The John Marshall Journal of Information Technology & Privacy Law

Volume 6
Issue 1 *Computer/Law Journal - Summer 1985*

Article 7

Summer 1985

Unauthorized Access to EFT Information: Who Should Be Responsible?, 6 Computer L.J. 171 (1985)

Leslie Susan Norman

UNAUTHORIZED ACCESS TO EFT INFORMATION: WHO SHOULD BE RESPONSIBLE?

Public concern over computer crime has skyrocketed in the last few years as the public has come to realize the tremendous potential for large-scale computer abuse. This concern, however, has been concentrated in the area of unauthorized transfers of funds—namely, theft. This is illustrated by the recent legislation enacted in response to such crime.[1] It is only recently that people have become aware of the potential threats to privacy raised by the ability of computers to accumulate and aggregate vast amounts of information and almost instantaneously record and extract that data.

This Note is concerned with the computer systems used by financial institutions to handle financial transactions—electronic funds transfer (EFT) systems. Virtually no federal legislation is currently in effect which sets forth the liabilities associated with unauthorized access to information in EFT systems. The purpose of this Note is to propose legislation which would hold financial institutions strictly liable to the consumer for all damages caused by unauthorized access to financial and/or personal information contained within EFT systems.

I. THE PRIVACY PROBLEM

A. WHAT IS AN EFT?

Electronic fund transfer is defined in the federal code[2] as "[a]ny transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account."[3] In simpler terms, EFT is merely "a process of value exchange achieved through the use of electronic devices."[4]

1. *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1982); Electronic Fund Transfer Act, 15 U.S.C. §§ 1693a-1693r (1982); 12 C.F.R. §§ 205.1-205.14 (1983).

2. 15 U.S.C. §§ 1693a-1693r (1982).

3. *Id.* § 1693a(6).

4. Katskee & Wright, *An Overview of the Legal Issues Confronting the Establishment of Electronic Funds Transfer Services*, 2 COMPUTER L.J. 7 (1980).

Although the concept of EFTs is relatively new, it already plays a significant role in financial transactions. As early as 1975, close to 76% of the almost forty-six trillion dollars of payments were handled by such systems.[5]

B. Benefits of EFT Systems

Financial institutions derive many benefits from EFT systems. The technology involved has greatly reduced the costs associated with gathering and processing financial information,[6] eliminating the need to physically transport, sort and store paper messages.[7] Also, the immediacy of access provided by EFTs greatly increases the value of such systems to financial institutions. Savings have been estimated at thirty to forty percent over the traditional system.[8] In addition to transaction cost savings, EFT systems offer financial institutions the flexibility to move and expand their facilities in response to population growth and movement without incurring the traditional costs associated with opening and moving bank branches.[9]

The consumer has also benefitted greatly from EFT systems. These systems provide consumers with faster access to funds and other banking services at more times and at more places than does the traditional system. The cost savings to financial institutions, mentioned above, will in all likelihood be passed on to the consumer in the form of additional and more economic financial services.

In addition to financial institutions and individual consumers, the public in general will benefit from a more efficient market system and the prospects of additional technology in this area.

C. The Privacy Problems of EFT Systems

The problems that arise from EFT transactions are caused by the informational nature of the system. EFT operates as a substitute for cash. The elimination of the tangible element of cash transactions results in a financial system composed of information transfers.[10] "[A]lthough a bank's tangible assets are an obvious lure for the crimi-

5. Comment, *The Emergence of the Electronic Fund Transfer System: Consumer Protection, Federal Antitrust, and Branch Banking Laws*, 10 OHIO N.U.L. REV. 323, 325 (1983).

6. OFFICE OF TECHNOLOGY ASSESSMENT, SELECTED ELECTRONIC FUNDS TRANSFER ISSUES, PRIVACY, SECURITY, AND EQUITY, BACKGROUND PAPER (1982) (hereinafter cited as BACKGROUND PAPER).

