The Use of Technology to Combat Identity Theft

Report
on the
Study Conducted Pursuant to Section 157
of the Fair and Accurate Credit Transactions Act
of 2003

February 2005

THE USE OF TECHNOLOGY TO COMBAT IDENTITY THEFT

Report
on the
Study Conducted Pursuant to Section 157
of the Fair and Accurate Credit Transactions Act of 2003

Acronyms

ACM	Automated Cashier Machine
AAMVA	American Association of Motor Vehicles Association
APWG	Anti-Phishing Working Group
ATM	Automated Teller Machine
AVI	Automated Vehicle Identification
CAC	Common Access Card
CISP	Cardholder Information Security Program
DHS	Department of Homeland Security
DLID	Driver's License Identification
DMV	Department of Motor Vehicles
DoD	Department of Defense
FACT Act	Fair and Accurate Credit Transactions Act of 2003
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FFIEC	Federal Financial Institutions Examination Council
FMR	False Match Rate
FNMR	False Non-Match Rate
FSTC	Financial Services Technology Consortium
FTA	Failure-to-Acquire Rate
FTC	Federal Trade Commission
GAO	Government Accountability Office
GLBA	Gramm-Leach-Bliley Act of 1999
HSPD	Homeland Security Presidential Directive

IAFIS	Integrated Automated Fingerprint Identification System (FBI Program)
IAPP	International Association of Privacy Professionals
ICAO	International Civil Aviation Organization
IBG	International Biometric Group
ID	Identity or Identification
IT	Information Technology
MSP	Member Service Providers
MICR	Magnetic Ink Character Recognition
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
ORC	Opinion Research Corporation
PDA	Personal Digital Assistant
PED	PIN Entry Device
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point of Sale
RF	Radio Frequency
RFID	Radio Frequency Identification
SDP	Site Data Protection
SIPC	Securities Investor Protection Corporation
SSA	Social Security Administration
SSL	Secure Socket Layer
SSN	Social Security Number
3DES	Triple Digital Encryption Standard
TWIC	Transportation Worker Identification Credential

TSA	Transportation Security Administration
URL	Universal Resource Locator
USB	Universal Serial Bus
U.S.C.	United States Code
User ID	User Identification
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

LIST OF FIGURES AND TABLES

FIGURES

TABLES

Chapter I

INTRODUCTION

The Fair and Accurate Credit Transactions Act (FACT Act, Public Law 108–159, 117 Stat. 1952), signed by President George W. Bush on December 4, 2003, amends the Fair Credit Reporting Act (FCRA).[1] The FACT Act amendments provide consumers new tools to fight identity theft and preserve certain national standards for consumer credit markets. This report satisfies the requirements of section 157 of the FACT Act, "Study on the Use of Technology to Combat Identity Theft." Section 157(a) of the FACT Act requires the Secretary of the Treasury to study "the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction." Section 157(d) requires the Secretary of the Treasury to report the findings and conclusions of the study, and any recommendations to the Congress. Treasury Secretary John W. Snow presents the findings and conclusion of the study in Chapter V.

Background to the Study

During 2003 the Congress and the Administration considered carefully whether to preserve the FCRA's existing national standards on affiliates' sharing of personal financial information about consumers. The uniform national standards were to expire on January 1, 2004, in the absence of legislative action. After comprehensive Congressional hearings and careful analysis, the Senate and the House of Representatives considered and passed legislation. The bill included Administration proposals announced by Treasury Secretary John W. Snow on June 30, 2003. President George W. Bush signed this important legislation on December 4, 2003.

The FACT Act provides consumers new tools for combating identity theft, preserves and enhances national standards that assure broad accessibility to U.S. credit markets for all Americans, and preserves the FCRA standards for information sharing among affiliated entities. The statute includes numerous improvements in the resolution of consumer disputes about credit information, provisions to improve the accuracy of records bearing on a consumer's creditworthiness, and measures governing the use of and consumer access to such information. The FACT Act also mandates several studies and reports bearing on these topics, including this technology report.

Scope of the Study

Development of the study began in December 2003. Initial research suggested that biometric technologies were unlikely to offer a single or fool-proof means of providing convincing evidence of who actually performed a given financial transaction. However, the potential opportunities for using biometric technologies to supplement existing technologies for

[1] Fair Credit Reporting Act, 15 U.S.C §1681 *et seq.*

reducing the risk of incorrectly identifying a party to a financial transaction appeared to exist. There were likely to be various circumstances in which biometric solutions could enhance authentication of parties to a transaction.

This report reflects the results of a general study with the objective of highlighting key issues affecting any decision to adopt biometric solutions to the challenge stated in the statute. The study did not attempt a technical assessment of particular technologies, or to develop a business case for the use of any specific technology. The study and the report focus on domestic market developments.

FTC regulations under section 111 of the FACT Act define identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] Effectively, "identity theft" occurs "[w]hen someone appropriates your personally identifying information (like your Social Security number or credit card account number) to commit fraud or theft."[3] This non-exclusive definition of the term is consistent with the crimes specified in the Identity Theft Fraud and Assumption Deterrence Act of 1998 (18 U.S.C.§1028). The misappropriation of a person's identifying information to take over an existing account belonging to that person or to establish a new account in his or her name also would be identity theft. Under this definition, misappropriation of a person's credit card number to make fraudulent purchases would be considered identity theft.

The term "financial transactions" is used broadly in this report to include transfers of information as well as payments activities, or account activity. For example, filling out an application to establish an account or obtaining access to account information about a person are financial transactions that require some assurance of who is involved.

Essentially, the report focuses on the "authentication" of individuals. To federal banking regulators, this may mean the verification of the identity of new, and the authentication of the identity of, existing customers, employees, and contractors based on presentation of unique credentials.[4] For purposes of this study, authentication focuses on authentication of the identity of existing customers and employees. Third party contractors employed by regulated financial institutions are considered to be subject to the same authentication controls as employees.

"Biometrics," in the context of this report, refers to any physical characteristic or personal trait that can be automatically measured to identify or verify the identity an individual is claiming (*e.g.*, fingerprint). Biometrics can be used for "identification": that is, matching one person's biometric to a database of biometric information to determine whether there is a match (*i.e.*, one-to-many match). Biometrics also can be used for "verification": that is, comparing a

---

[2] 16 C.F.R. section 603.2.

[3] Federal Trade Commission (FTC), National and State Trends in Fraud & Identity Theft January – December 2003 (Washington, DC: FTC, January 22, 2004), Appendix B.

[4] Federal Financial Institutions Examination Council (FFIEC), "Authentication in an Electronic Banking Environment," Washington, DC, August 8, 2001. Also, FFIEC, "E-Banking," IT Examination Handbook (Washington, DC: FFIEC, August 2003) Appendix B.

person's submitted biometric sample against a biometric reference template of the person to determine whether they match (*i.e.*, one-to-one match). For purposes of this study, the focus is on verification, although there is some discussion of identification. As a practical matter, a one-to-many biometric match is likely to be used to help establish the identity of a new customer, while one-to-one biometric matches may be more appropriate for an existing customer, whose identity has already been established.

Methodology

This report is based on data collected through a request for public comment; consultations with representatives of a broad range of organizations, agencies, and companies; and a literature search and review.

Subsection 157(b) of the FACT Act requires the Secretary of the Treasury in formulating and conducting the study on technologies to combat identity theft to:

> ''[C]onsult with Federal banking agencies, the Federal Trade Commission, and representatives of financial institutions, consumer reporting agencies, Federal, State, and local government agencies that issue official forms or means of identification, State prosecutors, law enforcement agencies, the biometric industry, and the general public in formulating and conducting the study.''

To ensure the general public and other interested parties an opportunity to provide relevant information and views on the topic outlined in section 157 of the FACT Act, the Treasury Department published a request for public comment in the *Federal Register* on March 2, 2004.[5] (The *Federal Register* notice appears in Appendix A.) The request contained eight questions (see also issues enumerated on the following page). The 30 respondents comprised six financial institutions or their representatives, two public policy advocacy organizations, three research or standards groups, eleven vendors or service providers, and eight individuals. These comments were reviewed and analyzed during the subsequent months. Summaries of the public comments appear in Appendix B. The comments may be reviewed at the Treasury Department library, by appointment (call 202-622-0990).

The MITRE Corporation (MITRE) was selected by Treasury in May 2004 to provide expert technical assistance on biometric and other similar technologies to the Secretary of the Treasury in formulating, conducting, and completing the study, and the report for Congress based on the study. MITRE assisted the Treasury Department during May, June, July, and August 2004. MITRE staff also compiled a table of Biometric Technical and Operational Features to Assess (Appendix C), a Glossary (Appendix D), a Summary of Biometric Standards Projects (Appendix E), and a short list of Current Academic Research Efforts in Biometrics (Appendix F).

---

[5] "Public Comment on Formulating and Conducting a Study on the Use of Biometrics and Other Similar Technologies to Combat Identity Theft," Notice and request for comments, Federal Register, Vol. 69, No.4/Tuesday, March 2, 2004/Notices.

Treasury Department and MITRE staff consulted with representatives of the entities listed in subsection 157(b) of the FACT Act. The on-site consultations took place in the Washington, D.C. metropolitan area, while telephone consultations extended throughout the country. The more that three dozen consultations included discussions with officials from federal banking agencies and the Federal Trade Commission (FTC); representatives of financial institutions and consumer reporting agencies; federal, state, and local government agencies that issue official forms or means of identification; state prosecutors; and law enforcement agencies.

The eight questions published in the *Federal Register* request for public comment highlight key issues which were investigated throughout the course of the study. These issues established the framework for research and for this report. They include:

- The chief characteristics of identity theft, the chief means or methods for perpetrating identity theft, and an indication of the scope of the problem such as number of crimes and value of losses.

- The range of biometric technologies and other similar technologies that are being used or could be used in the future to reduce the costs to society and the incidence of identity theft by providing convincing evidence of who performed a given financial transaction.

- The rate of adoption by the financial services industry and by other industries of biometric solutions and of other similar technologies for the purposes of verifying or authenticating who performed a given financial transaction.

- The costs and the risks of using biometrics, including the public's concerns with the use of biometrics, the tradeoffs for consumers in using biometrics, and the benefits to consumers of the use of biometrics.

- The experience of industries that have used biometrics as well as other similar technologies for the purpose of providing convincing evidence of who performed a given financial transaction, and customer reaction to the use of these technologies for this purpose.

- The barriers to greater use of biometric and other similar technologies to reduce the cost and incidence of identity theft and the incentives that exist to spur the use of biometrics for this purpose, including consideration of factors such as accuracy, affordability, reliability, convenience, law and regulation, and other critical determinants.

Additional research drew on the technology expertise of MITRE and on a search and review of literature pertinent to this study and to the report. The literature was drawn primarily from publicly available sources.

Results and Conclusions

The study confirmed the initial hypothesis that biometric technologies would not currently offer a single or fool-proof means of providing convincing evidence of who actually

performed a given financial transaction. Biometric technologies are not in widespread use by the financial services industry or in payments processes at this time. However, there is renewed interest in assessing on a case-by-case basis the potential for biometrics to afford faster, cheaper, and better methods for authenticating individuals engaged in financial transactions.

Familiar non-biometric mechanisms used for fraud detection include User ID and password filters, rules-based applications that "learn" typical consumer activity and provide an alert to atypical patterns, credit monitoring, and transaction monitoring. At present the incentives to early adoption of evolving biometric technologies generally are not sufficient to justify the costs or outweigh the perceived risks involved.

At a minimum, the following key issues must be examined and questions resolved before biometric technologies are likely to be adopted on a wide scale and in a manner that will help to reduce the costs and incidence of identity theft.

- *Cost*: The costs of implementing biometric technologies typically include, but are not limited to: feasibility assessment, design and testing; the purchase of new equipment; retrofitting existing equipment and systems; integration of new technology with legacy systems; establishing fallback systems and processes; process reengineering; system maintenance; and user training and education.

- *Technology Maturity*: Concerns about the immaturity of the technology arise from a number of factors, including: lack of interoperability; lack of standards within and across industries; uncertainty about reliability and accuracy; concerns about the stability (permanence) of biometric characteristics; and lack of widespread deployment and real world testing and experience.

- *Public Acceptance*: Factors that contribute to perceived widespread public resistance to the use of biometric technologies include: concerns about the potential misuse of biometric information by the private sector, such as combining the data with other information to track consumer activities; access to biometric information by government, or linkage of government and corporate databases; disclosure of information without consumer consent or knowledge; lack of confidence in the security of systems that store biometric information; concerns about compromised biometric data that cannot be reissued or revoked; and concern about health risks, invasiveness, and cultural attitudes.

- *System Integrity*: Several commenters and consultees mentioned the difficulty of establishing identity at the time of enrollment into a biometric system and the risk of enrolling an individual with the incorrect biometric (fraud/impersonation). In addition, the processes and procedures for collecting, storing, protecting, accessing and using biometrics need to be clearly established in order to sustain the accuracy of systems.

The implementation of biometric technologies for authenticating customers generally has been limited to pilot and prototype programs, although some institutions use biometrics internally to control employee access to sensitive locations and data. A better understanding of consumer concerns and greater consumer education would help to determine whether the

perception of broad public resistance to the use of biometrics is overstated. Consumers might benefit from using biometric authentication methods in a number of ways through enhanced security and convenience of transactions; easier and faster access to services; potential reduction in processing time; the intrinsic security of biometric encryption compared to the vulnerability of PIN numbers to loss or misappropriation; and the ability to check for multiple enrollments that reflect fraud. At this point, however, further development and study are needed on the circumstances in which biometric technology might be preferable to other technologies for reducing identity theft by improving the authentication of individuals engaged in financial transactions.

The Report

Chapter II, "Combating Identity Theft," examines the nature and extent of the problem of identity theft and the methods used to deter and detect it. Chapter II also examines the regulatory regime for the security of personal financial information and public perceptions of the need to improve the security of financial data. Chapter III outlines the chief types of biometrics and their characteristics, and presents an overview of the uses for biometrics, including their use by government. Chapter IV presents an overview of the use of biometric technologies in payments and financial transactions. Chapter V presents the findings and conclusions of the study.

Chapter II

COMBATING IDENTITY THEFT

The FTC classified 42 percent of the more than one-half million consumer complaints it received in 2003 as identity theft.[6] The largest single category of reported fraud, identity theft, involved credit card fraud, phone or utility fraud, bank fraud, employment-related fraud, government document or benefit fraud, and loan fraud.[7] This chapter examines the nature and scope of identity theft, aspects of regulation intended to prevent or detect misappropriation and misuse of personal financial information, and various non-biometric methods financial institutions use to avoid or spot identity thieves and potentially fraudulent transactions.

What Is Identity Theft?

The Identity Theft Fraud and Assumption Deterrence Act of 1998 establishes a federal, criminal offense for unlawfully transferring or using another person's means of identification with the intent to aid or abet a breach of federal law or commit a felony under state or local law (18 U.S.C. §1028(a)(7)). This federal criminal law provision for identity theft was fortified by the Identity Theft Penalty Enhancement Act (18 U.S.C. §1028A), which establishes the new crime of "aggravated" identity theft and effectively establishes a mandatory additional two-year sentence for identity theft. Identity theft is also related to other federal crimes such as credit card fraud (18 U.S.C. §1029), computer fraud (18 U.S.C. §1030), mail fraud (18 U.S.C. §1341), wire fraud (18 U.S.C. §1343), or financial institution fraud (18 U.S.C. §1344). In addition, state law may apply to identity theft or related crimes. While the law enforcement community has no single standard to guide its identification and pursuit of identity theft, it does have a broad choice of statutes for prosecuting criminals engaged in the fraudulent activity covered by the broad definition of identity theft.

Victims often may not learn for weeks, months, or even years that someone has been using information relating to them for financial gain because it may take that long for the warning signs to become evident. Identity theft occurs, for example, through:

- Theft and unauthorized use of a credit card, debit card, or ATM card;
- Skimming of credit card account numbers from the magnetic stripe, by criminals serving customers in a retail establishment perhaps;
- Impersonation of a legitimate account holder or his representative, over the telephone or online, to obtain account or other personal identifying information;

---

[6] "Identity theft" is the appropriation of personally identifying information of another person (*e.g.*, a Social Security number or credit card account number) to commit fraud or theft. FTC, National and State Trends in Fraud & Identity Theft January – December 2003, (Washington, DC: FTC, January 22, 2004), Appendix B.

[7] For some in the financial sector, identity theft is a definition in progress; true identity theft may not include the misuse of lost or stolen credit cards, for example. Law enforcement officials may also define identity theft according to the federal crimes enumerated in the Identity Theft Fraud and Assumption Deterrence Act of 1998 or other applicable statutes, including state law.

- "Dumpster diving" to obtain account or other personal identifying information from discarded statements, bills, or solicitations;
- Computer hacking of databases where personal identifying information or account numbers are stored;
- Eavesdropping and interception of an account number during transmission over phone lines or Internet;
- Misuse of information from credit reports; and
- Mail theft of credit cards, change of address forms, checks, or applications.[8]

There are many examples of schemes that involve identity theft. In a notorious case that began in 2000, one of the perpetrators of the crime stole names and passwords when he left his helpdesk job at a small software firm. He pleaded guilty in September 2004 to conspiracy, fraud, and wire fraud in the scheme which reportedly yielded thieves between $50 and $100 million. The information he stole provided access to credit reports of tens of thousands of Americans. He and his accomplice sold the information to street criminals, reportedly for $60 for each report. The criminals, using the credit report information, took the identities of others, changed addresses on their accounts, and depleted the bank accounts of the unknowing victims. The criminals were able to order new checks, new ATM cards, and new credit cards that were diverted for the fraudsters' use, and to open and quickly drain new lines of credit.[9]

Thieves have stolen information about individuals in order to reroute the victims' mail and attempt to take ownership of the victims' houses to sell or use for home-equity loans. The Federal Bureau of Investigation (FBI) recently reported that the number of open FBI mortgage fraud investigations increased from 102 in 2001 to 533 cases by June 30, 2004.[10] Older Americans who have paid off their mortgages are obvious targets of unscrupulous mortgage operators and crime groups engaged in mortgage fraud.

Fraudsters also have established websites using the names of legitimate securities brokerage firms registered with the Securities Investor Protection Corporation (SIPC).[11] Using a different address from the true brokerage firm to receive funds from the victim, con artists have taken in investors' funds by offering a security for sale, or requesting a "good faith deposit" as a condition for purchasing thinly traded shares that the victim may already own.[12]

---

[8] Please see also FTC website http://www.consumer.gov/idtheft/understanding_idt.html.

[9] Bob Sullivan, "Man Pleads Guilty in Huge ID Theft Case," MSNBC, September 14, 2004.

[10] Terry Frieden, "FBI Warns of Mortgage Fraud 'Epidemic': Seeks to Head Off Next S&L Crisis," CNN Washington Bureau, September 17, 2004.

[11] Securities Investor Protection Corporation (SIPC), created by Congress in 1970, restores assets to investors with assets held by bankrupt and otherwise financially troubled brokerage firms.

[12] SIPC, "SIPC Issues Warning About Web-Based 'Brokerage Identity Theft' Scams Targeting Investors," Washington, DC, December 11, 2003.

Children and the public have been victimized by thieves who reportedly paid $100 to hospital employees for every Social Security number the trusted workers provided. The workers stole information about child patients, which the fraudsters used to file fraudulent tax returns.[13] Thieves also have stolen patient information from pediatricians' offices to open credit card accounts under the children's identity, or to start a new life or build a new credit history.[14]

American soldiers on active duty are at risk as well. One reason is that career officers tend to have very good credit histories, and they may earn the higher credit limits that appeal to thieves. If the soldier is away from home on active duty, he may not be able to safeguard and pay close attention to bank account statements, credit card statements, and other records that may reveal personal information or provide evidence of identity theft. When a soldier is abroad and has his identity stolen, the theft can cause serious problems for family members back in the United States. Concern over such family problems only adds to the stress a soldier in a combat environment already faces.

As an example, a civilian Department of the Army employee and two other men recently allegedly conspired to use information they stole about military personnel to run up fraudulent purchases totaling as much as $100,000. The Army employee's position afforded him access to the personal data of Department of Defense employees who entered Fort Hamilton. The three men were charged with defrauding U.S. Department of Defense employees and military personnel. They used their victims' personal information and counterfeit drivers' licenses bearing the names and biographical data of the victims to apply for credit in their names and buy expensive merchandise. Some of the victims are believed to be on active duty in Iraq.[15]

Scope of the Problem

The lack of a standard definition makes it difficult to collect comprehensive, accurate data for quantifying the costs and incidents of identity theft. One of the largest credit card issuers, for example, reportedly attributes roughly 90 percent of its total fraud losses on its credit cards to lost, stolen, and counterfeit cards, and 10 percent to identity theft.[16] Another credit card issuer suggests 20 percent of its fraud may be attributable to identity theft. FTC statistics indicate that credit card fraud accounts for the largest proportion of consumer complaints about identity theft, and the highest proportion of the identity theft related credit card fraud involves establishing new accounts in the victim's name.

The FTC maintains the Consumer Sentinel database of consumer fraud complaints, launched in 1997. The Consumer Sentinel database contains more than one million total consumer fraud complaints. In late 1999, the FTC also launched the Identity Theft Data Clearinghouse as the sole national repository of consumer complaints about identity theft.

---

[13] Kristin Davis and Alison Stevenson, "They've Got Your Numbers," Kiplinger's Personal Finance, January 2004.

[14] Kristin Davis, "Targeting Kids for Identity Theft," Kiplinger's Personal Finance, January 4, 2004.

[15] "Three charged in identity theft scheme targeting military personnel," *Associated Press*, August 21, 2004.

[16] "ID theft hurts, but regular card fraud is worse,"ABA Banking Journal, September 2004.

Information in the Clearinghouse is available to law enforcement members via Consumer Sentinel. As a secured, password-protected government web site, Consumer Sentinel now holds information about consumer fraud and identity theft received by the FTC direct from consumers and from over 100 other organizations. The information is available to law enforcement officers nationally and internationally to use in their investigations.

Reports of identity theft grew by 150 percent, from 86,212 in 2001 alone to about 215,000 in 2003. The FTC found that the proportion of credit card fraud complaints declined from 42 percent of all identity theft complaints in 2001, to 33 percent in 2003, while the proportion attributable to bank fraud increased from 13 percent to 17 percent.

Recognizing that identity theft was a large and growing problem of considerable public policy interest, the FTC sponsored a survey in 2003 to gauge the magnitude of the problem. The *Identity Theft Survey Report* presents the results of over four thousand telephone interviews completed in March and April 2003 with randomly selected U.S. adults over the age of 17.[17] The FTC recognized three categories of identity theft:

- New accounts and other fraud such as misuse of a person's identity to rent an apartment, obtain medical care, take out new loans (considered the most serious category);
- Misuse of existing non-credit card account or account number (*e.g.*, checking account number, Social Security number)
- Misuse of one or more existing credit cards or credit card account numbers (considered the least serious misuse).[18]

Survey results show that 4.6 percent of survey participants reported being victimized by at least one of these three forms of identity theft within the past year. The FTC report states, "This result suggests that almost 10 million Americans have discovered that they were the victim of some form of identity theft within the last year."[19] Nearly one-third of these victims reported discovering that their personal financial information had been used to open new credit card accounts or commit other fraud within the last year. A little more than one-half reported misuse of one or more of their existing credit cards or credit card account numbers within the same time frame. A total of 12.7 percent of survey participants reported being victimized in some way by the misuse of their personal information within the past five years.

The monetary losses from identity theft fall principally upon businesses, including financial institutions. The FTC estimated that these losses amounted to $47.6 billion for identity thefts discovered within the previous year by the survey participants. Nearly $33 billion of this estimate was attributed to the misuse of victims' personal information to establish new accounts or commit other frauds. The average loss on these frauds amounts to $10,200 per victim. Losses

---

[17] FTC, Identity Theft Survey Report (Washington, DC: FTC, September 2003).

[18] FTC, Identity Theft Survey Report, pp. 3-4.

[19] FTC, Identity Theft Survey Report, p. 4.

resulting from misuse of existing accounts, combining both credit card and non-credit card accounts or account numbers, amounted to an estimated $14 billion, or an average $2,100 per victim. Generally, the sooner the crime was discovered, the lower were the losses.

The identity theft victims in the survey reportedly spent an average of $1,180 and 60 hours per person to resolve the problems arising from the "new accounts" thefts. Theft from the misuse of "existing accounts" cost an average $160 per person and took each individual 15 hours to resolve.[20] In total, victims of identity theft took nearly 300 million hours to repair the damage from the misuse of their personal information. The study highlights the fact that financial losses to the economy can be substantial, and individuals may be seriously inconvenienced, but it also shows that individuals may sustain large financial and non-financial costs indirectly, as well -- through routine administrative tasks such as letter writing, telephoning, and faxing.

Information from law enforcement authorities stresses the organized nature of the crime, its connection to other frauds, and its international reach, particularly via the Internet. The FBI's Internet Crime Complaint Center has documented "a continuing increase in both the volume and potential impact of cyber crime with significant international elements," for example.[21] The Center receives an average of over 17,000 complaints every month from consumers and other e-commerce stakeholders. Since its opening in 2000, the Center has received more than 400,000 complaints, one-fourth of which the FBI characterized as identity theft.

Phishing[22]

Phishing is a form of identity theft in which victims are tricked into turning over their personal information to criminals through bogus e-mails and websites. Phishing schemes, which rely on spam e-mail, emerged in 2004 as the latest method of capturing personal information to use in identity theft. In phishing schemes consumers receive e-mails that purport to convey some urgent message about their financial accounts. Recipients are encouraged to respond promptly by clicking a link in the message to what are imitations of legitimate, trusted websites. The online consumer, believing he or she is connected to a legitimate enterprise, divulges personal financial information, which is diverted to the location of the criminal perpetrator. Essentially the phishers have hijacked the trusted brands of well-known banks, credit card issuers, and online retailers, to obtain valuable personal financial information that can be misused or sold to others for the same purpose. Later phishing attacks have been more generic, but based on a similar pretext.

---

[20] FTC, Identity Theft Survey Report, p. 7.

[21] Testimony of Deputy Assistant Director of the Federal Bureau of Investigation, Steven M. Martinez, before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 22, 2004, p. 5.

[22] Anti-Phishing Working Group (APWG), Phishing Attack Trends Report (July 2004). See www.antiphishing.org. APWG is an industry association focused on eliminating the identity theft and fraud resulting from phishing. It reports regularly on the form and volume of phishing scams.

The spam e-mails easily reach thousands if not millions of unsuspecting consumers at a time. With perhaps 5 percent of recipients estimated to divulge personal financial information, the spam scams are lucrative.[23] In November 2004, the Anti-Phishing Working Group (APWG) reported over 1,500 new phishing attacks that month and a 28 percent average monthly growth rate in phishing sites from July through November. The APWG also identified a new form of fraud-based websites that pose as generic e-commerce sites, rather than brand-name sites, and perpetrate loan scams, mortgage frauds, online pharmacy frauds, and other banking frauds. While the United States hosts the largest number of phishing sites, South Korea, China, Russia, the United Kingdom, Mexico, and Taiwan have also been identified as hosts. Federal law enforcement and others work with foreign counterparts to take down offending sites.

Thus, phishing attacks and "spoofed" e-mails afford criminals an easy and cheap means of obtaining sensitive personal information from consumers which can be very lucrative even if the false website is shut down within 48-72 hours. Other electronic crimes also pose a danger. The use of spyware, for example, to log a user's keystrokes, is a silent way to obtain account numbers from a customer accessing his banking or brokerage accounts online. Spyware is a rapidly growing threat to consumer confidence in electronic finance and commerce.

