United States General Accounting Office

GAO

Report to the Honorable Kenneth E. Bentsen, Jr., House of Representatives

September 1995

ELECTRONIC BENEFITS TRANSFER

Use of Biometrics to Deter Fraud in the Nationwide EBT Program

GAO/OSI-95-20

GAO

United States
General Accounting Office
Washington, D.C. 20548

Office of Special Investigations

B-261923

September 29, 1995

The Honorable Kenneth E. Bentsen, Jr.
House of Representatives

Dear Mr. Bentsen:

In 1993, the National Performance Review recommended that the federal government consider the potential for providing all payments to individuals by using electronic, rather than paper, payments.[1] In 1994, the Federal Electronic Benefits Transfer Task Force—consisting of officials from the Office of Management and Budget, the Department of Health and Human Services, the U.S. Department of Agriculture (USDA), and the U.S. Department of the Treasury—reported that each year federal and state programs deliver almost $500 billion in cash benefits and food assistance and that at least 12 federal and state benefit programs could use electronic benefits transfer (EBT) to replace the current paper benefit delivery methods.[2] The task force estimated that over $110 billion in annual cash benefits and food assistance could be delivered with EBT, including such benefits as food stamps, social security, and federal pensions.

The task force determined that an electronic system would reduce the cost of benefit delivery, strengthen the management of program funds, and reduce fraud. Under such a system, federal, state, or local government agencies would issue access cards (similar to credit cards) and personal identification numbers (PIN) to recipients who could obtain benefits through automated teller machines (ATM) and point-of-sale terminals.[3] EBT is already assisting USDA by providing data that can be analyzed by computer programs to target stores trafficking food stamp benefits and identify individuals who frequent stores suspected of trafficking.

Because of the significant federal funding involved in government programs providing benefits, we examined various options for providing additional security to deter the potential for fraud in an EBT environment. We focused on the use of biometrics—automated methods to measure a physical characteristic or personal trait—to verify a recipient's identity and reduce the potential for fraud. Because of that potential for fraud, on

[1]From Red Tape to Results, National Performance Review (Washington, D.C.: Sept. 1993).

[2]Creating a Benefit Delivery System That Works Better & Costs Less, Federal EBT Task Force (Washington, D.C.: May 1994).

[3]A point-of-sale terminal is a device placed in a merchant location and connected to a bank's system by telephone lines. It is designed to authorize, record, and forward electronically the payment for each sale as it occurs.

August 11, 1995, you requested that we report to you on our work. Appendix I provides an overview of the biometric technologies we reviewed—fingerprints, hand geometry, retina scan, voice verification, and signature verification.

Results in Brief

Some states and municipalities have used biometrics to deter fraud in their social welfare benefit programs. They have realized substantial cost savings by requiring program applicants to submit to electronic fingerprinting as part of the enrollment process. Using this method, they have denied benefits to individuals who attempted to receive duplicate benefits. For example, the Los Angeles County Department of Public Social Services reported savings of $14 million solely attributable to such a system from June 1991 through July 1994. The U.S. Secret Service supports the use of fingerprint identification in the benefit enrollment process and commented favorably on the success of the Los Angeles County project.

Electronic fingerprint identification offers a promising solution for deterring fraud in both the enrollment and disbursement phases of the government's proposed EBT program. Of the biometric identification systems that we reviewed, we selected fingerprinting as the one most viable for verifying a recipient's identity in an EBT environment. We selected it because of (1) its universal acceptance as a positive means for identity verification and (2) its extensive history of reliability in the law enforcement arena. Fingerprinting benefit applicants during the enrollment phase would eliminate losses related to applicants' applying for duplicate benefit payments under different names and deter others so inclined. Such verification in the disbursement phase would directly link withdrawals to the recipients and effectively resolve the issue of potential losses and increased costs. Federal regulations would limit consumer liability when lost or stolen EBT cards are misused. However, the issue concerning who will be liable for losses over the consumer limit, which could be extensive, is still unresolved.

The effectiveness of an EBT program secured by biometric identification to deter fraud should be tested in an EBT environment before the program is expanded nationwide. The development and testing of a biometric system may delay the task force's proposed 1999 implementation date for the EBT program and would increase the program's initial cost. However, the long-term benefits of a biometric system would contribute to a more fiscally sound and secure EBT program.

This report contains a recommendation aimed at reducing potential fraud and abuse in the nationwide EBT program.

Background

The Federal Electronic Benefits Transfer Task Force has proposed that the federal government use EBT to disburse such benefits as social security; railroad retirement; federal civilian retirement; military pensions; food stamps; Aid to Families With Dependent Children (AFDC); and Women, Infants and Children (WIC) in all states by 1999. In fiscal year 1994, these programs disbursed about $433 billion in federal benefits through such delivery methods as electronic funds transfer (direct deposit) and Treasury checks. For example, in fiscal year 1994, the federal share of the food stamp program was about $24 billion, disbursed to over 27 million recipients in mainly food stamp coupons. Various law enforcement officials estimate the losses from fraud in existing programs, such as food stamps, to be up to 10 percent annually. We have not verified these loss estimates.

Because of the multiplicity of government agencies that could participate in the EBT program, the task force will develop and oversee the national EBT policy, manage EBT prototype projects, and coordinate budget requests related to implementation and operation of a nationwide EBT program. The U.S. Department of the Treasury will manage the federal government's financial operations associated with EBT. In March 1995, Treasury issued an Invitation for Expressions of Interest (IEI) to acquire EBT services for the Southern Alliance of States[4] as a prototype. Treasury expects to award a contract in October 1995. According to a member of the Federal EBT Task Force, the Treasury IEI strongly encourages financial institutions to recommend the use of innovative technologies, such as biometrics, when formulating a response to the IEI. In addition, he told us that the task force supports the most secure and cost-effective measures or technologies to safeguard EBT systems and is looking to the banking industry or existing commercial banking infrastructure to take the lead with innovative technologies.