7. Comment, *supra* note 5, at 324.

8. Pierce, *The Competitive Implications of EFT*, 2 COMPUTER L.J. 133, 136 (1980).

9. *Id.*

10. Brown, *Implications of the Informational Nature of Payments*, 2 COMPUTER L.J. 153, 157 (1980).

nal, its intangible assets are an even a grater attraction . . . ."[11] Moreover, the value of those intangible assets is much greater than just the value of the funds.[12] Thus, the problems arising from EFT systems are essentially information management problems.

EFT systems create privacy concerns because "(1) they create permanent records of transactions, which heretofore may not have generated such records, and (2) they pose information management problems through the increased centralization of data, and the improved capture and retrieval capabilities inherent in their technologies."[13] These differences between the manual and EFT systems have prompted financial institutions to realize that their use of EFT systems places upon them the responsibility to protect consumers from unauthorized transactions than does their use of the traditional system.[14] This increased protection is especially necessary due to the fact that financial institutions are privy to more private information than almost any other type of business.[15]

The continued existence of EFT systems is dependent upon public acceptance.[16] Because EFT systems have tremendous capacity to aggregate widely dispersed pieces of information, privacy for the users of such systems has become a matter of public concern.[17] The public wants assurance that the information accumulated within EFT systems will be used only for purposes related to the accomplishment of particular transactions of the customers' choosing.[18] Thus, maintaining the integrity of EFT systems is a major concern. "[A]n unacceptable number of security failures could undermine public confidence in financial institutions, thus weakening the national economy and ultimately the national security."[19]

To preserve the integrity of EFT systems and, hence, continue to derive the benefits from those systems, the consumer's right to privacy must be protected. In this type of payment system, privacy is violated when information is accessed without the consumer's consent and is made available to and used by those who are not parties to the payment transaction for purposes unrelated to the transaction.[20] Thus, "[o]ne

11. Augenblick, *Is Your Bank Bugged?*, BANKERS MAG., Mar.-Apr. 1983, at 44.

12. BACKGROUND PAPER, *supra* note 6, at 45.

13. Brown, *supra* note 10, at 160.

14. Winter, *Banking By Blip: Advent of the Checkless Society Raises Legal Questions*, 69 A.B.A.J. 263, 264 (1983).

15. Augenblick, *supra* note 11, at 44.

16. Comment, *supra* note 5, at 323.

17. BACKGROUND PAPER, *supra* note 6, at 53.

18. *Id.* at 53.

19. *Id.* at 46.

20. *Id.* at 31.

way in which privacy can be violated is by illegal or unauthorized access to EFT and other telecommunication systems."[21]

As the use of EFTs increases, the methods for gaining unauthorized access to personal information also increases.[22] Access to EFT systems can occur in a variety of ways. The more common of these are:

> (1) Electromagnetic pickups—intercepting the radiation generated by a computer's central processor, or telphone-teleprinter lines; (2) browsing—connecting an unauthorized terminal into an EDP system; (3) piggy-back entry—intercepting communications between legal users; (4) wire-tapping—tapping the systems telephone-teleprinter lines.[23]

Access to EFT systems is presently not very difficult. With several hundred dollars of equipment, a knowledgeable technician can wiretap telephone links to automated teller machines.[24] Invasion of privacy in such a case does not require the work of an expert.

The procedures currently being followed by financial institutions to protect privacy is extremely inadequate.[25] Based on a 1979 survey of 130 of the 300 largest commercial banks in the United States,[26] seventy-six percent of the banks that responded to the survey admitted that they do not ask their customers' permission before disseminating private information to third parties, nor do they inform their customers about the possibility of this being done. The survey also indicated that eighty-two percent of the banks always obtained additional information about their customers from outside sources and only thirty percent tell their customers the type of information that will be collected. Although this survey was not concerned with safeguards on EFT systems, it is indicative of the relaxed attitude of financial institutions toward the protection of private information. This survey also indicates that the banks do not provide as much protection of records as the public generally believes that they do.[27]

D. DAMAGES

The damages that could result from such invasion of privacy are numerous. One of the most obvious is the mental anguish and/or distress suffered by customers due to the use of personal information for

---

21. *Id.* at 30.

