GAO

United States General Accounting Office

Before the Subcommittee on Crime, Terrorism and Homeland Security and the Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives

For Release on Delivery
Expected at 4:00 p.m.
Tuesday, June 25, 2002

IDENTITY FRAUD

Prevalence and Links to Alien Illegal Activities

Statement of Richard M. Stana
Director, Justice Issues

G A P

Accountability * Integrity * Reliability

GAO-02-830T

Chairman Smith, Chairman Gekas, and Members of the Subcommittees:

I am pleased to be here today to discuss the significance of "identity fraud"—a term that encompasses a broad range of illegal activities based on fraudulent use of identifying information of a real person or of a fictitious person. A pervasive type of identity fraud is identity theft, which involves "stealing" another person's personal identifying information—such as Social Security number (SSN), date of birth, and mother's maiden name—and then using the information to fraudulently establish credit, run up debt, take over existing financial accounts, or to undertake other activities in another's name. Also, another pervasive category is the use of fraudulent identity documents by aliens to enter the United States illegally to obtain employment and other benefits. The events of September 11, 2001, have heightened concerns about the contributory role that identity fraud plays in facilitating terrorism and other serious crimes.

In this statement, I make the following points:

- The prevalence of identity theft appears to be growing. Moreover, identity theft is not typically a stand-alone crime; rather, identity theft is usually a component of one or more white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments. Since 1998, the Congress and most states have enacted laws that criminalize identity theft. The passage of federal and state identity theft legislation indicates that this type of crime has been widely recognized as a serious problem across the nation.

- According to Immigration and Naturalization Service (INS) officials, the use of fraudulent documents by aliens is extensive. At ports of entry, INS inspectors have intercepted tens of thousands of fraudulent documents in each of the last few years. These documents were presented by aliens attempting to enter the United States to seek employment or obtain other immigration benefits, such as naturalization or permanent residency status. The types of false documents most frequently intercepted by INS inspectors include border crossing cards, alien registration cards, nonimmigrant visas, and passports and citizenship documents (both U.S. and foreign). Also, INS has reported that large-scale counterfeiting has made fraudulent employment eligibility documents (e.g., Social Security cards) widely available.

- Federal investigations have shown that some aliens use fraudulent documents in connection with more serious illegal activities, such as narcotics trafficking and terrorism. This is a cause for greater concern.

- Efforts to combat identity fraud in its many forms likely will command continued attention from policymakers and law enforcement. Such efforts will include investigating and prosecuting perpetrators, as well as focusing on prevention measures to make key identification documents and information less susceptible to being counterfeited or otherwise used fraudulently.

My testimony today will be based primarily on the results of work that we have completed in recent years, namely our May 1998 and March 2002 reports on identity theft,[1] March 2002 report on the INS's Forensic Document Laboratory,[2] January 2002 report on immigration benefit fraud,[3] May 2000 report on alien smuggling,[4] July 1999 congressional testimony on illegal aliens and fraudulent documents,[5] and April 1999 report on INS's worksite enforcement efforts.[6] We also obtained information from the U.S. Secret Service, the Social Security Administration's Office of the Inspector General (SSA/OIG), the Federal Bureau of Investigation (FBI), the United States Sentencing Commission, and publicly available sources.

[1] U.S. General Accounting Office, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited,* GAO/GGD-98-100BR (Washington, D.C.: May 1, 1998) and *Identity Theft: Prevalence and Cost Appear to be Growing,* GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

[2] U.S. General Accounting Office, *INS Forensic Document Laboratory: Several Factors Impeded Timeliness of Case Processing,* GAO-02-410 (Washington, D.C.: Mar. 13, 2002).

[3] U.S. General Accounting Office, *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems,* GAO-02-66 (Washington, D.C.: Jan. 31, 2002).

[4] U.S. General Accounting Office, *Alien Smuggling: Management and Operational Improvements Needed to Address Growing Problem,* GAO/GGD-00-103 (Washington, D.C.: May 1, 2000).