Numerous methods exist to afford different levels of security to safeguard an EBT system. The methods range from magnetic stripes encoded with various information to such sophisticated biometric techniques as fingerprints, hand geometry, retina scan, voice verification, and signature verification. However, Secret Service investigations have shown that the

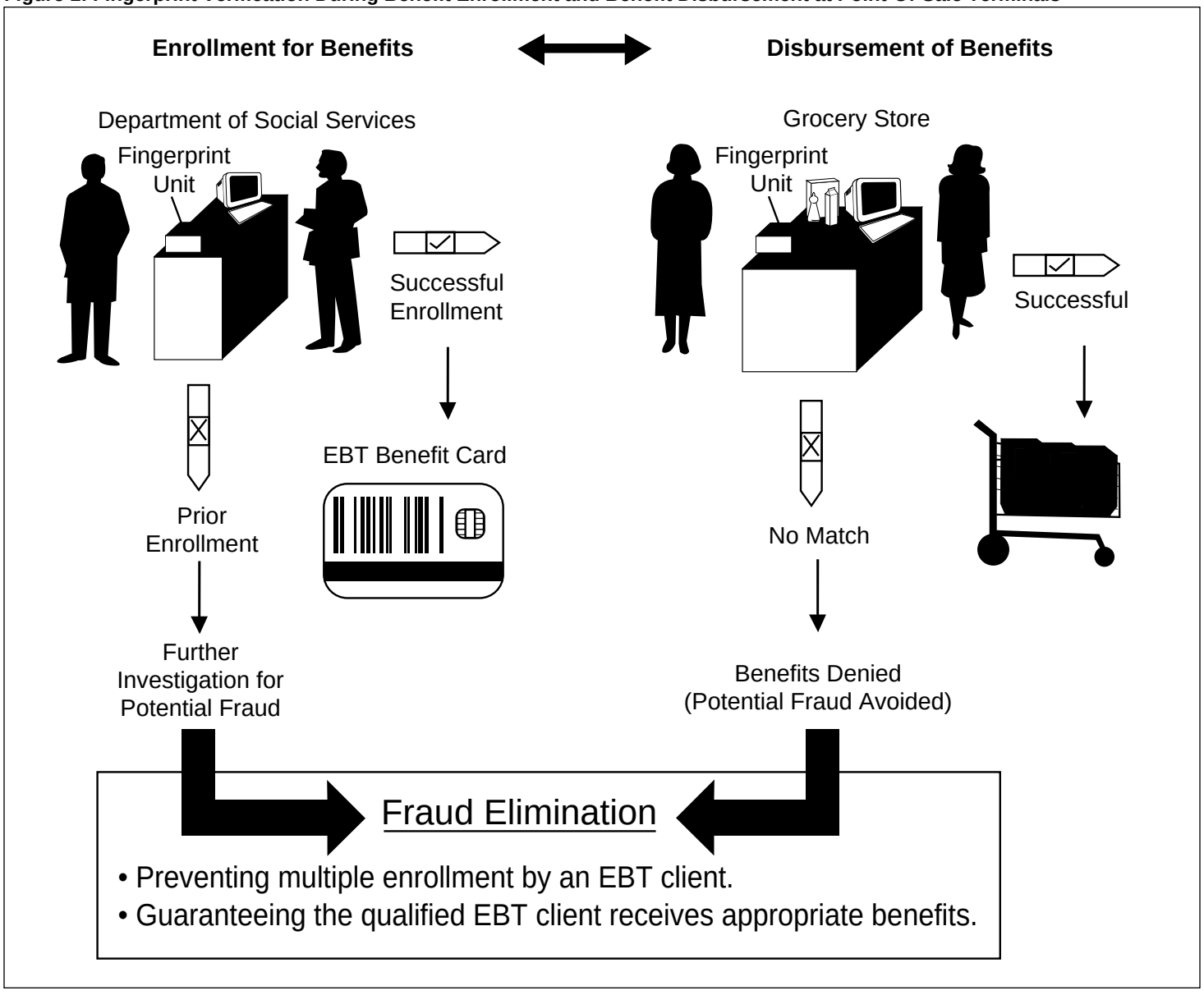
[4]The alliance is currently a coalition of nine southern states—Alabama, Arkansas, Florida, Georgia, Kentucky, Mississippi, Missouri, North Carolina, and Tennessee—that joined with the task force to develop the specifications for a prototype national EBT system.

less sophisticated levels of card security—such as those cited in Treasury's IEI, including magnetic stripes and holograms—have been counterfeited. Individuals have counterfeited credit/debit cards themselves and easily transferred the information encoded on magnetic stripes from one card to another. Of the physical characteristics and personal traits that are used for biometric verification, law enforcement agencies have used fingerprints most extensively. For almost 100 years, law enforcement has used fingerprints to identify criminals both upon arrest and after comparing crime scene fingerprints with already established criminal fingerprint files. Advances in electronic fingerprint identification have resulted in positive identifications in criminal cases once left unsolved after using manual fingerprint search methods. Some police jurisdictions are now using live scan fingerprint capture[5] to fingerprint individuals they arrest.

During benefit enrollment, live scan fingerprint capture allows for identity verification through database search. During disbursement at ATM or point-of-sale terminals, this technology allows for self-verification by using a fingerprint reader to compare a live scanned fingerprint with the same print encoded on an EBT card. Figure 1 depicts the use of electronic fingerprint verification during benefit enrollment (database search) and benefit disbursement at point-of-sale terminals (self-verification).

[5]This technology involves using equipment to directly scan a finger and store or transmit the data electronically.

Figure 1: Fingerprint Verification During Benefit Enrollment and Benefit Disbursement at Point-Of-Sale Terminals



With a fingerprint-secured EBT card, a program administrator could link the responsibility for use of the card to the recipient and, if fraud was alleged, have the information needed to determine a future course of action. A fingerprint-secured card could not be used by anyone other than the authorized recipient of the entitled benefits.