22. Greguras, *EFT and Privacy*, 26 SECURITY MGMT., June 1982 at 24, 27.

23. Bequai, *Legal Liabilities of EFT Systems*, MAG. BANK AD., Jan. 1983, at 25, 25-26.

24. Dentzer & Cook, *Tapping the Banks Wires*, NEWSWEEK, April 25, 1983, at 58.

25. BACKGROUND PAPER, *supra* note 6, at 34.

26. D. LINOWES, A RESEARCH STUDY OF PRIVACY AND BANKING (1979) (University of Illinois). Of the banks surveyed, only 26% responded. Thus, the results are not absolute but are indicative of the privacy problems.

27. BACKGROUND PAPER, *supra* note 6, at 34.

unauthorized purposes.[28] The possibilities for injury in this type of situation are limited only by the imagination.

In addition to personal injury, "some bankers worry that, by eavesdropping on EFT lines, snoopers could find out where large sums were being transferred, tipping them off to impending mergers and other transactions."[29] Access to such "insider" information could have a significant impact on our market system, severely undermining its integrity and resulting in the collapse of the free market system as we know it today.

II. CURRENT EFT LEGISLATION

A. THE EFT ACT AND REGULATION E

In response to the potential problems raised by the advent of EFT systems, Congress enacted two separate pieces of legislation: the EFT Act[30] and the Right to Financial Privacy Act.[31] Neither of these Acts specifically addresses the problem of unauthorized access to information within EFT systems.[32]

The EFT Act, enacted in 1978, was the first piece of EFT legislation. This Act and its later supplement, Regulation E,[33] address many of the issues raised by the use of EFT systems. The consumer protection provisions in these laws apply, however, only to unauthorized access to funds and not to information. "There is no specific privacy protection provision in the EFT Act."[34]

Section 1693h of the EFT Act addresses the liability of financial institutions.[35] This subsection is set forth in pertinent part as follows:

> 1693h. *Liability of financial institutions*
>
> (a) Action or failure to act proximately causing damages
>
> Subject to subsection (b) and (c) of this section, a financial institution shall be liable to a consumer for all damages proximately caused by—
>
> (1) the financial institution's failure to make an electronic fund transfer, in accordance with the terms and conditions of an

28. Bequai, *supra* note 23, at 27.

29. Dentzer & Cook, *supra* note 24, at 58.

30. 15 U.S.C. §§ 1693a-1693r (1982).

31. 12 U.S.C. §§ 3401-3422 (1982).

32. Although there have been cases dealing with financial institutions' liabilities with respect to EFT systems, generally these cases have dealt with the unauthorized transfer of funds and not access to information. *See, e.g.*, Evra Corp. v. Swiss Bank Corp., 673 F.2d 951 (7th Cir. 1982).

33. 12 C.F.R. §§ 205.1-.14 (1983).

34. Katskee & Wright, *supra* note 4, at 24.

35. 15 U.S.C. § 1693h (1982).

account, in the correct amount or in a timely manner when properly instructed to do so by the consumer, . . .

(2) the financial institution's failure to make an electronic fund transfer due to insufficient funds when the financial institution failed to credit, in accordance with the terms and conditions of an account, a deposit of funds to the consumer's account which would have provided sufficient funds to make the transfer, and

(3) the financial institution's failure to stop payment of a pre-authorized transfer from a consumer's account when instructed to do so in accordance with the terms and conditions of the account.

(b) Acts of God and technical malfunctions

. . .

(c) Intent

In the case of a failure described in subsection (a) of this section which was not intentional and which resulted from a bona fide error, notwithstanding the maintenance of procedures reasonably adapted to avoid any such error, the financial institution shall be liable for actual damages proved.[36]

B. The Right to Financial Privacy Act

The Right to Financial Privacy Act[37] was also enacted in 1978. This Act is quite narrow and applies only to customers' rights and the federal government's duties in regard to obtaining records on customers maintained by financial institutions.[38] This Act does not cover disclosure of information to state and local governments or to private institutions.[39] Nor does this Act cover access to information by individuals.

C. The Federal Wire Fraud Act

In addition to the two Acts above, which relate specifically to EFT systems, liability for unauthorized access to EFT systems can be imposed under the Federal Wire Fraud Act.[40] This Act imposes liability on persons who commit fraud by means of wire, radio, or television communication. To be held liable under this Act, a person must make a transmission of writings, signs, signals, pictures, or sounds. Thus, this Act does not cover unauthorized access to information without some additional transmission.