The Regulatory Regime for Financial Institutions

Federal financial regulators set standards or benchmarks for appropriate internal administrative, managerial, and operational policies and procedures for securing sensitive information from unauthorized access and inappropriate use. They leave flexibility for financial institutions to tailor their programs appropriately. In this context, there are a number of federal requirements that support the implementation of robust processes and procedures for accurately authenticating the person who is undertaking a financial transaction. The discussion below highlights a few key federal statutory and regulatory provisions that have a bearing on the security of personal financial information and the accurate identification or authentication of people and transactions. (State and local requirements are beyond the scope of this discussion.)

Operations and functions within a financial institution carry risks and require corresponding risk management controls. In August 2001, the Federal Financial Institutions Examination Council (FFIEC) issued interagency guidance for insured depository institutions. "An effective authentication program," the FFIEC stated, "should be implemented on an enterprise-wide basis to ensure that controls and authentication tools are adequate among products, services, and lines of business."[24] In addition, the FFIEC wrote:

> Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for customer

---

[23] Dennis Fisher, "Veterans Day Sees a Phishing Frenzy," eWeek.com, November 12, 2004. See http://www.eweek.com/article2/0,1759,1725770,00.asp?kc=EWRSS03129TX1K0000614

[24] FFIEC, "Authentication in an Electronic Banking Environment," Washington, D.C., August 8, 2001, p. 2. The FFIEC is an interagency regulatory group comprised of the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, and the National Credit Union Administration.

> services….[T]he level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.[25]

The transaction or application could be as varied as giving an employee access to consumer account information, allowing an ATM withdrawal, or signing a multibillion dollar loan agreement. In assessing risk, there are a number of factors to consider, such as the following:

- type of consumer whose identity is being verified;
- the financial institution's transactional capabilities;
- value of the information being disclosed to both the institution and its customer;
- ease of use of the authentication method; and
- size of the transaction.[26]

Authentication methods also need to be able to expand with the growth of the enterprise.

The guidance further states that the method of authentication used in a specific electronic application should be appropriate and "commercially reasonable" in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and service providers should periodically review authentication technology and ensure appropriate changes are implemented.

Verification of a new customer's identity also typically involves "positive verification," which entails checking the documentation provided against another source, and asking questions and checking the answers. While face-to-face verification of new customers may be preferable, it is not always possible. "Logical verification" involves checking that documentation is logically consistent – *e.g.*, that zip codes and street addresses match. "Negative verification" involves checking that the documentation does not include information that matches data already associated with fraud. In other cases, a trusted third party might issue a document or certificate verifying the identity of a person. The financial institution is responsible for ensuring that the third party uses the same level of scrutiny that the financial institution would use itself. Once a person's identity has been verified, then the financial institution needs secure, reliable systems for authenticating that person repeatedly when the customer engages in transactions.[27]

The FFIEC guidance notes that single-factor authentication tools, including passwords and personal identification numbers (PINs), are widely accepted and commercially reasonable for a variety of retail banking activities, including account inquiry, bill payment and account aggregation. The guidance warns, however, that financial institutions should continually assess

---

[25] FFIEC, Authentication in an Electronic Banking Environment, p. 2.

[26] FFIEC, Authentication in an Electronic Banking Environment, p. 2.

[27] FFIEC, p. 4.

the adequacy of existing authentication techniques in light of changing or new risks (*e.g.*, the increasing ability of hackers to compromise less robust single-factor techniques) and states that multi-factor techniques may be necessary. The FFIEC also cautions that financial institutions need to utilize reliable methods of originating new customer accounts online because electronic banking undercuts the ability to rely on traditional forms of paper-based authentication.

This authentication guidance does not exist in a vacuum. The federal banking regulators have issued a number of materials that provide consumer and institutional information on steps to take to combat identity theft and phishing. Others statutory and regulatory requirements also encourage and promote greater security for personal financial information and for information technology generally.

In May 2003, the U.S. Treasury Department and federal financial regulatory agencies jointly issued new rules for customer identification that implement section 326 of the USA PATRIOT Act of 2001 (Public Law 107-56).[28] The statute was enacted following the terrorist attacks on the World Trade Center and Pentagon on September 11, 2001, and is intended to help combat terrorism and the finance that supports it. Title III of the Act, "International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, adds several new provisions to the Bank Secrecy Act (31 U.S.C. §5311 *et seq.*) Section 326 requires the Secretary of the Treasury to prescribe regulations setting out the "minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution," the "verification" function noted above. Financial institutions are broadly defined and include travel agents, pawnbrokers, casinos, and many other organizations.[29]

Financial institutions must implement reasonable procedures for (1) verifying the identity of any person seeking to open an account; (2) maintain records of the verification information; and (3) determine whether the person appears on any list of known or suspected terrorists. Since October 1, 2003, financial institutions generally have been required to ask each customer for his or her name, address, date of birth, and tax identification number (usually a Social Security number) when opening a new account. Foreign nationals without a U.S. taxpayer ID number could provide a similar government-issued identification number, such as a passport number.

The institution also can verify a consumer's identity through alternate methods, such as reviewing the individual's credit report. Identification procedures may vary depending upon the type of account being opened and the policies of individual financial institutions, as well as the risks involved. For example, some institutions may require consumers to provide copies of certain documents through the mail if the account is not being opened in person.

---

[28] 31 U.S.C. §5318(l).

[29] A joint final rule implementing section 326 for insured depository institutions and some non-federally regulated banks was published on May 9, 2003, in the Federal Register (Vol. 68, No. 90, beginning page 25090): 31 C.F.R. Part 103, Department of the Treasury; 12 C.F.R. Part 21, Office of the Comptroller of the Currency; 12 C.F.R. Part 563, Office of Thrift Supervision; 12 C.F.R. Parts 208 and 211, Federal Reserve System; 12 C.F.R. Part 326, Federal Deposit Insurance Corporation; 12 C.F.R. Part 748, National Credit Union Administration.

There are other statutory requirements for ensuring that nonpublic personal information that financial institutions have regarding their customers is not inappropriately disclosed or misused. The Gramm-Leach-Bliley Act of 1999 (GLBA, Public Law 106-102), for example, establishes some general rules governing a financial institution's responsibilities with respect to the disclosure of nonpublic personal information about consumers to nonaffiliated third parties.[30] GLBA also outlines consumers' options for limiting such disclosures and imposes specific obligations on financial institutions to protect information that is disclosed for joint marketing purposes.[31] Financial institutions generally may not disclose unencrypted account numbers or access numbers or access codes for credit card, deposit or transaction accounts to nonaffiliated third parties for marketing purposes either.[32] There are general exceptions to the notice and disclosure requirements for transfers of nonpublic personal information to nonaffiliated third parties that permit disclosures to combat fraud and other illegal activities.[33]

Section 501(b) of GLBA touches on the area of authentication, specifically.[34] It directs the federal financial regulators and the FTC to establish standards for safeguarding customer records and information that: (1) insure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[35] The Interagency Guidelines Establishing Standards for Safeguarding Customer Information, published in 2001, direct financial institutions to:

> (1) identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

---

[30] 15 U.S.C, § 6802.

[31] 15 U.S.C. §6802.

[32] 15 U.S.C.§6802(d) and see*e.g.*, 12 C.F.R §40.12

[33] 15 U.S.C. §6802(e)(3)(B). For a brief discussion of GLBA rules on nonpublic personal information and on other statutes that may have implications for the treatment of biometric data, please see: Donald J. Mosher and Jessica Sklute, "Biometrics in the Financial Services Industry: Privacy," Banking & Financial Services Policy Report, Vol. 21, No. 4, April 2002.

[34] 15 U.S.C. § 6801(b).

[35] These safeguards were issued as regulatory guidelines by the federal banking agencies and the National Credit Union Administration (NCUA). Safeguards were issued as regulations by the FTC, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. Office of the Comptroller of the Currency, 12 C.F.R. Part 30; Federal Reserve Board, 12 C.F.R. Parts 208, 211, 225, and 263; Federal Deposit Insurance Corporation, 12 C.F.R. Parts 308 and 364; Office of Thrift Supervision, 12 C.F.R. Parts 568, and 570; NCUA, 12 C.F.R. Part 748; FTC, 16 C.F.R. Part 314; SEC, 17 C.F.R. Part 248; CFTC, 17 C.F.R. Part 160. Please see also National Association of Insurance Commissioners (NAIC) Standards for Safeguarding Customer Information Model Regulation, promulgated in 2002.

(2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(3) assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.' [36]

GLBA also tackles pretext calling."[37] GLBA section 521 prohibits anyone from using false pretenses to obtain or attempt to obtain, or cause or attempt to cause disclosure of someone else's personal information that a financial institution has.[38] Section 521 also prohibits anyone from asking another person to do the same. GLBA section 525 further requires the federal financial regulators and the FTC to check that their respective regulations and guidelines ensure that financial institutions have "policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect activities proscribed under section 521."[39] Section 523 imposes criminal penalties.[40]

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act, Public Law 108-159) is a key legislative effort to address the problem of identity theft. It amends and adds new sections to the federal Fair Credit Reporting Act (FCRA).[41] The FCRA generally limits the purposes for which consumer report information – *e.g.*, information about a person's credit worthiness, repayment characteristics, and general credit reputation – may be disclosed by consumer reporting agencies (*e.g.*, credit bureaus). It also requires that those who obtain consumer reports certify that they are going to use them only for a permissible purpose. Consumer reporting agencies have to take reasonable steps to verify the identity of new users of consumer reports, and of consumers who request copies of their own consumer reports. Under the FCRA, consumers also have a number of opportunities to prevent disclosure of their consumer report and other financial information about them.

Many of the amendments to the FCRA contained in the FACT Act aim to help consumers avoid becoming a victim of identity theft, or to repair the damage to their credit reputations if they are victimized. For example, the FACT Act:

- Provides consumers with the right to a free, annual copy of their credit report so they can monitor it for unauthorized activity;

---

[36] 66 Federal Register 8616 (February 1, 2001). Spurred by growing concerns about identity theft, in August 2003 the federal banking agencies proposed for public comment additional guidance that would require financial institutions to notify customers in writing in the event their sensitive customer information is compromised. The proposal provided for exceptions when the institution reasonably concludes that misuse is unlikely to occur. The agencies plan to publish the final guidance in the near future.

[37] 15 U.S.C. § 6821 *et seq.*

[38] 15 U.S.C. §6821(a)

[39] 15 U.S.C. § 6825.

[40] 15 U.S.C. §6823.

[41] 15 U.S.C. §1681 *et seq.*

- Requires merchants to omit all but the last five digits of a credit card number from credit card receipts;

- Establishes a statutorily defined national system of fraud reporting, enabling consumers to make only one call to receive advice and add a fraud alert to their credit report;

- Requires federal banking regulators, the National Credit Union Administration (NCUA), and the FTC to devise a list of red flag indicators for financial institutions to use to spot identity theft in customers' accounts;

- Requires rules for credit card issuers to follow when they receive suspicious change of address and new card requests on an existing account; and

- Requires federal banking regulators, the NCUA, and the FTC to issue regulations governing the proper disposal of consumer information.

The foregoing discussion highlights key statutory and regulatory requirements that encourage strong data security or authentication methods by financial institutions. The discussion also signals that regulation is technology neutral; it does not necessarily favor the use of biometrics or any other similar technology. The following discussion examines ways in which financial institutions and others are combating identity theft through improvements in the identification and authentication of people engaged in financial transactions.[42]

What the Private Sector Is Doing to Combat Identity Theft

Financial institutions and other organizations use an array of technologies, applications, and methods to reduce the costs and incidence of identity theft. These include processes for identifying new customers, authenticating known customers, and picking out transactions that may be fraudulent.

The process of identifying a customer initially is crucial to establishing an ongoing relationship in which each subsequent transaction or interaction can be conducted to a large extent on the basis of information that the financial institution already possesses about the customer. As noted earlier, it requires careful verification of core identifying documents and data, including for example a driver's license and a Social Security number.[43] There are vendors

---

[42] The financial sector as a whole also devotes considerable resources to consumer education, informing the public about self-defense steps everyone can take to make identity theft more difficult for the thieves. Financial sector institutions and associations work with government agencies to spread useful information through public channels, and they collaborate with others to develop training programs for employees as well. Less visible are the technical efforts. Please see www.ftc.gov for consumer education materials on identity theft and for links to other resources.

[43] Heightened Security: Can Financial Institutions Really Know Their Customers?, Star Systems 2002, p. 25. The Treasury Department's Office of Foreign Asset Control has lists of foreign nationals, drug traffickers, and terrorists, as well as sanctioned companies, businesses, and charities. There are directories of cell phone numbers and pagers, lists of drivers license codes and formats, and charts that can help determine whether a Social Security number

who provide document verification services that compare information from the presented documentation to information in databases. This may be done with devices that can read magnetic strips – on drivers' licenses, for example. The initial verification of a customer's identity would occur on "Day One" of a business relationship.

One major vendor, for example, offers to provide access to major databases containing over 4 billion searchable documents. The information includes data on motor vehicles and other assets, directories of people, multiple business locators and telephone sources, records of professional licenses, real property records, vital statistics records, other public records including court records of bankruptcies and other judgments, news sources, and other databases. The company explains that a software product that it developed in conjunction with a major national trade association in the banking industry is designed to streamline compliance with section 326 of the USA PATRIOT Act. The product is intended to validate documents by determining whether addresses, phone numbers and Social Security numbers are real, whether they exist, and whether they are formatted as the alleged issuer of the credential would have done. The client financial institution can verify whether the data belongs together and is accurate and can detect whether data presented are higher risk than other data (*e.g.*, a disconnected cell phone number). The same vendor also offers statistical scoring models designed to predict outcomes, like fraud, by assessing information on an application.[44]

Many transactions resulting from identity theft occur after the customer relationship with a financial institution has been established. In this second phase, customers seek access to ATMs, make credit card purchases, and seek other products or services. This constitutes "Day Two" (or subsequent) activity. Authentication is particularly relevant at this point in the customer relationship.

Generally, people's identity can be authenticated by something they **know** (PIN number), something they **have** (credit card), or something they **are** (biometric characteristic). A two-factor authentication system that relies on any two of these factors is more secure than a single-factor system, and a three-factor system will provide even greater assurance that a person is who he or she claims to be.

Knowledge-based authentication relies upon a user presenting some data elements that the verifier can approve on the basis of previous transaction and registration activity. Knowledge-based authentication tools may be as simple as a four-digit PIN code, include usernames and passwords, or may include personal data such as address, phone number, Social Security number, or transaction history.[45] Financial institutions rely on password, PIN and user

---

matches a person's stated age, a master list of Social Security numbers belonging to deceased account holders, lists of known mail drops and dubious addresses, lists of employer identification numbers, and lists correlating area codes, phone number prefixes, and zip codes. Please see also: Julia S. Cheney, "Identity Theft: A Pernicious and Costly Fraud" Discussion Paper, Payment Cards Center, Federal Reserve Bank of Philadelphia, December 2003.

[44] InstantID by LexisNexis-RiskWise: see www.LexisNexis.com.

[45] Who Goes There? Authentication Through the Lens of Privacy, National Research Council of the National Academies (Washington, D.C.: National Academies Press, 2001), p.109.

ID systems for authentication and employ Secure Socket Layer (SSL) or other encryption to transmit the data securely for online access.

Sometimes, anti-fraud systems reject a credit application or prevent a transaction from being authorized and sometimes they spot a suspicious transaction shortly after the fact so that a card can be deactivated before more fraud occurs. Important tools for this preventative action include the filters and rules-based decisional programs, scoring and behavior analysis, and credit and transaction monitoring. Automated systems can flag attempted identity fraud transactions by looking at suspicious patterns based on an individual's past behavior or by spotting suspicious patterns of activity across industries. Real-time authorization systems also can compare account information against a database containing known fraudulent accounts. Financial institutions also use internal databases to authenticate individuals and authorize transactions. Examples described here are illustrative only.

Another well-known vendor has a product widely used in the payment card arena that includes "neural network models" and is designed to "learn" a consumer's behavior and monitor credit card transactions. It ranks the risk that the transaction departs from the cardholder's behavior and is likely to be unauthorized. In this way, a transaction for a consumer who purchased something in person on the west coast of the U.S. is flagged when a second "in-person" transaction is recorded shortly afterwards on the east coast, for example. This highly suspicious activity would require verification with the cardholder to ensure the transactions were authorized.

Another of this vendor's products is designed to detect fraud at the time a credit application is made. Using a financial institution's internal data and various external data sources, the vendor describes a system that also can use proprietary cross-industry data on application fraud to quantify the identity fraud risk of an application. At the consumer level, this vendor offers services that monitor a consumer's credit report and score regularly and can report possible fraud activities. A version of this fee-based service may be provided by financial institutions to their customers.[46]

The credit card associations such as Visa and MasterCard, and the card issuers and merchant acquirers who sign up retailers to accept the cards have a number of initiatives aimed at combating card fraud, including identity theft. For example, activation of a credit card usually requires that the cardholder telephone an activation number from his or her home. The procedure helps to reduce the "not received but issued" credit card fraud that can occur when a fraudster takes someone's credit card from the mail. Signatures on the back of credit and debit

---

[46] Fair Isaac promotes Falcon Fraud Manager as "the industry-standard solution in payment card fraud detection, protecting 65 percent of the word's credit cards," Press Release (Minneapolis, MN: Fair Isaac, September 25, 2003). See www.fairisaac.com. Falcon ID is described as reducing losses and protecting consumers for any industry in which identity verification is critical, such as financial services and mortgage lending, through real-time sharing of critical information between companies in the same industry and across different industries to detect when an identity is compromised. "Provider launches new ID fraud solution, Consumer Financial Services Law Report, Vol. 8, No. 6, August 25, 2004.

cards are meant to enhance the authentication of an individual in face-to-face transactions when the salesperson can compare signatures.

Card companies advertise a number of security, merchant, and customer protection programs, some of which are aimed specifically at Internet shopping. Programs to reduce card fraud include Visa's Cardholder Information Security Program, which imposes security standards on merchants in the Visa system. The acquiring banks that sign up the merchants to the Visa system are responsible for ensuring that their merchants comply with the Visa security program and validate their compliance according to Visa specifications.[47] MasterCard's Site Data Protection program for online merchants is a similar security program intended to ensure that online merchants and Member Service Providers (MSP) are protected against computer hackers. The program includes, among its several features, the MasterCard Security Standard for acquiring members, online merchants, MSPs, and data security vendors. There are self-evaluation tools for assessing compliance, and for conducting vulnerability assessments.[48]

Verified by Visa protects a cardholder's card during online shopping and can streamline the check-out phase of the shopping expedition at participating online merchants. The protection can be activated by entering the card number over Visa's secure server, or by verifying one's identity with the issuer while shopping on the Internet. The cardholder also must create a *Verified by Visa* password that will be used for future shopping and will permit automatic recognition of the card. The passwords are secured on a Visa secured server only.

MasterCard's SecureCode program helps merchants avoid fraud and reduce chargebacks (where the merchant assumes the loss) from e-commerce transactions that are "cardholder unauthorized" (*i.e.*, when the cardholder claims of "I didn't do it"). The program runs on the merchant's website and interacts with the customer and the card issuer. At check-out time a pop-up box asks the customer to enter a private code, which has been registered with the customer's bank. The bank validates the code so that the merchant has a fully guaranteed transaction.[49]

Discover offers a free online shopping tool, Deskshop, for Discover cardholders. Deskshop provides single-use card numbers for online purchases so that the cardholder's actual account number is never used. Deskshop can be downloaded to the cardholder's personal computer or accessed through the Discover website. It generates a single-use card number and a single-use three-digit security code that is copied onto the retailer's checkout form. The number and code expire thereafter.[50]

MasterCard and Visa agreed in August 2004 to cooperate to align PIN Entry Device (PED) security requirements and approval procedures for point of sale or ATM transactions. Financial institutions will benefit from greater interoperability and improved security of the

---

[47] See www.usa.visa.com/business.

[48] See www.mastercard.com/sdp.

[49] See www.mastercard.com/securecd/welcome.do.

[50] See www.discovercard.com/deskshop/.

systems. In addition to programs or initiatives of the card associations like Visa or MasterCard, credit card issuers have implemented their own safety mechanisms. Some of these measures are manual, and are aimed at preventing account takeover, for instance, by carefully checking change-of-address notifications. Others are more sophisticated. Merchants, too, may seek their own fraud prevention products and services, particularly for the "card not present" environment.[51]

Cards, Smart Cards and Tokens

In order to strengthen pure knowledge-based authentication procedures, financial institutions leverage some form of physical identification. For example, ATMs not only rely on a user PIN (something you know), but also require that a physical card be present (something you have). Thus, the consumer uses two-factor authentication to withdraw cash from his account through the ATM outlet. The something you "are" generally refers to biometric authentication solutions, which will be discussed in the chapters that follow. Increasingly, financial institutions are seeking to improve upon the simple PIN and password formula for enhanced security, to two-factor authentication.

In the United States individuals are most familiar with plastic credit cards that convey information through letters and numbers visible on the card and a magnetic stripe on the back. The magnetic stripe is a ubiquitous 30-year-old technology which is being overtaken by smart card technology.[52] Encrypted codes or card verification algorithms on the back of the card add security to the plastic card itself, although fraudsters have found a way to decrypt verification codes.[53] Smart cards can offer an additional level of security because they contain embedded integrated circuit chips that can store and process data.[54] Smart cards are more widely used in Europe and elsewhere outside the United States than inside, but they are becoming increasingly familiar in this country.

---

[51] Experian, one of three key nationwide consumer reporting agencies, introduced a Cardholder Verification Service for Merchants in October 2004. The service aims to identify potentially high risk transactions before they are authorized by verifying identifying information, such as bill/ship to addresses, e-mail addresses, IP addresses. Using Experian's credit and noncredit databases, the service can offer consumer verification, credit card verification and online interactive challenge questions.

[52] Please note, for example, that MasterCard International announced on November 2, 2004, that it had sold more than 200 million MasterCard, Maestro, and Cirrus smart cards around the world. MasterCard has an M/Chip Deployment Program supporting the trend of migration to chip technology. With its OneSMART MasterCard Authentication Program, MasterCard's M/Chip 4 cards can be used in conjunction with SecureCode, described earlier, to generate authentication data needed to guarantee e-commerce transactions. "MasterCard International Surpasses 200 Million Smart Care Milestone," News Release, November 2, 2004. See www.mastercardintl.com/cgi-bin/newsroon.

[53] Steve Cocheo, "Debit's Downside," ABA Banking Journal August 2004. Linda Punch, "The New Fraudsters" American Banker-Bond Buyer, November 2004.

[54] Reportedly, Visa and MasterCard Acceptance networks outside of the United States will be adopting Europay/MastercCard/Visa (EMV) smart cards in the next few years. EMV is the global, interoperability standard for cards with smart chips. "An Open Invitation to Card Fraud?" by Peter Lucas, American Banker-Bond Buyer, July 2004.

Smart cards can combine a number of identity technologies like embedded chips, visual security markings, magnetic stripes, barcodes and optical stripes.[55] Smart cards and universal serial bus (USB) tokens can be used to add stronger authentication to computer networks.[56] USB tokens can use smart card chip technology in a form that does not need a reader but plugs directly into a computer through the USB port. Smart card readers and biometric scanners also may plug into USB ports on computers.

Sometimes the smart devices require the user to enter information or communicate with the device. Sometimes the devices simply communicate or interact with special purpose machines, through direct contact with a reader, for example, or by sending radio frequency signals that do not require direct contact.

ID Keeper the American Express free web tool for American Express Blue cardholders only, uses a smart chip and a Serial Port Reader, which cardholders can order for free. The cardholder connects the reader to his personal computer so that it can read information that is locked in the embedded chip on the card itself. The card carries the universal resource locators (URL) of shopping sites, user ID, password, card number and shipping address data. American Express indicates that ID Keeper can take the cardholder automatically to a favorite shopping site, fill out forms online, and otherwise streamline the Internet shopping experience in a secure environment.[57]

Sound or audio authentication is a novel approach to authenticating cards in the online world. One product, which looks like a credit card, contains a speaker and a sound chip. When a "button" on the card is pressed by the cardholder, it emits a tone recognizable by a personal computer. The string is non-repeating and is reproduced in software at the other end. To authenticate an online credit card purchase, the customer presents the card to the computer microphone and squeezes the card button. The sound is captured using a Java or ActiveX control and acts as an authenticator. This Beepcard prevents an attacker from recording one audible string and deducing the rest of them. The card verifies that the person making the transaction possesses the card.[58]

Token devices are generally smaller than smart cards and may look like a calculator or other small object such as a key. Smart tokens frequently use cryptography to generate a one-time password or code, like the RSA product, SecureID (see Figure 1) with a built-in clock and

---

[55] Smart Card Alliance, Secure Identification Systems: Building a Chain of Trust: A Smart Card Alliance Report (Princeton Junction, New Jersey: Smart Card Alliance ID-04001, March 2004), p. 10.

[56] "New Tokens With Fingerprint Scanners Enter Authentication Market," CardTechnology.com, August 2004. See www.cardtechnology.com.

[57] See www.americanexpress.com/blue/.

[58] See www.beepcard.com.

liquid crystal display.[59] Time-synchronized tokens generate a unique random value based on a set time-interval that is synchronized with a central server. With challenge-response tokens, a server generates a challenge (a random value) which the user enters into his token. The processor in the token calculates a response, a password or code that the user enters into the system to gain access. Less complicated tokens may require the user to enter a PIN or otherwise identify himself to the token so that the token can be used to authenticate the user.[60] The one-time use codes or numbers are used to grant access for online financial transactions, though the technology is not yet ubiquitous like a credit card.

Source: RSA Security Inc.

Figure 1. Example of a Time-Synchronized Token[61]

Source: © 2004 Secure Computing Corporation.

Figure 2. Example of a Challenge-Response Token[62]

---

[59] Who Goes There? Authentication Through the Lens of Privacy, National Research Council of the National Academies, p 115. The user enters a user ID and then the current number displayed on the card. The number displayed changes periodically. Some versions also require the user to enter a PIN into the card, thereby providing a two-factor authentication.

[60] U. S. GAO, Information Security Technologies to Secure Federal Systems, GAO-04-467 (Washington, DC: GAO, March 2004), pp. 30-33. Following an initial synchronization, the user of a time-synchronized token enters a PIN followed by a token value that is revealed when the user begins to log into a system. This token value is compared to a value generated by the central server, and if they are consistent, the user will be given access.

[61] U. S. GAO, Information Security Technologies to Secure Federal Systems, p. 32.

[62] U. S. GAO, Information Security Technologies to Secure Federal Systems, p. 32.

Smart cards and tokens are convenient technologies for granting access to information and physical locations, and can be used to identify and authenticate people and transactions online.[63] Generating one-time passwords provides greater security than relying on traditional static passwords systems. Their versatility allows them to be used in systems that require biometric authentication as well. IT companies strive to provide easy-to-use, versatile and portable products at acceptable costs. Tokens equipped with a built-in fingerprint sensor and USB tokens with digital signature (see description below) and fingerprint scanners are on the market. While more expensive than a fingerprint scanner that plugs into a computer, such tokens are smaller, more portable and have storage capacity. Combining biometrics with digital signature functionality does make a comparatively expensive product, and one which may still need to be combined with a PIN number for three-factor authentication.[64] Tokens and other cryptographic methods, discussed below, may help to allay consumer fears about the dangers posed by computer hackers and the risks to electronic commerce and finance from online transactions. Costs and operational challenges in implementing such a system inhibit use for the commercial purposes we have been discussing.

Recent announcements suggest touch or contactless cards may play a growing role in some retail payments. MasterCard in conjunction with Citigroup Inc. and J.P. Morgan Chase & Co. indicated they are testing the Pay Pass card in Dallas, Orlando, and New York, for example. McDonald's Corporation announced it would begin accepting the cards in its outlets that accept credit cards.[65] Customers tap the cards against special payment terminals. MasterCard International reportedly will be testing its contactless Pay Pass card in Canada as well.[66] These cards may be disseminated principally for customer convenience, however.

