Chapter 5

Security in Electronic Funds Transfer

Chapter 5

Security in Electronic Funds Transfer

Chapter Summary

Security means the protection of the integrity of electronic funds transfer (EFT) systems and their information from illegal or unauthorized access and use. Although the loss per theft appears to be greater than for paper-based payment systems, there is no real evidence that EFT systems to date have resulted in a higher than average crime rate. Why, then, is the security of EFT systems an important public concern and potentially a major policy issue? In comparison with other payment systems, EFT appears to have some additional vulnerabilities:

- EFT systems have many points of access where transactions can be affected in unauthorized ways because of direct customer involvement with the dynamics of the systems, the use of telecommunication lines, and the ways in which data are aggregated and transmitted among and between sites and institutions.
- Funds can be removed in currency almost instantly without review of individual transactions by officials.
- Because of the kinds of information recorded and the way it is aggregated, EFT data have an economic value above and beyond the value of the funds, and hence provide another source of temptation,
- It is possible, in theory, for large banks of data to be destroyed by remote agents, creating the opportunity for maliciousness, extortion, blackmail, or terrorism.
- EFT crime provides a sporting element, or intellectual challenge, to some people that is perhaps as enticing as the opportunity for financial gain.
- EFT crime is often difficult to detect because funds/data can be removed or manipulated by instructions hidden in complex computer software; the dynamics of the criminal action may be understood only by a few experts within the institution.
- EFT crime is poorly reported because publicity may draw attention to ways of attacking the integrity of the EFT system, may give organizations a poor public image, or may even raise insurance premiums.
- Existing legislation may not be fully adequate or appropriate for prosecuting EFT crimes.

A high degree of security is especially important to the future development and use of EFT because this is a relatively new technology that is challenging much older and well-established payment systems. Therefore, it is particularly dependent on the confidence of the public. The failure to gain and maintain the confidence of individual and organizational users during this period of rapid development could ultimately undermine the stability of financial institutions that have already heavily committed themselves to EFT systems and practices.

It is difficult at present to assess the level of EFT security violations because there is underreporting of EFT crime, a paucity of information about EFT security, and a lack of informed public discussion, although considerable public concern is voiced. Such evidence as is available suggests that EFT security violation is not a severe problem, although the magnitude of loss in individual EFT thefts may be much higher than that in conventional thefts from financial institutions. While there are some dangers that giving these problems higher visibility through public discussion may at first make them worse, the public is entitled to know what risks they are exposed to in using EFT services. Furthermore, both law enforcement agents and financial institutions would benefit by sharing information about vulnerabilities, defense strategies, and security-enhancing technologies.

Some believe that both effective technology and sound management procedures exist for adequately assuring EFT security, though even present technology and procedures are not all widely used. There is as yet no clear and consistent set of industrywide security standards for protection of computer systems. The use of security technology and procedures varies among institutions. The cost of providing a reasonable degree of security–equal at least to that provided for paper-based payment systems—is probably not excessively high, but information on this point is scanty.

Better information about EFT security would allow Congress and State legislatures to assess more effectively the possible need for new or modified legislation and/or regulations.

Security in Payment Systems

An important issue with regard to EFT is the level of security that will be required and its cost. Will new legislation be needed for prosecution of EFT-related crime? Will public discussion of EFT security problems exacerbate those problems, and if so, is some mechanism needed for sharing information about security problems and appropriate defense strategies?

Any payment system and any financial institution must be able to guarantee, at least to some reasonable degree, the safety of assets entrusted to it. It must be able to protect both funds and data against theft, loss, and misuse. Users must be assured that transactions will be carried out according to their instructions. The ability to guarantee the integrity of the payment system and the safety of both funds and information is what is meant by security.

Any medium of exchange, whether currency, checks, bills of credit, or recorded electronic signals, ultimately relies on public confidence that it will retain its value and continue to be acceptable to others in exchange for goods and services. Similarly, the continued viability of financial institutions depends on the confidence of their customers. Thus, the adequacy of EFT security systems is important, not only because individuals are entitled to protection of their accounts and to the confidentiality of the information that they provide, but also because an unacceptable number of security failures could undermine public confidence in financial institutions, thus weakening the national economy and ultimately the national security.