[5] Statement of Richard M. Stana, U.S. General Accounting Office, *Illegal Aliens: Fraudulent Documents Undermining the Effectiveness of the Employment Verification System,* GAO/T-GGD/HEHS-99-175 (Washington, D.C.: July 22, 1999), before the Subcommittee on Immigration and Claims, Committee on the Judiciary, House of Representatives.

[6] U.S. General Accounting Office, *Illegal Aliens: Significant Obstacles to Reducing Unauthorized Alien Employment Exist,* GAO/GGD-99-33 (Washington, D.C.: Apr. 2, 1999).

Prevalence of Identity Theft Appears to be Growing

No single hotline or database captures the universe of identity theft victims. Some individuals do not even know that they have been victimized until months after the fact, and some known victims may not know to report or may choose not to report to the police, credit bureaus, or established hotlines. Thus, it is difficult to fully or accurately measure the prevalence of identity theft. Some of the often-quoted estimates of prevalence range from one-quarter to three-quarters of a million victims annually. Generally speaking, the higher the estimate of identity theft prevalence, the greater the (1) number of victims who are assumed not to report the crime and (2) number of hotline callers who are assumed to be victims rather than "preventative" callers. However, we found no information to confirm the extent to which these assumptions are valid.

Nevertheless, although it is difficult to specifically or comprehensively quantify identity theft, a number of data sources can be used as proxies or indicators for gauging the prevalence of such crime. These sources include

- the three national consumer reporting agencies that have call-in centers for reporting identity fraud or theft;
- the Federal Trade Commission (FTC), which maintains a database of complaints concerning identity theft;
- the SSA/OIG, which operates a hotline to receive allegations of SSN misuse and program fraud; and
- federal law enforcement agencies—Department of Justice components, Department of the Treasury components, and the Postal Inspection Service—responsible for investigating and prosecuting identity theft-related cases.

Each of these various sources or measures seems to indicate that the prevalence of identity theft is growing.

Consumer Reporting Agencies: An Increasing Number of Fraud Alerts on Consumer Files

According to the three national consumer reporting agencies, the most reliable indicator of the incidence of identity theft is the number of long-term (generally 7 years) fraud alerts placed on consumer credit files. Fraud alerts constitute a warning that someone may be using the consumer's personal information to fraudulently obtain credit. Thus, a purpose of the alert is to advise credit grantors to conduct additional identity verification or contact the consumer directly before granting credit. One of the three consumer reporting agencies estimated that its 7-year fraud alerts involving identity theft increased 36 percent over 2 recent

years—from about 65,600 in 1999 to 89,000 in 2000.[7] A second agency reported that its 7-year fraud alerts increased about 53 percent in recent comparative 12-month periods; that is, the number increased from 19,347 during one 12-month period (July 1999 through June 2000) to 29,593 during the more recent period (July 2000 through June 2001). The third agency reported about 92,000 fraud alerts[8] for 2000 but was unable to provide information for any earlier year.[9]

FTC: An Increasing Number of Calls to the Identity Theft Data Clearinghouse

The federal Identity Theft Act (P.L. 105-318) required the FTC to "log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief" that one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired. In response to this requirement, on November 1, 1999, FTC established a toll-free telephone hotline (1-877-ID-THEFT) for consumers to report identity theft. Information from complainants is accumulated in a central database (the Identity Theft Data Clearinghouse) for use as an aid in law enforcement and prevention of identity theft. From its establishment in November 1999 through September 2001, FTC's Identity Theft Data Clearinghouse received a total of 94,100 complaints from victims, including 16,784 complaints transferred to the FTC from the SSA/OIG. In the first month of operation, the Clearinghouse answered an average of 445 calls per week. By March 2001, the average number of calls answered had increased to over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls. However, FTC staff noted that identity theft-related statistics may, in part, reflect enhanced consumer awareness and reporting.

[7] These estimates are approximations based on the judgment and experience of agency officials.