Radio Frequency Identification (RFID)

RFID is a technology similar in theory to bar code identification. RFID is used to transmit signals. RFID systems consist of an antenna and a transceiver, which read the radio frequency (RF) and transfer the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted. The transponder may be passive or active with internal power sources. RFID tags first appeared in tracking and access applications during the 1980s. These wireless systems allow for non-contact reading and are effective in a wide range of tracking systems including livestock identification, automated vehicle identification (AVI) systems, and manufactured products. The technology can be joined with PIN, biometric, or other means of authentication to enhance security.

---

[63] AOL teamed with RSA to offer AOL subscribers for a small monthly fee a SecureID device to use in addition to their user IDs and passwords. Anick Jesdanun, "AOL Moves Beyond Passwords for Log-Ons," Associated Press Online, September 20, 2004. VeriSign also teamed with RSA Security to offer a two-factor authentication solution that continually generates unique one-time use passwords. Dennis Fisher, "Changing the Face of Passwords; VeriSign, RSA to unveil two-factor solutions," eWeek, September 20, 2004.

[64] "New Tokens with Fingerprint Scanners Enter Authentication Market," CardTechnology.com, August 2004. See www.cardtechnology.com.

[65] Lavonne Kuykendall, "Discover Backs Biometric Payments Vendor," American Banker, September 1, 2004.

[66] "MC to Test Pay Pass in Canada," American Banker, September 24, 2004.

However, because RFID tags do not have to be in contact with a person to be read, unlike smart cards, RFID tags may have some security vulnerabilities that smart cards do not. RFID technology, however, offers distant communication that smart cards cannot.[67]

RFID technology will be used in passport issuance and may also be used in some jurisdictions in drivers' licenses. The U.S. Food and Drug Administration has approved tags for implantation in humans. Currently, a Florida theme park has issued RFID tags implanted in wristbands to help visitors keep track of members of their group.[68] While RFID can be used for enhanced security, it is also a technology that can improve the convenience of payments transactions through contactless payments devices.

Cryptography

Cryptography can be used to protect information from unauthorized access (confidentiality), assure that data has not been altered (integrity), prevent the sender from denying he sent a message or the receiver from denying he received it (non-repudiation), and to authenticate that information has come from the source that claims to have transferred it (authentication). Using a special value, referred to as a "key", and employing mathematical algorithms, cryptography is used to convert readable text or data (called plaintext) into a non-readable ciphertext. Cryptographic methods can be used to protect information in storage or in transmission, including over the Internet.[69] They cab be complex systems.

Symmetric or secret key cryptography requires both the sender and the receiver to use the same algorithm and same key. Generally, symmetric algorithms are public knowledge and not kept secret. Instead, the focus of security is on protecting the key. There is a wide range of techniques available to protect the key: some involve dissemination and storage, while others may involve encrypting the key itself.[70] The greatest limitation of a symmetric system is the Key Management System required to distribute (through a secure channel), revoke, and support the users.

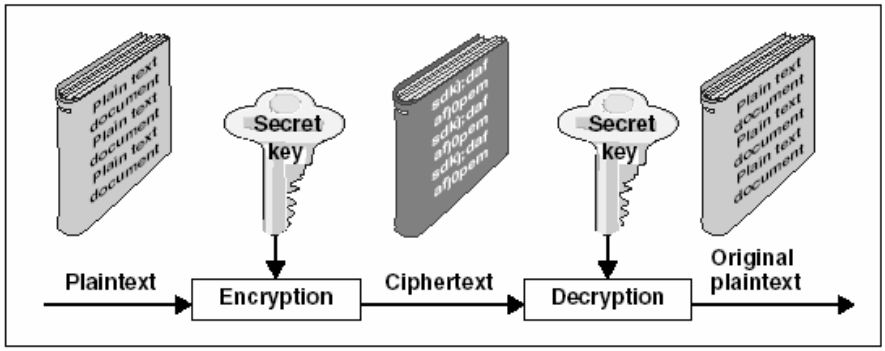
---

[67] Andy Dornan, "Smart Cards and RFID Are Not the Same," Network Magazine, InternetWeek, October 26, 2004.

[68] Alorie Gilbert, "Theme park takes visitors to RFID-land," CNET News.com, September 14, 2004.

[69] U.S. GAO, Information Security Technologies to Secure Federal Systems, p. 40.

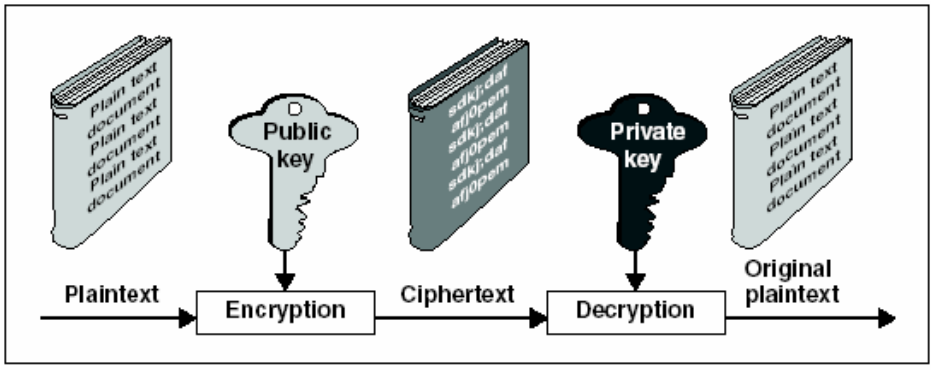
[70] Standards are in place for key generation making it very difficult, if not impractical to guess the value of the key. For example, using the Triple Digital Encryption Standard (3DES), employing a 56-bit key, generates over 72 quadrillion possible values.



Source: GAO analysis.

Figure 3. Encryption and Decryption with a Symmetric Algorithm[71]

Asymmetric or public key cryptography uses *two* keys: one that is *private* (user) and the other that is *public* (published). If a user needs to send a message to a group of people, which requires a high degree of assurance that the originator is who he claims to be, the user would encrypt the message using the private key. Only recipients with the corresponding public key would be able to decrypt the message. The two keys work in concert, when one key is used for encryption, only the second key can be used to decrypt. Therefore, if a user encrypted a message using a public key, only a specific individual with the private key would be able to decrypt the message. One major limitation of asymmetric systems is the practicality of all users having associations with other users in order to make use of public keys.



Source: GAO analysis.

Figure 4. Encryption and Decryption with a Public Key Algorithm[72]

These cryptographic systems depend on sound information security policies and procedures. If the underlying plaintext or the key is compromised, the system will fail regardless of the technology deployed. Development, distribution, management and security of the keys are

---

[71] U. S. GAO, Information Security Technologies to Secure Federal Systems, p. 41.

[72] U. S. GAO, Information Security Technologies to Secure Federal Systems, p. 42. See also, Electronic Authentication Issues relating to its selection and use, eSecurity Task Group, Business Facilitation Steering Group, APEC Telecommunications and Information Working Group, Asia-Pacific Economic Cooperation (APEC) Secretariat, 2002, pp. 32-33.

crucial not only to the smooth functioning of the system, but to maintaining the high degree of information protection expected. Keys can be changed frequently to avoid their being compromised, but this does add to the complexity of developing and maintaining the system. Sometimes symmetric and asymmetric systems are combined for greater efficiency and effectiveness.

Digital certificates are credentials that associate a specific user with his or her specific public key. In this way the certificate can be used to verify that a sender of a message is who he claims to be, and the recipient can send an encoded reply. Trusted third parties, Certificate Authorities, generate digital certificates. The certificate may be published in a repository or made available by other means such as in an online database of certificates available for retrieval and use in verifying digital signatures. Digital signatures and the supporting public key infrastructure (PKI) can be used in online transactions and electronic commerce to authenticate parties to Internet transactions. The application can be adapted to the physical world.[73]

Other new approaches combine public key encryption technology with smart cards to verify the legitimacy of the transaction. Deployment of such a PKI combats identity theft by guaranteeing that a transaction is being triggered by a properly-issued token (*e.g.*, credit card, mobile phone). However, as with PIN- and password-based systems, PKI does not fully protect the consumer or financial institution from thefts caused by stolen cards.

While innovative technologies for improving authentication of people and transactions are continually brought to market, they face numerous market place hurdles. They need to be easy for end-users to use, effective in delivering strong authentication, and the cost must be justifiable compared to the alternative technologies. New technologies or systems that handle data must be managed over time, so the resources it will take to maintain the system also are important considerations. Purchasers also may look for the product to be compatible with respect to existing equipment or technologies and to offer multi-purpose capability.

Consumer Expectations

A recent consumer survey conducted by the Ponemon Institute showed that 77 percent of the respondents expect that certain types of organizations and entities have stronger verification safeguards in place than others. Eighty-nine percent of the respondents said that banks should have strong identity verification and authentication safeguards in place, and 76 percent believe they do. Ninety-four percent said that credit card companies also should have strong safeguards, and 68 percent believe they do.[74] Consumer expectations are high; and while consumer confidence lags expectations, confidence also remains high.

---

[73] "Heightened Security: Can Financial Institutions Really Know Their Customers?," Star Systems (2002), p. 26.

[74] Dr. Larry Ponemon, Consumer Survey on Identity Management, (Tucson, AZ: Ponemon Institute, October 2004). The survey reached a sample of more than 7300 potential respondents who were at least 18 years old, and is based on the net response of 1041 individuals.

Forty-four percent of the respondents to the survey said they knew someone who was a victim of identity theft, and 6 percent identified themselves as victims. At the same time, two-thirds of the respondents said they are more concerned about being denied access to their personal information because the organization's identity management is not working, than about obtaining access without proper proof. Seventy-percent of the respondents said they would use biometrics to verify their identity, but 88 percent of those respondents would do so for convenience, while 56 percent of those respondents would use biometrics principally because they would be more secure. These survey results are consistent with public comments received in connection with this report and from discussions with representatives of various institutions, businesses, associations and research groups. Consumers seem to favor improvements in the security applied to their personal financial information, but they also appear to prize convenience very highly as well.

Some citizens feel strongly that less sharing of information, not more, is the better approach to combating identity theft. One response to the Treasury request for public comment of March 2, 2004, offers a number of recommendations for combating identity theft that focus on changing existing credit granting practices. The remedies would further restrict the disclosure of consumers' personal information.[75] For some individuals the creation of large databases also poses serious concerns about who will control access to the data and who will be able to obtain access, regardless of initial intentions. Many of these citizens look to the implementation of well-known fair information practices to protect personal information.[76]

Conclusion

Financial sector institutions have employed various methods productively for many years to identify, verify, and authenticate new and on-going customers and their transactions. PIN-and-password protections and point-of-sale authorization procedures remain the most widely used applications for deterring identity theft.

---

[75] Comments of the Electronic Privacy Information Center, April 1, 2004. This commenter views credit issuers as too lax in their marketing and authenticating efforts, and would reduce errors by having credit applications be reviewed more carefully for obvious errors or inconsistencies. The commenter also believes that standards for obtaining credit reports are too weak, and competition for new customers leads lenders to mail offers that can easily be stolen and to grant credit too quickly. Improvements in the way online retailers store sensitive customer information, and in the way financial institutions provide information to telemarketers would, in this commenter's view, reduce the likelihood of abuse. Similarly, reducing the use of the Social Security number as a record locator and personal identifier could help to reduce identity theft.

[76] Fair information practices have been articulated by various inter-governmental, governmental, private sector, and non-profit organizations, all based on a code developed in 1973 by an advisory committee in the U.S. Department of Health, Education, and Welfare. All include at least some of the following practices: limit the collection of information; ensure that the information is relevant and accurate; explain the purpose for collecting it; explain to the consumer his options for directing the way in which the information will be used; secure the information from loss, destruction, unauthorized disclosure and inappropriate use; let consumers know how to correct errors; and hold the data collector accountable for handling the information according to the established rules. Who Goes There? Authentication Through the Lens of Privacy, pp. 71-73.

As representatives of the securities industry have indicated, biometrics in combination with other factors is promising. However, there still is little actual deployment compared with cards or tokens, or User ID and passwords together with anomalous behavior detection.

The use of smart cards and PKI to supplement these tools has received some attention, but they add to overall costs significantly. Neither technology is in general use throughout the industry. One respondent to Treasury's March 2004 request for public comment expressed the view that the stronger authentication technologies like smart cards and smart tokens or fobs tend to be associated with commercial online transactions in the United States.[77] The knowledge-based "out of wallet questions" tend to be used more commonly for additional authentication in retail online banking.

At the same time, new products for identifying individuals, new payment devices, and new measures for authorizing financial transactions more accurately reach the market in response to new challenges from identity thieves and cyber criminals. The financial sector is sufficiently diversified and potential applications sufficiently diverse to encourage development of solutions to complex problems as they emerge.

[77] U.S. Bancorp announced that it hired VeriSign Inc. to secure customer access to online commercial banking services through multifactor authentication. U.S. Bancorp will provide universal serial bus tokens to more than 10,000 commercial banking customers for their online connections and will use VeriSign's Unified Authentication service to validate and secure interactions with the commercial banking customers. Paul Roberts, "Strong Authentication A Hard Sell for Banks," IDG News Service, November 2, 2004.

Chapter III

BIOMETRIC TECHNOLOGIES: WHAT THEY ARE, HOW THEY ARE USED, AND HOW THEY ARE ASSESSED

Biometric technologies have the potential to provide convincing evidence of who actually performs a given financial transaction, because each person's biometric characteristics are thought to be unique and difficult to reproduce. Biometric technologies work by measuring and analyzing human physiological or behavioral characteristics. Physiological characteristics are those associated with a part of the body. The fingerprint is probably the best known example; however, face and hand shape, and retina and iris patterns are also examples of physiological characteristics. Behavioral characteristics are based on data derived from a person's actions. For example, the way a person speaks, writes (*i.e.*, forms characters and words), or types are examples of behavioral characteristics.

Biometric traits are less susceptible to duplication or loss when compared to other authentication methods and, therefore, provide a higher level of security. Unlike conventional identification methods that use something you have—such as a credit card—or something you know—such as a password or personal identification number (PIN)—biometric characteristics are integral to something you are.

Perhaps the most prevalent current use of biometrics is in the area of physical access control systems that limit access to highly sensitive areas to authorized people. However, as with almost any security device, biometrics are not perfect and the technology may be impacted when environmental and physical conditions are not ideal (*e.g.*, injury to a finger or hand, or the presence of dust on scanning devices). These conditions and the impact on user acceptance will be discussed later in the report.

The primary biometric technologies in use today and supported by commercial industries are finger scan, which considers both the fingerprint and finger shape; face and hand geometry; and iris, retina, voice, and signature recognition systems. According to feedback and comments received, fingerprint technologies comprise half of the biometric technology in use.

Theoretically, when biometric technologies are used, the need to remember and protect passwords, PINs, or other secrets may be eliminated. If properly implemented, biometric systems prevent the sharing of secrets that could be used fraudulently. For example, customers would no longer need to share private, sensitive, or personal information with cashiers, customer representatives, or other financial institution employees while conducting a routine business transaction.

What Biometric Systems Are

How Biometric Systems Work

Biometric systems are comprised of a two process solution: (1) a thorough enrollment process and (2) an effective matching process. It was clear from both the public comments and consultations that enrollment is the most critical step when using a biometric technology. It is the step that binds a user to an identity. It relies on the user establishing his or her identity by presenting a birth certificate, passport, or other identity document. If the document is deemed authentic, the person's identity is established and the process continues.

Once the user verifies his or her identity, the individual presents the applicable biometric information (*e.g.*, fingers, hand, or iris) by using a biometric device (*e.g.*, scanner or camera). The distinctive features are extracted, encoded, and stored as a reference template for future comparisons. As a final step, the biometric is linked to the biographic identity (*i.e.*, legal name and address; date of birth; gender; and other identifiers such as eye and hair color, weight and height) and other relevant information, depending on the application.

The amount of computer memory that most reference templates use is relatively small and varies depending on the vendor and the technology. Templates can be stored remotely in a central database, within a biometric reader device itself, or on a smart card or token. Table 1 presents the leading biometric technologies and their template size as noted by the Government Accountability Office (GAO) in a November 2002 report. Responses received from public comment and during the consultations were consistent with these values and ranges.

Table 1. Leading Biometric Technologies and their Template Size[78]

Technology	How it works	Template size in bytes
Facial recognition	Captures and compares facial patterns	84 or 1,300*
Fingerprint recognition	Captures and compares fingerprint patterns	250-1,000
Hand geometry	Measures and compares dimensions of hands and fingers	9
Iris recognition	Captures and compares iris patterns	512
Retina recognition	Captures and compares retina patterns	96
Signature recognition	Captures and compares rhythm, acceleration, and pressure flow of signature	1,000-3,000
Speaker recognition	Captures and compares cadence, pitch, and tone of vocal tract	10,000-20,000

* Depending on the algorithm.
Source: GAO analysis of manufacturer data.

Preventing identity fraud during the enrollment process is critical. The vetting process for binding a biometric against an identity must be carefully designed so that it does not introduce a security risk at the point of enrollment. An identity thief may already have the victim's Social Security number or other personal information, including fraudulent documents such as a false driver's license in the victim's name with the thief's picture. If an identity thief can enroll his or her own biometrics with the stolen identity—before the rightful owner of the

[78] U.S. GAO, Using Biometrics for Border Security, (Washington, DC: GAO, November 2002), p. 46.

identity realizes it has been stolen—the thief can make a successful biometric claim against that stolen identity.

Fraudulent identities may also be detected during the enrollment process. For example, if a user has already established an identity with an organization (either a true or false identity) and he or she attempts to create a second identity using the same biometric data (*i.e.*, fingerprint, iris scan, hand geometry, etc.), the system should detect that the biometric data is already registered and identify the first and second enrollment as potential wrongdoing.

When some states began adding a biometric component to their drivers' license issuing processes, officials were surprised at the number of people who attempted to obtain second and third fraudulent licenses in someone else's name. When the fraudster presented his or her biometric data during enrollment, the systems flagged the person as already having a driver's license or state identification card. A representative from the state of Colorado Department of Motor Vehicles indicated that they identify approximately 15 to 20 attempts at obtaining fraudulent drivers' licenses or a state-issued, non-driver identification cards each month.

Once a user is enrolled in a biometric system with an organization, the user will subsequently present his or her biometric data and the system will compare it to what was captured at enrollment during the "matching" process. The process of matching compares presented biometric data against what is already collected in a repository. During matching, the chosen biometric is scanned and compared to the stored template. If a match is found, a matching score is generated (based on the type of biometric and confidence of a match) and provided. The matching score is then evaluated by comparing the score to a preset value established as a threshold for the particular business application in question. A low risk transaction usually has a low threshold value, while a potentially costly or high-risk transaction may require high confidence in the biometric match. Finally, a secure audit trail of system usage is recorded. The biometric verification provides added assurance that the legitimate user is accessing the system. Figure 5 shows the relationship of the enrollment and matching processes.

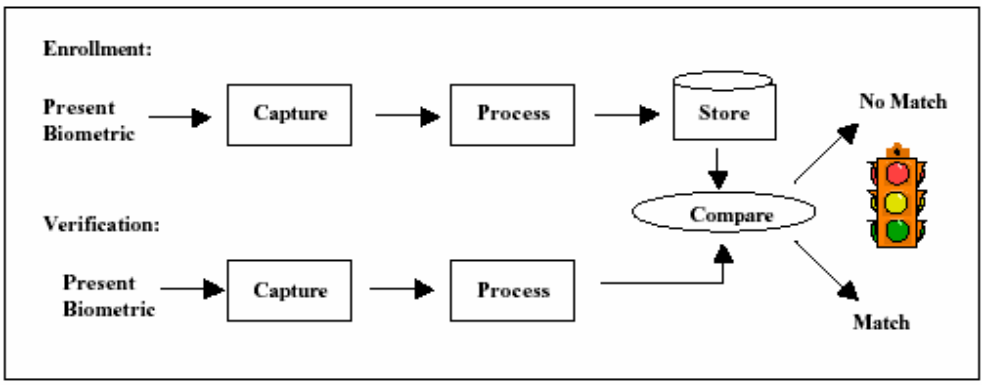


Figure 5. The Relationship Between Enrollment and Matching[79]

[79] F.L. Podio and J.S. Dunn, Biometric authentication technology: From the movies to your desktop, National Institute of Standards and Technology (NIST), Biometrics Resource Center Website, Retrieved October 13, 2004, p. 2. See http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf.

The actual matching process may operate in one of two distinct ways. The process may (1) verify a user or (2) identify a user. The process to verify a user—referred to as one-to-one matching—is the basis for authentication systems. When a person makes an identity claim in conjunction with presenting biometric data, the presented biometric data is compared against a reference biometric already established for that identity to determine if there is a match. The reference biometric may be stored in either a local repository or on a portable device, such as a smart card or token carried by the user.

The process to identify a user—referred to as one-to-many matching—occurs when a person's biometric data is presented with no identity claim and the presented biometric data is compared against the entire database of collected reference biometrics to determine the most likely identity. In this case, the reference biometrics are stored in a repository that can be continually updated with new biometric templates as appropriate. Figure 6 illustrates the matching processes for verifying versus identifying a user.

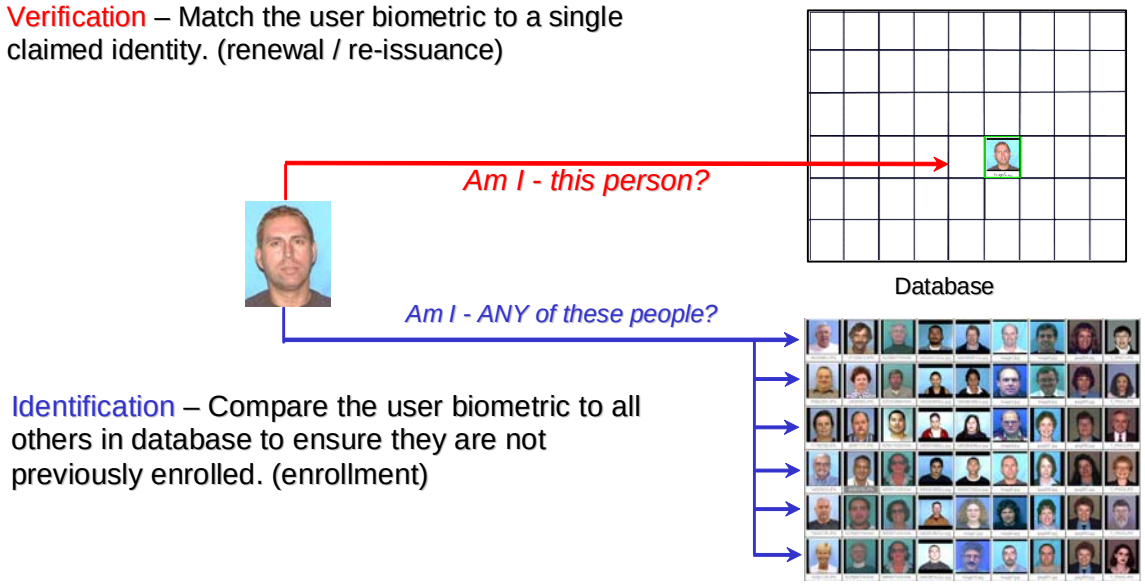


Figure 6. Sample Matching Process[80]

A third type of matching—called "watch list" matching and often referred to as one-to-few matching—is similar to identification matching. In this process, the presented biometric is compared against a smaller collection of reference biometrics. For example, the watch list reference biometrics may be comprised of wanted criminals or terrorists and matching may be used to determine if the individual is a security risk.

[80] Ian Williams, "Biometric Technology for DLID, An introduction to the science," prepared for Canada Day at DLID Summit, Houston, Texas, February 29, 2004. See www.idsysgroup.com.

Types of Biometric Technologies

Fingerprint Recognition

Fingerprint recognition has one of the longest histories of any biometric in use today. Since its introduction as a law enforcement tool in the late 1800s, it has become the primary law enforcement identification method used around the world. Historically, fingerprints were made by coating the fingertips with ink and transferring the pattern to paper or another surface. Fingerprints were then manually compared to determine matches and non-matches.

The use of computer technology, starting in the 1960s, allowed the law enforcement community to automate the labor-intensive activity of manually comparing fingerprints. Automated fingerprint identification systems are used by federal, state and local law enforcement agencies for criminal justice applications and civil agencies for background checks. These systems are typically designed to exchange information with the FBI's Integrated Automated Fingerprint Identification System (IAFIS).[81] Although automated, most of the fingerprints in these systems were initially captured using ink and paper.

Biometrics have allowed the law enforcement community and others to move away from ink and paper capture of fingerprints to "live-scan" image capture. Live-scan fingerprint images are scanned, measured, converted into biometric templates, and instantaneously stored in databases for future comparisons. A live-scan fingerprint is obtained directly from the finger without the intermediate use of paper. The most popular algorithm used to create the fingerprint biometric template measures minutiae points, or the breaks, in fingertip ridges. For example, ridge endings (where a ridge ends) and bifurcations (where a single ridge divides into two) comprise most such minutiae. A typical fingerprint image (figure 7) may produce between 15 and 50 minutiae points, depending on the portion of the image captured.

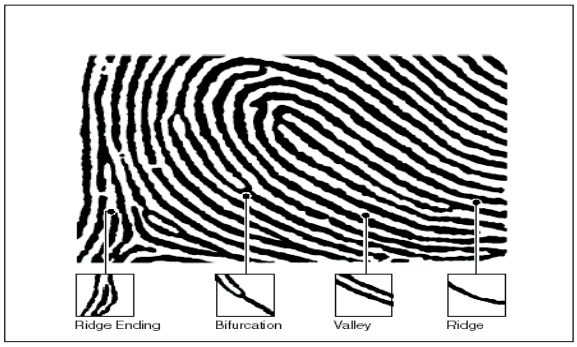


Figure 7. Common Fingerprint Features[82]

[81] IAFIS is a national fingerprint and criminal history system maintained by the FBI's Criminal Justice Information Services Division. The IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information for more than 47 million subjects in the Criminal Master File.

[82] U.S. GAO, Using Biometrics for Border Security.

While identifying minutiae, the algorithm searches the fingerprint image and filters out distortions and false minutiae caused by scars, sweat, or grime. Once the minutiae are identified, their exact locations are recorded and their angles are measured (typically by the direction of a ridge or valley ending). For each established minutiae point, neighboring minutiae and the number of ridges in between are recorded. Because of differences in the determination, placement, and analysis of minutiae points, no two algorithms can be expected to yield the same template from a given fingerprint.[83] Figure 8 depicts a graphic representation of this process.

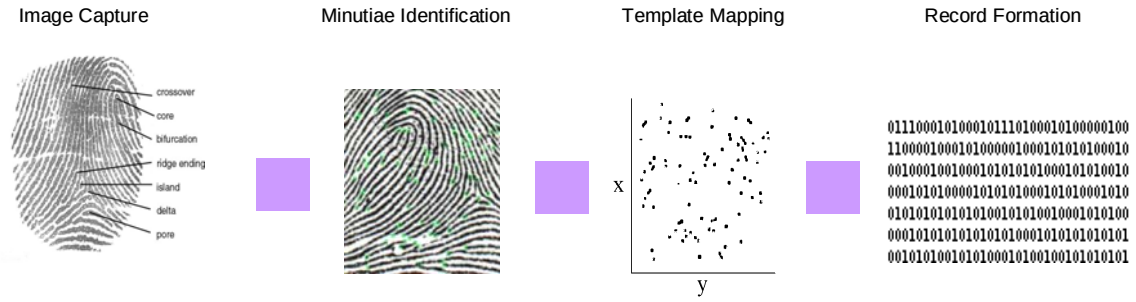


Figure 8. Common Finger Scan Process[84]

Fingerprints can be either flat or rolled. A flat fingerprint is limited to an impression of the central area of the finger between the fingertip and the first knuckle. Rolled fingerprint images capture more fingerprint area, acquiring the ridges on both sides of the finger as well, and perform better when matching against like images.[85] Logistically, rolled fingerprints are more challenging to capture, as they typically require the assistance of a trained attendant in a more controlled environment. This practice typically results in higher costs that have somewhat limited the use of rolled fingerprint recognition from gaining acceptance as a convenient and economical biometric identification method. The introduction of inexpensive, "Live-Scan" flat fingerprint capture devices and the development of reliable matching algorithms in recent years are setting the stage for fingerprint authentication technology to progress to more widespread use in a variety of unattended applications.