Wherever monetary value exists, and in whatever form, it becomes an object of greed and a target for criminal activity. Funds have been embezzled and banks robbed for as long as banks have existed. EFT offers some valuable opportunities for protecting individuals and organizations against loss of assets. The availability of automated teller machines (ATMs) and point-of-sale (POS) terminals enables individuals to carry less cash on their persons. Automatic deposit of payrolls and social security checks would reduce the volume of thefts from mailboxes. Merchants will suffer fewer losses from bad checks and credit card fraud. Financial institutions can reduce employee error, improve audit trails, and reduce overdrafts.

However, EFT also has some vulnerabilities that paper-based payment systems do not have, and it creates the opportunity for new kinds of white-collar crime (l). Most funds have always existed only as data in account ledgers or files. Before EFT, however, the customer was kept at a distance from all but the first and last steps of transactions, and financial institutions could control and guard most of the processing so that risks were at least limited to those internal to the financial institution (with the exception of bank robbers and check passers). Some time had to elapse before funds could actually be removed in the form of currency and could no longer be returned simply by reversing the paper transaction.

With some EFT procedures, however, customer involvement with the system is facilitated and funds are quickly removed, often without another human having overseen the process. Other EFT systems involve many third parties in encoding, transmitting, or storing data, thus providing many vulnerable points where security could be breached. Communication links are vulnerable to electronic eavesdropping and provide entry into the system at several points. The data needed for EFT systems are easily aggregated and accessed, thus creating a value apart from and in addition to the value of the funds. This also creates concern over security in relation to EFT systems.

Security also may be breached accidentally. EFT technologies can lose data through failure of hardware components or communication links, or deterioration of storage media. Where there is no backup documentation such data loss can seriously compromise the system.

Another difference between EFT and traditional security risks related to banking and payment systems is the sporting element. Armed bank robbers are almost always professional criminals. Embezzlers, while they may never before have committed a crime, are motivated just as clearly by greed for financial gain. But it appears that computer criminals are sometimes motivated, at least initially, by the sheer fun of beating the system. This kind of gamesmanship, for a lark as much as for funds, seems to provide the motivation for bright college students and even younger children breaking into institutional computers to discover, modify, or steal information or merely to play tricks on the system.

In the case of EFT systems, however, the sporting behavior is apt to be lavishly rewarded and the fun amplified by substantial financial gains at minimum risk. Some experts assert that most EFT crime is never detected, or if detected is not reported.

Financial institutions are reluctant to publicize EFT losses for several reasons. They fear that public confidence will be compromised and the institution weakened; that their insurance premiums will be increased; and that other computer buffs, or more professional criminals, will learn the system's vulnerabilities or will be challenged to surpass the achievement.

Losses from individual accounts may go undetected by the account owners because they are so small; one strategy is to instruct the computer to deduct a cent or two from each transaction handled, and deposit it in a fraudulent account. A sufficiently high volume of transactions could make such amounts accumulate rapidly. Since information, unlike money, can be owned and used by many people at the same time, data can be "stolen" without anyone being the wiser. By the time stolen information is actually used for unauthorized purposes it may be impossible to trace its origin. Often managers and law enforcement officials are not qualified to detect computer-based crimes and frauds, and are unlikely to challenge either the machine or the computer experts on the workings of the system.

Typical computer criminals are said to be young, intelligent, enthusiastic computer buffs with no prior criminal record and probably no previous criminal activity (2). If detected, they may be either hired or maintained as employees by the financial institution they victimized to help protect it against similar violators. In any case, they are unlikely to be severely punished. One estimate is that only about 3 percent of computer criminals who are apprehended ever go to jail (3).

Many States do not have legislation for prosecuting computer-based crimes, and even Federal law is unclear in some aspects. In one case, a Federal judge ruled that movement of a stolen program over telephone wires did not legally constitute theft of trade secrets, since the relevant statute required the stolen article to be tangible (4). The act of copying the program and taking it to the thief's office, however, was judged to be criminal. Legislation proposed in 1979 but not enacted, known as the Federal Computer Systems Protection Act, was designed to facilitate prosecution of offenders charged with computer-based crimes against Federal systems (5).