Available Technology Offers Potential to Reduce Fraud

In December 1994, we reported that the state EBT systems and pilot projects we reviewed, including those used to distribute food stamps, have not eliminated fraud.[6] For example, the first major fraud investigation by USDA's Office of Inspector General (OIG) involving EBT in Pennsylvania found that a small sandwich shop had conducted over $151,000 in fraudulent EBT transactions over a 2-year period. These transactions accounted for 76 percent of the shop's total EBT dollar volume, and 173 food stamp recipients were convicted for selling their EBT benefits. During another investigation in Pennsylvania, OIG agents found that a retail establishment had illegally obtained 79 EBT cards along with the recipients' PINs. In addition, in February 1995, the USDA Inspector General testified that his office, through analysis of EBT data, had identified about 7,500 food stamp recipients who appear to have sold almost $2 million of their benefits in Baltimore, Maryland, between August 1992 and February 1994.[7]

Available technology, including biometrics, exists to help reduce the potential for fraud in EBT programs. For example, some state and local governments have started to use the Automated Fingerprint Identification System (AFIS) to deter fraud in social service programs during the enrollment stage by identifying subsequent requests for duplicate benefits by an individual. The most widely publicized effort—the Los Angeles County Department of Public Social Services—began using live scan capture of index fingerprints to enroll applicants for participation in one of its social welfare programs in 1991.

Los Angeles County has the second largest county-operated welfare department in the United States, with a $3-billion budget. The county, using AFIS technology, piloted a fingerprint project—Automated Fingerprint Image Reporting and Match—with its General Relief program, which provides financial assistance to indigent persons and emergency assistance to individuals and families in temporary need. The county spent

[6]Food Assistance: Potential Impacts of Alternative Systems for Delivering Food Stamp Program Benefits (GAO/RCED-95-13, Dec. 16, 1994).

[7]Testimony by the Inspector General, USDA, before the House of Representatives, Committee on Agriculture (Feb. 1, 1995).

$9.6 million to purchase the hardware and software for the system and reported $14 million in savings solely attributable to the project from June 1991 through July 1994.

Of this amount, according to the county, it realized $5.4 million in savings during the first 6 months the project was used as a result of terminating over 3,000 approved cases and denying over 240 cases for failure to comply with its fingerprinting requirements. In an October 1994 preliminary evaluation of the project, the audit firm of Ernst & Young reported that (1) only 3 percent of the client population experienced negative feelings about being fingerprinted, (2) the system had not increased the amount of time clients wait in line to apply for benefits, and (3) the system can be replicated effectively and extended to other programs and locales. In addition, the California counties of Alameda and Contra Costa and the city of San Francisco have implemented fingerprint verification for use in some of their social benefit programs. These jurisdictions share data, and officials believe that the system has discouraged applicants from applying for duplicate benefits in more than one county.

The U.S. Secret Service has commented favorably on Los Angeles County's efforts because of the benefits that a fingerprint enrollment verification system offers. These same officials maintain that failure to use the available fingerprinting technology to deter fraud in the initial enrollment phase of the program may open the entire system to fraud and abuse.

Unresolved Issues Relating to Implementing a Fiscally Sound Nationwide EBT System With Enhanced Security

Action is necessary to help ensure the fiscal stability of a nationwide EBT system and enhance its security. Such action includes (1) resolving the issue of potential losses and increased costs related to consumer liability protection in the event of the misuse of lost or stolen EBT benefit cards and (2) pilot testing an EBT system secured by biometric identification before expanding the program nationwide.

Additional Costs Could Be Associated With Consumer Liability Protection Due to Fraud

Regulation E, under 12 C.F.R. part 205, implements the Electronic Fund Transfer Act, 15 U.S.C. sections 1693-1693r (1994). The act and regulation (1) cover any electronic fund transfer initiated through an ATM and point-of-sale terminal, automated clearinghouse, telephone bill-payment

system, or home banking program and (2) provide rules that govern these and other electronic transfers.

The act limits a consumer's liability for unauthorized use of credit and ATM cards, telephone bill-payment systems, or home banking programs. A consumer's liability is limited to $50 if the consumer notifies the account-holding institution within 2 days after learning of a loss, theft, or unauthorized use. The card issuer may then assume the losses in excess of $50. Effective February 28, 1994, the Federal Reserve Board amended Regulation E to apply the same consumer liability to EBT programs established by federal, state, or local government agencies. These entities must comply with the regulations by March 1, 1997.[8]

Some of those who commented on the proposed amendment to Regulation E noted that the liability protection may result in additional costs in an EBT program. These individuals pointed out that, presently, financial institutions can control their costs from misused EBT services by selecting the customers to whom they offer the services. However, government agencies must accept all who qualify for the benefit program. In addition, if a customer of a financial institution is suspected of engaging in fraud, the institution can terminate the account relationship. With the consumer liability protection of Regulation E, EBT recipients engaged in fraud could sell their cards and PINs, report the card and PIN as lost or stolen, obtain a new EBT card and replacement benefits, and be liable for only $50 in lost benefits. Many times that amount could be obtained fraudulently before the card was canceled. Such schemes would be difficult to police without evidence of intentional fraud on the part of the recipients. Directly linking the responsibility for withdrawals to individual recipients by using fingerprint verification could effectively eliminate this type of fraud.

The possibility of substantial fraud losses related to Regulation E implementation has been estimated by some of those responding to the proposed amendment to be between $164 million and $986 million annually. A few of the estimates were based on agency experience with the replacement of lost or stolen cards in EBT programs, but most of the cost estimates were based on loss and fraud experience under such existing paper-based benefit programs as food stamps. Some of those commenting on Regulation E also noted that private sector institutions handle losses related to the Regulation E customer liability limitations by spreading the losses over their entire customer base in the form of

[8]Pending legislation would exempt state or local government programs from Regulation E. See H.R. 4, 104th Cong., 1st Sess. § 802 (1995) and S. 131, 104th Cong. 1st Sess., § 1 (1995).

increased fees or reduced interest paid. Some explained that government agencies cannot do the same; therefore, losses would have to be paid out of tax revenues or by reducing benefits.