Three types of scanners are typically used: (1) optical scanners, (2) silicon-based scanners, and (3) ultrasound scanners. Optical scan technology is the oldest of the three and is the one most commonly used. Optical scanners use the same light sensor system used in digital cameras and camcorders to record a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (a finger, for example). Silicon-based scanners are generally smaller than optical scanners and the image quality is generally better. In silicon chip-based scanners, a coated chip measures skin

---

[83] U.S. GAO, Using Biometrics for Border Security.

[84] Williams, Biometric Technology for DLID, An Introduction to the Science.

[85] NIST, Studies of Plain to Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed, NIST IR 7112, Gaithersburg, MD, April 2004. See ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7112.pdf.

capacitance to discover the ridge pattern in the fingerprint. Small silicon scanners (smaller than a postage stamp and thinner than a dime) provide a low cost option for notebook computers, cellular phones, or personal digital assistants (PDAs). Ultrasound scanners generate an image (shape) of the live skin layer buried beneath the surface of the finger, which is seldom affected by damage or wear to the finger surface.

More devices are available for reading fingerprints than for any other biometric. Compared to alternative biometrics solutions, fingerprints are associated with lower cost, greater ease of use, and smaller device size. Keyboard manufacturers are already beginning to integrate fingerprint devices into keyboards, thus boosting opportunities for consumer acceptance in the longer term.

Face Recognition

Face recognition—the acquisition, segmenting, and matching of a given face against a database of faces—is a non-intrusive biometric method dating back to the 1960s. For over 30 years, the majority of work in face recognition has focused on use of two-dimensional images, using legacy data (*e.g.*, drivers' licenses, criminal photographs) for matching of images. Three-dimensional scanning and imaging has been used in several industries for years, and appears to be a natural progression as a biometric technology. Industries which have traditionally used three-dimensional scanners include health and fitness, fashion, automotive, cosmetic, geological, academic, museum, nuclear power, and aerospace.

Although face recognition can be less accurate than fingerprints, face recognition tends to be less invasive. Most of today's face recognition systems use appearance-based classifiers or attempt to measure some nodal points on the face—such as the distance between the eyes, the width of the nose, the distance from eye to mouth, or the length of the jaw line. Figure 9 is a notional flow of a simple facial recognition system.

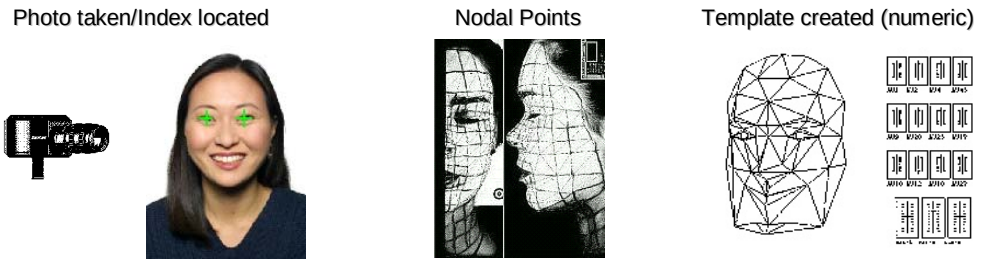


Figure 9. Facial Recognition System[86]

Two-dimensional face recognition has traditionally experienced some obstacles which three-dimensional face recognition partially or fully eliminates: (1) consistent illumination of a face and the corresponding shadows; (2) common orientation or pose of a face; and (3) varying facial expressions. Due to the richer set of three-dimensional geometric clues, including range information (*e.g.*, depth), face detection can be simplified. The inherent ability of three-

[86] Ian Williams, Biometric Technology for DLID, An Introduction to the Science.

dimensional face recognition systems to partially or fully compensate for pose, illumination, and expression may be needed in scenarios in which the capture environment is not controlled, such as at an ATM. Most ATMs do not have controlled lighting and require a specific pose or expression.

The large number of databases containing facial images (*i.e.*, driver's license enrollment) and the International Civil Aviation Organization's (ICAO) recent decision to include a facial biometric in passports or related travel documents, will boost the use of facial recognition technologies. However, facial recognition technology requires large investments in peripheral hardware. Overall, this type of biometric is expected to find its greatest utility in law enforcement, as facial databases are created to facilitate the capture of criminals. Facial scanning devices typically would be installed in police stations, airports, immigration offices, etc.

Hand Geometry

Hand geometry systems use an optical camera to capture two orthogonal two-dimensional images of the palm and sides of the hand, offering a balance of reliability and relative ease of use. They typically collect more than 90 dimensional measurements, including finger width, height, and length; distances between joints; and knuckle shapes. These systems rely on geometry and do not read fingerprints or palm prints. Although the basic shape and size of an individual's hand remains relatively stable, the shape and size of our hands are not highly distinctive. The system is not well suited for performing one-to-many identification matches. Hand geometry readers can function in extreme temperatures and are not impacted by dirty hands (as fingerprint sensors can be). Hand geometry devices are able to withstand wide changes in temperature and function in a dusty environment. They are commonly used for access control to facilities, time clocks, or controlled areas. Figure 10 shows a hand geometry system.

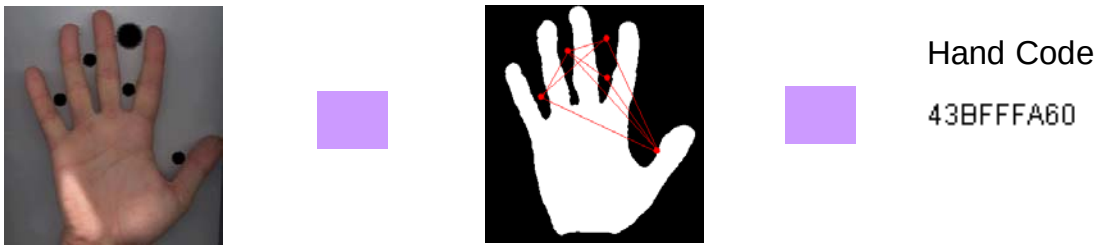


Figure 10. Hand Geometry System[87]

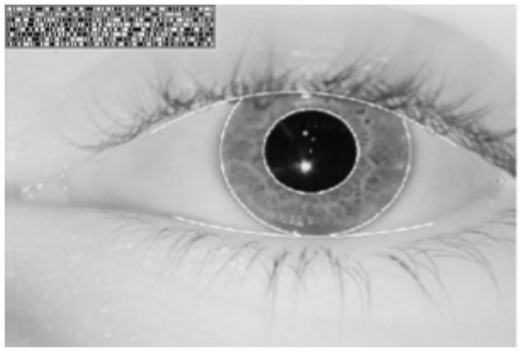
The large size of the actual hand geometry readers restricts their use in widespread applications such as those requiring a small user interfaces (*e.g.*, home computer user, keyboard). Hand-geometry readers could be appropriate for multiple users or where users access the system infrequently and are perhaps less disciplined in their approach to the system. Today, organizations are using hand-geometry readers in various scenarios, primarily for physical access control and recording work time and attendance. They are also used for the known traveler

[87] Ian Williams, Biometric Technology for DLID, An Introduction to the Science.

programs, such as the Transportation Security Administration's Registered Passenger Program, for streamlining airport security procedures for certain frequent travelers.

Iris Recognition

Iris recognition technology looks at the unique characteristics of the iris, the colored area surrounding the pupil (Figure 11). While most biometrics have 13 to 60 distinct characteristics, the iris is said to have 266 unique spots.[88] Each eye is believed to be unique and remain stable over time and across environments (*e.g.*, weather, climate, occupational differences).



Source: Dr. John Daugman, Cambridge University, Cambridge, U.K.

Figure 11. Iris Template Features[89]

Iris recognition systems use small, high-quality cameras to capture a black and white high-resolution photograph of the iris. Once the image is captured, the iris' elastic connective tissue—called the trabecular meshwork—is analyzed, processed into an optical "fingerprint," and translated into a digital form. Figure 12 depicts the process of generating an iris biometric. Given the stable physical traits of the iris, this technology is considered to be one of the safest, fastest, and most accurate, noninvasive biometric technologies. This type of biometric scanning works with glasses and contact lenses in place. Therefore, iris scan biometrics may be more useful for higher risk interactions, such as building access. Improvements in ease of use and system integration are expected as new products are brought to market.

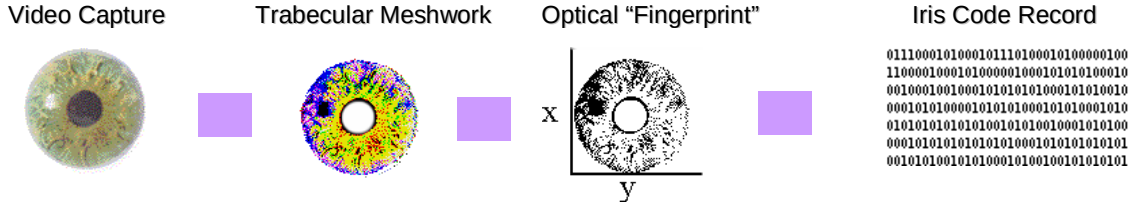


Figure 12. Mapping the Eye for Iris Recognition Systems[90]

---

[88] U.S. GAO, Using Biometrics for Border Security, p. 193.

[89] U.S. GAO, Using Biometrics for Border Security, p. 196.

[90] Ian Williams, Biometric Technology for DLID, An Introduction to the Science.

Voice Verification

Voice verification technology uses the different characteristics of a person's voice to discriminate between speakers. These characteristics are based on both physiological and behavioral components. The physical shape of the vocal tract is the primary physiological component. The vocal tract is made up the oral and nasal air passages that work with the movement of the mouth, jaw, tongue, pharynx and larynx to articulate and control speech production. "The physical characteristics of these airways impart measurable acoustic patters on the speech that is produced," as one expert explained.[91] The behavioral component is made up of movement, manner, and pronunciation.

The combination of the unique physiology and behavioral aspects of speaking enable verification of the identity of the person who is speaking. Voice verification technology works by converting a spoken phrase from analog to digital format and extracting the distinctive vocal characteristics, such as pitch, cadence, and tone, to establish a speaker model or voiceprint. A template is then generated and stored for future comparisons.

Voice verification systems can be text dependent, text independent, or a combination of the two. Text dependent systems require a person to speak a predetermined word or phrase. This information, known as a "pass phrase," can be a piece of information such as a name, birth city, favorite color or a sequence of numbers. The pass phrase is then compared to a sample captured during enrollment. Text independent systems recognize a speaker without requiring a predefined pass phrase. It operates on speech inputs of longer duration so that it has a greater opportunity to identify the distinctive vocal characteristics (*i.e.*, pitch, cadence, tone).

Voice verification systems can be used to verify a person's claimed identity or to identify a particular person. It is often used where voice is the only available biometric identifier, such as over the telephone. Voice verification systems may require minimal hardware investment as most personal computers already contain a microphone. The downside to the technology is that, although advances have been made in recognizing the human voice, ambient temperature, stress, disease, medications, and other physical changes can negatively impact automated recognition.

Voice verification systems are different from voice recognition systems although the two are often confused. Voice recognition is used to translate the spoken word into a specific response, while voice verification verifies the vocal characteristics against those associated with the enrolled user. The goal of voice recognition systems is simply to understand the spoken word, not to establish the identity of the speaker. A familiar example of voice recognition systems is that of an automated call center asking a user to "press the number one on his phone keypad or say the word 'one'." In this case, the system is not verifying the identity of the person who says the word "one"; it is merely checking that the word "one" was said instead of another option.

[91] John D. Woodward, Nicholas M. Orlans, and Peter T. Higgens, Biometrics: Identity Assurance in the Information Age (Berkeley, CA: McGraw-Hill/Osborn, 2003), p. 78.

Dynamic Signature Recognition and Keystroke Scanning

Dynamic signature recognition is a behavioral authentication method used to recognize an individual's handwritten signature. This technology actually measures how a signature is signed by treating the signature as a series of movements that contain unique biometric data, such as rhythm, acceleration, pressure, and flow. The signature is captured when a person signs his or her name on a digitized graphics tablet, which can be attached to a computer or part of a PDA. The signature dynamics information is encrypted and compressed into a template.

Dynamic signature recognition technology can also track a person's natural signature fluctuations over time. Dynamic signature recognition systems are different from electronic signature capture systems, which treat the signature as a graphic image. Electronic signature capture systems are commonly used by merchants to capture electronic signatures in the authorization of credit card transactions.

Keystroke scanning is another behavior technique. This technology uses samples from the keyboard at a very high rate (thousands of times per second) and analyzes the way a user types. The user is required to enter a script or key words (repeatedly) during enrollment. The most common use for keystroke scanning is to "harden" passwords. That is, it requires the password to be entered in a fashion consistent with the intended user. Unlike most other biometric technologies, keystroke scanning does not require any extra hardware or capture device. Keystroke dynamics are captured solely by software. Keystroke scanning may be used for a single authentication event or for continuous monitoring. Continuous monitoring may be used to ensure that only authorized use of an unattended computer. In other words, it the software determines that an unauthorized user has begun using a computer, because their keystroke dynamics are different from the registered, authorized user, it can shut down to prevent misuse.

Other Biometric Technologies

There are a number of other biometric technologies available. Some are early in their development and may not yet provide sufficient results (*e.g.*, result accuracy, cost effectiveness, timeliness) for practical implementation. As a summary, Table 2**,** on the following page, describes some of the emerging biometric technologies that were considered by the Government Accountability Office in its November 2002 report on Using Biometrics for Border Security.

Table 2. Emerging Biometric Technologies and their Maturity[92]

Technology	How it works	Maturity
Vein scan	Captures images of blood vessel patterns.	Commercially available.
Facial thermography	Infrared camera detects heat patters created by the branching of blood vessels and emitted from the skin.	Initial commercialization attempts failed because of high cost.
DNA matching	Compares accrual samples of DNA rather than templates generated from samples.	Many years from implementation.
Odor sensing	Captures the volatile chemicals that the skin's pores emit.	Years away from commercial release.
Blood pulse measurement	Infrared sensors measure blood pulse on a finger.	Experimental.
Skin pattern recognition	Extracts distinct optical patters by spectroscopic measurement of light scattered by the skin.	Emerging.
Nailbed identification	An interferometer detects phase changes in back-scattered light shone on the fingernail; reconstructs distinct dimensions of the nailbed and generates a one-dimensional map.	Emerging.
Gain recognition	Captures a sequence of images to derive and analyze motion characteristics.	Emerging; requires further development.
Ear shape recognition	Is based on distinctive ear shape and the structure of the cartilaginous, projecting portion of the outer ear.	Still a research topic.

Source: GAO analysis.

Using Multiple Biometric Technologies (Multimodal Systems)

An area of growing interest is the combination of multiple biometric technologies into "multimodal" systems. Most current biometric applications concentrate on a single biometric type (*e.g.*, fingerprint or iris recognition). However, the suitability of each type to a given application depends on various factors, including the attitudes of users and operational environments and conditions. A single type of biometric may not always be appropriate, convenient, or available. Therefore, researchers are exploring the use of multimodal systems for authentication that is required to be robust in natural environments (*e.g.*, in the presence of noise and illumination changes). Through the fusion of biometric data (*e.g.*, finger and face), it may be possible to provide a more statistically significant biometric. Early combinations include the use of finger, face and iris recognition into coherent biometric approaches.

At least one expert has indicated that biometric technologies currently fall into the following order of preference and biometric market share generally:[93]

Fingerprint recognition: 47-49%
Face recognition: 10-12 %
Hand Geometry: 10-12%
Iris recognition: 8-10 %
Voice verification: 5-6%
Dynamic signature recognition: 1-2 %

[92] U.S. GAO, Using Biometrics for Border Security, (Washington, DC: U.S. GAO, November 2002), p. 50.

[93] Joe Turek, "An Industry Group Viewpoint: Biometrics," SIA News, August 2004, p 20.

How Biometrics Are Being Used

The largest user of biometric technologies today is the federal government. Programs and initiatives are being undertaken by the Department of Homeland Security (DHS), the State Department, the Department of Defense (DoD), and others. For example, the DHS is using biometrics in its United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which calls for fingerprinting, photographing and running checks on suspicious visitors, has been in place at U.S. airports and seaports since January 5, 2004. The extra security requirements are being tested at border crossing gateways from Mexico at Laredo, Texas and Douglas, Arizona, and from Canada at Port Huron, Michigan, and are scheduled to be used at all 165 land border crossings in to the United States by the end of 2005. The US-VISIT program uses digital fingerscans and photos that are compared against databases to determine if visitors are wanted for immigration problems or are barred from entering the U.S. because of suspected terrorist ties. The system was developed in response to the September 11, 2001, terrorist attacks and has been in place for nearly all non-U.S. citizens since January 2004.

The DHS is also using biometrics in the development of a program to improve security at seaports, airports, rail, trucking and mass transit facilities by creating a nationwide credential that will prevent unauthorized persons from gaining access to secure areas. The credentials, called Transportation Worker Identification Credentials (TWIC), will be issued to transportation workers after thorough screening for ties to terrorism. The TWIC will be a tamper-resistant credential that contains biometric information about the worker. By using biometric data, each transportation facility will be able to verify the identity of a worker and prevent unauthorized individuals from accessing secure areas. The nationwide card will also eliminate the need for workers to obtain multiple credentials thereby making the identification process faster and more efficient.

The International Civil Aviation Organization (ICAO), an international inter-governmental organization, recently changed its policies to include a facial biometric in passports or related travel documents. To be consistent with this policy change, the U.S. State Department is developing a passport that contains biometric technology to authenticate the identities of U.S. citizens who travel abroad. Similarly Ministers for European Union member states and other countries have agreed to adopt biometric passports as well. The new passport documents are intended to be more secure, as they would include certain biographic data along with the traditional photograph of the passport holder. The European push for biometrics is heavily influenced by a U.S. policy change for passports for people from "visa waiver" countries. By October 26, 2005, all visitors from these countries will have to provide a machine-readable passport with biometric data.

The DoD's Common Access Card (CAC) serves as an identification card and is designed to enable authorized physical access to installations, buildings, and controlled spaces, as well as to gain access to military computer networks and systems. The CAC is a smart card with an embedded computer chip that is part of the DoD's nationwide effort to improve security at its installations worldwide. The CAC is intended to be the standard identification card for all active-duty military personnel, selected Reserve and National Guard, as well as the DoD's civilian employees and eligible contractors. More than one million cards have been issued to

date, with distribution expected to exceed four million in the next two years. The DoD's Biometrics Fusion Center—located in North-Central West Virginia—is working to add biometric technologies for physical access to the CAC.

On August 27, 2004, President George W. Bush issued Homeland Security Presidential Directive (HSPD) 12, which called for the development of a common identification standard for federal employees and contractors. It acknowledged wide variations in the quality and security of forms of identification used across federal agencies and called for a mandatory, government-wide standard. HSPD 12 specifies that the new means of identification should be: based on sound criteria for verifying an employee's identity; strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; rapidly authenticated electronically; and issued only by providers whose reliability has been established by an official accreditation process. It is likely that when the standard is finalized, it will include a biometric element.

In 2003, the U.S. Social Security Administration (SSA) began testing a voice verification system to control access to its Business Services website, where companies report earnings and withholding information about their employees. To use the website, a company must first apply for access and designate a supervisor with approval authority for future requests from employees of the company. The supervisor must also provide a recorded voiceprint. Subsequently, when employees of the company request access to the Business Services website, the designated supervisor is called by an automated system and his or her voice is compared with a previously recorded voiceprint. Once verified, the supervisor can then orally approve or disapprove the request. The system connects the website and the phone system to provide real-time authentication, using the phone system as confirmation. This biometric approach does not require additional hardware such as scanners or readers, works with the existing phone system, and integrates easily with the website.[94]

State Departments of Motor Vehicles (DMVs) are also starting to use biometrics as a tool to combat identity fraud. They are working with state revenue departments, law enforcement officials, and other government agencies to minimize fraud. During consultations, the West Virginia DMV noted it first adopted facial recognition technology in 1997 to help fight driver's license fraud. In 2001, after a recommendation from a task force and a change in legislation, the state of Colorado adopted biometric technology to fight fraud and curtail the issuance of duplicate drivers' licenses. In October 2002, Colorado began a facial recognition program with new applicants. Because Colorado is a central issuance state (all drivers' licenses are issued from one location), the image is sent to the central database where they conduct a "one to many" match. This system allows Colorado to catch fraudulent drivers' licenses. As an added security measure, DMV employees must use fingerprint technology in order to gain access to the central database. The state is pleased with the good quality control that results from the facial recognition system and they catch approximately 15 – 20 fraud cases per month. The state of Colorado DMV paid for the new system with a 70 cent increase in charges to customer per document.

---

[94] Authentify, "U.S. Social Security Administration begins first public testing of voice biometrics with web application developed by Authentify," Press Release, January 20, 2003.
See http://www.authentify.com/news/releases/030120SSA.html.

During discussions with American Association of Motor Vehicles Association (AAMVA), the chief constraint precluding the introduction of biometrics on a nationwide basis involves the fact each individual state DMV functions autonomously. For example, the state of Colorado chose the facial image as its biometric because it already had some ten million photos in its data bank and considered that it was therefore a simple rollout. The state of Georgia,[95] however, has encoded fingerprint data into the bar codes on some 8 million drivers' licenses. Arkansas, California, Texas, Hawaii, and Colorado already collect fingerprints from applicants even though they do not embed the data on licenses.

AAMVA conducted an evaluation of biometric technologies to look at the feasibility of a biometric program to cover all AAMVA jurisdictions and concluded that there were no biometric systems that could convincingly handle a "one to 300 million" matching process.[96] In the report "Phase I: Technical Capability of Biometric Systems to Perform 1:300m Identification," AAMVA, working with the International Biometrics Group (IBG), looked at fingerprint, facial recognition and iris biometric technologies. Although fingerprint technology had the largest databases of records with a few containing more than 10 million, the databases were well short of the 300 million records that the AAMVA system would have. However, the report did note that with the new United States requirements to add facial recognition to passports that follow ICAO standards, the number of facial recognition records will increase.[97]

While the issue of a standardized biometric for drivers' licenses remains unsettled, many states are undertaking efforts to make their drivers' licenses more secure. For example, on November 1, 2004, the Commonwealth of Massachusetts began issuing new state-of-the-art drivers' licenses. The new licenses have digital watermarks in two locations on their front in addition to a new translucent "ghost picture" of the identification holder prominently placed on the front of the card. A new complex background also works to make fraudulent duplication more difficult. Some changes are visible to the naked eye, while others are not. The back of the license features bar codes that contain information relative to the cardholder. States are also beginning to inspect more carefully the identification documents that drivers provide to receive a license. Many have invested in technology that scans documents like passports to verify their authenticity.

The biometrics market is currently experiencing rapid evolution as device multiplicity is increasing and devices that are less intrusive to users are being developed. We are seeing integration of biometric capture devices into computer keyboards, monitors, laptops, cell phones, and PDAs. This increased deployment and use are likely to boost consumer acceptance of biometric technologies. Similarly, biometric capture devices being used by the government, placed in retail environments (*e.g.*, point of sale terminals at cash registers, gas pumps), and used

---

[95] State of Georgia, "Identity Theft Prevention," DMV Stop Identity Theft site. See http://www.stopidentitytheft.org/press/pr_1.html.

[96] American Association of Motor Vehicles (AAMVA), Enhancing Driver's License Administration, Status Report to AAMVA Membership, (Arlington, VA: AAMVA, September 2003), p. 2.

[97] AAMVA, AAMVA UID9 Biometric Identification Report, Phase I: Technical Capability of Biometric Systems to Perform 1:300m Identification, Final Report (New York, NY: International Biometrics Group, 2003), pp. 10-13.

in work environments (*e.g.*, access controls, time and attendance systems) are expected to extend the customer experience and build user confidence over time.

How Biometric Technologies Are Assessed

Public comments received and remarks made during consultations indicate nonetheless that biometric technologies are still regarded as emerging technologies. This commentary highlighted both strengths and considerations associated with biometrics that can be grouped into the following general areas: (1) technological and operational issues (*i.e.*, accuracy, interoperability, and development of standards), (2) cost, and (3) consumer acceptance (*i.e.*, convenience, possible misuse). Each of these areas is discussed in this chapter.

Technology and Operational Issues

As noted, many of the public comments and consultations yielded a message that there are certain key Technology and Operational issues to consider when discussing full-scale implementation of biometric technologies. These include technology maturity, accuracy, interoperability and standardization, security, quality, and reliability. Each of these areas is discussed below.

Maturity

Although the first modern biometric device was introduced on a commercial basis over 25 years ago, biometric vendors continue to operate in an uncertain environment.[98] Biometric technologies represent a typical case study of a technology trying to move from the initial adoption phase to that of critical mass. The e-commerce boom in the 1990s was undoubtedly a key technology growth driver. Increasing needs for identity management and security authentication over the Internet attracted a lot of efforts to promote and utilize the technology. The tragic events of September 11, 2001, and increased concern over security and identity management have dramatically increased the visibility of biometric technologies. In more recent years, biometric technologies have attracted larger investments from multiple sources and market entrants (*i.e.*, hardware and software vendors), and companies are making more substantial investments in R&D. Looking forward, biometrics are projected to mature at a faster pace as most of the government sector contracts for biometric solutions are likely to be awarded in the next five years. One can anticipate that the continuing refinement of biometric systems will help to raise confidence in the reliability of the technology and reduce costs.

Accuracy

Biometric system performance is not 100 percent accurate. For example, the results of a government test in 2003, called the Face Recognition Vendor Test, cast doubt on the accuracy of face-recognition systems. The test used systems from ten leading firms and a database of over

[98] Western Carolina University website, Biometrics Overview discussion points available at: http://et.wcu.edu/aidc/BioWebPages/Biometrics_Introduction.html..

120,000 images of approximately 37,000 people. None of the systems worked well in a formal identification mode when shown a face and asked to identify the subject. However, three of the systems could be used for verifying identity in a controlled environment, such as the booths used to take passport photos.[99]

The effectiveness of a biometric system relies on its ability to discriminate accurately between the biometrics of different people. While biometrics are theoretically 100 percent accurate, in the mass consumer marketplace, perfect accuracy may be an unrealistic objective, particularly given the commercial need for cost effective solutions. If because of inaccuracies, the devices were to authorize the wrong person, access to an account would be given to an unauthorized user. Conversely, if a device fails to authorize a legitimate customer, access to an account would be denied, causing customer dissatisfaction and inconvenience.

Although human characteristics appear unique, the technology and techniques used to measure these characteristics have a built-in tolerance. This is due to the inaccuracies of the applied techniques and the different circumstances under which the characteristics are presented and measured. Organizations implementing biometric systems need to determine their tolerance for inaccuracy given the specific circumstances of the application. High value transactions are high risk transactions where an error in properly identifying a counterparty can have a devastating impact on an individual or a business. However, an application that allows entry to a theme park might have to sacrifice some degree of security and set a higher tolerance for inaccuracy to avoid the risk of irritating visitors by wrongly rejecting them. This higher tolerance results in false match and false non-match rates.

If a person were to match as someone else, it would be classified as a false match. The probability of this happening is referred to as the false match rate (FMR). If a person fails to match against his or her own template, he or she will be falsely rejected, or not matched. The probability of this happening is referred to as the false non-match rate (FNMR). False matches may occur because there is a high degree of similarity between two individuals' characteristics. False non-matches may occur because there is not a sufficiently strong similarity between an individual's enrollment and trial templates, which could be caused by any number of conditions. For example, an individual's biometric data may have changed as a result of aging or injury. A third important error rate measures the occurrence of new users to a biometric system being unable to enroll for some technological reason. This is called a failure to enroll (FTE) rate.