Types of EFT Crime or Breaches of Security

Breaches of security can be accidental as well as deliberate. They may affect individual accounts or threaten institutions or networks. EFT crimes may be aimed at theft of funds; at use, disclosure, alteration, theft, or destruction of data; or at disruption or destruction of the EFT system. Funds (or data) can be stolen by embezzlement within the financial institution, by intruders from outside of the institution, or by customer fraud.

Employees of the institution are frequently the source of EFT crime. They are likely to have access to the systems and often can mask criminal actions behind legitimate activities. They may hide unauthorized procedures within programs (the "Trojan horse" strategy) by building in instructions to abort or divert authorized transactions, and then remove this procedure from the computer's memory bank. Unauthorized copying of either programs or data, such as account numbers and personal identification numbers (PINs), usually cannot be detected or traced (6). However, most reported cases of EFT crime are not sophisticated.

Most of these criminal tactics can also be used by intruders from outside of the EFT payments systems (7). For example, in the hands of a computer expert, a home terminal can successfully "impersonate" a POS terminal and send perverse instructions over the EFT communication line. However, this is difficult to do at present.

EFT communication links can be tapped or used for eavesdropping under some circumstances. False information can be entered or legitimate information altered or destroyed. The lines themselves are also vulnerable.

Customers often abuse EFT systems by unauthorized overdrafts. Some ATM devices are not online; that is, they do not have access to customer accounts, Instead they limit the amount of money that may be withdrawn by a customer with proper identification (usually $100 per 24 hours), Some offline ATM devices cannot lock out stolen cards. Most ATMs, of course, require both an authorized card and a PIN for access. However, some require only a card, and users often carelessly discard receipts bearing their account number right at the site. Against all advice, some users insist on writing their PIN on the access card or on something that they keep with the card.

Access cards can also be forged, They may be stolen from the bank or from the mail enroute to the customer. (Sometimes they are sent to potential customers without having been requested, although an additional validation step is usually required before they can be used.) Account numbers and PINs can be lifted from the card's magnetic strip and transferred to blank cards (8).

ATMs and POS terminals were not in use during the height of political activism and protest demonstrations of the late 1960's and early 1970's, With any new wave of protest, however, they would be vulnerable to politically inspired vandalism. Spray paint, gum, glue, or objectionable substances would easily render a machine inoperable, at least temporarily.

Normal failures of EFT components or communication links also make EFT devices temporarily inoperable. ATMs currently have an outage rate of about 3 percent (9), which is frustrating to customers who depend on the machines to complete transactions outside of normal banking hours. As more and more customers come to depend on EFT, downtime will be even more unacceptable. Failure of system components can also cause loss of data, which is a more serious matter.

The vulnerability of EFT systems to natural disasters such as earthquakes, floods, fire, and severe ice and snow storms is a matter of some concern. As yet, however, there has been only one reported incident of EFT systems being affected by natural disasters. When Mount St. Helens erupted, many ATMs were disabled by dust and ashes from the volcano. A number of banks have reported that ATMs generally continued to function well during severe winter weather, even though user demands were much heavier than at other times (10). It has recently been suggested that electromagnetic pulses, such as might result from nuclear weapons use, could knock out systems over a very wide area (11). As EFT networks are built, such vulnerabilities become systemic rather than localized. (The larger issue of national security and systems vulnerability is discussed briefly in app. A.)

How Serious is EFT Crime at Present?

No one knows for certain how serious the problem of EFT theft really is, since much of it is either not detected or not reported. Clearly the potential for crime is great. In general, it is thought that EFT thefts aimed at institutions tend to be much larger than traditional forms of bank robbery. One expert estimates that the average armed bank robbery in the mid-1970's netted about $10,000 and the average conventional embezzlement about $20,000, but computer-based banking thefts averaged about $500,000. However, these figures are based on 46 cases of computer-based theft examined 5 years ago when EFT was much less widespread (12). A successful and undetected EFT thief could attack an institution repeatedly, and an institution with an unsuspected vulnerability could be victimized by multiple criminals,

The extent of petty theft from ATMs is also not known. A 1978 survey of financial institutions by the American Bankers Association reported that only 5 percent of the responding institutions were willing to say that ATM losses were greater than those experienced with paper-based transactions, 9 percent reported no losses, and 43 percent reported minor security problems. Of the losses reported, 65 percent by dollar volume resulted from stolen access cards, 22 percent from customer fraud, and 13 percent from "internal problems" (13). Customer fraud usually involved overdrafts at offline ATMs. Reliability failures of the machines (e.g., failing to print a record of disbursements) accounted for some losses. In 1979, the Federal Reserve System reported that ATM losses reported by 125 banks amounted to less than 1 percent of dollar volume of transactions and less than $0.03 per transaction (14). A survey by Payment Systems, Inc., estimated average annual losses at about $0.03 per active card (15).