However, neither the Federal EBT Task Force nor the Treasury has resolved who or what entity would be responsible for absorbing the costs above the $50 consumer liability limit that could result from the misuse of lost or stolen cards. According to the Federal EBT Task Force report, "[A]ll agencies are concerned about assuming liabilities of undetermined value."

Pilot Testing Needed to Assess Benefit of Biometrics in EBT Environment

Pilot testing of biometrics in an EBT environment before the EBT program is expanded nationwide would allow for an assessment of its practicality and effectiveness in combatting fraud in new EBT systems. For example, pilot testing of self-verifying live scan fingerprint readers in conjunction with stand-alone processing capabilities at ATMs and point-of-sale terminals would also help evaluate fraud deterrence at the disbursement level. Pilot testing would provide a means for determining the reliability and accuracy of the equipment in an actual ATM/point-of sale environment and serve to identify other possible problems.

User-friendliness and customer satisfaction could also be assessed during pilot testing of a fingerprint verification system. Such testing could also assist in determining the best placement of the equipment to make it easily accessible for participants.

Conclusions

EBT alone does not effectively deter fraud in the delivery of food stamp benefits. Thus, an EBT program without the enhanced security of biometric verification raises a genuine concern about the potential for increased program costs and losses. The concern increases with the proposal to expand EBT into other federal, state, or local government programs involving billions of dollars—such as AFDC, WIC, social security, and federal retirement benefits—and with full implementation of Regulation E.

Due to the universal acceptance of fingerprints as a means for verifying identities, its extensive history of reliability in the law enforcement arena, and successes with AFIS technology, we believe fingerprint verification is the biometric form that offers the greatest potential for success and acceptance in securing EBT systems from fraud. Further, an EBT system with fingerprint verification would effectively negate the cost/loss concerns raised by Regulation E implementation.

Development and testing of an EBT system with biometric safeguards would increase the cost, largely from purchasing hardware and software, and time to implement the nationwide system. Yet the development and testing are necessary to ensure that the future system is practical and not beset with the problems of fraudulent usage. Further, such development, testing, and ultimate use would reduce losses to the EBT program from fraud and abuse.

Recommendation

We recommend that the Secretary of the Treasury develop, if feasible, a biometric verification system, such as electronic fingerprinting, for use in an EBT environment. The use of biometrics could be assessed in a limited area, such as the Southern Alliance of States, and prior to expansion of the EBT program nationwide.

Agency Comments

The Department of the Treasury, in commenting on a draft of this report, agreed that biometrics may provide a cost/benefit advantage in the eligibility phase of the EBT program. Although Treasury did not dismiss the use of biometrics in the delivery of EBT benefits, it expressed reservations about the immediate use of biometrics in delivery, noting that such use would require considerable testing and study. Treasury also cited the existence of limited data concerning both the use of biometrics and the possible impact of Regulation E, the EBT program's need to be accessible and cost effective, and a concern to preserve the dignity of recipients. Treasury further stated that to enhance card security, it is requiring that EBT cards include countermeasures against counterfeiting. (See app. II.)

We agree that testing and study are needed to resolve technological and policy issues. However, because fraud other than counterfeiting persists in EBT pilots around the country, we believe that, if feasible, the evaluation should be completed before full implementation of the nationwide EBT program as envisioned by the Federal EBT Task Force in 1999. Further, we are optimistic that commercial and banking entities that use debit and credit cards will implement biometric safeguards, such as fingerprinting, to protect their customers and themselves. This will help create a convenient, cost-effective EBT environment in which most recipients should not feel singled out.

Methodology

To obtain the information in this report, we examined various biometric systems available for identification verification—fingerprints, hand

geometry, retina scan, voice verification, and signature verification. We interviewed officials of federal agencies that use such technologies, including the Federal Bureau of Investigation (FBI), the U.S. Secret Service, the U.S. Immigration and Naturalization Service, and the Federal Bureau of Prisons. We also interviewed state and law enforcement officials in California and various biometrics vendors. We visited sites where federal, state, and local governments and private entities operated various types of biometric identification programs. We attended conferences on biometrics at the FBI, Quantico, Virginia, and in Washington, D.C.

In addition, we reviewed numerous documents including the Federal Reserve Systems' final rule on Regulation E, the Federal Electronic Benefits Transfer Task Force's May 1994 report, a March 1994 U.S. Department of the Treasury IEI for EBT services, and an October 1994 preliminary evaluation by Ernst & Young of the Automated Fingerprint Image Reporting and Match system being used by the Los Angeles County Department of Public Social Services. We also reviewed various reports issued by the Department of Justice's Bureau of Justice Statistics, the FBI, the National Security Agency, and Sandia National Laboratories, as well as materials provided by biometrics industry vendors. We conducted our review from November 1994 through June 1995.

We will send copies of this report to appropriate congressional committees, the Secretaries of Agriculture and Treasury, and the Director of the Office of Management and Budget. If you have questions concerning these issues, please contact me or Assistant Director Houston Fuller of my staff at (202) 512-6722.