---

36. *Id.*

37. 12 U.S.C. §§ 3401-3422 (1982).

38. Katskee & Wright, *supra* note 4, at 24.

39. Background Paper, *supra* note 6, at 36.

40. 18 U.S.C. § 1343 (1982).

D. STATE STATUTES

It is apparent that some legislation is necessary to set forth the liabilities for unauthorized access to information maintained within EFT systems. Several states have enacted their own statutes which include privacy protection provisions.[41]

1. *Kentucky*

Kentucky is one of the few states which has enacted statutes making it a crime to intercept, tap, or alter electronic information between an automated banking device and the issuer.[42] These statutes hold the accessor liable for unauthorized access to EFT information, but these statutes have no provision for holding the financial institution liable, even if the information is obtained as a result of the financial institution's failure to properly protect it.

2. *Montana*

Montana has enacted its own EFT Act[43] because its legislature felt that there was no adequate federal or state regulation to control the development of the new EFT technology.[44] Montana's EFT Act regulates unauthorized disclosure of EFT records, but it only applies to a knowing disclosure of records to persons who have no legal rights to see the records. Section 32-6-105(1) of the Montana Act provides:

> *Protection of privacy*
>
> (1) No information relating to any transaction by electronic funds transfer, or application thereof, between a financial institution and its customers or prospective customer may be disclosed by the financial institutions to any person or government entity without consent of the customer or, if the customer refused to so consent, under subpoena issued by a court of record.[45]

And section 32-6-106(1) of the Act provides:

> *Unauthorized disclosure of electronic funds transfer records*
>
> (1) A person commits the offense of unauthorized disclosure of electronic funds transfer records if he has lawful access to such records by virtue of office or employment:
>
> (a) and permits another, who lacks lawful access to such records, to inspect, copy, or read such records; or
>
> (b) transfers such records to another who lacks lawful access thereto.[46]

---

41. Katskee & Wright, *supra* note 4, at 25.
42. KY. REV. STAT. § 39 (1978).
43. MONT. CODE ANN. §§ 32-6-101 to 32-6-402 (1983).
44. *Id.* § 32-6-102.
45. *Id.* § 32-6-105(1).
46. *Id.* § 32-6-106(1).

3. *New Mexico*

New Mexico has taken a new approach to the problem of privacy by enacting a Confidentiality Statute[47] which holds the financial institution responsible for failure to provide adequate safeguards against unauthorized access. This statute provides in pertinent part:

> A. Every seller of goods or services having a point-of-sale terminal on its premises and every financial institution contracting for use of or operating a remote financial service unit shall adopt and maintain safeguards to insure the safety of funds of any third party in situations where deposits are accepted or cash advances or withdrawals are made and to insure the safety of items and other information, which safeguards precautions consistent with the appropriate minimum security requirements specified by applicable federal or state law or by federal or state regulatory agencies having jurisdiction over such point-of-sale terminal or remote financial service unit.[48]

III. PROPOSED AMENDMENT

Most EFT transactions are controlled by the federal EFT Act. Although state laws providing greater protection than the EFT Act are not preempted unless inconsistent,[49] these laws cannot be relied upon to solve privacy problems inherent in EFT systems. Because of the security of state laws regarding EFT systems and the diversity in existing laws, federal legislation is needed to set forth uniform treatment of the violation of privacy caused by the use of EFTs.

To fill this need, this Note proposes an amendment to section 1693h of the federal EFT Act, which was set forth in pertinent part at section II A, above. This proposed amendment provides a civil remedy by adding a fourth subsection to section 1693h(a) of the EFT Act. Section 1693h(a)(4) would read as follows:

> § 1693h. Liability of Financial Institutions
>
> (a) Action or failure to act proximately causing damages. Subject to subsections (b) and (c) of this section, a financial institution shall be liable to a consumer for all damages proximately caused by—
>
> . . . .
>
> *(4) the financial institution's failure to prevent unauthorized access to consumer information contained in the electronic fund transfer system.*

Under this proposal, a financial institution would be strictly liable for all unauthorized access to consumer information in its EFT systems, subject to proof of actual damages suffered by the consumer.

