers malfunction for many reasons, it is often difficult to determine the cause of a particular error. Consequently, a victim of computer error may be unable to prove the malfunction resulted from a breach of duty, or that an act or omission by the tortfeasor proximately caused the damage.

When evidence of specific negligence is lacking, courts sometimes allow the plaintiff to prove negligence by inference (e.g., by applying the doctrine of res ipsa loquitur). Even this approach, however, would be difficult to apply in cases of computer malfunction. Since most of a computer system's operations are beyond direct supervision, discovering which element was the actual cause of a particular error or malfunction may be extremely difficult. Furthermore, because each computer system is unique in some respect, a characteristic of failure in one system may not be characteristic of the same failure in another system. In the future, the concept of due care used to determine whether proper controls were used may include the use of a "state of the art" standard in evaluating the duty of care required for a particular situation.

D. INFORMATIONAL PRIVACY

Computers create the potential to accumulate vast amounts of data and information that can be readily and easily stored and retrieved. Unfortunately, this also creates the potential for manipulation of information. The electronic financial transactions area is not immune to this manipulation. This raises questions regarding the extent to which individuals have a right to privacy. The issue of privacy of information collected in centralized computers was raised in Whalen v. Roe, but the U.S. Supreme Court skirted the issue.

Congress has attempted to provide statutory safeguards for individuals' disclosural right of privacy, where the U.S. Constitution and common law fail to provide adequate protection. EFTA provides no specific privacy protection. However, minimal protection was included in the Right to Financial Privacy Act of 1978 (RFPA), and the Privacy Act of 1974 (a counterpart to the Freedom of Information Act). RFPA provides privacy protection to an individual's financial records, but applies only to federal government agencies. It does not apply to local or state agencies, nor to private entities such

as credit reporting agencies. Additionally, RFPA merely provides procedural, not substantive rights.

EFT facilities deployment and consumer protection statutes of several states include privacy protection provisions, which apply specifically to EFT transactions.98 California has enacted privacy legislation which extends protection well beyond federal law.99 California courts have held that the state's constitutional amendment protects privacy in matters concerning bank records, credit card charges, college transcripts, medical records and personnel records.100 Twenty-two states have EFT or related computer statutes regulating information gathering practices or computerized data processing, although such major states as New York and Texas are not yet protected.101 Most of the state laws, however, only address situations in which a state government agency is involved.

III. COMPUTER SECURITY AND PROTECTIVE MEASURES

Although development of a penetration-proof computer is highly unlikely, much more can be done to discover, deter and punish those who commit computer crimes and fraud. Computer technology has outpaced computer security. Many recent studies have shown that the majority of computer systems, even when provided with security, are still open to attack and can be penetrated by sophisticated criminals.

A. EFT Security

The potential vulnerabilities of EFT systems, and security measures to counteract these problems, were not considered when EFT systems were designed, even though EFT's are well publicized sources of exposure of financial institutions' computer systems. The software vendor, who is equipped to deal with this problem, should assume responsibility for this problem. Application software performs the daily accounting data processing, so its programs are likely targets of subversion by computer professionals who want to misappropriate funds. Package software systems for financial institutions are inadequate in their provisions for data security and access.

101. Tyson, supra note 5.
B. PROTECTIVE MEASURES

Institutions should develop tight physical security for the computer facilities. An elaborate internal audit trail should be built into the system in which every significant communication between the user and the computer system is recorded. Where confidentiality is particularly important, cryptography or encryption (scrambling of information) should be employed. Also pressing is the need for more secure user identification techniques.

The possibility that customer account records can be destroyed as a result of physical damage or fraudulent misuse of a computer system is a serious EFT system security problem. An EFT computer system must contain physical safeguards, such as locks and fire and water protection, to prevent damage to the equipment and to its associated information. Communication lines between terminals and the main computer must also be secure from tapping, message insertions, modification of message content, and illegal surveillance.