Sincerely yours,

Richard C. Stiener
Director

Contents

Abbreviations

AFDC	Aid to Families With Dependent Children
AFIS	Automated Fingerprint Identification System
ATM	automated teller machine
EBT	electronic benefits transfer
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
IAFIS	Integrated Automated Fingerprint Identification System
IEI	Invitation for Expressions of Interest
INS	Immigration and Naturalization Service
OIG	Office of Inspector General
OSI	Office of Special Investigations
PIN	personal identification number
RCED	Resources, Community, and Economic Development Division
USDA	U.S. Department of Agriculture
WIC	Women, Infants and Children

Selected Biometric Technologies and Their Uses

Biometric technologies use an automated method to measure a physical characteristic or personal trait to verify an individual's identity. Some biometric technologies currently being marketed and used include (1) fingerprints, (2) hand geometry, (3) retina scan, (4) voice verification, and (5) signature verification. Federal, state, and local governments and the private sector have used these technologies to ensure the security of computers, facilities, welfare benefits, and credit/debit cards. An overview of these technologies follows.

Fingerprints

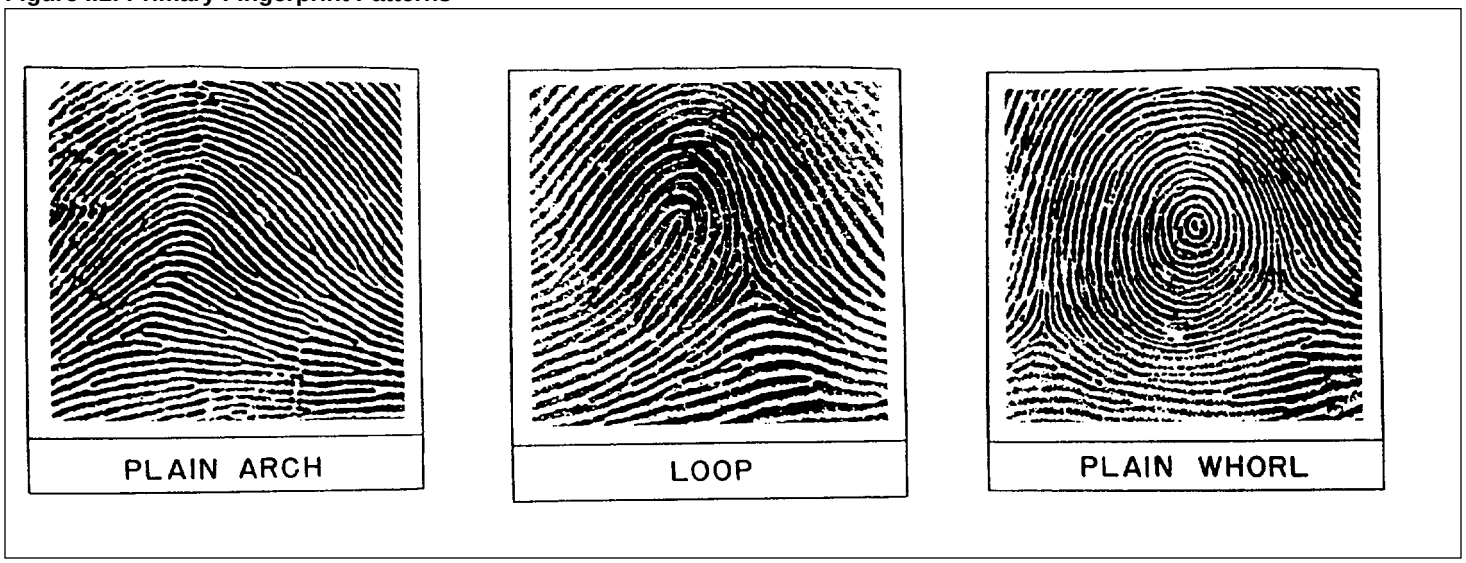
Fingerprints have been used by law enforcement agencies for almost 100 years to identify criminals both upon arrest and after comparison of crime scene fingerprints with already established criminal fingerprint files. Fingerprints provide both a permanent and positive identification system for law enforcement and civilian purposes. Although two fingerprint patterns may be similar, no two fingerprints have ever been found to contain identical individual ridge characteristics. These characteristics are present on normal hands and feet some months before birth and are constant, except for accidental damage, until decomposition after death.

The Henry Fingerprint Classification System

The Henry System, for years the predominant fingerprint classification system, assigns each finger to one of three primary fingerprint pattern types: arches, loops, or whorls.[9] In this system, the fingerprints are represented as a unit rather than as individual fingers by assigning to each 10-print set an alphanumeric designation reflecting the pattern characteristics of all 10 fingers. This classification system was a major step forward in the use of fingerprints because it enabled fingerprint forms bearing differing patterns to be placed in a certain order, thus enabling the search area to be minimized. Figure I.1 shows the primary fingerprint patterns.

[9]The Henry System, credited to an Englishman, Sir Edward Henry, became operational at Scotland Yard in 1901.

Figure I.1: Primary Fingerprint Patterns



Source: FBI

Benefits of the Automated Fingerprint Identification System (AFIS)

With the increasing size of fingerprint databases, manual searches under the Henry System have become too time consuming; and the identification of latent prints,[10] even more difficult. Thus, in the early 1980s, U.S. law enforcement agencies began using the Automated Fingerprint Identification System (AFIS), researched at the National Bureau of Standards[11] under the sponsorship of the FBI during the early 1960s. According to law enforcement officials, the system has been accurate between 98 and 100 percent of the time in searching and matching fingerprints. AFIS uses computers to scan and digitize fingerprints by automatically creating a spatial geometry or map of the unique ridge patterns of the prints and translating the spatial relationship into a binary code for the computer's searching algorithm. Figure I.2 depicts the plotting of fingerprint minutiae by AFIS.

[10]Latent fingerprints are generally obtained at crime scenes or from documents or material related to the crimes. These prints usually occur as isolated finger impressions or as fragmentary parts of two or three adjacent fingers and are often of poor quality.

[11]Now named the National Institute for Standards and Technology.

Figure I.2: AFIS Plotting of Fingerprint Minutiae

Source: FBI

The following briefly describes the success experienced by various law enforcement agencies with AFIS.