---

47. N.M. STAT. ANN. § 58-16-12 (1978).

48. *Id.* § 58-16-12A.

49. Comment, *supra* note 5, at 337.

IV. JUSTIFICATION OF THE PROPOSED AMENDMENT

A. SHOULD ANYONE BE RESPONSIBLE FOR UNAUTHORIZED ACCESS TO EFT SYSTEMS?

It can be argued that legislation holding anyone but the perpetrator liable for unauthorized access to EFT information is unnecessary. Realistically, any additional costs that a financial institution would incur for information protection would most likely be passed on to the consumer who the legislation is intended to protect. Additionally, it may be worth sacrificing some privacy in order to obtain the benefits provided by EFT systems. "Generally people accept . . . many acknowledged limitations on their privacy, not only because they may have no choice, but because they recognize that they derive substantial benefits thereby."[50] In effect, then, one could argue that by using a financial institution with an EFT system to process financial transactions, one has effectuated a waiver of all privacy rights connected with those transactions.

We do not need to take this extreme position in order to benefit from the advanced technology of EFT systems. As long as the benefits of EFT systems outweigh the costs, including the cost of protecting privacy, we will still benefit from their use. If financial institutions have the necessary cost/benefit information, the most economical and socially acceptable solution can be reached. However, when weighing the benefits of EFTs against the costs of protecting privacy, the costs of *not* protecting privacy should be considered as well.

B. WHY FINANCIAL INSTITUTIONS SHOULD BE LIABLE FOR UNAUTHORIZED ACCESS TO EFT SYSTEMS.

Financial institutions should be liable for damages that are caused by their failure to adequately safeguard the confidentiality of the information contained within their EFT systems. Financial institutions are in the best position to protect informational privacy because they have physical control over the system and are usually the most knowledgeable about systems in general. Because of the potential for liability, financial institutions would spend more resources on security systems. If existing security systems were not adequate, financial institutions would be motivated to invest in research and development to produce adequate security systems.

The perpetrators of EFT crimes are often employees of the financial institution.[51] If the financial institution is held liable for all such crimes, then the institution would find it economically efficient to implement extensive internal control procedures to prevent insider abuse.

50. BACKGROUND PAPER, *supra* note 6, at 31.

51. *Id.* at 48.

Financial institutions can take many precautions to protect themselves against liability. A few such precautions are: education and training of personnel, legal awareness, physical and software security, and communication security.[52] In fact, most legal problems related to EFT systems are "both within the control and ability of financial institutions to avoid or limit."[53]

One of the best methods of protecting the privacy of EFT information is encryption.[54] This is a process which transforms information contained within an EFT system into a code which is very difficult to decipher. Encryption often makes accessing the information not worth the trouble required to decipher the code.[55] The most widely used encryption formula is the United States Government's Data Encryption Standard.[56] Financial institutions have been reluctant to use it, however, because of the additional cost of installing it in automated teller machines.[57] With the incentives that additional liability would create, financial institutions may find it economically feasible to use such a protective device.

The American Bar Association has recommended that financial institutions use a "message authentication standard" which would enable the institution to know when a communication line has been tapped.[58] Another suggestion is forbidding existence of the information in human-readable form.[59]

The most persuasive argument for holding financial institutions liable for maintaining the privacy of the information that they control is that a financial institution will be able to fully evaluate the balance between the advantages of EFT systems and the related costs. The financial institution should be willing to spend on EFT system security an amount up to and including the amount of potential liability. If this amount exceeds the additional benefits derived from the use of EFT systems over the traditional system, then EFT systems would not be cost effective and probably would be discontinued.

Under current law, most financial institutions are unwilling to spend on security amounts exceeding their potential liability for unauthorized transfers of funds. Very little economic consideration is given to the costs related to the loss of privacy caused by unauthorized access to EFT information. Thus, the day-to-day decisions made by financial

52. Bequai, *supra* note 23, at 26.
53. *Id.* at 25.
54. BACKGROUND PAPER, *supra* note 6, at 51.
55. *Id.*
56. Dentzer & Cook, *supra* note 24, at 58.
57. *Id.*
58. *Id.*
59. BACKGROUND PAPER, *supra* note 6, at 51.

institutions regarding EFT security are based on only part of the necessary information. Considering the emphasis put on personal privacy in the United States and the tremendous possibilities of personal and economic damage that could occur, the result of this decision making is absurd.