Another survey reported that customers have been robbed while using ATMs at 2.5

percent of reporting institutions (16). All of these surveys are based on reporting by financial institutions (and only those institutions that responded to questions). They probably understate the facts, but there is no real evidence that EFT systems have resulted in greater losses by theft, fraud, or system failure than result from other payment systems. While EFT creates some vulnerabilities that are not associated with other payment systems, it also offers some advantages in terms of security. For example, it could reduce the number of thefts of checks from mailboxes. Thus, while wide implementation of EFT systems will almost certainly result in shifts in the types of crime associated with payment systems, the degree to which it might result in an increase in the number of crimes, or the dollar volume of losses, is unclear at present.

What is clear is that much of the risk to payment system security can be avoided or reduced with increased attention to protective procedures and security technology.

Technology and Techniques for Increased EFT Security

The major categories of threats to EFT security are summarized in table 7. In theory, nearly all of these can be minimized by the application of good management practices. The three lines of defense against breaches of EFT security are administrative procedures, physical protection, and technical/ electronic safeguards.

Personnel within financial institutions or associated with handling, transmitting, and storing data are probably the most important source of risk to security. Good management requires strictly limiting access to funds and data, and keeping full records of who has access and at what times. Personnel must, of course, be carefully selected and judiciously supervised. They can be rotated in their jobs to limit the time they have to experiment with EFT systems and probe for vulnerabilities. It may be possible to divide critical data, such as a transmission encryption key, between two or more people. In some cases, it is possible to divide processing duties so that few people know all of the procedures and programs. However, this is often difficult since EFT by its nature integrates the flow of processing. Audit trails can be established and transaction logs carefully isolated and physically protected. Account activity can be reviewed regularly to detect unusual increases in frequency or size of withdrawals or account balances.

ATMs can be protected by judicious siting—well-lit, heavily traveled locations, usually under public observation—and, if necessary, by armoring. Online ATMs (those with access to customer files to check account balances) prevent unauthorized overdrafts. Both ATMs and POS terminals can be designed so that the user’s hands and the keyboard are hidden from observers. In the future, the combination of access cards and PINs may give way to or be augmented by safer access systems using recognition of fingerprints or hand geometry, signature dynamics, or even voiceprints. Technology that allows reliable authentication of human and machine ‘‘signatures’ is already available (17).

These protective measures have some potential drawbacks. They increase the possibility of unjustified rejections that cause inconvenience, embarrassment, and frustration for the user. They remove the option of sending an agent to carry out a transaction, and at best may cause the devices to appear more “unfriendly” to customers who already are inclined to object to their impersonality.

Table 7.— Major Categories of Threats to EFT Security

- **Internal threats (within the institution)**
  - **System failure**
    - Failure of computer programs
    - Failure of hardware components
    - Loss of data from system malfunction
    - Deterioration of storage media
    - Failure of communication links
    - Failure of power, destruction of facilities
    - Deterioration of storage media
  - Employees
    - greed. malice, Ineptitude accidents, disgruntlement, challenge
    - Trojan horse (unauthorized procedures hidden within programs)
    - Bogus transactions
    - Unauthorized copying of data or programs
    - Modification of data
    - Unauthorized sale of data
    - Destruction
- **External threats to system**
  - **Natural disaster:** fire, flood, ice and snow, earthquake, etc.:
    - Direct damage
    - Lack of maintenance
    - Overload at terminals
    - Inaccessability
  - Human
    - criminals, terrorists, political (and religious, economic, racial) activists, “buff s,” Inept customers
    - Physical damage (Including vandalism) or destruction
    - Destruct Ion of data
    - Modification of data
    - Theft of data
    - Fake transactions
    - Impersonation of computer
    - Forged access devices
    - Unauthorized use of access devices

