UIC John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 6

1980

Authentication in EFT: The Legal Standard and the Operational Reality, 2 Computer L.J. 67 (1980)

Fred M. Greguras

David J. Sykes

AUTHENTICATION IN EFT: THE LEGAL STANDARD AND THE OPERATIONAL REALITY†

By FRED M. GREGURAS AND DAVID J. SYKES***

INTRODUCTION

Currently, in utilizing an electronic fund transfer (EFT) system, a consumer usually authenticates his transaction order at a terminal by having possession of and presenting his account card, and by exhibiting knowledge of the personal identification number (PIN) or code (PIC) associated with the account.[1] In a telephone transfer, knowledge of the PIN or PIC[2] is the primary element of authentication.[3]

Since possession of an account card and knowledge of the PIN

---

* B.A. 1966, University of Omaha; M.S. 1968, University of Nebraska, Omaha, Nebraska; J.D. 1975, University of Nebraska; associate at Kutak, Rock & Huie, Omaha, Nebraska. Mr. Greguras has acted as consultant for the Nebraska legislature in the areas of computer-assisted legal research and information processing (1974-75) and privacy and electronic funds transfer systems (1975), as well as the Nebraska Department of Banking and Finance, where he prepared an EFT study proposal (1976). For additional articles by Mr. Greguras on EFTS, see the Bibliography in this issue.

** Mr. Sykes' present position is as a consulting engineer for data communications products associated with the large information systems division of Honeywell Information Systems, Phoenix, Arizona. Before joining Honeywell, he was with RCA Defense Electronic Products and engaged in the design of equipment for data communications associated with spacecraft.

1. A check guarantee and credit card authorization system operated by a major Columbus, Ohio bank, in which possession was the only method of authentication, recently terminated operation, citing fraud as a primary reason for the decision. *See* Kutler, *Move by City Natl., Ohio to Eliminate Check Plan Does Not Spark POS Retreat*, Am. Banker, Mar. 20, 1979, at 2, col. 1; PAYMENT SYS. ACTION REP., Mar. 5, 1979, at 1.

2. Throughout this article, the acronym PIN will be used to represent both an identification number and a code of alphabetical or alphanumeric characters.

3. The consumer must also know to whom payment may be made. Since the set of payees is presently limited, the loss of knowledge of a PIN is not yet crucial.

can be transferred intentionally or inadvertently, or can be stolen, there is a growing need for an authentication method based on unique personal characteristics. Techniques for assuring that the identification is correct, such as fingerprints, voiceprints and signature analysis are being studied for EFT use. In the check payments mechanism, although a signature is theoretically the method of authentication for an order, identification of "who a person is" through items such as drivers' licenses is an essential element of authentication in over-the-counter transactions.

Since consumers are relatively satisfied with the checking system, and because greater convenience is a major factor in persuading consumers to use EFT, a fast and reliable means of authentication is crucial to consumer acceptance of EFT systems.[4] On the other hand, the cost to system providers of such authentication mechanisms cannot be so great as to be a disincentive to the development and implementation of EFT systems. The tradeoff must be measured by a cost-benefit analysis labeled "reasonableness" in a legal context.

The methods used in a checking account system for assuring that identification is correct do not appear to be a long-term solution in an EFT setting. The delay in completing transactions using these methods would be at least as great as for checks, a factor contrary to the need for greater convenience. Further, such methods are limited to supervised EFT transactions.

From a legal standpoint, the reliability and reasonableness of an authentication method is important in at least three ways. First, the security of a system should minimize total system losses from unauthorized transactions. The legislative allocation of risk between a financial institution and its customers for unauthorized transfers has been primarily based on the vulnerability of authentication methods.

Simultaneously, an authentication method must consistently identify valid transaction orders in order to reduce the frequency and amount of damages for wrongful dishonor.[5] Not only must access to unauthorized users be prevented, but access to authorized users must be virtually guaranteed. The avoidance of the wrongful rejection of authorized users is more important than preventing imposters from accessing an account. In addition to possible money

4. Greguras & Wright, *How the New EFT Act Affects the Financial Institution/Consumer Relationship*, 11 U.C.C.L.J. 207, 267 (1979); Bishop & Stafeil, *Consumers' Perception of Supermarket EFT Services*, BANK AD., Jan. 1979, at 37.

5. In traditional statistical terminology, the wrongful rejection of a properly authenticated order is called a Type 1 (T1) error, and the wrongful acceptance of an imposter is called a Type 2 (T2) error.

damages for wrongful dishonor, the inconvenience and consumer embarrassment caused by an unreliable authentication method would severely harm consumer acceptance—an important marketing consideration. The authentication method is also a factor in both state and federal regulators' decisions whether to authorize the deployment of EFT terminals and in their examination of such facilities after they have been established.

The federal Electronic Fund Transfer Act[6] is the primary law which establishes an allocation of risk for unauthorized transfers and wrongful dishonors. The Act's provision which allocates liability for unauthorized transfers is presently in force[7]; the section on allocating liability for failure to comply with a proper order will be effective on May 10, 1980.[8]

The EFT Act is applicable only to the financial institution-consumer relationship.[9] It applies to consumer transactions involving both federal and state financial institutions, but preempts state law only to the extent that the protection provided to consumers is greater than that afforded by state law.[10] The federal law does not address the terms or conditions of deployment of a network of terminals or the system configurations.

This article will first examine the legal implications of the selection of an authentication method, and will then evaluate alternative authentication methods and their current and future practicability.