Since EFT systems are vulnerable to fraudulent programming, comprehensive audit trails or records must be incorporated into the system in order to detect extraordinary use patterns. Further, to minimize the need for a wholesale reprogramming of the system when key employees leave the company, employee duties within the computer center must be under dual control such that no one person controls an entire step in the EFT system.102

Additionally, computer cryptography and communications scrambling is necessary to protect data and information being communicated to and stored in computer systems. In encryption, a complex algorithm or computer routine is used to scramble messages, which are unscrambled at the receiving end. Message authentication, similar to data encryption, uses the same algorithm to calculate an authentication code instead of scrambling the message. Message encryption is an option for making computer data storage and transmission more secure, especially as electronic in-home financial service evolves, increasing the need to provide adequate security measures for electronic financial transactions and customer data bases of financial institutions. Encryption of transmitted data ensures security of communication and prevents a computer embezzler from deciphering account information.

User identification methods currently in use (e.g., user's signature, driver's licenses, personal identification numbers) have failed

to provide much security and protection against unauthorized access to funds in an individuals' accounts. The key element lacking for a secure, effective EFT system is an identification device and terminal receptor oriented toward identifying the person seeking access. On-line terminals and computer-oriented identification verification procedures may be feasible and more secure alternatives to personal identification numbers.

Another alternative may be the use of electronic signatures which can be given unique characteristics, making them more easily identifiable and reliable than human handwriting or other forms of identification. Another potential device is one that will oblige the user of a terminal, before accessing the computer, to press a physical impression on a special pad or plate on the terminal or attached to it, allowing instantaneous comparison of the whorls and loops or other characteristics against a digital image previously stored in the computer data base. Indeed,

"the U.S. Army plans to test a new access method for ATMs, using a hand-print rather than a personal identification number. The characteristics of the soldier's hand is read by special equipment and recorded on a plastic card. The user inserts the card into the ATM and places his or her hand on an attached hand-reading device linked to the ATM. If the data captured by the hand-reader matches the data recorded on the card, the user can proceed with the transaction."103

C. CRIME INSURANCE FOR THE ELECTRONIC AGE

Rapidly expanding computer technology is likely to result in a proliferation of on-line systems, with terminals becoming almost as common as telephones. The massive dollar amounts involved, particularly in electronic transfer of funds, exposes financial institutions to possible losses of catastrophic proportions. New forms of insurance coverage will be needed to insure against the potential liability that might result from fraud, product liability, system errors and malfunctions.104

The original response of insurance companies was to offer separate policies covering specific risks. Later these separate policies were combined into one, a "bankers blanket bond," each of the former separate policies becoming an individual item of coverage in the combined policy. One of the key terms of coverage is that manifest intent to perform a criminal act must be found before the in-

104. Brouillette, supra note 4.
surer becomes liable. As a result, this coverage may be inadequate for exposures of electronic financial service products. Employee defalcations including those that are computer related may be covered by a standard blanket-bond provision, but non-employee fraud (e.g., fraud resulting from activities of independent consultants, engineers, programmers and former employees) probably would not be covered. Coverage for non-employee computer crime exposure risk and for electronic data processors or service bureaus, is being offered by several major insurance underwriters.

Discount brokerage, another service product being offered by financial institutions, can add potential errors and omissions exposure in stock clearing, stock transfer and order execution. Even though discount brokerage services may be farmed out to a non-owned discount broker, the institution cannot transfer all responsibility for these services to the broker, and may well be included in a suit for negligence. Such risk exposure should be specifically provided for in insurance coverage.

Finally, insurance policy terms and provisions must be flexible enough to cover risks inherent in EFT/PEP systems.

IV. ADMISSIBILITY OF COMPUTER-BASED EVIDENCE

The introduction of computer-based evidence poses a problem, whether it involves a computer crime case, or any case requiring computer information as evidence. Judges and juries, who know little about computers, may feel ill-equipped to question the credibility of computer evidence, particularly when its credibility is supported by the testimony of computer experts. Courts have experienced difficulty in dealing with admissibility of computer generated evidence. In one case, a circuit court held that the actions of the defendant (who had procured the issuance of a false check by a computer) did not constitute forgery, but the issuance of a genuine instrument containing a false statement of fact as to the true payee.