SOURCE Office of Technology Assessment

Measures are available to reduce the likelihood of access cards being forged. For example, they can be made sensitive to heat and pressure which are used in illegal duplicating of the magnetic strips. The French and others are experimenting with “intelligent cards” that use a microprocessor to provide access data (18). PINs are almost always transmitted to the customer separately, with instructions that they are not to be written on or attached to access cards. Sealed mailers are frequently used, with the PIN printed through the envelope so that it is never exposed to view even while still within the provider institution. Rather than being assigned a PIN, customers may be permitted to select their own. Technologies are available that prevent the exposure of a selected PIN, even to the system operators.

Institutional computers are generally enclosed and guarded: access is limited and sign-in procedures are used to record entry. They can be protected with monitoring devices and alarms to guard against fire, flood, and intruders. All equipment can be designed to require keys for access and operation. More sophisticated protective procedures include protocols to guard against unauthorized insertion of data or instructions, and procedures that record every modification and every use of programs. Communication lines can be protected with alarms against taps, and tested frequently for eavesdropping.

The best protection for data in transmission and in storage is probably encryption. One form uses encoding in which the coding and decoding procedures are public but the actual encryption keys used are secret and tightly controlled. The National Bureau of Standards has developed a national encryption standard called the Digital Encryption Standard (DES). Another technique never permits the data to exist as clear text that can be understood by humans. While encryption cannot be absolutely safe (every code can in theory be broken with the use of computers), procedures can be used that would take so long to unravel that it would never be worth the effort. For example, some experts suggest that it would take hundreds of millions of dollars and hundreds of years to crack DES (19). Another important but expensive security measure is the provision of backup for computer processing, data storage, communication lines, and power sources.

While technology both to provide and to breach security will undoubtedly continue to develop in parallel, it seems clear that the application of good management procedures —combined with physical protection, backup facilities, and electronic technology—can provide a substantial level of security, but at considerable cost. The issue, then, concerns the appropriate balance between cost and additional security.

Security and Public Discussion

The customer is often directly culpable in violations of security, quite apart from intentional customer fraud. EFT users often ignore all warnings and handle access cards, credit cards, PINs, and account numbers with great carelessness. They write PINs on ATM access cards, discard receipts beside ATMs, fail to report the loss or theft of cards, and leave bank statements lying around. Public education about EFT security risks and vulnerabilities therefore would seem desirable.

However, financial institutions are reluctant to call attention to these problems or to encourage public discussion of security issues. This is not entirely because the competitive position of their own services may suffer, or even because it might contribute to loss of public confidence in EFT. They are understandably reluctant to promote the realization that EFT offers a new and potentially lucrative field of crime, since this might encourage other professional and amateur criminals to try their hand.

Financial institutions are even less willing to publicize or encourage discussion of computer-based embezzlement and related crimes. Whereas almost everyone knows, at least in theory, how to rob a bank at gunpoint or how to kite a check, the strategies for computer crimes are far more complex, more numerous, and more diverse, and are based on knowledge of new technology as yet not widely available. The new breed of criminal often attacks vulnerabilities that the institution and its management did not know existed, and often creates or discovers avenues for theft (or maliciousness) that are specific to the institution's computer systems and programs. Clearly it would be unwise to disseminate this information to other potential offenders by public discussion. Moreover, there is a strong element of gamesmanship in some computer crimes. Institutions (and the police) are not inclined to reward the offender with public notoriety that may encourage others to try to beat the system.

Thus, there is considerable motivation, in some cases at least, for not reporting or prosecuting EFT crimes, whether petty or grandiose. In addition, formal reporting systems may not have appropriate categories for identifying EFT crimes as such. These and other factors have resulted in a paucity of information about the extent of EFT security violations, and about effective strategies and technologies for preventing such violations.

Both law enforcement agencies and financial institutions would benefit from better information to increase their capability to prevent, detect, and solve EFT crimes and to apprehend and prosecute perpetrators. The public also is entitled to know the extent of risk in selecting and contracting for EFT services, and would perhaps benefit from additional education about how to use such services without creating opportunities for criminal acts. Better information would allow Congress and State legislatures to assess more effectively the need for new or modified legislation to deal with EFT security, and to build a constituency for such legislation if it becomes necessary. Such information might also stimulate the development of improved technology for security. A possible danger is that information about and wide public discussion of EFT security problems might contribute to an increase in criminal activity.