I. Liability For Unauthorized Transfers[11]

A reliable authentication method is important to avoid total system losses, which increase the expenses of all system participants, including consumers. The level of protection provided and its cost should be related to the risk of loss involved. Both technology and human behavior are important factors that must be taken into account in examining how laws have allocated risks. The National Commission on Electronic Fund Transfers (NCEFT) recommended

6. 15 U.S.C. §§ 1693 *et. seq.* (1978), *reprinted infra* in the Appendix [hereinafter cited as the EFT Act]. For a comprehensive analysis of this law, *see* Greguras & Wright, note 4 *supra*.

7. 15 U.S.C. § 1693g (1978).

8. *Id.* § 1693h.

9. *Id.* § 1693a(5) & b.

10. *Id.* § 1693q.

11. For a detailed analysis of liability for unauthorized transfers, *see* Greguras, *The Allocation of Risk in Electronic Fund Transfer Systems for Losses Caused by Unauthorized Transactions*, 13 U.S.F.L. Rev. 405 (1979).

a risk standard based essentially on the behavior of the parties.[12]

Congress, however, did not adopt this standard in the EFT Act. Instead, it opted for what is basically a limitation on losses with only some of the potential losses allocable to a consumer for his failure to act to prevent losses or further losses.[13]

A. Liability Under the EFT Act

In the case of an unsolicited account access card, a consumer has no liability under the EFT Act until the card is activated at the consumer's request.[14] Activation involves the financial institution providing the second element of authentication—a PIN. Where an account card has been requested, the consumer bears no risk until he receives and signs or uses the card.[15] Typically, a financial institution will separate the delivery of each element of authentication. If a loss is caused by a forged card or an intercepted communication, the consumer bears no liability and has no duty whatsoever to prevent further losses.

If the consumer reports a lost or missing card within two business days after learning of the situation, he is liable for losses caused by unauthorized transfers only to the lesser of $50 or the total loss that has occurred as of the time the financial institution is notified of the missing card.[16] If the consumer delays in reporting the loss for more than two business days, his potential exposure increases to $500, but only if the loss could have been avoided by prompt notice.[17] Notice is effective at the time of mailing, rather than at the time of receipt by the financial institution.[18] These limitations on consumer liability apply even if the consumer has written his PIN on his account card or keeps it with his card. The importance of separating the elements of authentication is obvious.

Once the consumer notifies his financial institution, the institu-

---

12. NATIONAL COMM'N ON ELECTRONIC FUND TRANSFERS, EFT IN THE UNITED STATES 58 (1977) [hereinafter cited as NCEFT REPORT]. *See* Greguras, *Electronic Funds Transfers and the Financial Institution/Consumer Relationship*, 10 U.C.C.L.J. 172, 206 (1978), for an analysis of the consumer protection recommendations of the Commission.

13. 15 U.S.C. § 1693g(a) (1978).

14. *Id.* §§ 1693a(1) & g(a).

15. *Id.*

16. 44 Fed. Reg. 18,468, 18,482 (1979), to be codified as Regulation E, 12 C.F.R. § 205.6(b), *reprinted infra* in the Appendix. Hereinafter, citations to Regulation E will be to the C.F.R. only.

17. 15 U.S.C. § 1693g(a) (1978); 12 C.F.R. § 205.6(b)(1).

18. 44 Fed. Reg. 46,432 (1979). Initially, the Federal Reserve Board specified that notice would be effective at the time of receipt in order to encourage telephonic notification. 12 C.F.R. § 205.6(c).

tion is charged with immediate and continuing knowledge of his account status and is liable for all subsequent losses.[19] If the consumer fails to report an unauthorized transfer within sixty calendar days after it appears on his account statement, his potential liability is unlimited, but only with respect to additional losses from unauthorized transfers which occur subsequent to the sixty-day period, and only to the extent that notice within the period would have avoided the loss.[20] All three tiers of liability can apply to a series of unauthorized transfers involving a compromised card.

According to the legislative history of the EFT Act, the adoption of a limitation on consumer liability, rather than a fault standard will stimulate institutions to provide a "secure" EFT system.[21] "[T]his is an appropriate assignment of risks since the financial institution has established the EFT system and has the ability to tighten its security characteristics."[22] The PIN was considered a particularly vulnerable security characteristic. The legislative history argues that until more sophisticated authentication methods become feasible, "a liability standard which provides certainty against total loss to the consumer is of crucial importance."[23]

The legislative background also indicates that Congress believed that the potential loss of $50 adequately motivates the consumer "to guard his card and [authentication] code carefully and to report any loss or theft promptly."[24] The $500 potential loss, which was added later, is a backup motivator. The House legislation, which was not enacted, provided a greater incentive by shifting the risk of loss to the consumer if he has written his PIN on his card, *i.e.*, has failed to separate the elements of authentication.[25] This was also the minority position of the Senate committee.[26]

B. Liability Under State Laws[27]

The Michigan and Montana EFT laws are illustrative of other approaches taken to allocating the risk of loss from unauthorized

19. 15 U.S.C. § 1693g(a) (1978).

20. 12 C.F.R. § 205.6(b)(2).

21. S. REP. NO. 915, 95th Cong., 2d Sess. 6 (1978) [hereinafter cited as SENATE REPORT].

22. *Id.*

23. *Id.*

24. *Id.*

25. H.R. 13,007, 95th Cong., 2d Sess. § 909(a).

26. SENATE REPORT, *supra* note 21, at 29.

27. For a comprehensive analysis of state EFT laws, *see* Greguras & Wright, *The Preemption Dilemma Under the New EFT Act*, 12 U.C.C.L.J. 3 (1979).

transactions caused by a breach of an authentication method.[28] The Michigan legislature adopted the NCEFT standard. A financial institution must bear all liability for unauthorized transactions unless it can prove, "without benefit of an inference or presumption," that the customer's negligence substantially contributed to the loss and that the financial institution exercised reasonable care to prevent the loss.[29] Negligence includes writing the PIN on the card or keeping the PIN with the card,[30] *i.e.*, not separating knowledge from possession. The customer is not liable for any losses which occur after notice had been given to the financial institution that the card or PIN has been compromised.[31] This law is more favorable to the consumer than the federal law when a financial institution is unable to prove the consumer's negligence substantially contributed to the loss. On the other hand, the federal law would be more favorable when the consumer breached the greater standard of care, since there is no limitation on liability in that instance under the Michigan law.