Litigation involving the use of computers has presented the courts with an increased number of requests to admit into evidence computer records in the form of printouts. United States v. Russo

106. Oestreich, Rapid Change in the Banking Industry Increases the Chance of Loss, MAG. OF BANK AD., Jan. 1984, at 30-34.
109. 480 F.2d 1228 (6th Cir. 1973)
was the first case to address the conceptual problems presented by computer printouts. The court required that a firm foundation be laid describing the computer system and its operating environment before the computer printout could be introduced into evidence.

There are four possible bases for admission of a computer printout into evidence: (1) the original record or common law best evidence rule; (2) the business records exception to the hearsay rule; (3) statutory provisions; and (4) specific rules of evidence. Statements made out of court by an unavailable declarant which are offered for the truth of the matter asserted are inadmissible as hearsay under common law and the Federal Rules of Evidence.

Computer printouts may be considered hearsay. The business records exception to the hearsay rule has been relied on to admit computer-generated documentation into evidence. The "best evidence" rule provides that where the contents of a writing are in issue, an original copy must be produced unless justification for its absence is presented. Two exceptions to the best evidence rule have been held to include computer printouts: official records and voluminous writings. Courts have treated records stored in computers as if they had been traditionally prepared for purposes of the best evidence rule, and oral testimony pertaining to the contents of computer data files have been excluded as violative of the rule. The admissibility of computer generated documentation impacts on the outcome of any civil or criminal trial.

V. LAW ENFORCEMENT PROBLEMS

Current problems of crime and abuse connected with computers will be magnified by the growth of EFTS. These problems necessitate an investigatory and prosecutorial apparatus that can meet the expanding need to deal with computer criminals.

A. INVESTIGATION

The investigatory apparatus requires training and development of programs to detect and combat computer crime. Present prosecutorial machinery is also in need of training in this area. Few

112. FED. R. EVID. §§ 1001-1004.
113. FED. R. EVID. §§ 1005-1006.
prosecutors, local or federal, have had any experience with computer crime. For example, it is highly unlikely that law enforcement personnel would recognize as unlawful the activity of an interloper who uses a remote telephone-connected terminal to give privileged commands to a computer system to wipe out the table of contents of the entire disk-storage data base for more than 5000 users of the system and the operating system itself. Law enforcement officials will therefore be unable to effectively combat this crime. Frequently, theft by computer is difficult to discover, and even after discovery it may be difficult to trace the crime to a particular individual. Once the crime is discovered, local law enforcement officials are often reluctant to file criminal charges against the computer criminal, finding it difficult to structure a criminal complaint for these crimes.

B. PROSECUTION

Computer crime is one of the most sophisticated types of white-collar crime. This often has the effect of discouraging a prosecutor, who frequently has absolutely no knowledge of computers, from pursuing a case. Law enforcement agencies have neither the technical expertise nor the legal framework to detect, prosecute, or discourage computer crime. Prosecutors are forced to create a theory of prosecution which fits the computer crime within the framework of more traditional crimes such as theft or embezzlement. Crafting such a theory can be awkward and results far from perfect. Penalties are often too small. The current apparatus cannot possibly meet the challenge presented by different forms of computer crime.

A decade ago, attorneys did not need to educate themselves in the intricacies of technology to serve their clients or prosecute crimes. But in this highly technological society, many more clients are involved in complex technical matters which raise intricate legal questions that can be answered correctly only if attorneys understand the facts involved—facts which concern the nature of the particular technology. As a result, a significant number of prosecutors are being educated and trained in new technology enabling them to deal effectively with computer-related crimes.

C. LEGISLATION

The vulnerability of computer users, uncertainty regarding the applicability of existing common and statutory law to computer crime, and the complexity of the possible criminal acts all have led

to pressures at both federal and state levels to enact computer crime legislation.