Relationship of Security to Privacy and Equity

The question of EFT security is closely related to the concerns of privacy and equity. Because information about individual customers and their transactions, which in paper-based payment systems is either not recorded or is dispersed throughout the system, is more easily aggregated and easier to access in computer-based EFT processes, privacy for the user has become a matter of public concern. Users want to be assured of the confidentiality of this information—assured that it will be aggregated and used only for purposes integral to the payment system and necessary to the carrying out of the transactions as intended by the customer. This assurance rests on confidence both in the intent of the financial institution, and in its ability to protect the information and limit access to the institution's authorized agents. If security is breached, the institution cannot provide this protection and the user privacy may be violated. It should also be noted that some means of increasing security (e.g., audit trails) increase the possibility that privacy may be infringed because additional copies of data are created at various points in the system. Security then must be provided at more points in the system.

The relationship between security and equity is even more subtle and more equivocal. When transactions are handled and supervised by officials and employees of a financial institution, there is an element of real-time personal judgment involed that disappears when the customer interacts directly with an EFT device. A bank teller, for example, approves a withdrawal or cashes a third-party check for an unknown individual partly on the basis of established identification or other credentials and partly on trained judgment of the individual based on appearance and other factors. Where there is judgment there is also the opportunity for discrimination or prejudice.

On the other hand, EFT devices treat as equals anyone with an acceptable access card, validated credit card, etc., and do not discriminate between regular customers and purse-snatchers. At the same time, the movement toward impersonal electronic systems may create new credential requirements that will make it more difficult for some people (e. g., the poor, the young, foreign visitors) to gain initial access to EFT services.

Chapter 5 References

1. Some studies have concluded that these vulnerabilities are often overstated. *See*, for example, Kranzley & Co., *The Analysis of Certain Potential Threats to EFT System Sanctity* {conducted for the Electronic Industries Foundation under contract to the Office of Telecommunications Policy: December 1976); Federal Deposit Insurance Corporation, *Introduction to EFT Security* (August 1976): The Mitre Corp., *Study of the Vulnerability of Electronic Communication Systems to Electronic Interception* (conducted for the Office of Telecommunications Policy, January 19'77).
2. Leonard Krauss and Aileen MacGahan, *Computer Fraud and Countermeasures* (Englewood Cliffs, N. J.: Prentice Hall, 1979), p. 1z.
3. Edward H. Coughran, *Crime by Computer*, (University of California San Diego Computer Center: 1976), p. 24.
4. Ward v. Superior Court, 3 CLSR 206.
5. S240, Federal Computer Systems Protection Act, January 1979.
6. Telecommunications Systems to Unauthorized Use (1977), p. 11. Also FDIC, op. cit., pp. 7-8.
7. Ibid.
8. Ibid.

9. *American Banker, Dec. 7, 1978.*
10. "ATM Usage Surges During Snowstorms, " *EFT Digest,* March/April 1978.
11. *Science:* "Nuclear Pulse (I): Awakening to the Chaos Factor, " May 29, 1981, p. 1009; "Nuclear Pulse (II): Ensuring Delivery of the Doomsday Signal, " June 5, 1981; "Nuclear Pulse (111): Playing a Wild Card, " June 12, 1981, p. 1248.
12. Dorm Parker, Stanford Research Institute, in presentation to California Task Force on EFT, Feb. 20, 1978.
13. American Bankers Association, *Results of an ATM Security Suruey* (June 1976).
14. Comments issued by Federal Reserve on Regulation E, Mar. 30, 1979.
15. Ibid.
16. Linda Fenner Zimmer, *Cash Dispensers and Automated Tellers: Fourth Status Report (park* Ridge, N. J., 1977) p. *239.*
17. "PIN Systems Emerge as a Better Idea, " *Savings and Loan News,* June 1978, pp. 98-100. *Also* "Security Approaches When the Customer Activates the System, " *U.S. Banker,* Oct. 12, 1978, pp. 49, 51.

18, FDIC, *Introduction to EFT Security, 1976, Pp. 7-8.*

19. Ibid., pp. 13-16,