[8] The duration of this agency's fraud alerts can vary from 2 to 7 years, at the discretion of the individual consumer.

[9] An aggregate figure—totaling the number of fraud alerts reported by the three consumer reporting agencies—may be misleading, given the likelihood that many consumers may have contacted more than one agency. During our review, we noted that various Web sites—including those of two of the three national consumer reporting agencies, as well as the FTC's Web site—advise individuals who believe they are the victims of identity theft or fraud to contact all three national consumer reporting agencies.

SSA/OIG: An Increasing Number of Fraud Hotline Allegations

SSA/OIG operates a fraud hotline to receive allegations of fraud, waste, and abuse. In recent years, SSA/OIG has reported a substantial increase in calls related to identity theft. For example, allegations involving SSN misuse increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001. A review performed by SSA/OIG of a sample of 400 allegations of SSN misuse indicate that up to 81 percent of all allegations of SSN misuse related directly to identity theft.

According to the SSA Inspector General, the dramatic rise in SSN misuse over the years has resulted partly from opportunities for fraud associated with the status of the SSN as a "de facto" national identifier, which is used by federal and state governments, banks, credit bureaus, insurance companies, medical care providers, and innumerable other industries. For a May 2000 congressional hearing on SSN misuse, the Inspector General's statement for the record noted that:

"... our office has investigated numerous cases where individuals apply for benefits under erroneous SSNs. Additionally, we have uncovered situations where individuals counterfeit SSN cards for sale on America's streets. From time to time, we have even encountered SSA employees who sell legitimate SSNs for hundreds of dollars. Finally, we have seen examples where SSA's vulnerabilities in its enumeration business process [i.e., the process for issuing SSNs] adds to the pool of SSNs available for criminal fictitious identities."[10]

Federal Law Enforcement: Increasing Indications of Identity Theft-Related Crime

Although federal law enforcement agencies do not have information systems that specifically track identity theft cases, the agencies provided us with statistics for identity theft-related crimes. Regarding bank fraud, for instance, the FBI reported that its arrests increased from 579 in 1998 to 645 in 2000—and was even higher (691) in 1999. The Secret Service reported that, for recent years, it has redirected its identity theft-related efforts to focus on high-dollar, community-impact cases. Thus, even though the total number of identity theft-related cases closed by the Secret Service decreased from 8,498 in fiscal year 1998 to 7,071 in 2000, the amount of fraud losses prevented in these cases increased from a reported average of about $73,000 in 1998 to an average of about $218,000 in 2000.[11]

[10]SSA/OIG, Statement for the Record, hearing on SSN misuse before the Subcommittee on Social Security, House Committee on Ways and Means (May 9, 2000).

[11]In compiling case statistics, the Secret Service defined "identity theft" as any case related to the investigation of false, fraudulent, or counterfeit identification; stolen, counterfeit, or altered checks or Treasury securities; stolen, altered, or counterfeit credit cards; or financial institution fraud.

The Postal Inspection Service, in its fiscal year 2000 annual report, noted that identity theft is a growing trend and that the agency's investigations of such crime had "increased by 67 percent since last year."

Technology Affords Increased Opportunities for Identity Theft

Opportunities for identity theft-related criminal activities have been enhanced by growth of the Internet, which increases the availability and accessibility of personal identifying information. According to the FBI:

"The availability of information on the Internet, in combination with the advances in computer hardware and software, makes it easier for the criminal to assume the identity of another for the purposes of committing fraud. For example, there are web-sites that offer novelty identification cards (including the hologram). After downloading the format, fonts, art work, and hologram images, the information can be easily modified to resemble a state-issued driver's license. In addition to drivers' licenses, there are web-sites that offer birth certificates, law enforcement credentials (including the FBI), and Internal Revenue Service forms."[12]

Similarly, the SSA/OIG has noted that, "The ever-increasing number of identity theft incidents has exploded as the Internet has offered new and easier ways for individuals to obtain false identification documents, including Social Security cards."[13]

Aliens Use Fraudulent Documents to Obtain Entry, Employment, and Other Benefits

Aliens and others have used identity theft or other forms of identity fraud to create fraudulent documents that might enable individuals to enter the country and seek job opportunities. With nearly 200 countries using unique passports, official stamps, seals, and visas, the potential for immigration document fraud is great. In addition, more than 8,000 state or local offices issue birth certificates, driver's licenses, and other documents aliens can use to establish residency or identity. This further increases the number of documents that can be fraudulently used by aliens to gain entry into the United States, obtain asylum or relief from deportation, or receive such other immigration benefits as work permits or permanent residency status.