Federal authorities currently attempt to place computer crimes within the framework of the federal crimes of tax evasion and mail or wire fraud. They also rely on embezzlement and theft statutes covering federal agencies and instrumentalities, banking statutes, and laws dealing with false entries in records, reports and other transactions of financial institutions and federal credit institutions.\textsuperscript{117} In addition, authorities can now rely on new criminal sanctions in the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.\textsuperscript{118}

Thirty-eight states have enacted statutes making criminal various intentional actions taken with respect to telecommunications or computing. Twenty-two states have new "computer crime" laws.\textsuperscript{119} Most of these new enactments make criminal fraudulent activity perpetrated by use of a computer system. At least one of these statutes (Florida) creates a new crime for acts against intellectual property.\textsuperscript{120} Most of these statutes criminalize tampering with telecommunication services, or fraud in the use of free telecommunication services.

The purpose of these state computer crime laws has been to make prosecution of computer crime easier by creating laws dealing specifically with this problem. In some cases, they are also designed to deal with persons who are detected adding, removing or erasing data from a computer without authorization yet without a fraudulent scheme or an intent to steal.\textsuperscript{121}

\section*{VI. ELECTRONIC FINANCIAL SERVICES POWER}

Depository financial institutions (e.g., commercial banks, savings and loan associations, savings banks and credit unions) are strictly regulated and may exercise only those powers authorized by applicable state or federal statute. State-chartered financial institutions are subject to the laws of their "home" state regarding their powers and that state's definition of branch banking. The federal EFTA does not authorize financial institutions to provide electronic

---

\textsuperscript{117} Sokolik, supra note 65, at 377.
\textsuperscript{120} FLA. STAT. ANN. § 815.04 (West Supp. 1984).
\textsuperscript{121} Rhode Island, R.I. GEN. LAWS, §§ 11-52-1 to -5 (Supp. 1982).
financial services or to establish EFT terminal facilities. It merely establishes standards, rights and duties which must be adhered to in providing EFT services to consumers.\textsuperscript{122}

EFT systems are not only funds transfer systems, but also transfer of information systems, data storage systems, and data and information processing systems. A very important case on banking powers and their use held that a national bank which offered electronic data processing services to the general public in reliance upon an interpretative ruling of the Comptroller of the Currency,\textsuperscript{123} exceeded its powers\textsuperscript{124} by failing to limit use of its "Retail Information Service" to performance of an express power under the National Bank Act.\textsuperscript{125} The service offered "must be incidental or useful to business expressly authorized under the National Bank Act."\textsuperscript{126}

A. BRANCHING POWERS

A financial institution may receive deposits and conduct banking business only at its principal location, unless empowered to do so at other locations or facilities. Restrictions on geographic locations where a depositary financial institution may do business were imposed to restrict proliferation of offices and unsound competition leading to dangerous banking policies and practices.

Establishment of branches by depository financial institutions is subject to statutes of the chartering state, with federally chartered financial institutions subject to the branch office provisions of their chartering federal statute. National banks, although chartered by the federal government under the National Bank Act, are specifically made subject to the same limitations pertaining to branching that are applicable to state-chartered banks.\textsuperscript{127} Thus, a national banking association may not establish branches in a state which does not allow branches.\textsuperscript{128}

Both federal and state law presently prohibit a bank or a bank holding company from operating domestic banking offices in more than one state. Recent legislation and pending bills raise the issue of the continued viability of geographical restrictions on financial

\begin{footnotes}
\item 125. National Retailers Corp. of Ariz. v. Valley Nat'l Bank, 604 F.2d 32, 34 (9th Cir. 1979).
\item 126. M & M Leasing Corp. v. Seattle First Nat'l Bank, 563 F.2d 1377, 1382 (9th Cir. 1977), cert. denied, 434 U.S. 1021 (1977).
\end{footnotes}
depository institutions. As a practical matter, financial institutions do presently conduct a wide variety of business throughout the country, except the receipt of deposits.

B. ARE UNATTENDED ELECTRONIC TERMINAL FACILITIES BRANCHES

Off-premise EFT terminal service units provide deposit and withdrawal of funds services, transfer of funds between accounts, and debit accounts for purchases of goods and services at retail establishments. There has been a major legal dispute over the past few years regarding whether these off-premise EFT terminals are branches. ATMs, like POS terminals, may be installed away from the bank premises at shopping centers, retail stores, office buildings, factories, or other unattended electronic facilities where any customer with an approved access card and proper personal identification can effect financial transactions.