If financial institutions are not held liable for unauthorized access to EFT information, then the only person who could be held liable would be the perpetrator who actually accessed the information. This would present many problems. First of all, very few people ever get caught for committing computer crimes.[60] The method of access and the nature of the item "stolen" makes it virtually impossible to catch computer criminals. With EFT systems, several people can simultaneously gain access to the system and "steal" information undetected. There are, however, devices which financial institutions can use which will alert them when an outsider has tapped their lines.[61] Therefore, because only financial institutions have any real chance to catch computer criminals, the injured party would have no other means of reimbursement if financial institutions were not held liable.

Second, and most importantly, is the above-mentioned cost-benefit analysis which financial institutions should undertake when installing and maintaining EFT systems. If only the perpetrator is responsible, the financial institution need not consider any of the costs related to information disclosure. Such a failure to consider the full range of costs would result in a skewed analysis of the costs and benefits of EFT systems and may not result in the most economical solution.

Holding financial institutions personally responsible for information protection eliminates much of the need for government involvement in the control of computerized financial information. Avoiding government inducement not only benefits the public through reduced taxes, but also accords with most people's desire for less government intrusion in personal affairs. Many people fear that government controlled access to information would result in the type of society predicted by George Orwell in his book, *1984*.[62] Under the solution proposed by this Note, the financial institution itself would analyze the costs and benefits of EFT systems and would appropriately control access to information.

---

60. Dunn, *A Bug on the Wire Could Cost You Plenty*, BUS. WK., March 28, 1983, at 127.

61. Dentzer & Cook, *supra* note 24, at 58.

62. *Computerized Bank Accounts, Credit Cards, and George Orwell's "1984"*, 32 COMPUTERS & PEOPLE, Mar.-Apr. 1983, at 27.

C. STRICT LIABILITY

The liability of financial institutions for unauthorized access to EFT information should be determined by a strict liability standard as opposed to a negligence standard. Although the courts have been reluctant to extend strict liability to a business offering a service as opposed to a product,[63] the policy reasons justifying imposition of strict liability are present in the computer industry.[64] Also, the fact that computer information and programs can be stolen and duplicated tends to favor their being characterized as a service rather than a product.[65]

Strict liability is generally imposed when a business's activity poses a danger to society and the policies of loss spreading, accident reduction, and victim compensation are met.[66] The dangers to society posed by unauthorized access to private financial and/or personal information maintained within EFT systems are evident from the above discussion of the privacy problems inherent in such systems.[67]

The imposition of strict liability would support a policy of loss spreading because financial institutions are in a position to either insure against liability or, more likely, to pass on the cost to the public by increasing the costs of its services. This is fair, since the public also receives cost reductions because of the efficiency of EFT systems.

Under a negligence theory of liability, the consumer would recover only after proving that the financial institution was negligent in its protection of EFT information. This would be especially difficult if the amount of damages was not significant.[68] Thus, under such a theory, many injured consumers would probably be forced to absorb their own losses, and the policy of loss spreading would not be fulfilled.

Imposing strict liability would also serve the goal of accident reduction. Financial institutions are in the best position to prevent unauthorized access to EFT information. Strict liability provides an incentive for financial institutions to expend additional resources to protect the information as well as to develop new methods of protection. Under a negligence theory of liability, such incentives are greatly reduced, if not eliminated. Financial institutions would do only the minimum necessary to protect EFT information and would have very little incentive to

63. W. KIMBLE & R. LESHER, PRODUCTS LIABILITY 99-100 (1979).

64. Comment, *Computer Software and Strict Products Liability*, 20 SAN DIEGO L. REV. 439, 456 (1982).

65. *Id.* at 451.

66. *Id.* at 447; W. PROSSER, LAW OF TORTS 494-95 (4th ed. 1971).