[12]Statement of Lynne A. Hunt, Section Chief, Financial Crimes Section, FBI, hearing on "Internet Fraud: Illegal False Identification Websites," before the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs (May 19, 2000).

[13]Statement of Jane E. Vezeris, Deputy Inspector General of Social Security, "The Emergence of Identity Theft as a Law Enforcement Issue in California," before the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary (Aug. 30, 2000).

Reportedly, large-scale counterfeiting has made employment eligibility documents widely available. For example, in May 1998, INS seized more than 24,000 counterfeit Social Security cards in Los Angeles after undercover agents purchased 10,000 counterfeit INS permanent resident cards from a counterfeit document ring.

Attempting Entry into the United States with Fraudulent Documents

Generally, when a person attempts to enter the United States at a port of entry, INS inspectors require the individual to show one of several documents that would prove identity and/or authorize entry. These documents include border crossing cards, alien registration cards, nonimmigrant visas, U.S. passports or other citizenship documents, foreign passports or citizenship documents, reentry permits, refugee travel documents, and immigrant visas.

At ports of entry, INS inspectors annually intercept tens of thousands of fraudulent documents presented by aliens attempting to enter the United States. As table 1 shows, INS inspectors intercepted over 100,000 fraudulent documents annually in fiscal years 1999 through 2001. Generally, about one-half of all the intercepted documents were border crossing cards and alien registration cards.[14]

Table 1: Number and Type of Fraudulent Documents Intercepted by INS Inspectors, Fiscal Years 1998 through 2001

Type of document	Fiscal year 1998	Fiscal year 1999	Fiscal year 2000	Fiscal year 2001
Border crossing cards	30,631	30,797	38,650	30,419
Alien registration cards	28,137	33,308	34,120	26,259
Nonimmigrant visas	13,551	18,003	17,417	21,127
U.S. passports and citizenship documents	14,546	22,142	17,703	18,925
Foreign passports and citizenship documents	11,245	14,695	15,047	15,994
Reentry permits and refugee travel documents	271	1,107	153	702
Immigrant visas	790	663	447	597
Total	**99,171**	**120,715**	**123,537**	**114,023**

Source: INS data.

[14]Border crossing cards are issued to Mexican Nationals who frequently cross the border for business or pleasure. Most cardholders must stay within 25 miles of the border and limit each visit to 72 hours. Alien registration cards, commonly called green cards, are issued to permanent resident aliens.

Attempting to Obtain Employment with Fraudulent Documents

The availability of jobs is one of the primary magnets attracting illegal aliens to the United States. Immigration experts believe that as long as opportunities for employment exist, the incentive to enter the United States illegally will persist and efforts at the U.S. borders to prevent illegal entry will be undermined. The Immigration Reform and Control Act (IRCA) of 1986[15] made it illegal for employers to knowingly hire unauthorized aliens. IRCA requires employers to comply with an employment verification process intended to provide employers with a means to avoid hiring unauthorized aliens. The process requires newly hired employees to present documentation establishing their identity and eligibility to work. From a list of 27 acceptable documents, employees have the choice of presenting 1 document establishing both identity and eligibility to work (e.g., an INS permanent resident card) or 1 document establishing identity (e.g., a driver's license) and 1 establishing eligibility to work (e.g., a Social Security card). Generally, employers cannot require the employees to present a specific document. Employers are to review the document or documents that an employee presents and complete an Employment Eligibility Form, INS Form I-9. On the form, employers are to certify that they have reviewed the documents and that the documents appear genuine and relate to the individual. Employers are expected to judge whether the documents are obviously fraudulent. INS is responsible for checking employer compliance with IRCA's verification requirements.