Between the customer and his financial institution, the Montana law allocates the liability for unauthorized transfers to the institution, unless the transfer was made by the use of a lost or stolen card, in which case the customer is liable for the less of $50 or the loss incurred before notice.[32] If the unauthorized transfer was made after loss or theft of a card with a PIN attached or "readily available," the account holder is liable for one-half of the losses incurred before notice to the financial institution.[33] Like the potential $500 exposure under the federal law, this should be an adequate incentive to prompt the reporting of compromised cards. This allocation of risk, however, makes it unclear whether federal or state law is most favorable to consumers, a determination which must be made on a case-by-case basis.

II. Liability for Failure to Comply with a Proper Order

There is a risk that an authentication method will wrongfully reject an authorized user. State law does not focus on this risk; thus the federal EFT Act will generally prevail. Under the federal law, a financial institution which fails to make a transfer in the correct

28. *See* Mich. Comp. Laws Ann. § 488.1 *et seq.* (17 Mich. Stat. Ann. §§ 23.1137 (Callaghan 1979)); Mont. Rev. Codes Ann. § 5-1711 *et seq.* (Supp. 1977).

29. Mich. Comp. Laws Ann. § 488.14 (17 Mich. Stat. Ann. §§ 23.1137(14) (Callaghan Supp. 1979)).

30. *Id.*

31. *Id.* § 488.14(c) (17 Mich. Stat. Ann.§ 23.1137(14)(c)).

32. Mont. Rev. Codes Ann. § 5-1713(a) (Supp. 1977).

33. *Id.* § 5-1713(b).

amount, or in a timely manner, when properly instructed to do so, is liable to the consumer for the "proximately caused" damages.[34] This is the same allocation of liability as under the Uniform Commercial Code (U.C.C.) for checks[35] and as recommended by the NCEFT.[36] The rationale for creating a scope of liability in an EFT setting at least equivalent to that under the U.C.C. is persuasive since financial institutions control more of the components of an EFT system than in a checking environment.

A financial institution is excused from liability for such losses only when it can demonstrate, by a preponderance of the evidence, that the event was caused "by an act of God or other circumstances beyond its control" and that it took "reasonable" precautions to prevent the occurrence and otherwise acted diligently under the circumstances.[37] It is unlikely that the unreliability of an authentication method could be a general defense to this liability. The risk of loss from unreliability must be weighed against the cost of adopting alternative methods of authentication.

The EFT Act contains a middle ground for allocating liability, based upon the analogous position of the Uniform Commercial Code.[38] A consumer may recover only "actual," proven damages if the financial institution's failure to perform was unintentional and it acted reasonably to prevent the error.[39] If the institution made a "bona fide" mistake, as opposed to negligence or an intentional act, it is strictly liable, but its liability is limited.[40] Again, it is unlikely that the unreliability of an authentication method could be a defense under this requirement, particularly after initial failures to work properly.

III. System Deployment Requirements

The Bank Protection Act requires national banks to "design" ATM's "so as to be protected against actuation by unauthorized per-

34. 15 U.S.C. § 1693h(a) (1978).

35. U.C.C. § 4-402.

36. NCEFT Report, *supra* note 12, at 65.

37. 15 U.S.C. § 1693h(b) (1978). The Federal Reserve Board has declined to promulgate any regulations under this provision to clarify the standard for liability assessment. The Board suggests that financial institutions can contractually limit their liability for this risk based on § 1693h(a). However, given the consumer protection purpose of the law, it is unclear how much liability can be avoided without negating the overriding purpose of the law.

38. U.C.C. § 4-402.

39. 15 U.S.C. § 1693h(c) (1978).

40. *Id.*

sons."[41] No other authentication-related conditions for deployment are required.

The Federal Home Loan Bank Board regulations require federal savings and loans to demonstrate that security devices and procedures "reasonable in cost" are employed to discourage theft at EFT terminals.[42] Two other specific conditions for EFT terminal deployment are that a PIN must be an element of authentication, and that the method of communicating the PIN must be limited.[43] A PIN may not be disclosed during the authentication process to persons who are not employees of the savings and loan.[44] The operational effect of this requirement is that an input device (PIN pad) separate from the communications terminal on which the account holder himself keys his PIN is used at off-premise locations.

Though the procedures and conditions for deployment of EFT terminals or other EFT systems vary among those states in which some form of EFT is authorized, a general requirement is that reasonable security precautions be taken to protect customers from losses caused by unauthorized transactions. For example, financial institutions deploying terminals under the Minnesota law must "adopt and maintain" safeguards which are consistent with the requirements of the federal Bank Protection Act or alternative precautions which are approved by the regulatory agency.[45] The New Mexico deployment law also adopts the federal standards.[46] Under Wisconsin regulations, a terminal may not be deployed unless precautions "acceptable" to the regulator are provided, in order to prevent unauthorized "access to, or use of, the terminal."[47] The Iowa law, as well as other statutes, indicates that one of its primary purposes is that EFT systems "should not impair the safety and soundness of a person's funds."[48]

In many instances, though a regulator need not approve the authentication method prior to deployment, the method will be reviewed at the same time as the examination of the financial institution itself. When regulators assess the method chosen by a financial institution, the costs and benefits of all alternatives should be evaluated in determining "adequacy" and "reasonableness."