The federal legislative scheme and the Comptroller of the Currency's regulations governing deployment of off-premise ATM/POS terminals by national banks is complex. Deployment of remote service units (RSUs: ATM operations off-premise or at retail store locations which may be at service counters rather than POS terminals) by federally chartered financial institutions other than national banks, such as savings and loan associations and savings banks, is governed by Federal Home Loan Bank Board (FHLBB) regulations, and federal credit unions by the National Credit Union Administration (NCUA). This regulatory scheme has produced some anomalous results. For example, such federal thrift institutions or credit unions may establish branches anywhere approved by the FHLBB or NCUA. National banks, however, are governed by applicable state law restrictions on geographic location and state law determinations of whether the off-premise unattended EFT terminal facilities are deemed branches. The McFadden Act applies the state law requirements only to national banks.

Thirty-eight states had enacted EFT legislation and/or promulgated EFT regulations as of August 1983. Of these, only eight define EFT terminals as branches and subject them to restrictions which include any geographic or other limitations applicable to "brick and mortar" branches. Florida provides that neither a re-

132. See supra notes 46-47.
133. Delaware, Maine, Missouri, New Jersey, New Mexico, Ohio, Oregon and Utah. In addition, under Michigan law, EFT terminals not made available for sharing are deemed branches. See supra note 46.
mote financial service unit nor an unattended facility shall be considered to be a branch.\(^{134}\)

In *Independent Bankers Association v. Smith*,\(^{135}\) the appellate court held that all off-premise “CBCTs”\(^{136}\) performing at least one of the banking functions of receiving deposits, paying checks, withdrawal of cash, or making loans are branches within the terms of the McFadden Act of 1927.\(^{137}\) As a result, CBCTs must comply with the branching requirements of both federal and state laws.\(^{138}\) The result is that if a state permits its state-chartered banks to establish CBCTs or similar facilities to serve one of these functions, then national banks, in that state may establish CBCTs to perform similar functions. This result is true even in a state that otherwise prohibits branch banking.\(^{139}\)

North Dakota law provides that state banks may provide “services to its customers involving electronic transfer of funds to the same extent that other financial institutions chartered and regulated by an agency of the federal government are permitted to provide such services within this state.”\(^{140}\) The law further provides that CBCTs are not considered branches and that sharing of terminals is mandatory upon request of other banks.\(^{141}\) When Merchants National Bank of Fargo, North Dakota, was operating two CBCTs pursuant to the authority of the Comptroller of the Currency, the appellate court affirmed the trial court’s finding that under North Dakota law, a state bank can lawfully use a CBCT, because both are permitted to use remote service units which are similar to CBCTs and ATMs. Therefore, Merchants National Bank was legally authorized under federal law to maintain the CBCTs as branches.\(^{142}\)

The Federal Home Loan Bank Board is the federal chartering and supervisory authority for federally-chartered savings and loan associations and savings banks. In 1974, the FHLBB authorized First Federal Savings and Loan association to install RSUs in two


\(^{136}\) CBCTs (Customer-Bank Communication Terminals) are manned or unmanned electronic terminals that may permit an existing bank customer to accomplish various financial transactions, including deposits, withdrawals and transfers of funds between accounts. They are similar in function and purpose to ATMs or POS terminals.

\(^{137}\) 12 U.S.C. §§ 36(c), (d), (f), 51 (1982).

\(^{138}\) 534 F.2d at 948.

\(^{139}\) *Id.*

\(^{140}\) *N.D. Cent. Code* § 6-03-02(8) (Supp. 1983).