The expectations regarding matching and non-matching are very different for verification and identification systems. As stated in Chapter III, in a verification system, a user is checked against one or a few reference templates to confirm the user's claimed identity. A much higher standard is required for identification systems where checks are made against all reference templates in the database. Consequently, a much lower FMR is required for a large-scale positive identification system than for a similar size verification system, simply because even a small percentage of false matches for a system that performed billions of comparisons a day

[99] NIST FRVT2002: Overview and Summary, by P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone, March 2003, Page 3. See http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf.

would overwhelm the resources dedicated to investigating positive matches. The larger the identification database, the lower the FMR needs to be to maintain the number of false positives at a manageable amount.

Interoperability and Standardization

Public comments received and remarks made during consultations indicate that interoperability with current systems, as well as with other biometric systems, and establishing standards for hardware and software used to capture biometric information were crucial areas needing further development.

Biometric solutions of the future require a standard method for evaluation. Presently, there is no standard for evaluating biometric algorithm performance. Each biometric vendor develops unique test procedures and uses data sets of varying size, quality, and origin to establish performance metrics that typically include FMR, FNMR, and FTE rates. These variations make it difficult for customers and system designers to accurately assess the suitability of a given biometric algorithm for use in a particular biometric system. This also proves problematic when designing a system which combines multiple biometric algorithms to achieve customer-specified levels of performance.

Public comments also revealed that the vocabulary used to describe biometrics performance needs further standardization. Although biometric system performance has traditionally been stated in terms of decision error rates, conflicting definitions are found in biometrics literature. For example, literature on large-scale identification systems often refers to a "false rejection" occurring when a submitted sample is incorrectly matched to a template enrolled by another user. In access control literature, the same decision error is referred to as a "false acceptance." Confusing terminology occurs in many descriptions of error rates; in some literature, a distinction is made between "failure to enroll" and "failure to acquire"; in others, the terms are used synonymously. Likewise, the use of "False Match Rate" and "False Non-Match Rate" are often used as synonymous with "False Acceptance Rate" and "False Rejection Rate," respectively. Multiple definitions abound for terms as (seemingly) basic as user, identification, verification, template, and enrollment. Efforts to harmonize definitions are underway in national and international standards consensus bodies.

A few respondents and discussants suggested a role for the government in developing, and possibly setting standards, as a way to overcome a number of market disincentives to the adoption of biometrics for financial transactions. For the most part, however, people preferred that the market lead users to adopt the technology, recognizing that the government is playing a role through its demand for biometric applications to improve border and homeland security.

Continuing to develop standards for hardware and software performance, as well as refining the library of terms used to describe biometric performance, will help to raise confidence in the technology.

Security

To be successful, identity authentication using biometrics must ensure a higher level of security than currently available for traditional means of authentication. Consumers hear about or see in the news that databases of personal information are sometimes compromised through hacking, spyware, or even simple hardware theft. They are at least as concerned that their biometric data could be compromised, copied, or somehow imitated. In fact, research supports the possibility that many would be more concerned about the security of databases that store identifiable personal data such as fingerprints or voice patterns. The increasing number of phishing scams is alarming, and many consumers are now worried about e-mail fraudsters tricking them into divulging account numbers, user IDs, and passwords, and then using their identities for malicious purposes. System and network security will become increasingly more important as biometric systems are deployed. This is especially true when biometric data may be transmitted over networks and the Internet, particularly when public phone or telecommunications systems are used. Some may perceive that biometric systems that transmit data over the Internet are more susceptible to being comprised through data interception and used for criminal purposes.

Quality

The quality of the biometric when it is captured is important. If the scanning device is unable to adeptly capture biometric data, it can result in a false match or rejection. The failure to acquire (FTA) rate is the proportion of attempts for which a biometric system is unable to capture an image of sufficient quality. When a biometric system allows multiple attempts, FTA measures failure to capture over these multiple attempts. The quality of the capture can also be impacted when environmental and physical conditions are not ideal (*e.g.*, the presence of dust and grime on the scanning device). The quality of biometric systems that function in natural environments (*e.g.*, in the presence of noise, weather, and illumination changes) may diminish as those environmental factors change. Cameras used for iris or facial scans are most effective "inside" where the environment, lighting, and camera placement are controlled.

Reliability

The reliability of biometric systems, like other automated systems, is central to their success and acceptance. It must work efficiently and can not break down on a regular basis. In addition, biometric technologies need to be well integrated in the authentication process, requiring observation of how they will be used by people and whether their behavior will change over time as they learn how it operates. Otherwise, the technology may be prematurely rejected as unreliable.

Also, certain biometric characteristics may degrade and perform less well over time. Some individuals will find that they cannot be enrolled in a fingerprint system if their fingerprints are worn away, for example.

Cost Issues

During consultations, several parties suggested that the cost of implementation is one of the primary barriers to wide scale adoption of biometric technologies to combat fraud in financial transactions. Biometric systems are expensive compared with other security measures, such as passwords and PINs. While biometrics may provide extra security, the costs currently appear to outweigh the benefits in most cases.

Many of the cost components relating to the implementation of biometric systems are similar to those associated with any other information system: hardware, application software, and databases. Most biometric systems involve costs for additional software and biometric capture hardware, such as readers, scanners, and cameras. In general, biometric hardware costs are declining; however, the costs of replacing legacy systems, marketing, enrolling and educating customers, securing and maintaining databases, are all additional costs associated with implementation of biometric systems. Biometric usage cost may be relatively low, but implementation and maintenance costs are high, making biometrics relatively expensive to implement. For a typical national or regional retail chain, the fact that hardware will have to be rolled out on such a large scale (to all retail outlets) means that hardware cost will always be a concern.

During our consultations Treasury staff learned that biometric systems are generally regarded as an addition rather than a replacement for other systems. This may present potentially costly dual infrastructures. The actual costs of biometrics vary widely, depending on the biometric employed and the desired capacity of the system, and whether the system will be private to an organization or purchased as a service from a provider. Consultations and open literature also conveyed a trade-off between the level of security that can be achieved and the cost of implementing biometric technologies. Typically, the more secure or robust a system, the more costly it is. It is up to a company or organization to decide the level of authentication required for its business.

Figure 13, on the following page, illustrates that the relative cost of biometric systems range widely for the various biometric technologies. Cost also depends on the accuracy and setting of an application. One of the highest costs of implementing a biometric system occurs during enrollment (the process of populating the biometric database), when a high degree of accuracy is required.

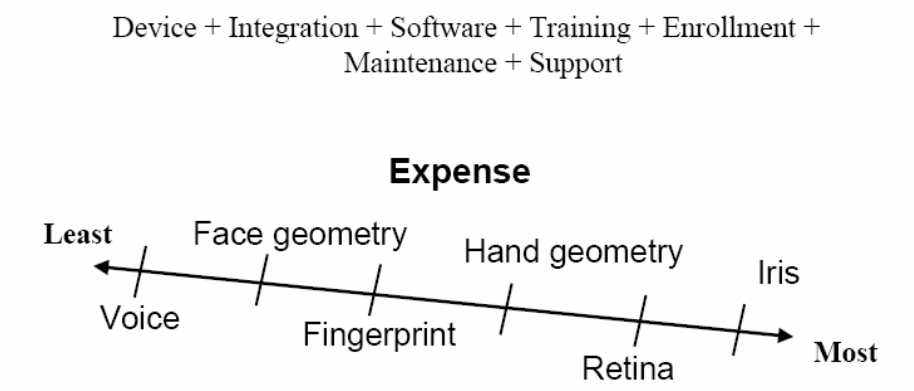


Figure 13. Cost Range for Different Biometric Scanning Technologies[100]

While a simple but effective fingerprint scanning peripheral device for a personal computer can be purchased for around $100, an enterprise-level implementation can easily exceed several hundred thousand dollars. A more complex live scan 10-print fingerprint reader could cost much more. In addition, the ongoing maintenance cost for the more complex machines would be much more as well.

Some biometric technologies require increased cost for training users while others may not. For example, training for a hand geometry device is generally minimal because its use is very intuitive. In addition a hand geometry system involves very little personnel costs because most devices are typically unattended.

The lack of standardization of the diverse biometric technologies that may not or do not operate across systems or industries also results in some costs being high. This lack of standards may require expensive system upgrades and enhancements or even replacement at a future date. At the present time, many biometric solution providers have their own proprietary technology and are reluctant to agree upon a single, global standard for biometric technologies.

Consumer Acceptance Issues

During our consultations and in the public comments received acceptance figured high or at the top of industry's considerations. Many people are concerned about the potential for governmental, as well as private sector, misuse of biometric data. Consumers also are concerned whether biometric systems offer increased convenience; and if the use of biometric systems may be biased. Each of these areas is discussed below.

Misuse

Some consumers believe that the use of biometric systems will create large databases of extremely personal information that could be used without the customer's consent. Consumers

[100] William Saito, "Biometrics, Understanding the Architecture, Standards, and APIs," NIST Conference on National Information System Security Conference Presentation titled, 2000, Slide 9. See http://csrc.nist.gov/nissc/2000/proceedings/papers/305slide.pdf.

are often concerned about the "Big Brother" nature of building databases that include biometric data as well as other personal identifying information. One public comment stated that the individual felt that biometric data could be used to track individuals without their knowledge. For example, it was noted that "fingerprinting" is often associated with criminality because they have historically been used by law enforcement agencies to track down those suspected of committing criminal acts. Therefore, collection of fingerprints has raised concerns over their potential and ultimate use. People are also afraid that their biometric data will be recorded in a national database, even if they do not have any criminal record.[101]

At the Department of Homeland Security, Chief Privacy Officer Nuala O'Connor Kelly addresses the issue of governmental misuse systematically. She asks DHS program managers to answer the "why, what, when, who, where and how" of data collection technologies, whatever they may be, and of information sharing procedures when assessing their impact under the Privacy and Freedom of Information Acts.[102]

In addition, consumers are concerned that their biometric data could be compromised, copied, or somehow imitated. Some consumers hold a general concern about security of databases that store identifiable personal data such as fingerprints or voice patterns. Some may perceive that biometric systems that transmit data over the Internet are less secure and that the data is susceptible to being intercepted and used for criminal purposes.

In today's environment, if a password is stolen, the issuer can simply re-issue a new one. If the biometric which is being used for authentication is stolen or misappropriated, this biometric can not simply be re-issued. A person only has one set of fingerprints.

Others feel that consumer acceptance of biometrics is improving. This is due in part to positive consumer experiences and increased public and private deployment of biometric solutions (*i.e.*, border access, internal security, time and attendance systems). Integration of biometric capture devices into computer keyboards, monitors, laptops, cell phones, and PDAs is also ultimately helping to boost consumer acceptance of biometrics.

A recent survey commissioned by EDS and the International Association of Privacy Professionals (IAPP) found that the general public is getting more comfortable with biometric technologies as an accepted form of identification.[103] Just over two-thirds of the U.S. consumers polled said they were open to the idea of using biometric information—such as digital fingerprints and iris scanning—to verify their identity.

---

[101] Testimony of Christer Berman, "Precise Biometrics, Advancements in Smart Card and Biometric Technology," U.S. House of Representatives Committee of Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and Census, September 9, 2003.

[102] Susan M. Menke, "DHS privacy office grapples with RFID, biometrics," Government Computer News, November 17, 2004.

[103] Gail Magnuson and Peter Reid, "White Paper: Privacy and Identity Management Survey," Privacy and Data Security Academy & Expo, International Association of Privacy Professionals (IAPP), New Orleans, Oct. 2004.

An earlier survey conducted by Opinion Research Corporation (ORC) International provides evidence that the use of biometric identification is increasing, albeit slowly.[104] Among all adults, including those who are unaware of biometric techniques, 5 percent provided characteristics in 2002, compared with 3 percent in 2001. Among those aware of the techniques 11 percent, up from 5 percent in 2001, have personally provided identifying characteristics to an organization for a computer-matched biometric comparison. The survey also indicated little change in public awareness of biometrics between 2001 and 2002 – in response to a description of biometrics, about half of those surveyed in both years were aware of biometrics identification techniques. (ORC surveyed approximately 1,000 adults via telephone in September 2001 and August 2002).

Survey data and anecdotal information suggests that sufficient consumer education is one of the keys to acceptance. Consumers are more likely to accept a biometric technology if they clearly understand how it is used to improve security and that the data is safely-encrypted. The driver's license bureau of West Virginia has a very high acceptance rate among its citizens, with 90 percent volunteering to provide biometrics at time of license enrollment or renewal. This is a result of customer education, focus on the specific use, and confidence in the services being provided.[105]

Convenience

U.S. consumers place a high value on convenience when it comes to conducting transactions. Technologies that improve efficiency and make things quicker usually receive wide-scale acceptance. Technologies that give the appearance of slowing processes, even if the increased time adds security or other features, are often rejected by consumers.

Historically, users have complained about having to keep track of multiple passwords for access to different systems, physical areas, or websites. Most users desire a way to simplify and standardize the authentication process. The EDS/ IAPP survey found that nearly 90 percent cited the convenience of biometrics—compared to remembering passwords—as the reason they would accept it.[106] It was noted during consultations that customers find it more convenient and quicker to authenticate themselves by repeating a phrase into their phone instead of memorizing and using a user ID and password, entering a long account number, or responding to other personal questions (*i.e.*, entering a date of birth, Social Security Number (SSN), or postal zip code).

---

[104] Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector was commissioned by SEARCH, funded by the U.S. Bureau of Justice Statistics, and developed by Dr. Alan F. Westin. Telephone surveys were conducted by Opinion Research Corporation (ORC) September 18-30, 2001 and August 15-18, 2002, among national probability samples of 1,017 and 1,046 adults 18 and older.

[105] A survey conducted at the University of Pretoria in South Africa of users and developers/implementers of biometric technology assessed user perceptions related to biometrics. Results of the study indicate the need to ensure that users are well informed and educated on how the biometrics technology is implemented, how it will work, how their biometric data is protected and, with whom and under what circumstances it might be shared with others. Ilse Geising, "User Perceptions Related to Biometrics," diss., University of Pretoria, 2004, Chapter 9. See http://upetd.up.ac.za/thesis/available/etd-01092004-141637/unrestricted/09chapter9.pdf.

[106] Magnuson and Reid.

Deploying biometrics in scenarios where customers are able to present a biometric at the beginning of the transaction (*i.e.*, as he or she approached an airline counter, over the phone to a customer service representative) may effectively eliminate the discussion of private information where others can hear the information. Customers no longer need to discuss sensitive data such as date of birth, SSN, or other personal data to conduct business.

Public comments revealed that some users have enrolled in biometric systems to participate in programs granting them expedited processing (*e.g.*, retail check out points, frequent travelers, student lunches)**.** People who participate in these programs relinquish anonymity for perceived convenience. The activities and behavior of consumers who carry grocery store loyalty cards or use debit or credit cards to pay for purchases may already be recorded for various reasons.

Conversely, if the use of the biometric technology is perceived to add time to a transaction, either because of increased time to process or increased errors, most consumers will reject it. Though not unique to biometric solutions, customers can become quickly frustrated with systems that create additional delays.

Potential Biases

Some consumer advocacy groups have noted biometrics may be biased and exclude a particular group or certain individuals from their use. The inability to enroll some individuals (*e.g.*, an amputee unable to provide images of both index fingers) makes the system unfair and possibly discriminatory. For example, people who are mute cannot use voice systems, and people lacking fingers or hands from congenital disease, surgery, or injury cannot use fingerprint or hand geometry systems. Also, the fingerprints of people who work extensively at manual labor are often too worn to be captured. Other groups have cited religious or cultural beliefs that may prevent some individuals from enrolling.

Discussions with vendors, manufacturers, and users of biometric solutions indicated that secondary systems or "workarounds" should be incorporated into the biometric system to deal with situations where a user does not have the body part required for using the system or is not able to enroll for other reasons.

Conclusion

This chapter has discussed the variety of biometric technologies, their application, and areas that need to be considered as the use of biometrics continues to expand. These included technological and operational issues, costs, and consumer acceptance. As biometric technologies mature, many of the technological and operational issues are being dealt with. Likewise, with more public and private sector organizations deploying biometric systems, costs are coming down. And finally, there are signs that consumer acceptance of biometrics is starting to change. Consumers are more willing to accept biometrics if they understand that the technology provides greater transactional security and convenience. Consumer demand for easy, multi channel access to information is also prompting acceptance. Integration of biometric capture devices into

computer keyboards, monitors, laptops, cell phones and PDAs is also helping to boost consumer acceptance of biometric security.

Table 3 provides a summary of the various strengths and considerations of four common biometric technologies (fingerprint recognition, iris recognition, hand geometry, and face recognition).[107]

Table 3. Biometrics Strengths and Considerations

Fingerprint Recognition: Strengths	Fingerprint Recognition: Considerations
▪ Most widely used technology[108] ▪ Proven technology capable of high accuracy ▪ Ability to enroll multiple fingers ▪ Wide range of deployment environments	▪ Perception of law enforcement, forensic uses ▪ Impaired or damaged fingerprints ▪ May require additional hardware and software ▪ Standards needed for interoperability
Iris Recognition: Strengths	**Iris Recognition: Considerations**
▪ Highly reliable, hands-free operation ▪ High stability of characteristic over lifetime ▪ Iris is a rich source of biometric data[109] ▪ Successful tests in air travel	▪ Acquisition of iris image requires more training and attentiveness than most biometrics ▪ Hardware and software licensing costs ▪ Glasses with strong lenses may impact performance ▪ Potential for false non-matching
Hand Geometry: Strengths	**Hand Geometry: Considerations**
▪ Able to operate in challenging environments ▪ Established, reliable core technology[110] ▪ Perceived as non-intrusive	▪ Design complicates usage by certain populations ▪ Perception of bio-hazard, passing germs ▪ Possible hand changes over time
Face Recognition: Strengths	**Face Recognition: Considerations**
▪ May operate without user compliance ▪ Leverage existing image databases ▪ Only technology capable of identification at a distance and surveillance[111]	▪ Susceptible to high false match rates in one-to-one and one-to-many applications ▪ Lighting, camera angle reduce matching accuracy ▪ Changes in physiological characteristics reduce matching accuracy

[107] The summary was compiled by MITRE and is based on public comments received, remarks made during consultations, and a review of open literature.

[108] U.S. GAO, Using Biometrics for Border Security, p. 46.

[109] U.S. GAO, Using Biometrics for Border Security, p. 47.

[110] U.S. GAO, Using Biometrics for Border Security, p. 47.

[111] U.S. GAO, Registered Traveler Program Policy and Implementation Issues, (Washington, DC: U.S. GAO, November 2002), p. 30.

Chapter IV

USES OF BIOMETRICS IN FINANCIAL TRANSACTIONS

The financial sector has been cautious in its adoption of biometric technologies to combat identity theft in the United States for many of the reasons raised in the previous chapter. Since the commercial introduction of the first modern biometric device occurred over 20 years ago, there have been periods of intensified interest in the potential benefits of using biometric technology, as in the mid to late 1990s, for example. Still, there is no industry-wide consensus to support widespread deployment.[112] Nonetheless, individual institutions and payments providers have tested and even deployed biometric systems for specific purposes, which include internal security, business-to-business operations, and occasionally for customer access to products and services. Discussions and public comments received indicate that major financial sector players continue to watch developments in the technology and to consider possible applications where a business case can be made for using biometrics.

Representatives of financial institutions and others have offered a number of reasons for the caution exhibited by the financial sector. These factors include:

- Reluctance to be early adopters of technology that continues to mature in technical capability and reliability;
- Concern about negative customer reaction;
- Few customer implementations demonstrating quantifiable cost savings;
- Higher internal system development priorities;
- Preferable expenditures on alternative technologies and consumer education about identity theft;
- Lack of clear structure and business model for cross industry/multi-company implementations;
- Difficulty of presenting and implementing new biometric solutions to a complex payment system;
- Operational issues such as data security; and,
- Cost and complexity of deployments given legacy system integration, interoperability concerns, and absence of standards.[113]

Continuing technical and operational improvements in biometric accuracy and delivery methods and the U.S. Government's intent to use biometrics to enhance border security contribute to renewed interest in evaluating the biometrics to improve the security of financial transactions. This chapter examines the choices confronting financial institutions, examples of how biometrics may be used to safeguard financial transactions, and recurrent issues that

---

[112] Orla O'sullivan, "Biometrics comes to life," ABA Banking Journal January 1997.

[113] Financial Services Technology Consortium (FSTC), "Comments on the Use of Biometrics and Other Similar Technologies to Combat Identity Theft," March 31, 2004. These comments include many, but not all, of the items listed.

financial institutions face when making the business case to deploy biometrics for the authentication of people and transactions.

Choosing Biometric Solutions in Financial Transactions

"The choice of which biometric to use, or the 'best' biometric to use is less a function of the core technology than it is a function of how, where, and why its *(sic*) deployed," one of the respondents to the Treasury Department's request for public comment stated.[114] Essentially, a financial institution must –

- Decide how the technology will be used;
- Conduct a detailed cost-benefit analysis; and
- Analyze the trade-offs between the increased security and other factors such as the accuracy of the system, and customers' comfort level.

In applications used by customers, "Day One" requirements for biometrics are likely to be limited. "Day One" activities include a consumer's effort to establish a customer relationship with a financial institution, usually the initial relationship. If a person passes the application process and enrolls his or her biometric, the technology most likely would be used to authenticate the customer during "Day Two" (or subsequent) activities. This utility factor is an important consideration in any choice to use biometrics.

In the absence of an existing relationship with a customer, the financial institution is unlikely to have a stored biometric of the individual. Consequently, the financial institution would not be able to match a biometric provided by the prospective applicant, at least not without assistance. As one commenter advised:

> This would seem to preclude the use of biometrics for preventing many identity thefts involving new account openings, unless: (a) the creditor can determine that the person named in the new account application has a biometric template on record with some trusted third party, and (b) the biometric template can be accessed for identity authentication.[115]

The commenter strongly suggests that rather than simply discounting the utility of a biometrics solution for catching fraudulent new account openings, it would be useful to explore the potential role for trusted third parties. A trusted third party might have a biometric template of the victim whose name is being used to establish a new account. In the case of a remote or online application, the remote biometric would benefit from being a biometric that is "live" – rather than static. The third party might be another financial institution that retains biometric templates of its own customers, or it might be a trusted repository of biometric templates.[116]

---

[114] FSTC, p. 2.

[115] Comments from Bob Pinheiro, April 1, 2004.

[116] Pinheiro.

(The trusted third party model is familiar to us through the use of digital certificates and digital signatures, discussed in Chapter II.)

Vendors are beginning to combine technologies that verify identification documentation initially and create a biometric for authentication. One vendor reportedly offers identity check technology that reads, analyzes, and verifies encoded data in magnetic stripes and barcodes on government-issued IDs to determine whether the content and format are valid. The vendor integrates the identity verification with creation of a signature biometric for future authentication.[117]

"Day Two" activities are usually transactional in nature. Representatives of major credit card issuers have volunteered that transaction fraud accounts for about 80 to 90 percent of the fraud committed, while identity theft in the form of application fraud or account takeover fraud accounts for the other 10-20 percent. For them, technologies that reduce "Day Two" transaction fraud would reduce the principal source of credit card fraud. Considerable non-recoverable costs begin to show on "Day Two" as well, for example, from closing accounts and opening new ones.

However, biometric technology may not be an appropriate choice in the credit card environment, where cards are issued without face-to-face contact with customers and transactions occur at remote sites. Fingerprint biometrics, for example, where the customer is known but never seen by financial institution personnel, may be more appropriate for use in a bank branch, where customers personally appear and are enrolled.

Another commenter suggested consideration of federated, or securely shared, identity technology, a concept of growing interest for those managing identity data and processes. The practice would enable different companies or web sites to share customer identity information securely. A company in the federated system could rely on the authentication of identity by another company. The customer would not need to repeat requests for information for authentication purposes, thus reducing the number of times he or she discloses PINs, passwords, Social Security numbers, or other sensitive data. Financial institutions would be able to mask sensitive identifying information that they legally and routinely supply to third parties.

Database storage is another critical operational factor that affects the choice of biometrics systems for the financial sector.[118] Storage and maintenance of biometric databases are costly and the costs are on-going. Database collection, storage and maintenance also raise sensitive issues of database security, maintenance, and accuracy, as well as citizens' concern about the future use, and potential disclosure of personal biometric data.

---

[117] "Intelli-Check Enters into Licensing and Strategic Alliance Agreement with SiVault Systems," Businesswire August 31, 2004. See www.businesswire.com.

[118] Comments from Kathy Pappas, Regulatory Compliance Analyst, Technical Editor, RDS, Indianapolis, IN, April 1, 2004. Note another anticipated development, described by another public respondent, representing a core data processing company that serves financial institutions. The respondent envisages that eventually it would "interface with software and hardware provided by third-party vendors to acquire, store, and verify biometric data. The company's core processing application might store part or all of that biometric data." The company also might act as a reseller for third-party software and hardware.

Authentication, as discussed throughout most of this study, will involve matching an individual's biometric data against a biometric template of the same biometric feature that was created when an individual enrolled in the biometric system. The template must be stored somewhere for future matching purposes. One-to-one matching or verification of a claimed identity does not necessarily require a central database. A biometric template can be stored on a smart card or token. The user might gain access or authorization by providing a PIN or coded identification card and placing his finger on a platen of the biometric security system. The system would compare the finger on the platen with the previously recorded template stored on the card to verify that the person with the card is the person enrolled in the system. Knowledge of the PIN or code in conjunction with presentation of the biometric reduces the risk that an imposter is involved.

This raises again the crucial importance of clear policies and procedures for the enrollment process, discussed earlier in this report. Enrollment is the key to the accuracy of the system and thus to the level of risk to which the biometric application will be applied. If enrollment of individuals into a biometric system is based on fraudulent data used for initially verifying the identity of the individual, then biometrics will facilitate identity theft. An erroneous enrollment on "Day One," for someone new to the financial institution for example, actually would facilitate "Day Two" fraud. On the other hand, close scrutiny at enrollment, with enhanced non-biometric procedures for verifying the identity of the enrollee, will help to ensure the integrity of the biometric data and increase the reliability of the biometrics.

A traditional fingerprint check of prospective employees with the database of the Federal Bureau of Investigation may improve the integrity of a subsequent biometric enrollment process. The internal biometric system could use fingerprints, hand geometry, iris scans, or other types of biometrics for a system that controls employee access to sensitive places or data.

Whatever choice may result, biometrics solutions generally are regarded as supplemental, providing a second and/or third factor authentication in financial services. Fingerprint, voice, hand geometry, and iris recognition seem to be the most commonly used or contemplated biometric technologies for financial transactions or communications. The Director of Business Development at International Biometric Group reportedly has cautioned that biometric tokens, for example, should be used for three-factor security (*i.e.,* something you have, something you know, something you are). Looking at the fingerprint sensor tokens for two-factor security, in his view, does not increase network protection sufficiently compared to the traditional token and PIN.[119]

Use of Biometric Solutions in Financial Transactions

A number of large banks and financial institutions have developed prototypes of biometrics to use for employee access control and other limited internal functions, as well as for access to specific products and services used by customers. The results of the trials with customers often have been positive in terms of functionality and customer acceptance. A few

[119] "New Tokens with Fingerprint Scanners Enter Authentication Market," CardTechnology.com, August 2004.

smaller banks and credit unions, despite limited research and development budgets, have launched similar experiments and received positive feedback as well.

The prototypes and pilots have led to production-level implementations on a company by company basis. In the payments field, grocery and other retail outlets are introducing customers to speedier transaction processes that are also secure. The examples below are anecdotal, selective, based largely, though not exclusively, on press reports, and, therefore, illustrative only.

Physical and Logical Access

As indicated earlier, fingerprint biometrics is used by financial institutions for internal access control. Citibank uses fingerprint scan technology for employee access to its retail branch network in locations throughout the country and for employee log on at a customer service facility in San Antonio, Texas. Clarendon Insurance Group installed fingerprint readers to control employee access to their building as well as log on access to computers.[120] The Purdue Employees Federal Credit Union (PEFCU) uses hand geometry internally for employee access to buildings.