41. 12 C.F.R., pt. 21, app. A, at 434 (1978).
42. *Id.* § 545.4-2.
43. *Id.* § 545.4-2(e).
44. *Id.*
45. MINN. STAT. ANN. § 47.68 (West Supp. 1979).
46. 1977 N.M. LAWS, ch. 359, § 12(a).
47. WIS. AD. CODE, *Banking* § 14.06 (1978).
48. IOWA CODE ANN. § 527.1(2) (West Supp. 1979).

IV. PRACTICAL METHODS OF AUTHENTICATION[49]

The various techniques being studied for identification of an individual based on personal characteristics, *i.e.*, "who a person is," include fingerprints, biometrics, voiceprints and signature analysis. Presently, the only true, positive, personal identification techniques are those requiring supervised tests in controlled surroundings on the actual person. An example is the taking of fingerprints of a criminal suspect by the traditional ink method.

A. Criteria for Selection[50]

Before any authentication method should be seriously considered, the cost must be related to the risk of the event to be prevented. A $50,000 device used to restrict entry to a computer room could not be justified for authentication at an automated teller machine.[51] When evaluating the total cost involved, the expenses of training and downtime must be taken into account. Also, the cost of lost business due to disgruntled customers cannot be ignored.

Once a cost-risk balance has been determined, the next concern is the acceptability of the system by employees and customers. The system should be painless, rapid, and not embarrassing for customers to use. Though some economic incentive for use might counteract possible embarrassment, anxiety and inconvenience, the rates of false rejection and false acceptance should be low—one in one thousand transactions (.001) has been suggested as an upper limit for these occurrences. False rejection rates should be even smaller than false acceptance rates.[52] It may be necessary to repeat the au-

---

49. For a more detailed technical description of the alternatives, *see* Sykes, *Positive Personal Identification*, 24 DATAMATION, Nov. 1, 1978, at 179; WARFEL, I.D. WHERE ARE WE NOW? (1977) (published by I.D. Code Indus.).

50. *See, id.* at 51, for a more detailed analysis of evaluation criteria.

51. For a thorough analysis of contemporary access control systems, including some applications case histories, *see* M. DIMEO, ACCESS CONTROL SYSTEMS (1979) (available from Cardkey Systems, 20339 Nordhoff St., Chatsworth, CA 91311).

52. Mr. Robert H. Courtney of IBM Corporation, a nationally known computer security expert, reviewed an earlier version of this article. On this point he commented:

> What seems almost unknowable are the actual requirements for T1 and T2 errors. I can agree that your 0.001 is desirable but I don't believe that you will ever see it in any low-cost, reasonably fast and socially acceptable technology. I cannot imagine that we need to assure dishonest people that we will detect attempts at dishonesty 999 times out of 1000 tries to discourage such attempts. There are too many procedural steps available to discourage such attempts.

Letter from Robert H. Courtney to Fred M. Greguras, dated Nov. 12, 1979 [hereinafter cited as Courtney Letter].

thentication query if a negative result is obtained the first time.[53] However, no more than five to ten percent of the queries should require a second attempt because of the resulting delay and frustration. Finally, any automatic device should be operationally reliable; it should not require frequent maintenance, adjustment or repair.

B. Fingerprints

Fingerprints have long been accepted as a principal means of uniquely identifying an individual. In a high volume setting such as EFT, however, it is not possible to compare all of the details of a print with a reference print, as is done in the controlled setting and with the expensive equipment used by the police. Instead, when a speedy determination is required, the identification process is based upon the relative positions of ridge endings and joins called "minutae." Figure 1 shows a fingerprint with some of the minutae circled.

A practical, automated fingerprint system is based on testing whether the minutae of the person being identified exist at the same places that the reference data indicates for that person. To read the fingerprint of the person in question, an inkless process has been developed, based upon the large change in reflectivity of a thermochromic material with a small temperature change. The finger is placed on a surface where the reflectivity is different when the ridges are in contact. Optical scanning is used to locate the minutae, based on the differences in reflectivity. The comparison process, however, is very elaborate due to inaccuracies in the positioning of the finger, and the products which employ this technique are very expensive. Equipment is currently available at a price of $50,000 for the central controller station plus $4,000 for each terminal at which authentication can occur. A system with ten terminals would thus cost approximately $9,000 per terminal. This expense can only be justified for protecting bank vaults, important military

53. For example, hand geometry and fingerprints are relatively insensitive to the effects of alcohol and drugs, while voice, signature and PIN are sensitive to them. On the other hand, fingerprint, PIN and hand geometry are relatively static measurements so that T1 error is unlikely of rectification by a simple retry. Voice and signature, particularly signature, offer the possibility of greatly improving T1 without necessarily heavy attendent jeopardy to T2 by a second and even third try. For example, if correlation is good, but not good enough, try again. If it is terrible, reject and deny a second try. If it improves the second time, and is not much worse, try a third. If it is much worse the second time, end there.

Id.