\(^{141}\) *Id.*

Nebraska "Hinky Dinky" supermarkets. Using such an RSU, a depositor/customer of First Federal could deposit or withdraw money at the Hinky Dinky market. The state sued the owners of the supermarket,\footnote{Nebraska ex rel. Meyers v. American Community Stores Corp., 193 Neb. 634, 228 N.W.2d 229 (1975).} claiming that these services constituted unlawful banking by the supermarket in violation of Nebraska law.\footnote{Neb. Rev. Stat. § 8-114 (1983).} The court found that Hinky Dinky was simply acting as an intermediary, assisting in the transfer of funds between First Federal and its depositor, and those acts did not amount to engaging in the business of banking.\footnote{Nebraska ex rel. Meyers v. American Community Stores Corp., 193 Neb. 634, 228 N.W.2d 229 (1975).} The court noted that the POS computer terminal is analogous to communication equipment of other kinds in that it simply transmits information to a central computer. The deposit and withdrawal transactions are electronically effected and performed by the computer on the records and premises of First Federal.\footnote{Id. at 639, 228 N.W.2d at 302.}

A new angle has been added to the confused legal status of ATMs. The Comptroller of the Currency has maintained that an ATM is not a branch as long as the bank using it does not own or rent the terminal.\footnote{Weinsein, Federal Court Ruling Calls ATMs Banks, Am. Banker, April 13, 1984, at 1, col. 1.} This position has recently been eroded. In New York, supermarket owners installed a number of ATMs in their stores and permitted the ATMs to become a part of the shared ATM network of a national bank operating in New York state. The court held that if a national bank uses an ATM, it becomes a branch location regardless of the fact that the ATM is owned by a third party.\footnote{Independent Bankers Ass'n of N.Y. State v. Marine Midland Bank, 583 F. Supp. 1042 (W.D.N.Y. 1984).} If upheld on appeal or followed in other states, this decision will have serious implications for retailers interested in installing their own ATMs or POS terminals. As third party nondepository institutions install their own electronic terminals with capacity for financial transactions the branch office issue will become increasingly important for depository financial institutions.

C. INTERSTATE BANKING IMPLICATIONS

Electronic financial services and transactions defy geographic boundaries. Because of this, federal regulations which attempt to deal with these services and transactions are inadequate and should be repealed. The appropriate first step toward geographic deregula-
tion at the federal level would be to allow interstate operation of full-service automated transaction machines. A statutory declaration that ATMs are not branches for legal purposes would open the way for state, regional and nationwide electronic branching. The banking industry is advocating federal legislation authorizing depository institutions to permit depositors/customers to use electronic terminals regardless of location. This should allow interstate operation of full-service ATMs.

D. Antitrust Issues in Shared Proprietary Terminals or Networks

The objective of American antitrust law is to protect competition at all levels and preserve its benefits, i.e., lower prices, innovation, higher quality and availability of alternatives. Most antitrust enforcement in the computer industry is based on section 1 (contracts or combinations in restraint of trade), section 2 (monopolization) of the Sherman Act, and section 3 of the Clayton Act (restraints on dealings with competitors).

Electronic financial services are flexible and competitive. The purposes of antitrust regulation will be achieved if POS terminals are capable of connecting with any depository institution, merchants and depository institutions are unable to exclude other institutions from participating, and networks of EFT terminals provide an adequate mix of packages at competitive prices. An unregulated system does not appear to have beneficial implications for retail depository institutions or for the consuming public. In an unregulated world, there would be a significant further concentration of financial and economic power in the hands of giant depository institutions, major merchant conglomerates or their holding companies. Such concentration could have unfortunate results and implications for the nation's EFT/PEP systems, and for the economy as a whole.149

Antitrust implications for EFT and PEP systems will grow as technology becomes widespread. One important issue is mandatory sharing. As a general rule, joint activities must be limited to those necessary to accomplish legitimate functions of the joint venture.150 Joint activities are tested by their "tendency" towards monopoly, or their "reasonable likelihood" of substantially lessening competition in the market.151 The existing legal and regulatory scheme gov-

149. For a more extensive discussion, see Pierce, Competitive Implications of EFT, 2 COMPUTER L.J. 133 (1980).
erning sharing of proprietary EFT terminals and systems is complicated and unclear. There are no federal statutes expressly applicable to the sharing of EFT systems.

Antitrust policies of the Department of Justice came into conflict with state law in the 1970s when many states had enacted laws requiring institutions deploying EFT machines to provide equal access to customers of any other institution which desired it.\textsuperscript{152} The manner in which these state laws fit into the regulatory scheme of federal antitrust policy is not clear, and many sharing arrangements may in fact violate familiar antitrust prohibitions.