The Los Angeles County Employees Retirement Association turned to fingerprint scanners to increase security and reduce the cost of managing passwords. The association manages retirement, disability, and death benefits for tens of thousands of county employees. The Association found that as employees faced the need to store multiple passwords, they started storing their passwords by writing them down. The organization implemented a centralized ID management with a single log on for all its critical applications. Employees gain access to data via a fingerprint scan instead of passwords. Use of the fingerprint scanners has decreased the cost of managing passwords. The implementation went smoothly, except for a small number of employees whose fingerprints are very faint.[121]

Customer Authentication

A representative of one large financial institution noted that the bank had a pilot underway using hand geometry to permit customer access to safe deposit boxes. However, the representative indicated that the pilot was instituted more to assess productivity, than for security gains.[122] Another pilot, with an element of security and an element of customer convenience, relies on a smart token containing fingerprint biometrics housed in a key-chain fob. A Bank of America customer uses a fingerprint reader at the teller window to match his fingerprint against the biometric fingerprint data on the fob. A match causes the device to transmit account

---

[120] Jeff Caruso, "Biometrics Early Adopters Reveal Secrets, Challenges," Network World Fusion, October 28, 2004.

[121] "Biometrics, A Future Identity Solution?," Identity Theft 911, September, 2003. See http://www.identitytheft911.com/education/article/idtheft_biometrics.jsp.

[122] "Biometrics Gaining Ground with Banks, Customers," American Banker, November 10, 2004. Bank of America reportedly has been using handprint scanners since 1996 for this purpose.

information stored in the device to the teller, thus authorizing a transaction. Reportedly, all the information transmitted is encrypted, and the device does not transmit transaction information.[123]

San Antonio City Employees Federal Credit Union announced that it added a layer of security to employees' laptop computers with keystroke biometrics. A two-factor authentication system for employees, the BioPassword system combines traditional password with biometric recognition of the unique keystrokes of the individual typing the password.[124]

PEFCU deployed biometric systems as early as 1997. Responding to a request from Purdue University to open additional sites on campus, PEFCU opened kiosks and chose to deploy fingerprint imaging biometrics. The biometric replaces the usual picture identification. Roughly 60 percent of PEFCU's membership has enrolled. Initial enrollment occurs at a service branch or kiosk where a photo ID is scanned and a live photograph taken. A fingerprint image is registered. The biometric is used with a PIN. PEFCU plans include fingerprint biometric devices at teller stations as well expansion of internal uses for fingerprint biometrics. Technology Credit Union (Tech CU), San Jose, California, began a pilot of customer fingerprint scanners at its teller stations in 2003. Tech CU officials were encouraged by PEFCU's success. The Tech CU biometric PIN pads allow members to use their fingerprint or PIN for authentication for in-branch transactions.[125]

CitiCard is testing and plans to roll out a voice or speaker verification biometric for cardholders contacting its call center. In addition to the security feature, the application is expected to speed the enquiry process for the customer and cut call handle times for the financial institutions, for substantial cost savings. AIM Investment Services adopted voice recognition technology for customer access to account information over the telephone.[126]

Check Cashing

Check cashing enterprises that deal with customers who do not necessarily have a bank account but want to cash a check are beginning to look to biometric solutions for cutting fraud losses. BioPay, LLC, based in Herndon, Virginia, has developed a system that uses biometrics to identify and authenticate people cashing checks. The system first scans the customer's driver's license to determine whether it is authentic. For enrollment, the customer also must provide a unique identifying number. In addition, index finger prints are captured for conversion to biometric form. The BioPay system performs a one-to-many search to see whether the fingerprint biometric matches one that is already enrolled and authenticates the individual for subsequent check-chasing transactions.

---

[123] Bob Brewin, "Bank test Bluetooth-based biometric ID system," ComputgerWeekly.com, May 12, 2004.

[124] "San Antonio City Employees FCU Introduces Biometrics for Laptops," Credit Union Journal, July 14, 2004. See www.cujournal.com.

[125] Daniel Wolfe, "Biometrics Gaining Ground with Banks, Customers," American Banker, November 10, 2004.

[126] "Biometrics Adds Security in Insecure Times," Wall Street Technology, April 2004, p. 42.

Signature recognition could eliminate the need to manually compare signatures for check cashing or for making account changes. Dynamic signatures could be captured by using electronic signing pads when a customer opens a new account. Subsequently the signature could be used to authenticate the identity of anyone claiming the account holder's identity in a future financial transaction. Looking ahead, if the biometric signatures could be shared with retailers, then the authentication process could be extended to point of sale transactions.

ATMs and Retail Point of Sale

There have been a number of successful ATM trials using fingerprint, iris and facial recognition over the years. Bank of Tokyo-Mitsubishi (BTM) recently announced a major pilot using palm vein patterns as the biometric. BTM will become the first major bank in Japan to incorporate biometric security with a multi-function banking card. Using palm vein recognition, the identity of the cardholder will be verified with the biometric in combination with the regular cardholder PIN. The biometric data will be stored inside of the integrated circuit chip forming part of the smart card. BTM will not hold the biometric data. Cardholders will scan their palms to match the enrolled palm vein pattern data on the card.

Biometric technology has drawn interest from the retail sector to serve as a way to identify customers, reduce credit card and check fraud, and enhance customer service. Numerous manufacturers make biometric software and sensors, which are installed on POS terminals. Customers register a fingerprint scan with a store or restaurant and enter their credit or debit card account numbers to set up their accounts. When a customer is ready to make a purchase, she places her finger on the sensor for identity purposes and pays without having to present her credit or debit card. These systems can also be used with checking accounts, where electronic debits are processed through an automated clearing house at a reduced cost to merchants. Once customers have registered, merchants can also use the technology to keep track of loyalty programs and eliminate paper coupons.[127]

Pay By Touch systems reportedly have been deployed by West Seattle Thriftway, where customers use the fingerprint technology almost exclusively for PIN debit payment. The company announced a pilot of the technology at Piggly Wiggly grocery stores in South Carolina, with full scale deployment anticipated; and testing in Pick 'n Save stores in Milwaukee, WI.[128] The Pay By Touch system scans two fingers of each participating customer and creates an algorithmic number from each print that is matched with one created when the print is read again during a purchase. At enrollment customers can register their debit or credit cards, or they can use the Magnetic Ink Character Recognition (MICR) data from a check of theirs for payments that will be routed through the Automated Clearinghouse system. Other vendors offer competing payment processing system.

---

[127] John Burtzloff, "Are your customers ready for biometrics*?*," Entrepreneur.com, November 11, 2002. See http://www.entrepreneur.com/article/0,4621,304503,00.html.

[128] "While Encouraging Use of Debit PINs, Merchant Says Fingers Do The Talking," Debit Card News, October 14, 2004.

Thriftway reportedly found that two percent of the time its print readers could not get a good print read, and has upgraded its readers. Piggly Wiggly offered a sweepstakes enticement to help overcome some customers' reluctance to embrace the new technology.[129] Discover Financial Services, a unit of Morgan Stanley, announced a deal with Pay By Touch to promote the biometric solution as a way of drawing more merchants to Discover Card. To attract merchants, Discover offers to charge them "card-present" fees, rather than the costlier "card not present" fees, and reportedly may cut fees further for merchants that use Pay By Touch and accept Discover cards exclusively.[130]

Online Authentication

In consultations with a representative of an online bank, the representative described a successful pilot in 2001 in which hundreds of customers were provided a fingerprint optical reader built into a computer mouse. The bank wanted to evaluate the security enhancing technology and customer interest in using it to log in. Initially the bank had a client ID and a PIN to authenticate the customer at home, whom the bank subsequently enrolled in the biometric system. The test showed some performance improvement in the log in, but insufficient economic justification for a full roll out. When asked, those who tried the system admitted they would prefer to receive the cash equivalent of the cost of the device (roughly $50), than to have the more secure device in use. The bank found the technology useful for internal control of building access, however. Generally, the bank looks to improvements in authentication from other sources until such time as biometric readers are more ubiquitous on personal computers and costs of rolling out a system to customers can be leveraged.

Beepcard has developed a prototype that incorporates biometrics into smart cards. The prototype is an enhancement to the sound authenticator system described in chapter II, and includes an on-card microphone. The prototype requires users to provide a spoken password that is authenticated using a built-in voice-recognition chip. Beepcard has developed the concept to prevent the use of stolen or fraudulently obtained credit card to purchase goods online. Use of the card does not require any special card reader hardware, so it could potentially be used on a randomly chosen computer at an Internet cafe.[131]

In December 2003, a European vendor announced forthcoming trials by a number of European banks of facial biometrics intended to facilitate Internet banking. The facial biometric would be stored on a personal computer or on a smartcard to be read by a home personal computer. The personal computer would need to be equipped with a web camera and software costs could be a deterrent to proceeding with such a solution.[132]

---

[129] Debit Card News.

[130] Lavonne Kuykendall, "Discover Banks Biometric Payments Vendor," American Banker September 1, 2004.

[131] See www.beepcard.com.

[132] Andy McCue, "Online banks plan face-recognition trials," ZDNet UK December 12, 2003. See http://news.zdnet.co.uk.

Voice authentication for online access to financial accounts requires minimal hardware investment on the user side because most personal computers already contain a microphone. By using query/response techniques, it would be possible to assure that the individual at the remote site is a live person whose voice is being verified. However, poor quality and ambient noise can impact the accuracy of verification. Keystroke dynamics is also being explored for authentication of customers for online banking applications, although its use is not prevalent.

Automated Cashier Machines

In early 2001, Infonox, Santa Clara, California, installed automated cashier machines (ACM), at Seneca Niagara Casino, and more than a dozen other gaming properties subsequently signed contracts to use the products and services that allow customers to get a cash advance from a credit card without using a PIN.[133] The ACMs use facial recognition. For first time users, the machine takes the customer's picture and delivers a receipt to be presented to the cashier. The cashier retrieves the picture taken at the ACM, and checks it against the customer's picture ID and then swipes the customer's credit card. At that point, the customer is enrolled in the system. Following initial enrollment, a customer steps up to the ACM, has his or her picture taken, and if it matches the original photo, keys in the amount of cash desired. Viisage, a provider of facial recognition software, promotes its supply of biometric software to over 150 other casinos.[134] However, the most widespread use of facial recognition in casinos is for surveillance purposes – to detect known cheaters who have been banned from gambling establishments.

The abundance of potential solutions is an indication of market vitality, but not necessarily an indication of market acceptance. "The stability of a technology with actual use of standards in an application will produce the best results," according to one expert.[135]

Conclusion

Comments, discussions, and research all lead to a set of key issues confronting financial sector organizations as they assess the feasibility of using biometric technologies to enhance security. The key issues facing the financial services sector mirror those facing other sectors. They can be grouped into the following areas: (1) technological and operational issues, (2) cost, and (3) consumer acceptance.

The technical and operational issues center on technology maturity, interoperability and lack of standards, accuracy, security, and reliability. These factors are viewed by the financial services sector in the same ways they are viewed by other sectors in the overall acceptance and deployment of biometric technologies.

---

[133] "GCA gets more casino ATM business," Infonox, January 31, 2003.
See http://www.atmmarketplace.com/research_story.htm.

[134] "Visage – Advanced Technology Identity Solutions, Civil ID, Criminal ID, Border and Area Security," *Visage*, available at http://www.viisage.com/ww/en/pub/company/corporate_profile.html

[135] Turek "An Industry Group Viewpoint: Biometrics," p. 20.

The costs associated with biometrics appear higher than traditional e-security techniques. In a retail financial services setting, for example, the fact that hardware will have to be rolled out on such a large scale (across all customer touch points) means that hardware cost is a concern. In some cases, it may be necessary to maintain legacy systems alongside new biometric system during a transition period. Costs are easier to identify and measure than savings.

"There's really no pull. There's really no push. It's kind of in 'levitation' right now," according to a technology strategist for a major credit card issuer, who was asked about the implementation of biometrics.[136] In his case, corporate resistance coalesced around costs of $5 million over the first two years, tapering to $400,000 per year upkeep afterwards for the network sign-on application he was contemplating.

Crucially, every financial institution places a priority on customers' likely reaction to the introduction of biometric technologies. Consumers are concerned about what happens if their biometric data is stolen or copied along with their financial information. In today's environment, if a PIN is stolen, the financial institution can re-issue the PIN; biometric data can not be re-issued. In addition, the stolen biometric might then be used for access to other institutions' accounts.

Financial institutions must also resolve the question of what happens to biometric data of customers that no longer have a relationship with the institution that initially collected the biometric data. It is not uncommon for a customer account to be sold from one financial institution to another. Similarly, customers transfer their business from one institution to another, or cease to be customers for other reasons.

Survey data and anecdotal information suggests that with sufficient education consumers generally may accept the introduction of biometrics. The Purdue Employees Federal Credit Union and the Technology Credit Union, for example, initially were concerned there would be customer resistance to the introduction of finger scan technology, but their fears proved unfounded. PEFCO found that members 50 and older embraced the technology because they believe it is more secure.

Consumers may accept a biometric if they understand that the technology will provide greater transactional security and that the data is encrypted in such a way that it is unlikely to reveal the source or to be misused. However, these same sources suggest that consumers are unwilling to embrace biometric technology that is invasive, not readily available, inconvenient, inaccurate, or costly.

Currently there are numerous pilot implementations but not a great many product implementations of biometric technologies by the financial services industry. One commenter wrote:

> "Day-to-day production-level implementations are generally focused on populations where the financial institution has a certain

[136] Jeff Caruso, "Biometrics Early Adopters Reveal Secrets, Challenges," Network World Fusion, October 28, 2004.

> degree of control over the users (*e.g.*, employees). In these cases, biometrics are much more widespread in applications for controlling employees' physical access to data centers and other high security buildings and to a much lesser extent, for accessing the corporate network."[137]

Relinquishing the familiar and relatively successful password system can also be a hard sell to security officials unfamiliar with the newer technology, particularly in the face of such costs. The challenge remains how best to present the business case for adopting biometric solutions to problems that may have been resolved satisfactorily by other means.

[137] FSTC, p. 4.

Chapter V

FINDINGS AND CONCLUSIONS

The FACT Act called for the Secretary of the Treasury to undertake a study and report to Congress on "the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction." The results of the Treasury Department's study indicate that there is no single solution to this challenge. We can expect to see continuing improvements in the security that surrounds the collection, use, and storage of consumers' personally identifiable information, the transmission of that information, and its disposal. We also can expect to see improvements in the security of data transmission and processing relating to financial payments and other transactions. These security enhancements will include the ability to verify identities and authenticate people more accurately and to identify erroneous or fraudulent transactions more quickly and frequently. Biometric technologies will play a role in these improvements. This optimism is reflected below in the findings and conclusions drawn from the Study on the Use of Technology to Combat Identity Theft, required under section 157 of the FACT Act.

Findings

Non-biometric technologies and anti-fraud systems already authenticate individuals and assist in authorization of transactions, and innovative vendors continue to improve upon these tools for combating identity theft. The tools have performed sufficiently well in the past to have promoted a broad and deep consumer credit market in the United States that is widely accessible by the citizenry. Improvements of these systems should and do continue, providing the private sector tested alternatives to biometric solutions, which in the future may in some cases be augmented or replaced by biometrics for specific applications when a sufficiently compelling business case can be made to do so.

Biometric technologies are not in widespread use for payments transactions or by the financial services industry for a number of reasons. Financial institutions have had limited success in making the case for adopting biometric technologies due to concerns about consumer acceptance, initial and on-going costs, and the efficacy and efficiency of biometrics compared to proven alternatives.

- Consumers generally are concerned over how biometric information will be collected and protected, who will have access to it, how it will be kept up-to-date and discarded, how it will be used, whether it is necessary, and whether it will be inconvenient.

- Costs appear to be a substantial barrier, while it is difficult to measure savings that may result from productivity gains, for example. Hardware costs for fingerprint readers are declining, yet the costs of replacing legacy systems and ubiquitous magnetic stripe payment cards, enrolling customers, securing and maintaining databases, are all among the considerable costs associated with developing and integrating biometric systems.

- Biometric technologies are not mature technologies in most cases and therefore tend to deter early adoption. Current biometric technologies are not absolutely accurate or reliable, and the tolerance for error rates or false readings may be too great for financial institutions to accept.

- The absence of interoperability of biometric systems and failure to adopt standards inhibit adoption of biometrics widely in the financial sector and payments networks.

Conclusions

We can expect to see continued improvements in non-biometric technologies along with increasing use of biometric security and identity products on a case-by-case basis. As the economy responds to the problem of identity theft, the sophistication of identity thieves, and the threats to our physical and cyber security, merchants, payments system operators, processors and other service providers, as well as regulated financial institutions, will revamp their security programs and upgrade their systems.

The impetus to biometric research, development, and implementation from governmental programs to secure borders, improve identity documents like passports and drivers' licenses, and control access to sensitive civilian and military sites will promote greater acceptance of the technology as well. Governmental research agencies such as NIST will continue to develop standards and test products that promote the utility and adoption of biometrics in appropriate circumstances.

A few vendors, biometric researchers, and representatives of financial institutions suggested a greater role for the government in setting standards and requiring compliance with them. On the whole, however, the study yielded no general appeal for greater government intervention to promote the use of biometrics to combat identity theft. The general consensus was to leave the dissemination of biometrics to the market place.

The study led to the conclusion that biometric technology is not a "silver bullet" for reducing identity theft generally or identifying the party to a financial transaction specifically. Biometrics are not likely in the near term to be very useful to confirm the true identity of an individual at the initial point of opening an account or submitting an application to a financial institution if the person has no prior relationship with the institution. An exception, fingerprint comparisons with a third-party database, will continue to be useful for this purpose to the extent that such databases are reliably accessible. Non-biometric techniques like knowledge-based data checks will continue to be necessary to verify the identity of an unknown person who presents himself. Biometric technologies may provide solutions to specific problems of securing physical space, securing access to data and equipment, and authenticating individuals at a particular point in a transaction, following their enrollment in a biometrics system.

Following enrollment, biometrics can and are being used to authenticate whether a person is who he or she claims to be. There are numerous discrete applications that can be found in limited production and in various pilot projects around the country, as the financial sector

reassesses the feasibility of specific biometric applications, often as a supplement to single-factor or two-factor authentication.

Before a financial institution can roll out a biometric system for its customers, however, the management must dispel or resolve customer concerns. Many people are concerned about the potential for governmental, as well as private sector, misuse of biometric data. Private sector organizations, like governmental agencies, must develop policies and procedures for collecting, using, storing, transferring, and disposing of biometrics. Private sector organizations, however, are likely to have greater scope for offering biometric technologies on a voluntary basis (or alternatively, are less likely to be able to mandate use, particularly by customers).

Others mistrust the integrity and accuracy of the information over the long term, and wonder how an organization will purge incorrect biometrics, or biometrics of past customers. While a PIN number is easier to lose or compromise than a biometric template, it is also easier to replace than a biometric that may have been stolen or spoofed. What happens when a biometric is compromised? Some also may fear physical harm from the more intrusive technologies, while others may have cultural reasons for not enrolling in a biometric program.

With education, consumers may become more aware of the benefits of using biometrics and the added security that attaches to an authentication system based on biometric templates. Biometric systems may benefit consumers in a number of ways, by increasing the security of identity information, improving convenience and speed of service, and possibly reducing the costs of transactions over time. Survey data suggests a broad acceptance of the need for enhanced security measures in recent years and the potential acceptance by most people of the use of biometrics if they are convenient to use and provide the promised security enhancements.

Recommendations

The Secretary of the Treasury makes no recommendations for legislative or administrative actions at this time.

Appendix A

Federal Register Notice

DEPARTMENT OF TREASURY

Public Comment on Formulating and Conducting a Study on the
Use of Biometrics and Other Similar Technologies to Combat Identity Theft

AGENCY: Department of the Treasury, Departmental Offices.
ACTION: Notice and request for comments.
Federal Register/Vol. 69, No. 41/Tuesday, March 2, 2004/Notices

SUMMARY: The recently enacted Fair and Accurate Credit Transactions Act of 2003 (FACT Act or Act) requires the Secretary of the Treasury (Secretary) to conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction. The Act also requires the Secretary to consult with a number of entities and the general public "in formulating and conducting the study." In order to fulfill its obligations under the Act, the Department of the Treasury (Treasury) seeks public comment on how Treasury should formulate and conduct the study.

DATES: Comments must be received at the specific address(es) listed below on or before April 1, 2004.

ADDRESSES: Because paper mail in the Washington, DC area and at Treasury is subject to delay, please consider submitting your comments by e-mail. Commenters are encouraged to use the title "FACT Act Biometric Study" to facilitate the organization and distribution of comments. All submissions must be in writing or in electronic form. Please send e-mail comments to factabiometricstudy@do.treas.gov or facsimile transmissions to FAX Number (202) 622–2310 re: FACT Act Biometric Study. Comments sent by paper mail should be sent to: Susan Hart, Financial Economist, Office of Critical Infrastructure Protection and Compliance Policy, U.S. Department of the Treasury, Annex Room 3174, 1500 Pennsylvania Avenue, NW, Washington, DC 20220, ATTN: FACT Act Biometric Study. Anyone submitting comments is asked to include his or her name, address, telephone number, and if available, FAX number and e-mail address. Treasury will consider all timely comments, and will make all comments in their entirety, including any personally identifying information such as name and address, available for public inspection and copying. Please do not submit confidential commercial or financial information. Comments may be inspected at the Treasury Library, Room 1428, Main Treasury Building, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. Before visiting the library, visitors must call (202) 622–0990 to arrange an appointment. (Treasury reserves the right to display all comments in their entirety electronically via the Internet, subject to Treasury's assessment at a later date of the practicability of managing and maintaining such a channel of access in this instance.)

FOR FURTHER INFORMATION CONTACT: Susan Hart, Financial Economist, Office of Critical Infrastructure Protection and Compliance Policy, Department of the Treasury, (202) 622–0129.

SUPPLEMENTARY INFORMATION:

I. Background

The President signed the FACT Act into law on December 4, 2003, Public Law 108–159, 117 Stat. 1952. The FACT Act amends the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and will provide consumers, companies, consumer reporting agencies, and regulators with new tools that enhance the accuracy of consumers' financial information and help fight identity theft. These reforms make permanent the uniform national standards that support our credit markets, and institute new consumer protections. Section 157 of the Act provides that the "Secretary of the Treasury shall conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction." Section 157 further requires the Secretary to submit a report to Congress containing the findings and conclusions of the study, together with recommendations for legislative or administrative actions as may be appropriate, within 180 days from the date of enactment of the Act. Section 157 also requires the Secretary to ''consult with Federal banking agencies, the FTC, and representatives of financial institutions, consumer reporting agencies, Federal, State, and local government agencies that issue official forms or means of identification, State prosecutors, law enforcement agencies, the biometric industry, and the general public in formulating and conducting the study.''

II. Request for Comments

This request for comment is issued pursuant to the requirement in section 157 that Treasury consult broadly in formulating and conducting the study on the use of biometric and other similar technologies. (Other means of consultation in formulating and conducting the study will also be used.) Treasury seeks comment on the questions set forth below and requests that respondents label comments with the corresponding question number and letter to which the comment relates. Additional relevant comments are welcome.

1. a. What range of biometric solutions could the private sector use to reduce the incidence and costs to society of identity theft by providing convincing evidence of who performed a given financial transaction?
   b. How are biometric technologies being applied now to reduce the costs and incidence of identity theft?
   c. What other technologies are being applied now to reduce the costs and incidence of identity theft?
   d. What biometric technologies could be applied in the future to reduce the cost and incidence of identity theft?
   e. Does the private sector have adequate incentives to adopt biometric and other technologies to reduce the costs and incidence of identity theft?

2. a. What is the rate of adoption by the financial services industry of biometric solutions for the purpose of verifying or authenticating who performed a given financial transaction? By other industries?
   b. What is the rate of adoption of other similar technology solutions provided by the private sector for the same or similar purpose?

3. What are the public's concerns with the use of biometrics?

4. What are the costs of the use of biometrics? What are the risks of using biometrics?

5. What are the tradeoffs for the consumer in using biometrics?

6. What are the benefits to consumers of the use of biometrics?

7. a. What has been the experience of industries that have used biometrics for the purpose of providing convincing evidence of who performed a given financial transaction? What has been the customer reaction?
   b. What has been the experience of industries that have used other similar technologies for the same or similar purpose? What has been customer reaction?

8. What barriers are there to the greater use of biometric and other technologies to reduce the cost and incidence of identity theft?

Dated: February 25, 2004

Michael A. Dawson,
Deputy Assistant Secretary, Department of the Treasury.
[FR Doc. 04–4604 Filed 3–1–04; 8:45 am]
BILLING CODE 4810–25–P

Appendix B

List of Respondents to the Federal Register Notice and Request for Comments, March 2, 2004

Public Comments were received from the parties listed below in response to the Federal Register Notice and Request for Comment on the Use of Biometrics and Other Similar Technologies to Combat Identity Theft published March 2, 2004. The are summarized on the following pages.

Accredited Standards Committee X9, Incorporated, Cynthia L. Fuller
Axalto, Neville Pattison
ChoicePoint, Charisse Chisolm Wilson
Countrywide Financial Corporation, Erik Stein, Christine Frye
CUNA & Affiliates, Michelle Q. Profit
Electronic Privacy Information Center, Chris Jay Hoofnagle
Financial Services Technology Consortium
Robert Gatenby
Dale Hill
ID Analytics, Inc., Steven S. Gal
Identix, Frances Zelazny
Individual, no signature, warnpc1
International Biometric Industry Association
Iridian, Robert J. Levin
Ed Kemo
Langley Federal Credit Union, S. Diane Nortness
LexisNexis, Thomas M. Regan
William Maner
Norm Marple
Max
Mortgage Bankers, Kurt Pfotenhauer
National Biometric Security Project
Pay By Touch, Steven L. Zelinger
Bob Pinheiro
Privacilla, Jim Harper
RDS, Kathy Pappas
Sagem Morpho, Inc., Jean-marc Suchier
ValidX Technologies Corporation, James Byers
Verdasys, Inc. Mounil Patel
WanuaFCU, Terry Nickerson
Wells Fargo, John D. Wright

Section 157 Study on the Use of Biometrics and Other Similar Technologies

Summary of Public Comments Received

In Question #1a of the Federal Register notice, respondents were asked about the range of biometric solutions that the private sector could use to reduce the incidence and costs to society of identity theft by providing convincing evidence of who performed a given financial transaction. There were twelve respondents. Their comments generally discussed the various biometric applications that are either currently in use by the financial sector or being examined for potential future uses. Respondents listed biometric applications such as fingerprint analysis, retina and iris scans, hand geometry, voice verification, facial recognition, signature and handwriting analysis, and keystroke dynamics.

Ten respondents, who included representatives of financial institutions, trade associations and technology companies, discussed the use of fingerprint analysis. One representative of a financial institution trade association stated that a small percentage of its members have reported using fingerprint scanning for employee access control; to streamline employee password usage; to verify credit union members at ATM kiosks; to authenticate members at shared credit union branches; and to authenticate members and nonmembers who attempt to use financial services, such as check cashing. Three respondents referenced using fingerprint image readers to authenticate employees attempting to enter restricted areas or computer systems. One representative of a technology vendor stated that the fingerprint has the longest history of use for personal identity, and, consequently, has the largest body of jurisprudence. One financial institution representative commented that fingerprints are now placed on checks at some financial institutions and check cashing establishments; however, in these cases, the fingerprints are flat prints (not biometric data) and their purpose is mainly evidentiary for law enforcement if it is determined that the check is fraudulent after it is cashed. The respondent suggested that enhancing the process to include biometric data would deter fraud in addition to making its use as legal evidence more compelling. One financial institution representative stated that taking fingerprints may be viewed as invasive and inconvenient by consumers, and, in addition, will require investment in developing and maintaining a database.