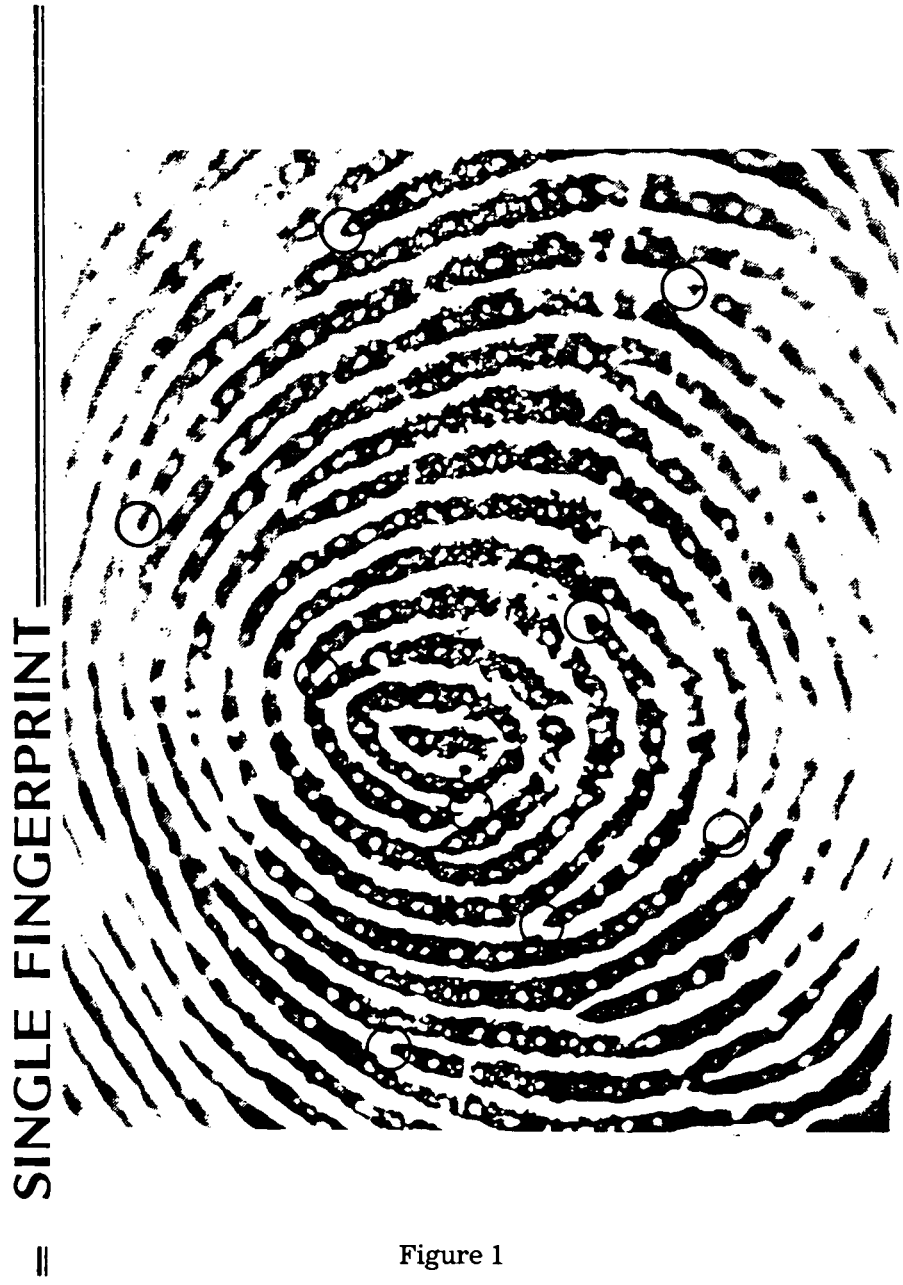

Figure 1

computing systems, or other highly valued assets,[54] and is simply not cost justified in an EFT setting.

C. Biometrics

A Stanford Research Institute study showed that the combination of individual finger lengths vary from one person to another.[55] This variation in hand geometry, known as biometrics, is used in a personal identification product illustrated in Figure 2. The hand is accurately positioned by guides and a high intensity light shines down onto the hand. Photoelectric devices are used to detect the lengths of the fingers and also their translucency. The unit is designed to disregard the length of fingernails and can detect an artificial plaster "hand" made to the same dimensions as the hand of the authorized person.

These devices cost approximately $3,000 each and do not require a central controller station. They are used primarily for controlling access to secure areas. The reliability of these units in use has proved to be quite good.

D. Voiceprints

In everyday life it is possible to recognize people by their voices. This attribute is a natural candidate for an authentication method. One person's voice is different from another's, because of the variance in relative amplitudes of the different frequency components of the speech. A method of authentication using voiceprints involves the quantification of the sounds of a particular person when speaking certain words, and the comparison of the observed voiceprint with the reference data for that person. Figure 3 illustrates a method of performing this quantification. The person reads a sequence of words from a display into a microphone. To prevent an imposter from using a recording of the real person, the words to be spoken are displayed one at a time in a random sequence. The voiceprint equipment is resistant to impersonation by other human beings because it is much more sensitive to amplitude/frequency variations than the human ear. There are problems, however, with rejection of authorized users due to voice variations resulting from

54. *See* COMPUTER DECISIONS, Apr. 1979, at 4, for a brief description of an operational system.