Mandatory sharing laws were designed to prevent domination of EFT business by the largest banks in a state. The Justice Department initially took a dim view of mandatory sharing. The Justice Department faced the issue in fall, 1981, when Hartford National Bank sought clearance for its shared EFT program. The Department approved the program but reserved its right to sue if the arrangement was found to diminish competition.

In its most recent elaboration of antitrust policies and law as it applies to shared EFT networks, the Department of Justice ruled that a savings association in Texas could belong to both of the state's major ATM networks.\textsuperscript{153} However, the Department's antitrust division added that the ruling applied to that factual situation only, leaving the law no clearer than it had been prior to this decision.\textsuperscript{154}

Another antitrust concern is restrictive cross-market tie-in sales of other financial services at competitively unfair prices, which might prevent other EFT service providers from entering the market. Mandatory sharing laws should be interpreted so as to discourage this activity.

The National Commission on Electronic Funds Transfers recommended that federal legislation be enacted to nullify state compulsory sharing laws to the extent that they were inconsistent with federal antitrust law. The Commission believed that a voluntary sharing approach would provide users with the widest choice of services, the lowest prices and the most advanced technology while imposing the least regulatory burden on the taxpayer and the industry. The Commission pointed to the flexibility of federal antitrust


\textsuperscript{154} Id.
laws as a guarantee of such benefits. Federal preemption of state sharing laws is supported by federal regulators and larger financial institutions who recognize that remote service units, ATMs, and POS terminals are essentially regional in utilization and in economic effect.

Are multiple EFT/PEP networks necessary to insure a competitive marketplace? Do networks constitute utilities to which all parties have the right to use on the same terms? No definitive answers can be given in light of the current state of antitrust regulation in this area.

CONCLUSION

An EFT/PEP system is both a communications and transfer of funds system, transferring data and other information relating to the financial transaction over a series of communication networks. Under an EFT system the movement will be electronic: electrical impulses transmitted from terminal to terminal, computer to computer, utilizing thousands of miles of wire, microwave or satellite carriers.

EFT/PEP transactions often cross state lines, and uniform laws setting forth the basic rights and duties of the parties are necessary to codify the desirable rules and regulations. This would create an opportunity to limit the powers of institutional providers of EFT/PEP services to act arbitrarily or to make these providers insurers of the processing of EFT/PEP transactions. Variation by agreement, banking usage and administrative regulation will be needed to provide flexibility in such a code.

Further, there is an urgent need for improvement in the area of computer security. Computer information is most vulnerable to alteration or destruction by employees at computer installations; this should be a primary concern of those who seek to improve computer security.

Computer crime will take on new forms and pose serious problems for law enforcement officials. Criminal laws, in many cases, still fail to address the uniqueness of computer crime, because "physical property" language in statutes cloud over movement of funds by electrical impulses. There is a need for a computer crime statute which addresses this uniqueness.

Individual privacy may also be open to violation by government, credit investigators or computer criminals. Both institutions and in-

155. NCEFT, Appendix C, supra note 8.
individuals have rights requiring legal protection from abuse of computer information.

The way in which the law evolves is important to the electronic financial services industry, and of particular importance to the developing point-of-sale payments sector. If today's EFT terminal networks are to become tomorrow's nationwide ATM/POS networks, then they must have the capability to merge, or at least interchange transactions. Legislators are recognizing that traditional restrictions in geographical market areas and electronic financial services that may be offered by financial institutions are not well suited to today's environment. Regulators of the financial industry are reassessing the applicability of the McFadden Act to today's financial service needs; more liberal rules governing geographic limitations are likely to be the long-term result. Federal legislation may also be forthcoming, enabling federally-chartered depository institutions to establish and operate EFT/PEP terminal systems under uniform rules less restrictive than those governing "brick-and-mortar" branches.

Electronic financial services present an opportunity for financial and non-financial enterprises to offer new and exciting products to their customers. The legal issues raised by this technology are not adequately covered by existing laws. The law must be updated to meet the needs of electronic banking.