- One large urban police department that has used AFIS since 1983 found that the system can conduct a "cold search"[12] in a database of 340,000 10-print cards in about 1 minute. The same police department can run a 10-print card against its latent file of 6,000 prints in about 40 seconds and realize a positive identification about 22 percent of the time, compared with 8 percent prior to the system's implementation. In the first year of operation, the department conducted 5,514 latent print searches on its AFIS system and made 1,001 identifications, an identification rate of over 18 percent. The department cleared 816 of those cases compared with 58 cases cleared the previous year on the basis of latent print identifications.
- According to California law enforcement officials, they have realized a 98-percent accuracy rate for matching a single 10-print card with the 8.5-million 10-print cards in the state's AFIS system and a 15-percent rate on latent print searches. Several noteworthy cases were solved through searches conducted on latent prints in California's AFIS system. In 1985, three murder suspects were arrested after a single thumbprint was found on a vehicle owned by one of the victims. The vehicle was found abandoned and burning, with little chance of obtaining other evidence. In 1987, approximately a decade after a man was murdered and his son paralyzed by an assailant's bullets, the state identified a suspect with a single thumbprint found on a kitchen window at the crime scene. And in 1988, nearly 21 years after a murder was committed, the state identified a suspect by searching latent prints found at the time of the murder.

  California is a member of the Western Identification Network, a multistate organization formed in 1989 to exchange automated fingerprint information. As a result, California exchanges information with the member states of Nevada, Oregon, Idaho, Utah, Wyoming, and Montana, and three associate member states, as well as the U.S. Postal Inspection Service and the U.S. Immigration and Naturalization Service (INS).

- The U.S. Secret Service, a member of the Northern Virginia Regional Identification System with a database of over 200,000 fingerprints from 10 Virginia police departments, uses AFIS as an investigative tool in identifying suspects, for example, by matching latent prints found on threat letters addressed to the President.
- INS is developing a database of fingerprints for all aliens intercepted when illegally entering the United States over the border with Mexico. INS takes a live scan of both index fingers, photographs the individual, and records certain biographical data on each subject. In January 1995, INS had about

[12]A cold search is one conducted with no identifiers available on the subject/suspect that would assist in narrowing the search within a system.

75,000 prints in the system and conducted about 2,000 searches a day. According to INS officials, the combined false positive and error rate[13] is less than 2 percent. The INS system, whose development began in 1990, is used to identify aliens that are recidivists, reduce the time required to process the aliens before returning them to Mexico, and determine whether an alien is wanted on criminal charges.

FBI Developing the Integrated Automated Fingerprint Identification System (IAFIS)

The FBI has about 72 million individual criminal and civil 10-print cards on file and processes 35,000 to 50,000 new 10-print cards each day. According to an official, the FBI is scanning the inked hardcopy 10-print cards into the Integrated Automated Fingerprint Identification System (IAFIS) and digitizing the prints. An FBI official said that by searching the prints electronically, the FBI can respond to a routine law enforcement query in about 16 hours and to special requests in about 2 hours. The system, by searching digital prints electronically, eliminates the need for the old manual system and speeds up the process. The FBI plans to completely automate its system by 1998.

Benefits of Fingerprint Technology for the Private Sector

With the development of live scan equipment and the technology enabling the electronic storage and transmission of fingerprints, the private sector has started to use fingerprint technology. Figure I.3 shows one example of a live scan fingerprint reader.

[13]A false positive occurs if the system identifies someone that is not in the database. An error occurs when the system provides a negative response even though the prints are in the database.

Figure I.3: Live Scan Fingerprint Reader

For example, one company that we visited is planning to use fingerprint technology to verify an individual's identity in self-check grocery stores, eliminating the need for checkout clerks. According to company officials, they also plan to institute a store credit card. The card will include a digitally encoded fingerprint on the magnetic stripe that can be used with a live scan fingerprint device to verify ownership of the card prior to charging the purchases on the card. The system will verify the print encoded on the magnetic stripe with the customer's fingerprint.

Officials from the firm marketing this technology told us that the digitally encoded fingerprint uses only 100 bytes of space on a magnetic stripe. This is particularly important, they noted, because the stripe has limited storage capacity due to the credit/banking information on the card. The officials also said that the card would not be usable if anyone attempts to encode a new print on the card. In addition, after encoding the fingerprint, the card can be presented at any location that has installed the company's fingerprint reader. According to officials, the company is marketing the technology for such uses as employee time cards, alarm systems, entry doors, computer files, credit or electronic benefit transfer cards, checks,

driver licenses, social security cards, and controlled-substance (cigarettes and liquor) vending machines.

Hand Geometry

Hand geometry is based on the premise that each individual's hands, although changing over time, remain characteristically the same. An electronic hand geometry device being used at selected locations by the Federal Bureau of Prisons stores a template of the hand in the device's memory. The hand geometry unit measures the height of the hand, the distance between knuckles, and other information that is converted to an algorithm. According to agency officials, the more times a hand geometry device reads or scans a particular hand the more accurate the reading on that hand becomes. The hand geometry unit will reject any verification attempts with a hand that has not been stored in memory. Figure I.4 shows a hand geometry device.

Figure I.4: Hand Geometry Device

The Bureau of Prisons is using a personal computer on a local area network to capture the hand geometry, photograph, and biographical data of each staff member, visitor, and inmate. The agency provides a photo identification card with a magnetic stripe encoded with a PIN to each individual that is in the system. In this way, a prison checkpoint person can use facial recognition and a database match by having the card read electronically during the hand geometry verification process. According to agency officials, their system of eight hand geometry units, cameras, and necessary software costs about $90,000, exclusive of the costs for the personal computers or local area network.

In addition, a Bureau of Prisons official told us that the system has been very reliable. For example, the agency had conducted over 200,000 hand geometry checks at one prison site with no errors. As currently designed, if the system does not match an individual's hand after three attempts, a sound alerts the guards, a "reject" appears on the computer screen, and the photograph and file of the appropriate individual appear on screen. The Bureau of Prisons plans to expand the hand geometry program to its Washington, D.C., headquarters and later to establish a wide area network allowing headquarters staff immediate access to the database that will provide timely information on the location of inmates and correctional staff in the event of a riot or disturbance at a federal correctional institution.