55. D. Cone, Personnel Identification by Hand Geometry Parameters (Stanford Research Inst. 1969).

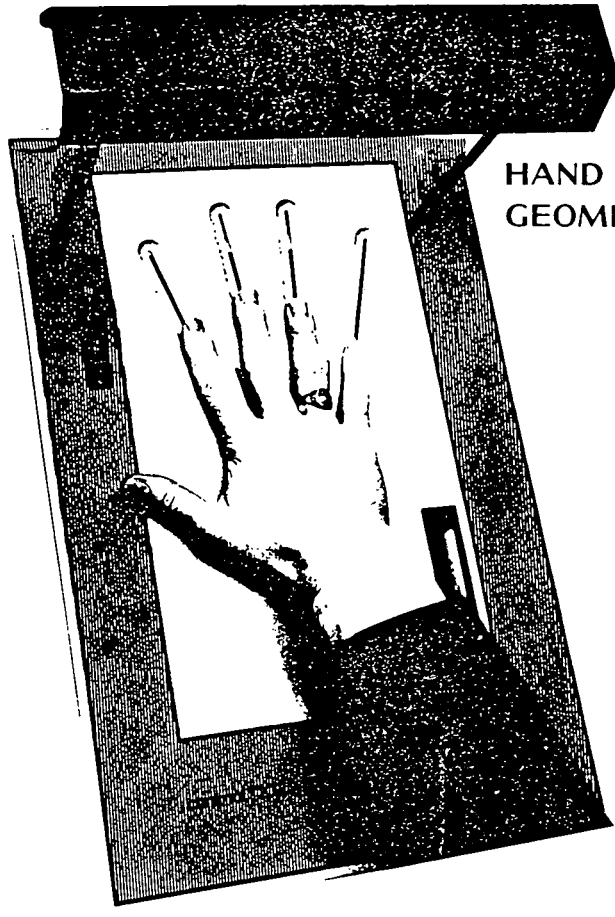

Figure 2

RECOGNITION BY
VOICE ANALYSIS

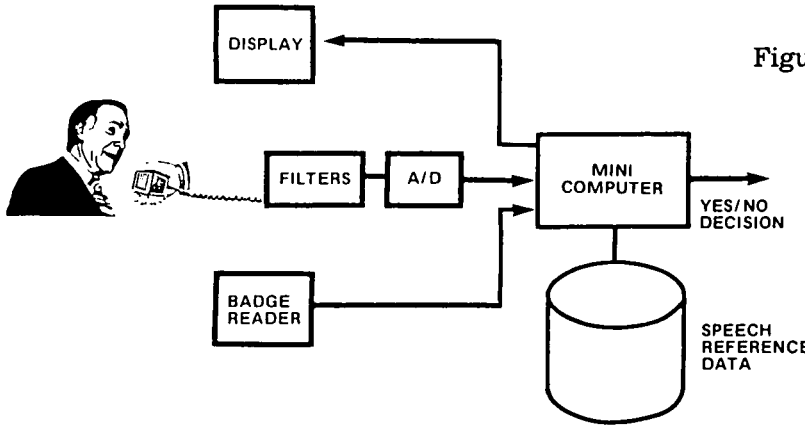

Figure 3

emotional stress, laryngitis, colds and other illnesses.[56]

Voiceprints have been used to control access to secured areas where the number of persons involved is relatively small, unlike an EFT setting.[57] This method can be used in data entry applications where the set of words is repeated by a defined group of operators, and where a person would normally have to interrupt a task to enter data into a computer.[58] The cost of these systems is high, about $40,000, but the economies of scale reached by increased volumes of use could reduce this price substantially.

E. Signature Analysis

Of all the techniques of personal identification, automatic signature analysis has probably been given the most attention during the last few years. Signature verification is the most acceptable method to the general public, since it is the least change from the identification method used in the traditional checking system. The general acceptance of this technique accounts for the many research projects in this area.[59] There is a great deal of consistency in the way that individuals sign their names. This is the basic principle involved in signature analysis. However, no two genuine signatures are precisely the same, as Figure 4 illustrates. The problem is to discriminate between normal variations in a real signature and between a real signature and a forgery.[60]

Two approaches to signature verification are being studied. One approach is based on measurement of the dynamics of the pen during the actual signature process. The other involves an analysis by

---

56. The problem with voice is the telephone network. No one to our knowledge has made it work well on the conventional voice-grade lines available from the common carriers. Incidentally, we did not find colds, hay fever, and such things so large a problem as were the distortions and noise contributed by the telephone networks. We know of no voice systems working into the public networks and beyond the confines of a single facility.

Courtney Letter, *supra* note 52.

57. *See generally,*, G. DODDINGTON, PERSONAL IDENTITY VERIFICATION USING VOICE (published by Texas Instruments, Dallas, Texas); *Voice Inputs: Where It Stands*, DATAMATION, May 1978, at 274.

58. *See, e.g., Voice Data Entry Unit Speeds Can Inspection*, Computerworld, July 10, 1978, at 45, col. 3; *Voice Recognition System Upgraded*, Computerworld, July 30, 1979, at 50, col. 1; *Voice Response Unit Unwrapped by Votrax*, Computerworld, Aug. 20, 1979, at 29, col. 1.

59. *See, e.g.*, Herbst & Liu, *Automatic Signature Verification Based on Accelerometry*, IBM J. RESEARCH & DEV. 245 (1977).