Eight respondents, including representatives of financial institutions, trade associations and technology companies, mentioned the use of retina scans as a biometric solution that could be used to reduce identity theft. One financial institution representative and one financial institution trade association representative commented on the use of retina scans by the ATM industry to authenticate customers. Another financial institution representative commented that retina scans have not gained a great deal of consumer acceptance, primarily due to concerns about the long-term effects of the laser scanners on the retina. Another respondent stated that retina scanning can be perceived as intrusive and this may make widespread adoption unlikely. One privacy advocate commented that some consumers fear that retina scans may make the eye susceptible to disease.

Seven respondents, including representatives of financial institutions, trade associations and technology companies, commented on the use of iris scanning technologies. One financial institution representative commented that iris scanning can be used by the ATM industry to authenticate customers or to detect the presence of a known criminal at the ATM and provide subsequent evidence of fraudulent withdrawals. However, this respondent did not cite any examples of current or planned use by the ATM industry. Another financial institution representative stated that the perceived intrusiveness of iris scanning may make widespread adoption unlikely. One technology vendor stated that iris recognition is the most accurate biometric identifier. The respondent described iris recognition technology as identifying people by the unique patterns of the iris—the colored ring around the pupil of the eye—and added that iris recognition is the highest accuracy single-factor identification method in the world.

Six respondents, who included representatives of financial institutions, trade associations and technology companies, discussed the use of hand geometry. One respondent described hand geometry as measuring and analyzing the shape and other characteristics of the hand. One financial institution representative stated that in using hand geometry, the number of false positive rates can be high and the training to ensure proper capture of the consumer's hand geometry can be fairly complicated.

Six respondents, who included representatives of financial institutions, trade associations and technology companies, discussed the use of voice verification. One financial institution representative stated that voice biometrics are the least invasive, with the broadest potential for use. The respondent added that, since the consumer need not be physically present to provide the biometric measure, voice biometrics can be used in both an "in-person" situation and remotely, for example for telephonic transactions. Implementation costs are therefore relatively low. Another financial institution representative stated that voice biometrics can be added to interactive voice recognition systems supporting telephone delivery channels. The respondent added that while not yet common practice, this technology could be used to secure telephonic transactions. Another respondent stated that voice recognition may be a good candidate for online Internet and personal computer-based delivery channels because home computer microphones are ubiquitous and inexpensive.

Six respondents, who included representatives of financial institutions, trade associations and technology companies, discussed the use of facial recognition. One respondent described facial recognition as the analysis of the geometry of the face and/or the heat on the face caused by the flow of blood under the skin. One financial institution representative stated that facial recognition is potentially affected by changes to facial structure such as by plastic surgery, growth of facial hair, and a variety of environmental factors. This respondent added that it is also not useful in remote transactions, such as via phone or the Internet.

Only four respondents discussed using signature or handwriting analysis as a biometric solution. One respondent described signature or handwriting analysis as analyzing the speed, velocity, and pressure of the hand as an individual signs his or her name. One representative of a financial institution stated that biometric signatures can be captured through electronic signing pads when customers open new accounts and that, while not yet common practice, these

signatures could be used to authenticate the identity of persons in subsequent financial transactions.

Only two respondents mentioned the possible use of keystroke dynamics. One representative of a financial institution described keystroke dynamics as measuring the speed, pressure, and cadence of an individual's keystrokes as he or she types on a keyboard.

In Question #1b, respondents were asked how biometric technologies are currently being applied to reduce the costs and incidence of identity theft. Ten respondents generally described uses such as physical and network access control for financial institution employees, physical access control to safe deposit box areas for customers, authentication at Point of Sale (POS) terminals, and other examples where biometric technologies are being used in the delivery of products and services to customers.

Five respondents, who included representatives of financial institutions, technology companies, and others, discussed the use of biometric technologies as a control mechanism limiting access to physical areas or networks. One respondent stated that some financial institutions have tested biometric access devices to ensure that only authorized employees have access to networks containing sensitive financial data. Another respondent listed specific examples such as password reset using voice authentication; and physical and computer network access control using hand geometry, finger image, and facial recognition. A technology vendor also described an example of a financial institution in Southeast Asia that uses biometric technologies to ensure that only authorized personnel handle bank transactions. Management of the Asian vendor has replaced traditional passwords with a system that biometrically verifies the identity of employees who authorize withdrawals, deposits and electronic transfers over a threshold value. The vendor stated that the system has been deployed in more than 700 branches of the client financial institution.

Three respondents discussed the use of biometric technologies to control access to physical areas for customers. One financial institution representative stated that fingerprints and hand geometry have been successfully integrated into some safe deposit box areas, adding that they offer a safeguard that prevents a thief from claiming customer valuables. The respondent also stated that dynamic signatures could be used to strengthen and ease signature verification for safe deposit box access.

Three respondents mentioned that some retailers have introduced the POS application of biometrics by using the technology to confirm the consumer's identity. One representative of a technology vendor recalled news articles about three retail grocery chains that have begun to implement fingerprint biometric solutions for their customers to use in the checkout line. Customers are able to purchase groceries by providing a fingerprint and PIN. A customer does not need to present a driver license/photo ID, credit card or check, as long as his or her fingerprint and credit card or bank account information is pre-registered with the retailer. The respondent also stated that in one case, the retailer has 40,000 customers participating in the program and that losses from fraudulent checks have been reduced by more than 60%.

Only two respondents described other examples where biometric technologies are being used in customer applications. One stated that keystroke dynamics could be used for authentication of customers for online banking applications. The other, a technology vendor, listed examples of two South American financial institutions that use biometric technologies to provide customers with a higher level of security for their transactions. In both examples, the institutions are using fingerprint technologies for customer verification at the teller window, as well as at selected ATMs. According to the respondent, customers are pleased that the use of a biometric eliminates the need to remember passwords and facilitates faster service. In one of the examples, the respondent reported that the institution also installed fingerprint readers at its credit card centers to verify customer identification prior to making a withdrawal from a credit card.

In Question #1c, respondents were asked about the range of other (non-biometric) technologies are being applied now to reduce the costs and incidence of identity theft. There were twelve respondents, who generally agreed that the most common form of authentication used today involves two factors (1) something you have (*i.e.*, a credit card, ATM card, account number, etc.) and (2) something you know (*i.e.*, passwords, hint questions, etc.). However, at least one respondent pointed out that this two factor system can fail when the "something you have" is lost or stolen and the "something you know" factor is revealed. Several of the respondents listed specific, non-biometric applications such as public key infrastructure (PKI) encryption, transaction monitoring and behavior analysis, and credit monitoring tools.

According to a representative of a research foundation, the most used technologies to fight identity theft are PIN, password, and user-ID capabilities. A representative of a technology company indicated that passwords are the primary technology used for access control in over 90% of companies. Representatives of another technology company and a trade association noted that many companies use basic authentication technologies, which also include magnetic card identification, photo ID and background checks. A few respondents remarked on several other low technology systems to prevent identity theft, which include greater staff and consumer education. One technology company cited from a Merchant Risk Council survey which indicated that 70% of responders use address verification systems, 54% use customer follow-up and real-time authorization, and 43% use post-process fraud management to combat identity theft.

Three of the respondents, including representatives of a financial institution trade association and technology companies, discussed the use of PKI encryption. A financial institution trade association representative stated that PKI encryption is a superior alternative to passwords. In this process, one key—known as the "public key"—is stored in a public repository where anyone can access it. The other key—known as the "private key"—is generated from a secure location where only the rightful holder is presumed to have access. Examples of this secure location include a computer chip on a "smart" card; or a magnetic stripe on a card. A second respondent stated that deployment of PKI encryption raises the bar against identity theft by guaranteeing the transaction is being triggered by a properly-issued token (*e.g.*, credit card); however, as with PIN and password based systems, PKI does not fully protect the consumer or institution from thefts caused by cards that are stolen.

One of these respondents, a representative of a technology company, offered two white papers which discussed several real world uses of smart cards. The first white paper, "Secure Identification Systems: Building a Chain of Trust," for instance, discusses the Department of Defense's (DoD) smart card program with over 4.4 million enrolled individuals in fifteen different countries. The program is expanding and future plans include extending the program to incorporate other communities with close ties to DoD. Future uses for the smart card, as discussed in one of the white papers, include encrypting e-mails, physical access with a contactless chip, and adding a biometric to have a 3-layer authentication process.

That same white paper noted that Rabobank uses smart card technology both internally and externally. The company has distributed at least 33,000 cards for employees to use in conjunction with their password to provide a two-layered security feature. Employees use the system to gain both physical and virtual access to the company's systems. Rabobank has also begun issuing smart cards to its large customers for certain types of transactions, in response to customer concerns and desires for stronger security on accounts. In order to centralize the security of the systems, Rabobank made all applications available on all distribution channels. "Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology" describes an example of the use of smart cards is in mobile phones. In a phone system, the smart card works to authenticate the device in order give access to the network. However, it does not work as an identifying system. This white paper also provides the example of the Western Governors' Association's Health Passport Program in which the pilot smart card program includes 25,000 women and children. The smart card helps enrollees to receive benefits as well as update their personal information.

In contrast to this widespread adoption, one representative of a technology company noted the lack of widespread smart card adoption in the case of a program introduced by a major charge card company. Two other respondents, representatives from a research foundation and a financial institution, stated that smart cards and PKI technology have a slow adoption rate in the private sector because the systems are expensive, do not produce a large rate of return on investment, and are not shown to help deter identity theft. Finally, a financial institution representative remarked that smart card technology pre-dates off-the-shelf biometric technology and smart cards are still in an early adoption phase in the United States.

Only two respondents discussed the use of transaction monitoring and behavior analysis. This involves using computer algorithms that search for irregularities in charge patterns in the hopes of identifying credit card fraud or theft. One of these respondents also stated that systems exist for financial institutions to verify addresses and Social Security numbers when accounts are initially opened and to perform real-time comparisons of account information against a database of known fraudulent bank accounts.

Finally, only one respondent, from a financial institutions trade association, stated that financial institutions can monitor credit reports and place "alerts" on accounts to notify consumers when suspect activity occurs, such as an unusually large purchase.

In Question #1d, respondents were asked about the range of range of biometric technologies that could be applied in the future to reduce the cost and incidence of identity theft.

The ten respondents to this question generally reiterated the various biometric applications listed in the responses to question 1a (*i.e.*, fingerprint analysis, retina and iris scans, hand geometry, facial recognition, etc.). A representative of the biometric industry wrote that all proven biometric technology could be used for this purpose.

Three respondents discussed storing the algorithm representing the biometric information on a chip-based, "smart" card. One of these respondents stated that storing the information on a smart card would permit a one-to-one match to be accomplished when needed. The respondent added that combining the biometric data with a PIN or pass code, and potentially PKI encryption, would create a strong three-factor authenticated transaction. Another respondent pointed out that chip-based smart cards have the ability to store account information, shipping/billing addresses, phone numbers, passwords, membership numbers, discounts, receipts, etc. Moreover, these chip-based cards can be embedded with digital identity information, such as biometric identifiers, for secure identity verification during credit and debit card transactions.

Finally, one respondent discussed the fact that broad implementation of biometric solutions in the future would require a significant reconfiguration of computers, ATMs, and POS terminals. The respondent also stated that new wireless-based biometric security solutions that use hand-held devices, such as an electronic key fob or mobile phone, are being developed and can take advantage of the existing wireless infrastructures.

In Question #1e, respondents were asked about whether the private sector has adequate incentives to adopt biometric and other technologies to reduce the costs and incidence of identity theft. Eleven respondents responded to this question. Only one respondent said "yes," two said "yes and no," and three respondents said "no." The other respondents provided general information on the topic, including positive views on efficiencies and cost savings.

The respondent who answered "yes" indicated the incentives were loss reduction, cost reduction, and enhancement of customer satisfaction and loyalty. However, the respondent also felt that the high cost of developing and implementing biometric solutions has resulted in slow, tentative and diverse adoption. The respondent added that public sector research and development funding is needed to help develop biometric solutions which can be cost-effectively adopted by the industry.

Most respondents who answered "yes and no" or that did not declare a position one way or another felt similarly. Most noted that the incentive to implement biometric solutions was to reduce fraud and loss. However, they also felt that this loss might not be offset by the cost to develop and implement biometric solutions. In contrast, a representative of the biometric industry indicated that savings and return on investment could be high for properly deployed biometrics used for security, efficiency, and customer service purposes.

The respondents who answered "no" said that the costs of implementing biometric solutions, including installation, software, hardware, on-going transaction, and maintenance costs, may be greater than the total cost of identity theft related fraud. One respondent stated that many financial institutions may find it difficult to integrate newer technologies with their legacy systems. Another respondent stated that some form of encouragement, such as a regulatory

requirement or tax break—or a negative incentive, such as requiring the financial institution to absorb some or all of the customers' losses—is needed. Another respondent replied similarly saying that an incentive for creditors would be to limit immunity from liability in identity theft cases only if the creditor can demonstrate that a good faith effort was made to verify the identity of the account applicant.

In Question #2a, commenters were asked what the rate of adoption by financial institutions of biometric technologies was. There were thirteen respondents. Their comments ranged from the overall slow adoption rate by financial institutions, examples of internal uses of biometric technology, some customer-facing applications, possible future uses, and other industries that currently use biometric technology.

Ten respondents, who included financial institutions, trade associations and technology companies, thought that financial institutions had a slow adoption rate of biometrics. One representative of a technology company reported that a study by Meridien Research released in January 2002 indicated that many financial institutions were considering using biometrics in the future driven by fraud losses and customer concerns. However, there has not been a large scale adoption by financial institutions since that report. Representatives from a financial institution and a technology company both noted that the financial services sector has a "wait-and-see" attitude and is more reactive in adopting new technologies. Another representative of a financial institution indicated that although the rate of adoption is slow in the financial sector, relative to other sectors, except possibly the transportation sector, the financial sector could be considered aggressive in adopting biometric technologies.

Only three respondents discussed examples of financial institutions using biometrics in customer-facing applications. One representative of a trade association noted specific cases where credit unions are employing biometrics such as fingerprints to identify members during check cashing transactions and access to self-service kiosks.

In question #2b, commenters were asked about the private sector rate of adoption of other similar technologies to combat identity theft. Responses came from financial institutions, trade associations, researchers and technology companies. Comments ranged from a discussion of passwords and PIN technologies to smart card technology.

A technology company noted that since customer authentication systems are less expensive, easier to integrate and cause less consumer concerns over privacy, those systems have higher adoption rates than biometric technologies. Another company also indicated that information-based authentication has a high adoption rate in several sectors. The company cited a survey by Gartner Group which showed that all 60 surveyed banks use some type of information-based identity authentication.

In question #3, commenters were asked what the public's concerns with the use of biometrics were. Twenty-two commenters responded to the question. Respondents suggested a range of concerns from basic unease about unauthorized use of information, to maintaining the integrity of the data, securing it against misuse by others, the capabilities of the technology, and fear of physical harm, for example from retina scans. One representative of a financial services

trade association described public concerns as revolving around the processes and procedures for gathering, storing, protecting, accessing and using the unique biological characteristics. A number of respondents, however, noted that public resistance to the use of biometrics may be overstated.

Of the four individuals who submitted brief comments, three expressed the view that the use of biometrics was an invasion of personal privacy. Two indicated that it would be more effective to focus on limiting the collection and use of Social Security numbers as a means of combating identity theft. Views from the six financial institutions or their representatives indicated sensitivity to potential customer reaction to the introduction of biometrics. At least half of the financial services respondents referred specifically to consumer privacy concerns as a key factor when considering the use of biometrics.

A number of other respondents also mentioned their concerns that consumers fear inadequate security for biometric information and biometric systems that would lead to unauthorized access and unintended use. A few respondents noted concern specifically about the linkage of government and corporate databases and the potential for disclosure of information to government or to others without the citizen ever knowing about the transfer.

A privacy advocacy organization recommended improvements in credit granting policies and procedures, which the organization noted had resulted in credit cards being issued to pets, as a better method to reduce identity theft than trying to enroll Americans in biometric systems. Generally, the privacy advocacy organization views biometric systems as too invasive, too easily compromised, too costly to correct, too costly to implement on a wide-scale basis, too unreliable to safeguard personal information, and too likely to exclude a substantial number of people (*e.g.*, those with worn or missing fingerprints).

In one attachment submitted with the response from the privacy advocacy group, the writer suggests an approach to combating identity theft that would change the "architecture of vulnerability" to the misuse of personal information in which we operate. The new architecture would establish controls over the data security practices of institutions and would afford people greater participation in the uses of their information based on "Fair Information Practices."[138]

Other supporting information provided by the privacy advocacy organization indicated that biometric systems are technically vulnerable -- to replay attacks, for example, when forged identification documents are used by an imposter to enroll his or her biometric in a system. Alternatively, biometric systems could be susceptible to electronic replay attacks by hackers intercepting a master template or a presented template that authenticates a user by successfully feeding the electronic information back into the system, the imposter can assume the corresponding identity.[139] Another supporting document noted the possibility of direct attack on

[138] "Identity Theft, Privacy, and the Architecture of Vulnerability," by Daniel J. Solove, *Hastings Law Journal*, Vol. 54, April 2003, p.37.

[139] Deutsche Bank Research, Economics, Internet revolution and new economy, May 22, 2002.

the biometric database by, for example, exchanging sets of data used as data reference sets. An assailant could forge user data, if the data sets did not have separate protections of their own.[140]

The organization also mentioned the difficulty of issuing a new biometric, compared with the relative ease of issuing a new Personal Identification Number (PIN). This concern is related to the problem of how to revoke privileges in a biometric system and can suggest the use of security tokens, like smart cards, to facilitate the use of biometrics as an added measure of security. Other technical issues of concern include the lack of interoperability among systems, which limits the scale of the solution to be remedied by the use of biometrics, and the robustness of hardware used to capture biometric information, which will determine the accuracy of the system.

A representative of a financial institution noted the importance of system compliance with the Americans with Disabilities Act of 1990 (ADA), and that certain ethnic or religious minorities also may have social concerns about using biometrics. Another representative of financial institutions indicated that some consumers may fear for their health or safety, for example in the case of retina scanning. One respondent from outside the financial sector raised the question of whether the biometric system would be compulsory, or would rely on voluntary participation of the willing.

A few representatives of financial institutions indicated, however, that customers would accept biometrics if well-informed about their use and security, satisfied that biometrics were producing efficiencies, and not deterred by the degree of intrusiveness. A representative of the biometric industry noted that privacy protecting attributes of biometrics are powerful and need to be better understood. Vendors and a processor also cited specific studies indicating potentially high public acceptance of biometric technologies for safeguarding information. A number of respondents placed priority on establishing standards and guidelines that would safeguard biometrics by, for example, protecting against unauthorized dissemination, assuring accuracy and fairness, and reassuring individuals about how information moves, where it goes, and how and why it is retained. A few commenters pointed to the need for concerted consumer education about a technology that is essentially neutral and can enhance the security of personal information.

In the two-part question #4, commenters were asked what the *costs of the use of biometrics* were and what *the risks of using biometrics* were. There were twelve respondents to the questions of costs, comprising representatives of a privacy advocacy group, four financial institutions, two research entities, the biometric industry, one processor, and three vendors of biometric and related products. None provided comprehensive insight into the assessment of costs.

The research entities explained that the actual costs of implementing biometrics can vary widely, and that costs can only be determined on a case-by-case basis. One financial institution respondent indicated that the cost of usage may be relatively low, but implementation costs are

[140] "Body Check," Heise Zeitschriften Verlag.

high. A credit union respondent stated that the costs for smaller credit unions was too high to be absorbed.

The privacy advocacy organization noted that biometric systems may need to be run in conjunction with other systems, perhaps requiring a biometric sensor and a card reader. This would mean maintaining potentially costly parallel infrastructures and would present unique revocation challenges. Fall back systems also may be expensive. A processor noted that there are intellectual property costs related to setting a national standard for biometric enrollment, which would help to facilitate expansion of the use of biometrics. A representative of financial institutions noted that a very strong security policy would be necessary for storage of biometric data, which could be costly to implement and maintain.

Implementation of a biometrics program at the enterprise level could easily cost hundreds of thousands of dollars, even if the cost of fingerprint readers has dropped considerably in recent years. One of the research group respondents noted consideration had to be given to the number of sites to be affected, the degree to which existing devices must be modified, and the cost of enrollment. This respondent also mentioned the importance of assessing the impact on legacy systems. Potential costs also must be assessed against hard numbers on the losses from identity theft, expenses related to PIN and password administration, staff required to maintain adequate physical security without biometrics, and outdated business processes for conducting audits and reducing vulnerabilities.

Many of the components of costs, like hardware and application software, are similar to other systems, while others, like retina scanners, are unique to biometrics. A representative of a financial institution explained that if the costs (such as device hardware, enrollment /verification software, storage/database, installation/implementation labor, annual maintenance, testing and tuning, support staff training and labor, help desk staff training and labor, and customer communication) exceed the savings (*e.g.*, productivity gains), a business case may not exist.

Twelve commenters responded to the question about risks of implementing biometric technologies to combat identity theft. One research entity alone stated that there were no known physical or safety risks and that the security features of using biometrics diminished privacy risks. The representative of the biometric industry reiterated earlier comments that when used properly, biometrics post virtually no risk. The remaining respondents suggested a variety of risks. One representative of a financial institution specifically mentioned the risk of inaccurate identification of a person when he or she enrolls in the biometric system, thus undermining the accuracy of the biometric data from the outset. At least two respondents specifically mentioned the potential negative reaction of customers or users to intrusive biometric technologies. At least five respondents cautioned that the potential for false rejections and acceptances presents a technical risk of unreliability. One credit union noted that this could lead to legal liability, for example, for denial of access to customer accounts.

A few respondents noted that the technology and its effective use is evolving, and also that biometrics lack sufficient certification of security, accepted solutions or standards, and interoperability. A few others indicated that poor implementation and lack of adequate security present risks, as does picking the wrong biometric for the application or risk scenario at hand.

Both the technology and its implementation at the retail level must be good enough that the consequences of a failure are not worse than they are today when someone is erroneously authenticated.

A privacy advocacy organization stated:

> Because of the numerous practical, logical, and technological flaws inherent in any biometric implementation, use of biometric technologies will not serve to effectively prevent identity theft. Instead, it will create new liabilities while draining away resources and threatening privacy.[141]

A representative of a technology company discussed the importance of collecting high quality biometric data and the difficulty of managing data on large populations. Enrollment challenges contribute further to risk. Often, as claimed by a research foundation, the enrollment piece of the system is seen as a "labor-intensive process," since the initial identification of a customer is often difficult. An individual respondent noted that remote enrollment creates even greater challenges since there is greater possibility to use counterfeit or stolen data.

In question #5, commenters were asked what the tradeoffs for consumers in using biometrics were. There were nine respondents, two of which indicated that there was no loss to consumers using biometrics. Four respondents saw a tradeoff between privacy and security. Three respondents, including one of those already mentioned, saw a tradeoff between inconvenience and enhanced security. Inconvenience might include the risk of false rejections or acceptances, or of following new processes, like enrolling in a biometric system. The privacy advocacy organization indicated that increased speed in transactions might be obtained at the expense of errors. One of the supporting documents provided by this respondent also indicated a tradeoff between security and convenience. A representative of the biometric industry indicated that biometric substitutes for alternative technologies provide cost-effective increases in productivity, fraud reduction,, and consistent and reliable service.

In question #6, commenters were asked what the benefits to consumers of the use of biometrics were. There were thirteen respondents, eight of whom found that increased security was the chief benefit of using biometrics. One representative of a financial institution indicated that biometric technologies can help to protect personal information. Another respondent noted that the inability to steal or reverse engineer a biometric template generally benefited consumers. More than half the respondents also believe that consumers will benefit from improved convenience, while at least two saw the possibility of reduced costs to consumers ultimately resulting from efficiencies.

In Question #7a, respondents were asked about the experience of industries that have used biometrics for the purpose of providing convincing evidence of who performed a given financial transaction. There were nine respondents, most of whom cited examples such as pilot programs using biometric technology at ATMs and in the retail/POS environment. The

---

[141] EPIC, p. 11.

respondents also cited non-financial industry examples such as the Departments of Motor Vehicles capturing biometric data, government agencies using biometrics in travel documents and border control, and the Department of Defense using fingerprint images in military identification cards.

A representative of the biometric industry noted highly positive reaction to properly deployed biometrics. One respondent from a technology research group stated that customer reaction has been favorable in many cases (fingerprint to cash checks, signature pad to open accounts, voice verification to activate credit cards), and mixed in others. This respondent also said that there have been a number of pilot programs using biometric technology involving facial, fingerprint and iris recognition at ATMs. The respondent reported that, while there has been some negative reaction to iris scans, there have been positive reactions as well. The respondent stated that in a 1998 ATM pilot of iris recognition, 80 percent of the customers eligible to enroll did so, and of those, 95 percent said they were satisfied with the biometric ATMs.

With regard to the retail/POS environment, a technology vendor stated that customer reaction has been very positive, and that some grocery store retailers are now expanding their programs. The respondent felt that grocery store experiences provide a very good view of public reaction because this represents an ordinary customer experience.

One representative of a technology company also noted several examples of other industries that have used biometrics. For instance, the Department of Defense (DoD) has a pilot program in which it uses biometrics and other forms of identification for authentication of DoD officials and contractors from multiple companies. The Transportation Security Administration (TSA) was mandated by federal legislation to develop an identification program for 12-15 million individuals. TSA plans to include biometrics during the initial phase. The U.S. Passport program intends to incorporate a digital picture as a biometric on a limited basis initially, but plans to use biometrics on all new passports by the end of 2005. A representative from a technology company cited a healthcare company that uses fingerprint technology. Although the healthcare company managed initial concerns about consumer acceptance, they found that consumers liked the program. A representative from the technology company noted that the State of Colorado uses facial recognition biometrics with a database of 11 million records in order to control and reduce the issuance of duplicate driver's licenses and to prevent fraud. A representative of a third technology company commented on the State of Washington's voluntary program that permits drivers to add a biometric component to his or her license in order to reduce the issuance of duplicate licenses and identity theft. That technology company representative and a representative from a research foundation both discussed a grocery store chain that offers customers the ability to use their fingerprints at the point-of-sale for convenience.

Biometrics have also been used in at least 45 school districts nationwide according to a fourth technology company. Those school districts use finger-scanning technology to track student expenses. The representative from the company also asserted that one school district was considering the use of thumbprint technology for access onto its buses.

In Question #7b, respondents were asked about the experience of industries that have used other similar technologies for the same or similar purpose. There were eleven respondents. Two respondents stated that other forms of authentication have been more successful with commercial banking customers who execute high dollar amount transactions and, therefore, are subjected to greater risk. The respondents cited examples such as onetime password tokens, smart cards and radio frequency identification (RFID). The respondent added that the increased risk of these transactions, combined with the relative technical sophistication of commercial business customers, makes the added expense and challenge of strong authentication acceptable.

A technology vendor stated that its customers' experience in the application of information-based identity authentication solutions has been exceptionally good. The vendor cited a bankcard commercial customer as an example. Over a six month period following the implementation of an information-based identity authentication solution, the client reportedly realized a 77 percent reduction in charge-offs due to fraud.

In question #8, commenters were asked what barriers there are to greater use of biometrics and other technologies to reduce the cost and incidence of identity theft. There were seventeen responses coming from representatives of financial institutions, trade associations, researchers and technology companies. Most of the comments noted several barriers to greater adoption such as cost, consumer concerns, privacy issues, interoperability, and the lack of standards.