Significant numbers of aliens unauthorized to work in the United States have used fraudulent documents to circumvent the employment verification process designed to prevent employers from hiring them. For example, INS data showed that about 50,000 unauthorized aliens were found to have used 78,000 fraudulent documents to obtain employment over the 20-month period from October 1996 through May 1998. About 60 percent of the fraudulent documents used were INS documents; 36 percent were Social Security cards, and 4 percent were other documents, such as driver's licenses. Also, we noted that counterfeit employment eligibility documents were widely available. For instance, in November 1998 in Los Angeles, INS seized nearly 2 million counterfeit documents, such as INS permanent resident cards and Social Security cards, which were headed for distribution points around the country.

[15]P.L. 99-603, 8 U.S.C. 1324a *et seq.*

Attempting to Obtain Other Benefits with Fraudulent Documents

Aliens have also attempted to use fraudulent documents or other illegal means to obtain other immigration benefits, such as naturalization or permanent residency. Document fraud encompasses the counterfeiting, sale, or use of false documents, such as birth certificates, passports, or visas, to circumvent U.S. immigration laws and may be part of some benefit application fraud cases. Such fraud threatens the integrity of the legal immigration system.

Although INS has not quantified the extent of immigration benefit fraud, agency officials told us that the problem was pervasive and would increase.[16] In one case, for example, an immigration consulting business filed 22,000 applications for aliens to qualify under a legalization program. Nearly 5,500 of the aliens' claims were fraudulent and 4,400 were suspected of being fraudulent. In another example, according to an INS Miami District Office official, during the month of January 2001 its investigative unit received 205 leads, of which 84 were facilitator cases (e.g., cases involving individuals or entities who prepare fraudulent benefit applications or who arrange marriages for a fee for the purpose of fraudulently enabling an alien to remain in the United States). In both of these examples, fraudulent documents played a role in the attempts to obtain immigration benefits.

Identity Theft and Fraudulent Documents Can Be Components of Serious Crimes

Federal law enforcement officials have acknowledged that identity theft often is an essential component of many criminal activities, ranging from bank and credit card fraud to international terrorism. At a May 2, 2002, press conference to announce an initiative to crack down on identity theft, the Attorney General said that:

"In addition to the credit card and financial fraud crimes often committed, identity theft is a major facilitator of international terrorism. Terrorists have used stolen identities in connection with planned terrorist attacks. An Algerian national facing U.S. charges of identity theft, for example, allegedly stole the identities of 21 members of a health club in Cambridge, Massachusetts, and transferred the identities to one of the individuals convicted in the failed 1999 plot to bomb the Los Angeles International Airport."

The events of September 11, 2001, have increased the urgency of being able to effectively authenticate the identity of individuals.

[16]GAO-02-66 (Jan. 31, 2002).

Alien Smugglers Use Fraudulent Documents

In addition to using identity theft or identity fraud to enter the United States illegally and seek job opportunities, some aliens have used fraudulent documents in connection with serious crimes, such as narcotics trafficking and terrorism. For instance, according to INS, although most aliens are smuggled into the United States to pursue employment opportunities, some are smuggled as part of a criminal or terrorist enterprise.

INS believes that its increased enforcement efforts along the southwest border have prompted greater reliance on alien smugglers and that alien smuggling is becoming more sophisticated, complex, organized, and flexible. In a fiscal year 2000 threat assessment, INS predicted that fraud in obtaining immigration benefits would continue to rise as the volume of petitions for benefits grows and as smugglers search for other methods to introduce illegal aliens into the United States. Also, INS believes organized crime groups will increasingly use smugglers to facilitate illegal entry of individuals into the United States to engage in criminal activities. Alien smugglers are expected to increasingly use fraudulent documents to introduce aliens into the United States.