60. This assumes, of course, that the reference signature being used for comparison is that of the account holder.

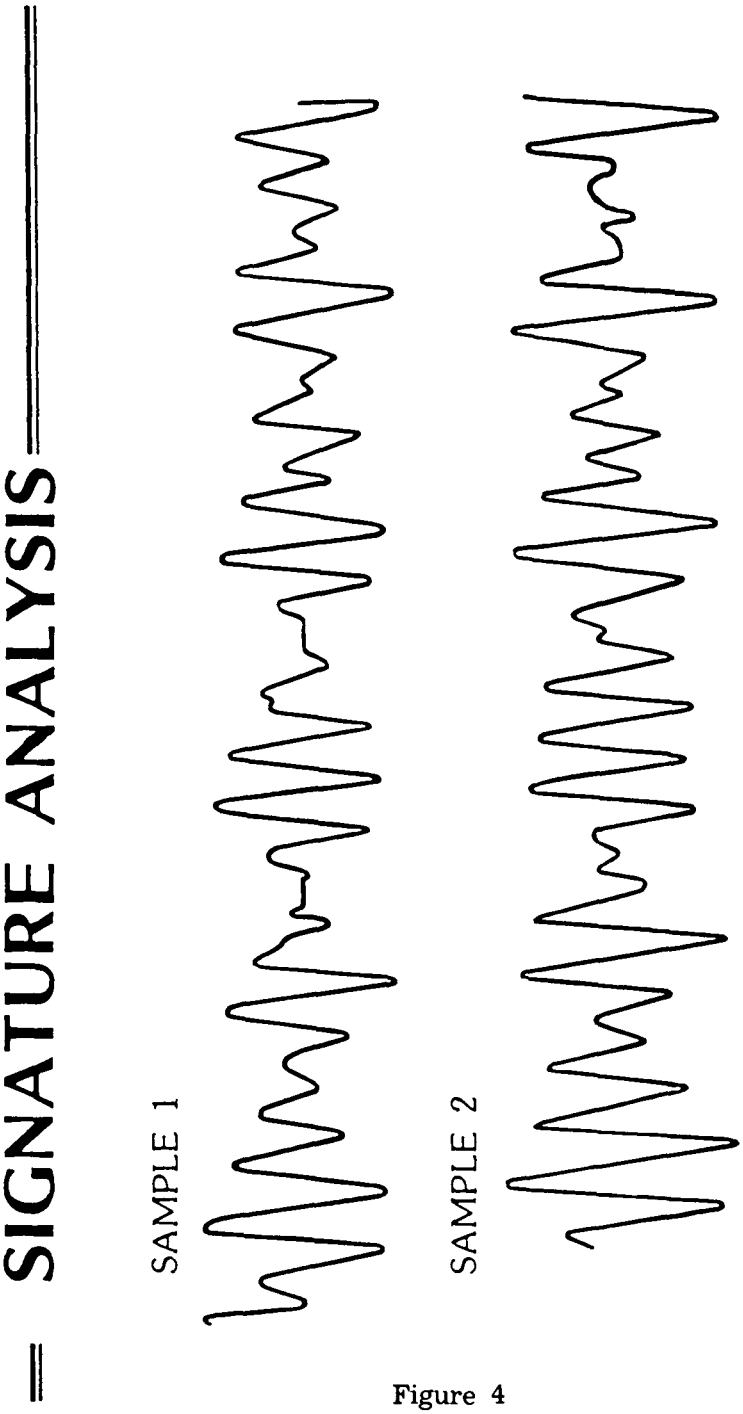

Figure 4

optical means of the signature after it has been written. Currently, there are no products available based on either method that will provide the instant verification required in an EFT setting.

The optical method of signature verification is initially being used in teller transactions or after checks have been deposited.[61] This gives the bank an opportunity to reject bad checks before it "owns" them.[62] Presently, because visual inspection is time-consuming, it is impossible to verify all checks; thus, except in teller situations, only the higher valued ones are scrutinized. Since the average forged check is written for $35.00, most are not discovered until it is too late to return them.

As a logical extension of off-line check processing, the signature analysis method can be utilized for point-of-sale (POS) authentication. The characteristics of the signature, such as the size of the letters and angle of slant, are encoded into a pattern of dots called a mosaic. The mosaic can be printed on the account card to avoid the need of communicating with a central data base for signature information. A microprocessor in the POS terminal can perform all of the necessary computations. This approach has considerable potential if the cost of the opto-electronics can be reduced to a satisfactory level of about $1,000. The operational value of this technique, however, depends on the procedure for creating the reference signature. It will not reject an imposter who has breached the card issuance and reference signature creation procedures. In such a situation, a card would be issued with the imposter's reference signature on it.

V. CONCLUSION

It is clear that a cost effective EFT system must be based on a sound authentication method. The requirements for an ideal method can be summarized as follows:

1. It must be acceptable to the general public. Its use should not result in any embarrassment, anxiety or inconvenience to the consumer. Repeated attempts should only be necessary in not more than five percent of the transactions.

2. It must provide for a low probability that a legitimate customer will be rejected (less than .001).[63]

---

61. *See, e.g., F & M Installs Signature System*, Am. Banker, Aug. 29, 1979, at 6, col. 3.

62. *See* U.C.C. §§ 4-212, 4-213.

63. *But see* notes 52 & 53 *supra*.

3. It must provide for a low probability that an unauthorized person will be accepted (less than .001).

4. The cost of the system must be sufficiently low to justify its use; that is, the cost must be related to the risk.

5. The time to perform a transaction must not be noticeably longer than in today's payment systems environment.

6. The equipment should be highly reliable and should not require constant adjustment.

7. It should be extremely difficult to bypass the authentication process by simulating, from an external source, the signals normally transmitted into the EFT system by the authentication devices.

To satisfy the seventh requirement, it is necessary to build, install and operate the equipment in a secure manner. Encryption can be used to guard PINs against wiretapping and injection of false information from an external source. Satisfying this requirement involves equipment and system design, together with administrative procedures, rather than solely the features of the authentication method.

TABLE 1

Comparison of Authentication Methods

	PIN	Finger	Hand	Voice	Signature
Acceptability by public	Good	Poor	Poor	Fair	Good
Rejection of imposter[64]	Poor	Fair	Good	Good	Fair
Acceptance of authorized person	Good	Poor	Fair	Fair	Fair
Cost (dollars/terminal)[65]	100	9,000[66]	3,000	5,000[66]	1,000
Time to verify (processing time in seconds)	5	10	5	20	5
Operational Reliability	Good	Poor	Fair	Good	Good

64. It is very difficult to rank Type 1 (T1) errors (rejection of friends) and Type 2 (T2) errors (acceptance of enemies) in tabular form without misleading the reader almost as much as you inform them. Most systems which examine some personal parameter, such as fingerprints, lend themselves to the adjustability of T1/T2 relationships. It is fairly apparent that the acceptance of friends will improve if we loosen the restriction or rejection of enemies. This is only to say the lowering the numerically stated correlation criterion will permit more T2 but will help T1. Conversely, raising the required correlation will improve T2 at the expense of T1.
Courtney Letter, *supra* note 52.