A representative of the biometric industry indicated that inertia and lack of education are principal barriers. Eleven respondents regarded both cost and consumer concerns as the two main barriers to the wider adoption of biometric technology in the financial sector. Most of the commenters, including representatives from trade associations, financial institutions and technology companies, stated that implementation costs are a large barrier to biometric use. The representative of one trade association, for example, noted that the costs associated with integration and infrastructure upgrades are large. Four commenters were also concerned with equipment costs which would include installation, hardware, software, operation, and maintenance costs. Representatives from a trade association and a technology company were also concerned with the costs of training staff to manage the biometric systems, as well as the costs to educate their customers. Those same commenters stated that the total costs are too great for many smaller institutions. A representative of another trade association noted that during analysis few institutions could show quantifiable cost savings from implementation. Finally, one individual noted that biometrics for online transactions would include high equipment costs for consumers to have the necessary hardware and software products on their personal computers.

Eleven respondents noted consumer concerns, including privacy, security and acceptance rates, were a difficult hurdle to greater use of biometric technologies. Representatives of several institutions noted that consumers are concerned about their personal privacy. A representative of one technology company and one financial institution noted that customers do not feel comfortable releasing their biometric data and are concerned with any invasive procedure. The representative of a second technology company asserted that consumers are concerned that biometric data can reveal race, ethnicity or gender, which they fear could create fair lending issues. The representative from a third technology company stated that biometric systems do not

have adequate security, while a think tank claimed the biometric data can be copied or scanned easily. Apart from privacy concerns, a few representatives from financial institutions were uncertain of the consumers' reactions to biometric systems. The representative of one financial institution noted that companies must gain consumer trust in order to implement greater use of biometric systems.

Representatives of seven institutions remarked that interoperability and the complexity of biometric systems is a barrier to greater use of the systems. The representative of one technology company and one trade association indicated that the biometric systems must be compatible with existing infrastructures, which is often a complex and difficult outcome to achieve. A representative of one technology institution asserted that many credit bureaus do not have the capabilities to support such systems at this time. In addition, the representative of a technology company and research foundation were concerned that different systems will not be able to communicate and members will need to carry multiple forms of identification for access to multiple systems.

Along those lines, six respondents claimed that the lack of standards is a barrier to the wider adoption of biometric systems. Most of the representatives of those institutions indicated that if standards were in place to preserve the integrity and stability of the systems, many of the other barriers would no longer hold. For instance, a representative of one company noted that standards for security to protect the privacy of the members would calm some of the consumer concerns regarding privacy. That same company remarked that if there were better standards that could be applied across the sector, then the accuracy and stability of the biometric systems would be better. The representative of one financial institution noted that the lack of compliance with established standards from accredited standards committees is a deterrent.

Appendix C

Biometric Systems:
Some Technical and Operational Features to Assess

Features	Assessment
Acquisition Ease	The relative simplicity (and accuracy) of a biometric measurement (*e.g.*, finger print scan, iris scan) to be gained from the sensor device.
Acquisition Repeatability	The ability of a biometric, or sensor, to acquire the same metric in successive acquisitions.
Acquisition Time	The average time a sensor needs to acquire a metric.
Biometric Uniqueness	A relative strength of a specific biometric to uniquely identify a subject.
Biotrait Template Stability	A statement of relative biological impacts (*e.g.*, aging, disease, surgery) on a specific biometric.
Costs	Cost components include • biometric capture hardware • back-end processing power to maintain the database • research and testing of the biometric system • installation, including implementation team salaries • mounting, installation, connection, and user system integration costs • user education, often conducted through marketing campaigns • exception processing, or handling users who cannot submit readable images because of missing appendages or unreadable prints • productivity losses due to the implementation learning curve; and system maintenance.[IEEE2001-LIU][142]
Crossover Error Rate (CER)	"A comparison metric for different biometric devices and technologies; the error rate at which false match rate equals false non-match rate. The lower the CER, the more accurate and reliable the biometric device." [IEEE-LIU][143]
Database Storage	The average size, in bytes, of a specific biometric template (not raw unprocessed image).
Distance To Sensor	The maximum (ideal) distance, between sensor and subject, for a specific sensor (implementation specific) to perform optimally.
Enrollment	"The initial process of collecting biometric data from a user and then storing it in a template for later comparison." [IEEE-LIU]
Enrollment Ease	The relative simplicity (and accuracy) of a biometric measurement (*e.g.*, finger print scan, iris scan) to be acquired and entered into a database.
Inherent Channel Robustness	An indication of biometrics differences based on a change of sensors, vendors, templates, different media (*e.g.*, hardcopy fingerprints vs. Electronic)

[142] [IEEE2001 – LIU] Simon Liu, Mark Silverman, *A Practical Guide to Biometric Security Technology*, IEEE Computer Society.

[143] [IEEE – LIU] Simon Liu, Mark Silverman, *A Practical Guide to Biometric Security Technology*, IEEE Computer Society.

Features	Assessment
Population Subgroup Sensitivity	Identification of any anthropological deviations based on race, geographical location, age, sex, et al.
Processing Time	Processing of three distinct aspects: (1) segmentation of a biometric sample, (2) isolating and extracting relevant features, and (3) creation of and storing a biometric template.
Representation Stability	"Organizations should consider a biometrics' stability, including maturity of the technology, degree of standardization, level of vendor and government support, market share, and other support factors. Mature and standardized technologies usually have stronger stability." [IEEE-LIU]
Spoof ability	A statement of the ease or difficulties of a subject to obscure his/her identify or impersonate another person.
Susceptibility to Noise	Identification of environmental "contaminants" which introduce a level of difficulty in accuracy of a biometric.
Test Data Availability	A statement whether there is available biometric test data, data set size, etc
User Acceptance	"Generally speaking, the less intrusive the biometric, the more readily it is accepted. However, certain user groups—some religious and civil-liberties groups—have rejected biometric technologies because of privacy concerns." [IEEE-LIU]

Sourcing obtained from open sources, academia, technical literature and existing government documents referenced unless otherwise noted.

Appendix D

Glossary

Automated Fingerprint Identification System	A system originally developed for use by law enforcement agencies, which compares a single fingerprint against a database of fingerprint images.
Algorithm	A sequence of instructions that tells how to solve a problem. Used by biometric systems to tell whether a sample and a template are a match.
Attempt	The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.
Biometrics Application Programming Interface (BioAPI)	A standard that defines an open API that allows software applications to communicate with a broad range of biometric technologies in a common way
Biometrics	Automated methods of recognizing a living person through the measurement of distinguishing physiological or behavioral traits.
Biometric Data	The information extracted from a biometric sample and used either to build a reference template on enrollment, or to compare against a previously created reference template.
Biometric Feature	A representation from a biometric sample extracted by the extraction system.
Biometric Sample	Raw data captured as a discrete unambiguous, unique, and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric data collection system (for example biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).
Biometric System	An automated system capable of capturing a biometric sample from an end user, extracting biometric data from the sample, comparing the data with one or more reference templates, deciding on how well they match, and indicating whether or not an identification or verification of identity has been achieved.

Biometric Template	The biometric enrollment data for a user. A machine-encoded representation of the trait created by a computer software algorithm that enables comparisons (matches) to be performed to score the degree of confidence that separately recorded traits identify (or do not identify) the same person.
Biometric Identification Record (BIR)	Any biometric data that is returned to the biometric application; including raw data, intermediate data, processed sample(s) ready for verification or identification, as well as enrollment data.
Capture	The process of taking a biometric sample via a sensor from a user.
Common Biometric Exchange File Format	A standard that describes a set of data elements necessary to support biometric technologies in a common way
Comparison	The process of comparing a biometric sample with a previously stored reference template or templates. See also *One-To-Many* and *One-To-One*.
Enrollee	A user with a stored biometric reference template on file.
Enrollment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates and associated data representing that person's identity.
Extraction	The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
Failure to Acquire Rate (FTA)	The proportion of attempts for which a biometric system is unable to capture an image of sufficient quality. When a biometric system allows multiple attempts, FTA measures failure to capture over these multiple attempts.
Failure to Enroll Rate (FTE)	The proportion of the user population for whom the biometric system is unable to generate reference templates of sufficient quality. It is the equivalent of FTA for the enrollment process, and depends on the procedures used in enrollment (which may differ from the procedures for later identification). It includes those who, for physical or behavioral reasons, are unable to present the required biometric feature.
False Acceptance Rate (FAR)	The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts.

False Match Rate (FMR)	The rate for incorrect positive matches by the matching algorithm for single template comparison attempts. For a biometric system that uses just one attempt to decide acceptance, FMR is the same as FAR. When multiple attempts are combined in some manner to decide acceptance, FAR is more meaningful at the system level than FMR. Alternative to *False Acceptance Rate,* it is used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'.
False Non-Match Rate (FNMR)	The rate for incorrect negative matches by the matching algorithm for single template comparison attempts. For a biometric system that uses just one attempt to decide acceptance, FNMR is the same as FRR. When multiple attempts are combined in some manner to decide acceptance, FRR is more meaningful at the system level than FNMR. Alternative to *False Rejection Rate*, it is used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'.
False Rejection Rate (FRR)	The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. The False Rejection Rate normally excludes 'Failure to Acquire' errors.
Feature Extraction	The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template.
Flat Fingerprint Image	Impressions of the finger that can be captured on an inexpensive single finger scanner. Flat fingerprints can be acquired quickly with little operator training, but the overall area of flat fingerprints is usually less than half that of rolled fingerprints, with a corresponding loss of information content.
Gallery	The database of biometric templates of persons previously enrolled in the biometric system.

Identification	The one-to-many, or 1:N, process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the person whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with *Verification*.
Identity	The common sense notion of personal identity. A person's name, personality, physical body, and history, including such attributes as educational achievements, employer, security clearances, financial and credit history, etc. In a biometric system, identity is typically established when the person is registered in the system.
Image	The digital representation of a biometric as typically captured via a video, camera or scanning device.
Impostor	A person making a false claim about identity to the biometric system.
Latent Fingerprint Image	Fingerprints collected from a crime scene. Latent searching and identification require great expertise, and is very computer-intensive—searching one latent is about as computer-intensive as searching 50 sets of ten rolled fingerprints. A highly-trained latent examiner is required to prepare a latent search, and to make the identification.
Live Capture	The process of capturing a biometric sample by an interaction between a person and a biometric system.
Live Processing	Direct enrollment/ identification of potential users via the normal biometric capture process. Compare off-line processing.
Match/Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. If the score exceeds the threshold, the result is a match; if the score falls below the threshold, the result is a non-match.
Matching Score	A measure of similarity or dissimilarity between the biometric data and a stored template, used in the comparison process.
Multimodal Biometric	A system or device that utilizes more than one physiological or behavioral characteristic for enrollment, verification, or identification, *e.g.* fingerprint and hand shape; or fingerprints from two separate fingers. All statistical analysis of multimodal systems should consider how the modes are combined in the comparison process.

Minutiae Points	Local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.
Negative Claim	A claim by a user *not* to be enrolled in the biometric system. This may be needed to establish that double claims are not being made.
One-to-Few Matching	A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a "watchlist" of persons who warrant detailed identity investigation or are known criminals, terrorists etc. See also *Watchlist*.
One-to-Many Matching	See *Identification*
One-to-One Matching	See *Verification*
Operational Testing	Testing a biometric system to measure its statistical properties (*e.g.* FAR and FRR) in a specified operational environment, with a specific target population.
Plain Fingerprint Image	The image captured from a finger placed on a platen without any rolling movement – the center portion of a rolled image.
Rolled Fingerprint Image	The image area captured that is located between the two edges of the fingernail. It is acquired using a rolling motion from one edge of the fingernail to the other.
Positive Claim	A claim by a user to be enrolled in the biometric system. An explicit claim is often accompanied by user identification, and may also be associated with a password or PIN.
Probe	An image containing the face of an unknown individual that is presented to an algorithm to be recognized. Probe can also refer to the identity of the person in a probe image.
Probe Set	A set of images containing the face of an unknown individual that is presented to an algorithm to be recognized.
Registration	The process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Receiver Operating Characteristics (ROC)	A collection of data points that describe a biometric system's numerous FAR/FRR associations. ROCs show the performance of the biometric system over a range of decision criteria – usually as a graph that relates FAR to FRR as the decision threshold varies.
Scenario Testing	Testing a biometric system to measure its statistical properties (*e.g.* FAR and FRR) in an environment modeled to simulate a particular application.
Score	A number on a scale from low to high, measuring the success that a biometric probe records (the person you are looking for) matches a particular gallery record (a person previously enrolled).
Sensor	The physical hardware device used for biometric capture
Slap Fingerprint Image	Four-finger simultaneous impressions are a special case of flat fingerprints in which the four fingerprints from each hand are simultaneously captured in a single image.
Technology Testing	Testing one or more biometric systems to measure statistical properties (*e.g.* FAR and FRR) to compare various algorithms and technologies – usually achieved by off-line processing**.**
Template	A user's stored reference measure based on biometric feature(s) extracted from biometric sample(s).
Template/Reference Template	Data representing the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.
Threshold	A parametric value used to convert a matching score to a decision. A threshold change will usually change both FAR and FRR – as FAR decreases, FRR increases. The threshold is often controlled by a biometric system administrator and establishes the degree of correlation necessary for a comparison to be deemed a match.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Normally used in one-to-one systems. Verification requires that an identity be claimed, after which the individual's enrollment template is located and compared with the verification template. Contrast with *Identification*.

Vulnerability	The potential for the function of a biometric system to be compromised by *e.g.* intention (fraudulent activity); design flaw (including usage error); accident; hardware failure; or external environmental condition.

Appendix E

Summary of Biometric Standards Projects

Standards are an integral part of discussion of Biometrics. The GAO Report titled, *Technology Assessment, Using Biometrics for Border Security*, November 2002 provides an overview for the development of a Biometric Standard. The following discussion was extracted from the GAO-03-174 Report:

> "Identifying, exchanging, and integrating information from different and perhaps unfamiliar sources and functions are essential to an effective biometrics application. Without predefined standards, system developers may need to define in detail the precise steps for exchanging information, a potentially complex, time-consuming, and expensive process. The risks associated with not adopting standards for a system are significant, because of the length of time the system must remain operational and the rapid pace of technological change. The proprietary technology of choice today may not be cost-effective or even supported tomorrow.
>
> Attempts to standardize biometrics are under way in various areas, such as the mechanics of image capture, the accuracy of data as they are extracted, and device interoperability. However, the majority of biometric devices and their software are still proprietary in many respects. For example, the method for extracting features from a biometric sample such as a fingerprint differs among most, if not all, vendors. Templates containing biometric data, time stamps, encryption features, and device information are also not standard. Devices from company A do not necessarily work compatibly with devices from companies B and C. Incompatibility is also an issue for communication between devices and host computers, since programs are developed from vendors' software development kits. Each vendor designs a software development kit for its own products, so that the programs developed for one vendor's product generally cannot be used with another vendor's products."[144]

The following table lists the current status of biometric standards within the American National Standards Institute (ANSI) and the International Organization of Standards (ISO). ANSI is a private, non-profit organization (26 U.S.C. §501(c)(3)) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.[145] ISO provides a network of national standards institutes from 146 countries working in partnership with international organizations, governments, industry, business and consumer representatives.[146] Within ANSI,

---

[144] GAO-03-174 Technology Assessment, *Using Biometrics for Border Security*, November 2002, Pages 62-63.

[145] ANSI definition obtained from ANSI Homepage at http://www.ansi.org/about_ansi/overview.

[146] ISO definition obtained from ISO Homepage at http://www.iso.org/iso/en/ISOOnline.frontpage.

the average time for the development of a standard is 12 – 18 months; within ISO, the average time for the development of a standard is 2 years. This table also includes two biometric standards developed outside of the ANSI and ISO processes, NISTIR 6529-A (the Common Biometrics Exchange Formats Framework) and the OASIS XCBF (XML Common Biometric Format) specification.

Designation	Title	Status
Interfaces		
Common Biometric Exchange Formats Framework	NISTIR 6529-A ISO/IEC FCD 19785	Original CBEFF standard published as NISTIR 6529 in 2001; NISTIR 6529-A published in 2004 Candidate for INCITS M1 Fast Track Process; In FCD ballot
Information Technology—Biometric Application Program Interface™ (BioAPI™)	ISO/IEC FCD 19784	Second Final Committee Draft ballot to be issued in July 2004
BioAPI™ Specification, Version 1.1	ANSI/INCITS 358-2002	Published as ANSI Standard in 2002
Information Technology—Biometric Interworking Protocol	ISO/IEC WD 24708	Working Draft
Information Technology—Common Biometric Exchange Formats Framework (CBEFF)—Part 1: Data Element Specification	ISO/IEC FCD 19785-1	Final Committee Draft
Information Technology—Common Biometric Exchange Formats Framework (CBEFF)—Part 2: Procedures for the Operation of the Biometrics Registration Authority	ISO/IEC FCD 19785-2	Final Committee Draft
OASIS XML Common Biometric Format, V 1.1	OASIS XCBF v1.1	Published as OASIS Standard in 2003
Modality		
Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Tattoo (SMT) Information	ANSI/NIST-ITL 1-2000	Approved ANSI standard in use by the FBI and other federal, state, and local agencies. It is also a de facto standard used by the UK's Home Office and Interpol.
Information Technology—biometric data interchange formats—Part 1: Framework/Reference Model	ISO/IEC WD 19794-1	Working Draft
Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data Interchange Format	ISO/IEC FCD 19794-2	Final Committee Draft under ballot
Information Technology—Biometric Data Interchange Formats—Part 3: Finger Pattern Spectral Data Interchange Format	ISO/IEC FCD 19794-3	Committee Draft under ballot
Information Technology—Biometric Data Interchange Formats—Part 4: Finger Image Data Interchange Format	ISO/IEC FCD 19794-4	Final Committee Draft under ballot
Information Technology—Biometric Data Interchange Formats—Part 5: Face Image Data Interchange Format	ISO/IEC FCD 19794-5	Final Committee Draft under ballot

Designation	Title	Status
Information Technology—Biometric Data Interchange Formats—Part 6: Iris Image Data Interchange Format	ISO/IEC FCD 19794-6	Final Committee Draft
Information Technology—Biometric Data Interchange Formats—Part 7: Signature/Sign Behavioral Data Interchange Format	ISO/IEC WD 19794-7	Working Draft
Modality		
Information Technology—Biometric Data Interchange Formats—Part 8: Finger Patter Skeletal Data Interchange Format	ISO/IEC WD 19794-8	Committee Draft Under Ballot
Information Technology—FR Format for Data Interchange	ANSI INCITS 385-2004	Recently approved ANSI standard
Information Technology—Finger Image Based Interchange Format	INCITS 381	Completed Public Review
Information Technology—Finger Minutiae Format for Data Interchange	ANSI INCITS 378-2004	Published as ANSI standard in 2004
Information Technology—Finger Pattern Based Interchange Format	ANSI INCITS 377-2004	Published as ANSI standard in 2004
Information Technology—Hand Geometry Format for Data Interchange	INCITS PN-1643-D	Completed Public Review
Information Technology—Iris Image Interchange Format	INCITS 379	ANSI approval expected by Q2 2004
Information Technology—Signature/Sign Image Based Interchange Format	INCITS PN-1603-D	Completed Public Review
Conformance Testing		
Information Technology—Conformance Testing Method and Procedure for BioAPI™ of ISO 19784 Part 1	ISO/IEC WD 24709	Working Draft
Information Technology— Conformance Testing Methodology for the Finger Image Data Interchange Format	N/A (new)	Project proposal approved by M1, May 2004
Information Technology— Conformance Testing Methodology for the Finger Minutiae Interchange Format	N/A (new)	Project proposal approved by M1, May 2004
Information Technology— Conformance Testing Methodology for ANSI/INCITS 358-2002, BioAPI™ Specification	N/A (new)	Project proposal approved by M1, May 2004
Performance Testing		
Information Technology—Biometric Performance Testing and Reporting	BSR INCITS PN-1602-9	Working Draft
Information Technology—Biometrics Performance Testing and Reporting—Part 1: Test Principles	ISO/IEC WD 19795-1	Working Draft
Information Technology—Biometrics Performance Testing and Reporting—Part 2: Testing Methodologies	ISO/IEC WD 19795-2	Working Draft
Information Technology—Biometrics Performance Testing and Reporting—Part 3: Specific Testing Methodologies	ISO/IEC AWI 19795-3	Approved Work Item

Designation	Title	Status
Information Technology—Biometrics Performance Testing and Reporting—Part 4: Specific Test Programs	ISO/IEC AWI 19795-4	Approved Work Item
Information Technology—Evaluating Multi-Modal Biometrics Systems: Concepts of Operation and Methods of Performance Evaluation (study project)	INCITS PN-1627-S	Study Project
Application Profiles		
Biometric Profiles for Interoperability and Data Interchange—Part 1: Biometric Reference Architecture	ISO/IEC WD 24713-1	Working Draft
Biometric Profiles for Interoperability and Data Interchange—Part 2: Biometric Profile for Employees	ISO/IEC WD 24713-2	Working Draft
Information Technology—Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric Based Personal Identification for Border Management	BSR INCITS PN-1567D	In Public Review
Information Technology—Application Profile for Point-of-Sale Biometric Verification/Identification	BSR INCITS PN-1573-D	30-day M1 letter ballot will be issued on whether to advance to Public Review
Information Technology—Application Profile—Interoperability and Data Interchange—Biometrics Based Verification and Identification of Transportation Workers	BSR INCITS PN-1566-D INCITS 383	In Second Public Review
Information Technology—Biometric Profile—Interoperability and Data Interchange—DoD Implementations	INCITS PN-1676-D	Working Draft
Information Technology—Biometric Profile—Application Profile for Residential and Commercial Access Control	N/A (new)	Project proposal approved by M1, May 2004
Security-Related		
Biometric Information Management and Security	ISO/WD 19092	Working Draft
Biometric Information Management and Security for the Financial Services Industry	ANSI X9.84-2003	Published in 2003 (replaces 2001 edition)
Information Technology—Security Techniques—Framework for Security Evaluation and Testing of Biometric Technology	ISO/IEC AWI 19792	Approved Work Item
Others		
Identification Cards—Integrated Circuits(s) Cards with Contact—Part 11: Personal Verification Through Biometric Methods	ISO/IEC FDIS 7816-11	Pending final approval as an International Standard
Information Technology—Motor Vehicle License—Part 3: Biometrics, Image Processing and Cryptography	ISO/IEC AWI 18013-3	Approved Work Item
Multi-Modal Biometric Fusion	ISO/IEC AWI 24722	Approved Work Item
Multi-part Technical Report on Cross Jurisdictional and Societal Aspects of Implementations of Biometric Technologies	ISO/IEC AWI 24714	Approved Work Item
Standing Document on Harmonized Biometric Vocabulary	JTC1/SC37 Standing Document 2	Document Under Review

Appendix F

Current Academic Research Efforts in Biometrics

Institution	Country	URL	Face	Finger	Iris	Voice	MultiModal	Testing	Details
Brown University	USA	http://www.cog.brown.edu	✓						Face Detection and enhancement, cognitive understanding
Carnegie Mellon University	USA	http://amp.ece.cmu.edu/projects/	✓			✓	✓	✓	3D face matching algorithms, face detection, enhancement, sensor fusion, PIE face database
Chinese Academy of Sciences	China	http://www.sinobiometrics.com/index.html	✓		✓		✓	✓	Face and Iris image databases, multimodal classifier integration, various FR, iris recognition
Colorado State University	USA	http://www.cs.colostate.edu/evalfacerec/index.html	✓						FR algorithms (eigenvector), evaluation
Ecole Polytechnique Federale de Lausanne	Switzerland	http://diwww.epfl.ch/lami/cvision/person_authentication.html	✓				✓		Face tracking, audio/video fusion
IDIAP – Dalle Molle Institute for Perceptual AI	Switzerland	http://www.idiap.ch	✓			✓	✓		Skin color, speaker id/verification, face/speech fusion
Kyushu University	Japan	http://www.mis.atr.co.jp/~mlyons/jaffe.html	✓					✓	Facial expression classification
Michigan State University	USA	http://biometrics.cse.msu.edu/	✓	✓			✓		Face detection, modeling, tracking, algorithms, multibiometric fusion
Microsoft Research [Beijing]	China	http://research.microsoft.com/~szli/FaceGroup/default.asp#Mission	✓		✓				Face detection, tracking, pose estimation, and recognition. Probable iris development.
Microsoft Research [Redmond]	USA	http://research.microsoft.com/~zhang/Face/default.htm	✓						Facial 3D modeling from video
MIT	USA	http://www-white.media.mit.edu/	✓					✓	Facial 3D Morphable Models, FR using color, eigenface algorithms, head/expression tracking, face database
Notre Dame	USA	http://www.nd.edu/~engineer/bioeng/inform.htm	✓				✓		Face evaluation framework, HumanID, corpus development, face/ear multimodal
Peking University (National Lab on Machine Perception)	China	http://www.cis.pku.edu.cn/							
Purdue University	USA	http://www.tech.purdue.edu/it/resources/biometrics/	✓					✓	FR algorithms (eigenvector), corpus development, AR Face database

Institution	Country	URL	Face	Finger	Iris	Voice	MultiModal	Testing	Details
Royal Military Academy	Belgium	http://www.sic.rma.ac.be/~beumier/	✓						3D Face acquisition, identification
Ruhr University	Germany	http://www.ruhr-uni-bochum.de/index_en.htm	✓						FR, detection, gesture analysis
Rutgers University	USA	http://www.caip.rutgers.edu/	✓			✓			FR, sensor fusion, speech identification and mimicry
San Jose State University	USA	http://www-engr.sjsu.edu/biometrics/	✓	✓				✓	Face algorithms, evaluation and testing
Technical University of Denmark	Denmark	http://www.imm.dtu.dk/~aam/	✓						Active appearance models, face tracking
Universidad Politecnica de Madrid	Spain						✓		
Universite Catholique de Louvain	Belgium	http://www.tele.ucl.ac.be/PROJ/BM2IV_e.html	✓			✓	✓		Face, voice fusion (M2VTS, BANCA)
University of Bologna	Italy	http://bias.csr.unibo.it/research/biolab/bio_tree.html	✓	✓				✓	Face localization, FR, multiple search, fingerprint system comparison, synthetic fingerprint generation
University of Cambridge	United Kingdom	http://mi.eng.cam.ac.uk/milab.html	✓			✓			Face localization, tracking, 3D modeling
University of Freiburg	Germany	http://graphics.informatik.uni-freiburg.de	✓						Facial 3D Morphable Models
University of Glasgow	United Kingdom	http://www.psy.gla.ac.uk/research/index.asp?Subject=cogn#Face%20recognition	✓						FR, 3D Digitization, cognition
University of Kentucky	USA	http://www.engr.uky.edu/~dllau/Research/surveillance.html	✓						3D Surveillance/Video
University of Maryland	USA	http://www.engr.umd.edu/							
University of Munich	Germany	http://www.bas.uni-muenchen.de/Bas/BasSmartKomPubliceng.html	✓				✓		Multimodal corpus development Human-computer interaction
University of Oulu	Finland	http://www.ee.oulu.fi/mvg/mvg.php	✓					✓	Color face analysis, image tracking, face database
University of Southern California	USA	http://iris.usc.edu/USC-Computer-Vision.html	✓						Human body tracking, FR, algorithms, 3D tracking and reconstruction
University of Stellenbosch	South Africa	http://www.dsp.sun.ac.za/index.php3	✓			✓			3D FR, motion processing
University of Stirling	United Kingdom	http://www.psychology.stir.ac.uk/general/research.htm	✓						Face perception
University of Surrey	United Kingdom	http://www.ee.surrey.ac.uk/Research/VSSP/03%20-%20CVSSPMultiSigProcFrameset.html	✓			✓	✓		Multi-biometric face/voice/lip integration,
University of Tennessee	USA	http://imaging.utk.edu/	✓						FR, video tacking, harbor surveillance
University of Texas	USA	http://www.cs.utexas.edu/home/home/	✓						Face perception and recognition labs, protocols, facial expression
West Virginia University	USA	http://www.wvu.edu/~forensic/						✓	Ties to government (FBI), CITeR

Institution	Country	URL	Face	Finger	Iris	Voice	MultiModal	Testing	Details
Yale University	USA	http://cvc.yale.edu/projects/yalefacesB/yalefacesB.html	✓					✓	Yale Face Database