67. *See supra* notes 23 & 24 and accompanying text.

68. If the court hears only evidence of the individual consumer's damages and those damages are not significant relative to the cost to the financial institution of information protection, the consumer is not very likely to succeed with a claim against the financial institution based on a theory of negligence.

develop new technologies for the protection of privacy. Although eliminating all possibility of unauthorized access to EFT systems may not be economically feasible, providing incentives to reduce those possibilities is a legitimate goal.

The victims of unauthorized accesses to EFT information would be compensated more often for their damages under a strict liability theory. As mentioned above, the victim has a much better chance of obtaining relief under strict liability than under a negligence theory. Since the financial institution is in a better position to bear the burden of the risk of unauthorized access to EFT information, the goals implicit in a strict liability system are achieved. Also, internalizing all of the costs and benefits of EFT systems encourages an efficient level of investment by financial institutions in privacy protection.

D. CAUSATION

Under a strict liability theory, the consumer would still have to prove that his damages were a result of his private financial and/or personal information being accessed from the financial institution's EFT system. In other words, the consumer would have to prove that the financial institution's failure to maintain the privacy of the information *caused* it to be accessed without authorization. Proving this may be a problem when such information is readily available from other sources. The law's major concern, however, is that of maintaining the privacy of truly private and/or personal information which by its very nature would not be readily available from many other sources. Although problems of proving causation may prevent some consumers from recovering from financial institutions for breaches of privacy, this should not be used to justify a rule preventing all consumers from recovering from financial institutions for privacy invasions.

What may well be cause for greater concern is that much information may be accessed from EFT systems without the knowledge of the consumer. In this case, although a wrong has been committed, the proposal presented in this Note would provide no cause of action against the financial institution, since such a wrong would probably occur most often against individual consumers and involve smaller financial transactions, while most cases arising under the proposed amendment would probably concern large financial transactions by large entities. Still, since the financial institution would attempt to protect itself from these suits by providing adequate safeguards against privacy invasion, the proposed amendment would benefit both the individual consumer and the large corporate entity.

E. DAMAGES

Once causation has been established, the consumer must also prove damages in order to recover from the financial institution. Under this proposal, the amount of damages that can be claimed by the consumer is the "actual damages proved." In the case of stolen funds, actual damages would be easy to prove, as they would equal the amount of the funds stolen. But how are damages measured when the harm is the prevention of a corporate takeover or merger? In addition, what is the measure of damage resulting from public exposure of personal information? These losses are very difficult to quantify. This difficulty, however, is no reason to deny the consumer recovery.

In other areas of the law, we accept the necessity of placing values on things which are virtually impossible to value. Values have been put on pain and suffering, mental anguish, lost mobility, and even human life. The difficulties involved in determining these values have not kept us from attempting, to the best of our ability, to compensate those who have been harmed.

This proposal requires that the consumer set forth facts sufficient to establish to the court's satisfaction a particular amount of damages. Although this may often be difficult, it is not an insurmountable burden.

An additional problem that may undercut the effectiveness of this proposal is the feasibility of instigating actions for unauthorized access to EFT information. In cases where the amount of damages is insignificant or difficult to prove, it may not be worth the time and money necessary to file a claim against the financial institution.[69] Most cases in this area would probably involve only large entities and/or large transactions; but, as mentioned above, the work done by the financial institutions to protect themselves from those suits would benefit all the consumers.

V. CONCLUSION

It is time that we look closely at *all* of the costs and benefits associated with the new technology of EFT systems. This technology has provided us with significant reductions in financial transaction costs and has generally improved our standard of living. It is apparent that EFT systems are here to stay. These benefits cannot be fully evaluated without also considering the associated costs—specifically, the increased likelihood of privacy invasion through such systems.

This proposal suggests an amendment to existing legislation that

69. A similar problem has arisen under Article 3 of the Uniform Commercial Code, relating to the ability to obtain a remedy for bad checks.

would impose liability on financial institutions for unauthorized access to EFT information in a manner which would minimize the need for government intervention and encourage the most economical solution to such problem of keeping information private. The importance of the privacy of personal and financial information in the United States mandates the adoption of such a proposal.

Leslie Susan Norman