Conspirator in World Trade Center Bombing Used Fraudulent Document to Enter United States

In February 1993, a massive explosion at the World Trade Center complex in New York City killed 6 people and injured approximately 1,000 others. According to a report by the Department of Justice's Office of the Inspector General:

"One of the conspirators in the World Trade Center bombing entered the country on a photo-substituted Swedish passport in September 1992. The suspect used a Swedish passport 'expecting to pass unchallenged through the INS inspection area at New York's Kennedy Airport—since an individual bearing a valid Swedish passport does not even need a visa to enter the United States.' When the terrorist arrived at John F. Kennedy International Airport (JFK), an INS inspector suspected that the passport had been altered. A search of his luggage revealed instructional materials for making bombs; the subject was detained and sentenced to six months' imprisonment for passport fraud. In March 1994 he was convicted for his role in the World Trade Center bombing and sentenced to 240 years in prison and a $500,000 fine."[17]

[17]U.S. Department of Justice, Office of the Inspector General, *The Potential for Fraud and INS's Efforts to Reduce the Risks of the Visa Waiver Pilot Program*, Inspection Report Number I-99-10 (Mar. 1999).

Furthermore, regarding this terrorist incident, a United States Sentencing Commission report noted that, "The World Trade Center defendant used, and was in possession of, numerous false identification documents, such as photographs, bank documents, medical histories, and education records from which numerous false identities could have been created."[18]

FBI and State Department Views on Links between Identity Theft or Fraud and Terrorism

At a February 2002 congressional hearing, an FBI representative testified that various FBI field offices had begun criminal financial investigative initiatives focusing on fraud schemes having a potential nexus to terrorist financing.[19] The FBI representative's statement for the record included the following point:

"Terrorist financing methods range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been utilized by terrorists and terrorist groups. Traditionally, their efforts have been aided considerably by the use of correspondent bank accounts, private banking accounts, offshore shell banks, ... bulk cash smuggling, **identity theft,** credit card fraud, and other criminal operations such as illegal drug trafficking. (Emphasis added.)

Also, at a March 2002 congressional hearing, a Department of State representative testified that:

"There often is a nexus between terrorism and organized crime, including drug trafficking. ... Both groups make use of fraudulent documents, including passports and other identification and customs documents to smuggle goods and weapons."[20]

[18]United States Sentencing Commission, Economic Crimes Policy Team, *Identity Theft Final Report* (Washington, D.C.: Dec. 15,1999).

[19]Mr. Dennis M. Lormel, Chief, Financial Crimes Section, FBI, Statement for the Record before the Subcommittee on Oversight and Investigations, House Committee on Financial Services (Feb. 12, 2002).

[20]Mr. Rand Beers, Assistant Secretary of State for International Narcotics and Law Enforcement Affairs, Department of State, at a hearing on "Narco-Terror: The Worldwide Connection Between Drugs and Terrorism," before the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary (Mar. 13, 2002).

SSA/OIG Investigating Links between SSN Misuse and Terrorism

Since the September 11 attacks, the SSA/OIG has reported increasing its efforts to work with federal, state, and local law enforcement officials to investigate and prosecute SSN misuse, including cases in which SSNs may have been used to facilitate or camouflage terrorist crimes.[21] In its May 2002 report, the SSA/OIG summarized the interim results of a task force investigation ("Operation Safe Travel"), which began in September 2001 when SSA/OIG agents developed information that individuals working at the Salt Lake City International Airport were misusing SSNs for security badge applications and employment eligibility verification:

"Under the direction of the U.S. Department of Justice (DOJ), investigators subpoenaed records for all 9,000 airport employees with security badges to identify instances of SSN misuse. They identified 61 individuals with the highest-level security badges and 125 individuals with lower level badges who misused SSN's. A Federal grand jury indicted 69 individuals for Social Security and INS violations. Sixty-one of the 69 individuals arrested had an SSN misuse charge by the U.S. Attorney. On December 11, 2001, SSA's OIG agents and other members of the Operation Safe Travel Task Force arrested 50 individuals. To date, more than 20 have been sentenced after pleading guilty to violations cited in the indictments. Many are now involved in deportation proceedings. There were other similar airport operations after the Salt Lake City Operation, and more are underway."