65. These figures are based on ten terminals located at transaction points which share one control station.

66. The $9K for a fingerprinting station is far lower than is currently anticipated by anyone I know who has been working closely with the technology. This price closely approximated the cost of hand geometry devices the last time I looked at them.

In Table 1, the four techniques along with the plastic card and PIN method are evaluated against the criteria for an ideal authentication method. The table indicates that the only viable alternatives are the card/PIN combination and signature analysis. This situation does not appear likely to improve in the near future. The other techniques will continue, however, to find use in non-EFT applications, such as the control of physical access to secure areas where the number of people involved is small and the risk per event is high.

Signature analysis, though promising, has a long way to go before it becomes a reality in everyday life.[67] IBM's director of research recently predicted that this technique is "some" years away.[68] Several products have been announced, but there is no accumulation of experience in the field.[69] Some products have been withdrawn from the marketplace because of technical difficulties. The fundamental problem is the difference between signatures of the same person. Though a small group of persons can be "trained" to be consistent in the way they sign their names, it is unrealistic to expect the general populace to be so trained. There is a huge market waiting for a signature verification system that has acceptable performance and low price—$1,000 each in large quantities.

In the meantime, EFT systems will rely almost entirely on the possession and knowledge approach for authentication. According to the Technical Issues and Standards Committee of the EFT Association, this technique will be utilized for the next five to ten years.[70]

Proper PIN management, however, can reduce the risk of loss in several ways. First, allowing a consumer to select his own alphabetical, numerical or alphanumerical code will reduce the chance that the consumer will write it on his account card or keep it with his card. Consumers will more likely remember codes that they select themselves. By allowing the PIN to be a variable length greater

---

> I know of no reason why voice should require so high a price per station. The cost per station should be very low—in fact, far lower than any of the others except PIN, which it should approximate.

Id.

67. Crane, The SRI Pen System for Automatic Signature Verification (paper presented at the IEEE Symp. on Computer Security, May 1977).

68. *IBM Views Advanced Signature Verification as Some Years Off*, Am. Banker, Apr. 11, 1979, at 6, col. 3; *see also Experimental System Picks Out Forgeries*, Computerworld, Oct. 16, 1978, at 6, col. 3.

69. *See, e.g., Opticode Proposes "Cryptocheck,"* Am. Banker, Aug. 2, 1978, at 6, col. 3.

70. Electronic Funds Transfer Ass'n memorandum (no date) (concerning the decisions made at the Technical Issues & Standards Comm. meeting, Feb. 12, 1979).

than four characters, the chance is also reduced that the consumer will select an easily guessed four letter word or number.

Though the PIN method is still vulnerable to observation or being overheard when it is provided orally, a consumer-selected code, rather than one generated by an algorithm from an account number, minimizes the chance that every accountholder's PIN is exposed if a single PIN is compromised. At least one vendor's product, the ID Code system, seeks to minimize the observation risk by allowing selection of an easily remembered password, which is converted to a different, but easily determined, number for each transaction.[71] Unfortunately, this conversion equipment adds a great deal of expense to each transaction point.

The vulnerability of PINs to insiders, such as computer center and other EFT system employees, can also be minimized. Using another vendor's product, Atalla Technovation's Identikey, the PIN need never be disclosed to any individual and is not kept in any written records or stored in computer data files.[72] The PIN, in conjunction with the consumer's account number, is used to produce a third number which is stored. Since the third number, called a PIN offset, is a function of two variables, the generation algorithm (or key) is also more difficult to break. The Identikey method addresses all of the major vulnerabilities of the PIN, except observation, and provides a reasonable remedy to match the present risk.

The X9.A3 Committee of the American National Standards Institute is preparing a standard to cover the management and security of the PIN. This standard will cover all aspects of the PIN during its life cycle, including generation, issuance, storage, entry, transmission and destruction.[73]

The federal EFT Act does not promote the objective of minimizing total losses. To encourage EFT development, system providers must be able to manage the risk of loss. The consumer has shared the responsibility and liability in the check payments system, a mechanism which was created and operated by financial institutions. Given the probable useful life of the PIN in EFT, the cardholder must also be responsible to some extent for its security, in order to minimize total system losses. From a design vantage, the best solution for a secure authentication method is a combination of

71. For more information, contact I.D. Code Systems, 4116 Matthen Drive, Palm Springs, CA 92262.

72. For more information, contact Atalla Technovations, 505 W. Olive Avenue, Sunnyvale, CA 94086. PINPACK, the product of Interbank Card Ass'n, 888 Seventh Avenue, New York, NY 10019, should also be considered for use.

73. *See* AMERICAN BANKERS' ASS'N, PERSONAL IDENTIFICATION NUMBERS: THEIR MANAGEMENT AND USE (1979).

technical safeguards and required human behavior.[74] To the clamor for individual rights must be added an equally loud cry for fundamental, individual responsibility.

74. This combination of approaches is one of the basic guidelines for designing a computer security program in general. *See* COMPUTER SECURITY INST., GUIDELINES FOR ESTABLISHING A COMPUTER SECURITY PROGRAM § III.B (1979).