Retina Scan

Retina scan is being used for both access control and for identifying and releasing felons from custody. Retina identification is based on a medical finding in 1935 that no two persons have the same pattern of blood vessels in their retinas. The retina scan device was developed by an ophthalmologist and is used to capture the unique pattern of blood vessels in a person's eye. The data are converted to an algorithm and then stored in a computer or in the scanner's memory. Enrollment with a retina scan device can be done with one or both eyes depending upon the user's requirements. For identity verification, an individual would enter a PIN and place his or her eye over the lens in proper alignment for scanning. The reading is compared with the eye signature stored with the PIN in the system. If there is a match, the individual is identified. The system scores the eye signature in percentages from 0 to 100 with a minimum score of 70 percent being recommended by the manufacturer for an accurate eye measurement. According to a local police official familiar with retina scan, an eye signature pattern is adversely affected only by a serious eye illness

or injury, such as a detached retina, or eye surgery. Figure I.5 shows retina scan devices.

Figure I.5: Retina Scan Devices

In 1990, a sheriff's office in a large urban, Midwestern county purchased and installed retina scanners in its jurisdiction for the purpose of prisoner identification and release. At that time, the cost of the system was about $500,000 and included 23 scanners and other necessary hardware to run an integrated system. An individual scanner was priced at about $7,000, but the manufacturer's current model is about $3,500.

According to an official at the sheriff's office, approximately 250 to 300 prisoners are scanned per day, and the database includes more than 300,000 eye signature templates. A system search on an eye template takes about 2 minutes. However, a response time of several seconds was evident in a retina scan device being used for access control by legal staff in the same jurisdiction. The device being used by the legal staff was not connected to a large database but used its stand-alone memory capacity and contained a very limited number of templates.

Although the manufacturer has recommended requirements for the scanner's maintenance and environmental operating conditions related to temperature and humidity, a sheriff's office official indicated that the scanners were not cleaned on a regular basis nor were measurements on temperature or humidity taken in the 5 years since the equipment had been installed. The official advised that the equipment had already exceeded the manufacturer's duty life and if a scanner is not operating, it is usually due to a dirty lens or a power surge. The sheriff's office representative indicated that a proposal had been submitted to the county to upgrade the system's equipment, including the installation of about 210 new retina scan units.

Voice Verification

Voice verification is primarily used to secure building access. According to one vendor, the voice verification process utilizes such characteristics of the voice as bass and treble tones, vibration in the larynx, throat and nasal tones, and air pressure of the person speaking. According to the vendor, the premise that these characteristics are distinct for individual voices is based on research conducted by another firm about 10 years ago. In addition, the vendor said that each individual voice print is encoded with a proprietary algorithm.

One Eastern city we visited used voice verification for employee access and theft prevention at one of its maintenance buildings. The system at this facility controls both entry to and exit from the building and secures the use of an elevator in the same building. An employee gains access by

using a dedicated phone at each door. After the phone is taken off the hook, the voice verification system prompts the individual to enter his or her PIN number. When the system locates the employee's voice record, it prompts the individual to recite a password; and if verified, the system automatically unlocks the door. After three unsuccessful attempts, the system responds with "unable to verify." Access rejection usually results from the use of an incorrect PIN number or password. The system automatically records both failed and successful attempts by date and time. Since the system must be accessed for entry or exit, it can be used for employee time and attendance. The system is used to control access by particular groups for specific time periods; for example, the janitorial crew's access is limited to the time they report to work in the evenings.

According to the city official with whom we spoke, three voice reads were entered by each enrollee to create a voice template for verification purposes. He also advised that the system has an adjustable threshold for verification. The official attributes no voice access problems to individual voice changes due to such things as colds or sinus problems. The same official told us that since the system's installation in 1993, it has required very little maintenance other than the replacement of keypads on the phones used with the system. He indicated that the city paid less than the market value for its system, but a standard voice verification access system that includes a personal computer, software, and other hardware for controlling door locks is priced at about $50,000. But, he added, the system has saved the city about $100,000 annually in security guard costs; and the city plans to add the same system to another building.