In the May 2002 report, the SSA Inspector General noted that identity theft begins, in most cases, with the misuse of an SSN. In this regard, the Inspector General emphasized the importance of protecting the integrity of the SSN, especially given that this "de facto" national identifier is the "key to social, legal, and financial assimilation in this country" and is a "link in our homeland security goal."

[21]SSA/OIG, *Social Security Number Integrity: An Important Link in Homeland Security*, Management Advisory Report, A-08-02-22077 (May 2002).

Efforts to Prevent Identity Theft and Other Forms of Identity Fraud Are Important

In its 1999 study of identity theft, the United States Sentencing Commission reported that SSNs and driver's licenses are the identification means most frequently used to generate or "breed" other fraudulent identifiers.[22] Also, in early 1999, following passage of the federal Identity Theft Act, the U.S. Attorney General's Council on White Collar Crime established the Subcommittee on Identity Theft to foster coordination of investigative and prosecutorial strategies. Subcommittee leadership is vested in the Fraud Section of the Department of Justice's Criminal Division, and membership includes various federal law enforcement and regulatory agencies, as well state and local law enforcement representation. The subcommittee chairman told us that, since the terrorist incidents of September 11, 2001, the subcommittee has begun to focus more on prevention. For example, the chairman noted that the American Association of Motor Vehicle Administrators attended a recent subcommittee meeting to discuss ways to protect against counterfeit or fake driver's licenses.

The May 2002 SSA/OIG report, cited previously, stated that, "while the ability to punish identity theft is important, the ability to prevent it is even more critical." In this regard, the Inspector General noted that effective protections to prevent SSN misuse must be put in place at three stages—before issuance of the SSN, during the life of the number holder, and upon that individual's death.

Other prevention efforts designed to enhance technologies in support of identification and verification functions include the following:

- The Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173), signed by the President on May 14, 2002, requires that all travel and entry documents (including visas) issued by the United States to aliens be machine-readable and tamper-resistant and include standard biometric identifiers by October 26, 2004. Also, the act requires the Attorney General to install machine readers and scanners at all U.S. ports of entry by this date so as to allow biometric comparison and authentication of all U.S. travel and entry documents and of all passports issued by visa waiver countries.

- The USA Patriot Act (P.L. 107-56), signed by the President on October 26, 2001, has various provisions requiring development of technology

[22]United States Sentencing Commission, Economic Crimes Policy Team, *Identity Theft Final Report* (Washington, D.C.: Dec. 15,1999).

standards to confirm identity. Under the legislation, the Department of Commerce's National Institute of Standards and Technology is to develop and certify accuracy standards for biometric technologies.

In November 2001, to support implementation of the USA Patriot Act, the Executive Board of the InterNational Committee for Information Technology Standards[23] announced establishment of a technical committee to help accelerate biometric standardization. In its announcement, the Executive Board noted that biometric standards will permit faster deployment of better security solutions and also greatly help in the prevention of identity theft.

Chairman Smith and Chairman Gekas, this concludes my prepared statement, I would be pleased to answer any questions that you or other members of the subcommittees may have.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Richard M. Stana at (202) 512-8777 or Danny R. Burton at (214) 777-5600. Individuals making key contributions to this testimony included Michael P. Dino, Bonnie Hall, Shirley A. Jones, Robert J. Rivas, Ronald J. Salo, and Ellen T. Wolfe.

[23]The InterNational Committee for Information Technology Standards is sponsored by the Information Technology Industry Council, a trade association representing the leading U.S. providers of information technology products and services. Also, the InterNational Committee is accredited by, and operates under rules approved by, the American National Standards Institute. These rules are designed to ensure that voluntary standards are developed by the consensus of directly and materially affected interests.