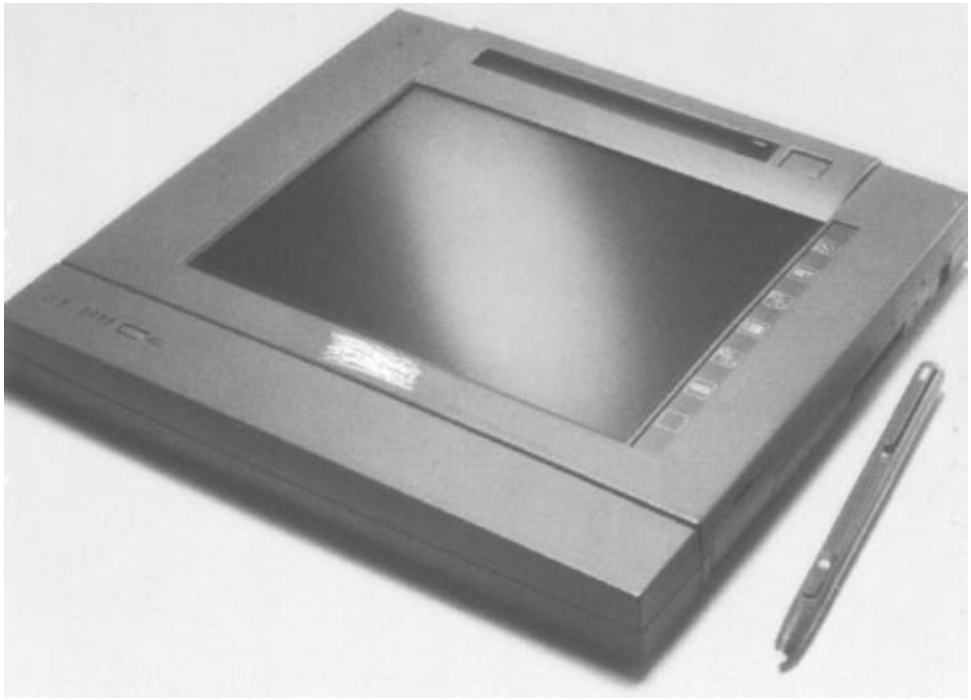
Signature Verification

Electronic signature verification as an identity authentication technique is being piloted for such applications as access to safe deposit boxes, check verification, and computer access for purchase order authorization control. According to one vendor, signature verification examines the way a signature is written, rather than the way it looks. The basic premise of the system is that people have a tendency to write or sign their names in a consistent and unique manner.

The same vendor told us that the firm's signature verification device measures four components: (1) signature shape or form, (2) writing velocity, (3) pen pressure, and (4) the tracking of the pen when it is lifted off the tablet. These measurements are automatically encrypted to ensure that an individual's signature cannot be reproduced. Signature enrollment by an applicant consists of writing multiple signatures using a pressure

sensitive pen on an electronic pad or tablet to create a template for signature verification. The signature files or templates can be stored on barcodes and on smart cards. Normally a four-digit PIN number is assigned to an individual's signature template for quick retrieval and comparison; and the process takes no longer than a normal ATM transaction. The signature verification system compares a signature written on the electronic tablet with the signature template previously created by the user, which is stored in a personal computer or within an integrated system. Figure I.6 displays an example of a signature verification device.

Figure I.6: Signature Verification Device



According to one vendor with whom we spoke, the signature verification system "learns" the changes or variations that occur in an individual's signature over time and adapts to those changes. In addition, the vendor said that the system can record and store signatures in any style or language. Experimentation with the writing of Xs and scrawls by illiterate persons and subsequent verification appears to work, according to one of

the vendors. The same vendor says the system has an adjustable acceptance range for allowing leeway for signature acceptance.

During our observations of two different signature verification systems, one user had repeated difficulty during the verification process after enrollment. According to one vendor, approximately 1 percent of the population has difficulty with signature enrollment and verification; and in such cases, additional templates may have to be taken and the system acceptance range adjusted for easier acceptance. On the basis of pilot tests and sites where the system has been applied, the same vendor reports a 0.7-percent false rejection rate and a 0.4-percent false positive rate.

A research and development firm reports successful results with a prototype signature verification system. The firm enrolled 4,000 users in the project and found that the system accepted 98 percent of all sign-on cases (about 300 a day) and 94 percent required only one signature attempt. According to the firm's report, the project data indicates that the false rejection rate is about 0.1 percent, including problems with the system algorithm.

Comments From the U.S. Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

ASSISTANT SECRETARY

September 15, 1995

Dear Mr. Stiener:

This is in response to your letter to Secretary Rubin requesting the Department of the Treasury's comments on the General Accounting Office's (GAO's)draft report entitled Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program. We commend GAO's efforts to identify controls which will deter fraud in the nationwide EBT program.

Your draft report recommends the use of biometrics technology as a fraud deterrent at both the point of benefit eligibility and the point of benefit delivery. While it appears that there may be a cost/benefit advantage to apply this technology to the benefit eligibility phase, we have reservations about its immediate use in the benefit delivery phase. We agree with the position of the Federal EBT Task Force that the use of biometrics identification for EBT delivery would require considerable testing and study to resolve technological and policy issues.

The basis for our conclusions on the immediate use of the technology with respect to delivery are:

- There is very limited cost or benefit data available on the use of biometrics for a nationwide delivery system. Further, there is not sufficient information on potential Regulation E impact to properly address your assumptions relating to fraud and the allocation of responsibility for losses associated with unauthorized use.
- In order to make the EBT program convenient, accessible, and cost effective to a large and diverse population, it is necessary to utilize the existing infrastructure of the commercial debit card industry to the greatest extent possible. The debit card industry has yet to adopt this technology as a cost effective way of reducing fraud.
- For the nationwide EBT system, Treasury is requiring high standards for card security, including countermeasures to deter counterfeit cards.

Page 2 - Mr. Stiener

- It is unclear how fingerprint verification at the delivery point would impact on the dignity of recipients. One of the objectives of the nationwide EBT program is to create a card and system that looks and operates like commercial credit and debit card systems widely used across the nation. We would like to be sensitive to the appearance of discrimination against the poor or otherwise disadvantaged segments of the population.

We have not dismissed the use of biometrics in the future delivery of benefits. There are many parties to any such decision. The use of biometrics must be acceptable to the commercial infrastructure as well as the State and Federal program partners. In the short term, we feel we must continue to move ahead, as we are within days of selection, based on responses to the Invitation of Expressions of Interest process for the Southern Alliance of States.

Please be assured that we will continue to pursue our common goal of implementing those methods which prove to be cost effective and otherwise acceptable in reducing the Government's exposure to losses in Federal benefit programs. We will also continue to participate in efforts such as those of the EBT Task Force's Risk Advisory Forum to research and explore the uses of finger-imaging and other controls.

We appreciate the opportunity to provide comments on your draft report.

Sincerely,

Gerald Murphy

Gerald Murphy
Fiscal Assistant Secretary

Mr. Richard C. Stiener
Director
Office of Special Investigations
General Accounting Office
Washington, D.C. 20548

Major Contributors to This Report

Office of Special Investigations, Washington, D.C.

Houston R. Fuller, Assistant Director
Thomas L. Sipes, Senior Special Agent
M. Jane Hunt, Senior Communications Analyst

Office of the General Counsel, Washington, D.C.

Leslie J. Krasner, Attorney Adviser

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested