United States General Accounting Office

GAO

Report to the Honorable Sam Johnson
House of Representatives

June 2002

IDENTITY THEFT

Greater Awareness and Use of Existing Data Are Needed

GAO-02-766

Contents

Tables

Abbreviations

EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
IRS	Internal Revenue Service
LEGIT	law enforcement getting identity thieves
OIG	Office of the Inspector General
SSA	Social Security Administration
SSN	Social Security number
UCR	Uniform Crime Reporting

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

June 28, 2002

The Honorable Sam Johnson
House of Representatives

Dear Mr. Johnson:

This report responds to your request that we review federal and state efforts to address identity theft, which has been characterized by law enforcement as the fastest growing type of crime in the United States. As noted in our May 1998 report,[1] identity theft or identity fraud generally 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, or take over existing financial accounts. Later that year, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (the Identity Theft Act).[2] Enacted in October 1998, the federal statute made identity theft a separate crime against the person whose identity was stolen, broadened the scope of the offense to include the misuse of information as well as documents, and provided punishment—generally a fine or imprisonment for up to 15 years or both. Also, since 1998, most states have enacted laws that criminalize identity theft. Thus, various federal and numerous state and local law enforcement agencies are responsible for investigating identity theft crimes. Relevant federal agencies include the Secret Service, the Federal Bureau of Investigation (FBI), and the Postal Inspection Service, as well as the Social Security Administration's (SSA) Office of the Inspector General (OIG), which receives SSN misuse and other identity theft-related allegations on its fraud hotline.

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

[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 Fraud: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

[2]Public Law 105-318 (1998).

nation. Now, a current focus for policymakers and criminal justice administrators is to ensure that these laws are effectively enforced.

Specifically, in response to your request, this report provides information on

- law enforcement results (such as examples of prosecutions and convictions) under the federal Identity Theft Act;
- law enforcement results under state statutes that, similar to the federal act, provide state and local law enforcement officials with the tools to prosecute and convict identity theft criminals;
- the means used to promote cooperation or coordination among federal, state, and local law enforcement agencies in addressing identity theft crimes that span multiple jurisdictions; and
- actions taken by the SSA/OIG to resolve SSN misuse and other identity theft-related allegations received during fiscal year 1999.

To address these questions, we interviewed responsible officials and reviewed documentation obtained from the Department of Justice and its components, including the Executive Office for United States Attorneys (EOUSA) and the FBI; the Department of the Treasury and its components, including the Secret Service and the Internal Revenue Service (IRS); the SSA/OIG; and the Federal Trade Commission (FTC). Also, we conducted a literature search to obtain examples of cases prosecuted under the federal Identity Theft Act. Regarding state and local law enforcement efforts, we focused on 10 states—Arizona, California, Florida, Georgia, Illinois, Michigan, New Jersey, Pennsylvania, Texas, and Wisconsin—which we judgmentally selected on the basis of having either the highest incidences of reported identity theft or the longest-standing applicable statutes. We conducted our work from July 2001 to May 2002 in accordance with generally accepted auditing standards. Appendix I presents more details about the scope and methodology of our work.

Results in Brief

We found no comprehensive or centralized data on enforcement results under the federal Identity Theft Act. However, according to a Deputy Assistant Attorney General, federal prosecutors are using the 1998 federal law. Moreover, in response to our inquiries, Justice Department Criminal Division officials said that federal prosecutors consider the Identity Theft Act to be a useful statute because it provides broad jurisdiction and is

another tool to use in combating white-collar or financial crimes—such as bank fraud, credit card fraud, and mail fraud—that typically have elements of identity theft. Our review of selected cases prosecuted under the federal act illustrate that identity theft generally is not a stand-alone crime. Rather, identity theft typically is a component of one or more other white-collar or financial crimes.

As with the federal act, we found no centralized or comprehensive data on enforcement results under state identity theft statutes. However, officials in the 10 states we selected for study provided us with examples of actual investigations or prosecutions under these statutes. Presented for illustration purposes only, these cases are not necessarily representative of identity theft crimes in these or other states. Officials we contacted in these states also noted various continuing challenges encountered in enforcing identity theft statutes. For instance, because identity theft is still a "nontraditional" crime, some police departments may be unaware of the importance of taking reports of identity theft, much less initiating investigations. Also, it is important that law enforcement resources be allocated to meet priorities. In this regard, officials in several of the 10 states told us that limited resources are allocated to priorities such as violent crimes and drug offenses and, thus, the number of investigators and prosecutors for addressing identity theft often is insufficient. Further, according to some of the officials we contacted, because many identity theft cases present multi- or cross-jurisdictional issues—such as when a perpetrator steals personal information in one city and uses the information to conduct fraudulent activities in another city or state—law enforcement agencies sometimes tend to view identity theft as being "someone else's problem."

Generally, the prevalence of identity theft and the frequently multi- or cross-jurisdictional nature of such crime underscore the importance of having means for promoting cooperation or coordination among federal, state, and local law enforcement agencies. One of the most commonly used means of coordination, task forces, can have participating agencies from all levels of law enforcement—federal, state, and local—and, in some instances, can have participants from banks and other private sector entities. Another relevant coordination entity is the U.S. Attorney General's Identity Theft Subcommittee, whose membership includes various federal law enforcement and regulatory agencies, as well as state and local representation. In 1999, among other purposes, the Attorney General's White Collar Crime Council established the subcommittee to promote cooperation and coordination in addressing identity theft cases involving multiple jurisdictions.

Another vehicle for coordination is the FTC's Consumer Sentinel Network, which is a secure, encrypted Web site for use by law enforcement agencies. In 1999, FTC established a central database (the Identity Theft Data Clearinghouse) to collect information reported by identity theft victims. Law enforcement agencies can use the Consumer Sentinel Network to access the Clearinghouse database and scan consumer complaints matching certain criteria to determine, for example, if there is a larger pattern of criminal activity. However, relatively few law enforcement agencies have used the Consumer Sentinel Network, and centralized analysis of database information to generate investigative leads and referrals has also been limited. FTC staff said that the availability of the database as an aid for law enforcement is still relatively new and some potential users may still be unaware of this investigative resource. We are recommending that the Attorney General have the Identity Theft Subcommittee promote greater awareness and use of the Consumer Sentinel Network and the Clearinghouse database by all levels of law enforcement.

While SSA/OIG's fraud hotline annually receives thousands of allegations involving either (1) SSN misuse or (2) program fraud with SSN misuse potential, the agency concentrates its investigative resources on the latter category of allegations because the protection of Social Security trust funds is a priority. In these 2 categories, SSA/OIG received approximately 62,000 allegations in fiscal year 1999, and the agency opened investigative cases on 4,636 (about 7 percent) of these allegations. About three in four of the investigative cases involved program fraud-related allegations. SSA/OIG statistics for investigative cases opened in fiscal year 1999 indicate that a total of 1,347 cases had resulted in criminal convictions or other judicial actions, as of April 30, 2002. During our review, the SSA Inspector General told us that his office does not have enough investigators to address all of the SSN misuse allegations received on the agency's fraud hotline. However, FTC staff noted that, starting in February 2001, FTC began to routinely upload information from SSA/OIG's fraud hotline about these allegations into FTC's Identity Theft Data Clearinghouse, thereby making the information available to law enforcement agencies via the Consumer Sentinel Network.

In a letter dated June 19, 2002, the Department of Justice generally agreed with the substance of this report and the recommendation made. Further, Justice noted several actions that it has taken or will take to directly address the recommendation.

Background

Under the federal Identity Theft Act, a criminal offense is committed if a person "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law …" The relevant section of this legislation is codified at 18 U.S.C. § 1028(a)(7)("fraud and related activity in connection with identification documents and information"). According to an analysis of the new law by the United States Sentencing Commission:[3]

- Before passage of the 1998 act, the unauthorized use or transfer of identity documents was illegal under title 18 of the U.S. Code, section 1028—which included subsections (a)(1) through (a)(6). The unauthorized use of credit cards, personal identification numbers, automated teller machine codes, and other electronic access devices was illegal under another section of the U.S. Code—that is, 18 U.S.C. § 1029 ("fraud and related activity in connection with access devices").

- The addition of subsection (a)(7) to section 1028 expanded the definition of "means of identification" to include such information as SSN and other government identification numbers, dates of birth, and unique biometric data (e.g., fingerprints), as well as electronic access devices and routing codes used in the financial and telecommunications sectors.

- Under the Identity Theft Act, the new definition of means of identification includes prior statutory definitions of "identification documents."

According to the United States Sentencing Commission, a key impact is to make the proscriptions of the new identity theft law applicable to a wide range of offense conduct, which can be independently prosecuted under numerous existing statutes. That is, any unauthorized use of means of identification can now be charged either as a violation of the new law or in conjunction with other federal statutes.

In further elaboration of the breadth of the definition of means of identification and its impact, the Sentencing Commission's analysis noted the following:

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

- The new law covers offense conduct already covered by a multitude of other federal statutes. The unauthorized use of credit cards, for instance, is already prosecuted under 18 U.S.C. § 1029, but now also can be prosecuted under the newly enacted 18 U.S.C. § 1028(a)(7).

- Other examples of offense conduct include providing a false SSN or other identification number to obtain a tax refund and presenting false passports or immigration documents by using the names and addresses and photos of lawful residents or citizens to enter the United States.

In total, according to the Sentencing Commission, the violation of some 180 federal criminal statutes can potentially fall within the ambit of 18 U.S.C. § 1028(a)(7).

Regarding state statutes, at the time of our 1998 report, only a few states had specific laws to address identity theft. Now, as table 1 shows, 44 states have specific laws that address identity theft, and 5 other states have laws that cover activities included within the definition of identity theft. Almost one-half (22) of these 49 states enacted relevant laws in 1999. According to FTC's analysis, identity theft can be a felony offense in 45 of the 49 states that have laws to address this crime.[4]

[4]Many state statutes provide that identity theft of credit, money, goods, services, or other property over certain amounts is a felony. Under the specified amounts, the offense would be a criminal misdemeanor.

Table 1: States That Have Identity Theft Statutes (by Year of Enactment)

Year of enactment	States with specific laws to address identity theft	Number
1996	Arizona	1
1997	California and Wisconsin	2
1998	Georgia, Kansas, Massachusetts, Mississippi,[a] and West Virginia	5
1999	Arkansas, Connecticut, Florida, Idaho, Illinois, Iowa, Louisiana, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Tennessee, Texas, Washington, and Wyoming	22
2000	Delaware, Kentucky, Michigan, Pennsylvania, Rhode Island, South Carolina, South Dakota, Utah, and Virginia	9
2001	Alabama, Alaska, Indiana, Montana, and New Mexico	5
Total		**44**

Note: According to the FTC, five other states—Colorado, Hawaii, Nebraska, New York, and Maine—have laws that cover activities included within the definition of identity theft but are not coterminous with it, and one other state (Vermont) is collecting data to consider enacting possible identity theft legislation.

[a]Mississippi possibly enacted the nation's first identity theft statute (Miss. Code Ann. § 97-19-85), even though it was titled as a "false pretenses" statute rather than specifically labeled as an "identity theft" statute. Originally enacted in 1993, the statute was amended in 1998 to include additional identifiers and increase punishment from a misdemeanor to a felony.

Source: FTC data. Also, note "a" is based on our analysis of the Mississippi statute and a follow-up discussion with an official in the Mississippi Attorney General's Office.

In the view of Justice Department Criminal Division officials, the enactment of state identity theft laws has multi-jurisdictional benefits to all levels of law enforcement—federal, state, and local. In explanation, Justice officials commented that the various state statutes, coupled with the federal statute, provide a broader framework for addressing identity theft, particularly when a multi-agency task force approach is used. The Justice officials noted, for instance, that it is very plausible for a task force to generate multiple cases, some of which can result in federal prosecutions and others in state or local prosecutions.

Generally, law enforcement agencies widely acknowledge that SSNs often are used as identifiers by thieves to obtain or "breed" other identification documentation. Through its fraud hotline, SSA/OIG annually receives thousands of allegations of fraud, waste, and abuse. Most of these allegations are classified by SSA/OIG as involving either (1) SSN misuse or (2) program fraud that may contain elements of SSN misuse. In these two categories, SSA/OIG received about 62,000 allegations in fiscal year 1999, about 83,000 allegations in fiscal year 2000, and about 104,000 allegations

in fiscal year 2001. SSA/OIG officials explained these two categories of allegations as follows:

- Allegations of "SSN misuse" include, for example, incidents where a criminal uses the SSN of another individual for the purpose of fraudulently obtaining credit, establishing utility services, or acquiring goods. SSNs are also misused to violate immigration laws, flee the criminal justice system by assuming a new identity, or obtain personal information to stalk an individual. Generally, this category of allegations does not directly involve SSA program benefits.

- On the other hand, allegations of fraud in SSA programs for the aged, survivors, or disabled often entail some element of SSN misuse. For example, a criminal may use the victim's SSN or other identifying information for the purpose of obtaining Social Security benefits. When hotline staff receive this type of allegation, it is to be classified under the appropriate category of program fraud.

In 1999, SSA/OIG analyzed a sample of SSN misuse allegations and determined that about 82 percent of such allegations related directly to identity theft.[5] The analysis covered a statistical sample of 400 allegations from a universe of 16,375 allegations received by the fraud hotline from October 1997 through March 1999. The analysis did not cover the other category mentioned previously, that is, allegations of program-related fraud with SSN misuse potential.

[5]SSA/OIG, *Management Advisory Report – Analysis of Social Security Number Misuse Allegations Made to the Social Security Administration's Fraud Hotline* (A-15-99-92019, Aug. 1999).

No Comprehensive Data on Law Enforcement Results under the Federal Identity Theft Act, but Case Examples Illustrate Use of the Law

There are no comprehensive statistics on the number of investigations, convictions, or other law enforcement results under the Identity Theft Act. As noted in our March 2002 report,[6] federal law enforcement agencies generally do not have information systems that facilitate specific tracking of identity theft cases. For example, while the amendments made by the Identity Theft Act are included as subsection (a)(7) of section 1028, Title 18 of the U.S. Code, EOUSA does not have comprehensive statistics on offenses charged specifically under that subsection. EOUSA officials explained that, except for certain firearms statutes, staff are required to record cases only to the U.S. Code section, not the subsection or the sub-subsection.

Given the absence of comprehensive statistics, we obtained relevant anecdotes or examples of actual investigations and prosecutions under the federal statute. For instance, about 2 years after passage of the Identity Theft Act, a senior Department of Justice official testified at a May 2001 congressional hearing that U.S. Attorneys' Offices throughout the nation were making substantial use of the new federal law that recognized identity theft as a separate crime.[7] In testimony, the Justice official said that federal prosecutors had used the new statute—18 U.S.C. § 1028(a)(7)—in at least 92 cases to date. One example cited in the testimony involved a defendant who stole private bank account information about an insurance company's policyholders and used that information to withdraw funds from the accounts of the policyholders and deposit approximately 4,300 counterfeit bank drafts totaling more than $764,000. The case was prosecuted in the Central District of California. The defendant pled guilty to identity theft and related charges and was sentenced to 27 months of imprisonment and 5 years of supervised release.

Another case cited by the Justice official illustrates that identity theft crimes can have fact-pattern elements encompassing more than one jurisdiction. The case involved a California resident, who committed fraudulent acts in the state of Washington by, among other means, using a Massachusetts driver's license bearing the name of an actual person not

[6]GAO-02-363.

[7]Prepared statement of Mr. Bruce Swartz, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, for a hearing ("On-line Fraud and Crime: Are Consumers Safe?") before the Subcommittee on Commerce, Trade, and Consumer Protection, House Committee on Energy and Commerce (May 23, 2001).

associated with the criminal activities. Also, this case further illustrates that identity theft is rarely a stand-alone crime; rather, it frequently is a component of one or more white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or wire fraud. Pertinent details of this case, prosecuted in the Western District of Washington, are as follows:

- Over a period of time in 1999 and 2000, the defendant and other conspirators assumed the identities of third persons without their consent and authorization and fraudulently used the SSNs and names of actual persons. Also, the conspirators created false identity documents, such as state identification cards, driver's licenses, and immigration cards. Using the identities and names of third persons, the conspirators opened banking and investment accounts at numerous locations and obtained credit cards.

- The defendant and other conspirators presented and deposited at least 12 counterfeit checks (valued in excess of $1 million) to various banks and investment companies in western Washington. Also, the conspirators purchased legitimate cashiers checks, in nominal amounts, and then altered them to reflect substantially greater amounts. The conspirators presented or deposited at least five altered checks (worth almost $350,000) in the Seattle area.

According to Justice, in July 2000, the defendant pled guilty to committing three felony counts of identity theft, conspiring to commit wire fraud involving attempted losses in excess of $1 million, and using an unauthorized credit card.

During our current review, Justice Department Criminal Division officials told us that federal prosecutors consider the Identity Theft Act to be a very useful statute. The officials said, for instance, that prosecutors endorse the statute because it provides broad jurisdiction. Further, the Justice officials noted that the Identity Theft Act provides another tool for prosecutors to use, even though in many instances the defendants may be charged under other white-collar crime statutes. The officials explained that identity theft is rarely a stand-alone crime. Thus, cases involving identity theft or identity fraud may have charges under a variety of different statutes relating to these defendants' other crimes, such as bank fraud, credit card fraud, or mail fraud. Appendix II summarizes selected federal cases prosecuted for such multiple charges, including charges of violations of 18 U.S.C. § 1028(a)(7).

No Comprehensive Data on Enforcement Results under State Identity Theft Statutes, but Case Examples Illustrate Use of Such Laws

As with the federal Identity Theft Act, we found no centralized or comprehensive data on enforcement results under state identity theft statutes. However, officials in selected states provided us with examples of actual cases illustrating the use of such statutes. Also, officials in these states noted various challenges encountered in enforcing identity theft statutes—challenges involving topics such as the filing of police reports, the use of limited resources, and the resolution of jurisdictional issues.

Case Examples Illustrate Use of State Identity Theft Laws

The crime of identity theft is not specifically recorded as an offense category in the FBI's Uniform Crime Reporting (UCR) Program.[8] Further, our inquiries with various national organizations—the National Association of Attorneys General, the National District Attorneys Association, and the International Association of Chiefs of Police—indicated that these entities do not have comprehensive data on arrests or convictions under state identity theft laws.

In the absence of national data on enforcement of state identity theft laws, we contacted officials in 10 states—Arizona, California, Florida, Georgia, Illinois, Michigan, New Jersey, Pennsylvania, Texas, and Wisconsin.[9] As table 2 shows, each of these 10 states has a specific statute that makes identity theft a crime and provides for imprisonment of convicted offenders. The length of imprisonment varies by state, ranging upward to as long as 30 years.

[8]The UCR Program is a nationwide, cooperative statistical effort of nearly 17,000 city, county, and state law enforcement agencies voluntarily reporting data on crimes brought to their attention. According to the FBI, during 2000, law enforcement agencies active in the UCR Program represented nearly 254 million U.S. inhabitants, or 94 percent of the total population as established by the Bureau of the Census.

[9]We judgmentally selected these states on the basis of their having either the highest incidences of reported identity theft or the longest-standing applicable statutes (see app. I).

Table 2: Sentencing Provisions of Selected States' Identity Theft Laws

State	State code citation	Sentencing provisions
Arizona	Ariz. Rev. Stat. § 13-2008	Imprisonment of 2-1/2 to 12 years.
California	Cal. Penal Code § 530.5	Imprisonment not to exceed 1 year, or fines up to $10,000, or both.
Florida	Fla. Stat. Ann. § 817.568	Imprisonment of up to 5 years and fines up to $5,000, or both. In addition, the defendant may be ordered to pay up to double the pecuniary gain of the defendant or pecuniary loss of the victim.
Georgia	Ga. Code Ann. §§ 16-9-121	Imprisonment of 1 to 10 years and the defendant may be ordered to make restitution.
Illinois	720 Ill. Comp. Stat. 5/16G	Imprisonment from 1 to 30 years.
Michigan	Mich. Comp. Laws § 750.285	Imprisonment up to 5 years, or fines up to $10,000, or both.
New Jersey	N.J. Stat. Ann. § 2C: 21-17	Imprisonment up to 10 years.
Pennsylvania	18 Pa. Cons. Stat. Ann. § 4120	Imprisonment up to 10 years, or fines up to $25,000, or both
Texas	Tex. Penal Code § 32.51	Imprisonment up to 10 years and a fine not to exceed $10,000.
Wisconsin	Wis. Stat. § 943.201	Imprisonment up to 10 years, or fines up to $10,000, or both

Source: GAO summary of state statutes.

As with the national organizations we contacted, state officials could not provide aggregate data on law enforcement results (e.g., total number of arrests, prosecutions, or convictions) under their respective state's identity theft statute. However, the officials were able to provide us with examples of actual cases prosecuted under these statutes. The following sections discuss case examples for three states—California, Michigan, and Texas. Presented for illustration purposes only, these cases are not necessarily representative of identity theft crimes in these or other states. Also, as with federal cases, the state case examples also indicate that identity theft can be a component of other crimes, such as check and credit card fraud, as well as computer-related crimes.

California: High Prevalence of Identity Theft

Effective January 1, 1998, under section 530.5 of the California Penal Code, any person "who willfully obtains personal information … of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain credit, goods, services, or medical information in the name of the person without

the consent of that person, is guilty of a public offense."[10] According to the officials we contacted in California, there is not a centralized source of aggregate or statewide statistics regarding the number of investigations, arrests, or prosecutions under California's identity theft statute. However, federal law enforcement officials told us that, relative to many other states, the prevalence of identity theft appears to be high in California. The federal officials also commented that new or different types of identity theft schemes often appear to originate on the west coast and then spread east.

Regarding identity theft cases handled at the state level, in October 2001, one California deputy attorney general told us that she was handling four active cases, and she commented that these were a "tiny drop in the bucket" in reference to prevalence. Further, she noted that the four active cases had one thing in common, that is, the number of victims was "in the hundreds" or even "never ending." Also, in October 2001, another California deputy attorney general told us that, at an identity theft conference hosted by the California attorney general in May 2001, two local law enforcement agencies reported thousands of active cases. Specifically, the Los Angeles County Sheriff's Office reported 2,000 active cases, and the Los Angeles Police Department reported 5,000 active cases.

More recently, in March 2002, we contacted the Los Angeles Police Department to obtain updated information. According to the detective supervisor of the Identity Theft and Credit Card Squad, over 8,000 cases of identity theft were reported to the department in calendar year 2001. He estimated that about 70 percent of these identity theft-related cases involved utility or cellular telephone fraud and the other 30 percent involved credit card fraud and check fraud. Further, the detective supervisor said that the department accepts reports of identity theft only if the victim is a resident of Los Angeles.

Michigan: Cases under the State's 5-year Felony Statute

Michigan's identity theft statute—codified at Mich. Comp. Laws § 750.285—was adopted by the state legislature on December 7, 2000, and became effective April 1, 2001. This new law created a 5-year felony offense for identity theft, making it illegal for a person to obtain or attempt to obtain, without authorization, the "personal identity information" of

[10]According to a California deputy attorney general, the state's identity theft statute was amended in 2000 to remove certain language (i.e., "without the authorization") in order to cover cases where victims give information willingly (e.g., to car rental companies), but the information is later used for unlawful purposes.

another person with the intent to use that information unlawfully to (1) obtain financial credit, employment, or access to medical records or information contained in them; (2) purchase or otherwise obtain or lease any real or personal property; or (3) commit any illegal act. One state-level entity that handles investigations and prosecutions of identity theft is the High Tech Crime Unit of the Michigan Department of the Attorney General. This unit deals with computer crimes and crimes committed over the Internet—crimes in which identity theft is often an aspect.

According to the Michigan assistant attorney general who serves as Chief of the High Tech Crime Unit, the state's first criminal prosecution under the 5-year felony statute was initiated by the unit in August 2001. In this case, a woman was charged with stealing personal identity information from her former employer, using that information to apply over the Internet for several credit cards, and making purchases (approximately $1,000) on such cards, without authorization. The woman pled guilty and was sentenced to 1 year probation and required to pay restitution. The Chief also said that, as of June 2002, three other cases were pending under Michigan's identity theft statute.

We also contacted the Office of the Prosecuting Attorney for Oakland County, Michigan.[11] A deputy prosecutor told us that in the approximately 8 months since Michigan's identity theft statute has been in effect—that is, from April 1, 2001, to the time of our inquiry in early December 2001—one case had been initiated in Oakland County under the statute. This official said that the case, which involved a defendant who had obtained the victim's personal information and used it to apply for a credit card, was still ongoing in the county's court system.

Texas: State Statute Modeled after Federal Law

Texas' identity theft statute—codified at Texas Penal Code § 32.51—became effective September 1, 1999. Modeled after the federal Identity Theft Act, a person commits the offense of identity theft under Texas' law if he or she "obtains, possesses, transfers, or uses identifying information of another person without the other person's consent or with intent to harm or defraud another." According to officials we contacted in Texas, there is not a centralized source of aggregate or statewide statistics

[11]The Oakland County Prosecuting Attorney's Office is located in Pontiac, Michigan. According to a deputy prosecutor, investigations of crimes are handled by each of the 42 local police departments in the county.

regarding the number of identity theft investigations, arrests, or prosecutions under Texas Penal Code § 32.51

In response to our inquiry, the Internet Bureau of the Texas Attorney General's Office reported that it had opened 12 identity theft cases during the period September 2000 through August 2001. According to an Internet Bureau official, these cases had resulted in three arrests and indictments, as of November 2001. In one of these cases, a temporary employee of a technology company allegedly stole personal identifying information from the company's employee database and provided the information to an accomplice, who used the information to apply for bank credit online and collect fees paid by the banks for each application. Reportedly, the scheme affected hundreds of employees. The Internet Bureau official told us that each application using a stolen identity was considered a separate violation and that two suspects had been criminally charged.

We also contacted the Dallas County District Attorney's Office. While the office did not have any readily available statistics on identity theft cases, an assistant district attorney said that the office had handled a variety of identity theft cases, involving check and credit card fraud, as well as fraudulent purchases of vehicles and the acquisition of utility services. The assistant district attorney noted that some of these crimes had been perpetrated by organized rings. One example cited involved a group of three individuals, who made approximately $750,000 in illegal transactions in less than 180 days by using identity fraud coupled with other traditional crimes such as credit card abuse, forgery of commercial instruments, and securing loans through deception.

Enforcement Challenges Regarding State Statutes

Generally, many of the 10 states' officials with whom we talked noted various challenges or obstacles to enforcing identity theft statutes. As discussed in the following sections, these challenges involved topics such as the filing of police reports, the use of limited resources, and the resolution of jurisdictional issues.

Local Police Are Not Always Documenting Identity Theft Crimes Reported by Victims

Efforts taken by identity theft victims to file reports with law enforcement agencies are an important first step in being able to investigate such crime. Also, police reports can be useful to consumers who are victims of identity theft and who need to provide documentation of such to creditors and debt collectors. However, FTC data show that 59 percent of the victims who contacted the FTC during a 12-month period (Nov. 1999 through Oct. 2000) had already contacted the police, but 35 percent of these victims reported that they could not get a police report. Partly because identity

theft is still a non-traditional crime, some police departments are unaware of the importance of taking reports of identity theft, much less initiating investigations.

To help address this issue, FTC staff, in conjunction with the Identity Theft Subcommittee (see app. III), began working with the International Association of Chiefs of Police to encourage police officers to write police reports for victims of identity theft. As a result, in November 2000, the association adopted a resolution calling for "all law enforcement agencies in the United States to take more positive actions in recording all incidents of identity theft." Regarding the need for more positive actions, the resolution noted that

"… reports of identity theft to local law enforcement agencies are often handled with the response 'please contact your credit card company,' and often no official report is created or maintained, causing great difficulty in accounting for and tracing these crimes, and leaving the public with the impression their local police department does not care…"

According to FTC staff, even though the association's resolution is not binding, it sends an important message to police around the country. Also, FTC staff indicated that the same message has been reinforced by FTC staff in numerous law enforcement conferences throughout the nation. FTC data show that 46 percent of the victims who contacted the FTC in calendar year 2001 reported that they had already contacted a police department, and 18 percent of these victims reported that they could not get a police report—which represents a reduction of about half from the percentage of victims who reported being unable to get a police report in the November 1999 through October 2000 period.

Despite progress, the importance of police reports is a topic for continuing focus. For example, in January 2002, a Florida study reported that some of the state's law enforcement agencies "are reluctant to take identity theft complaints and do not generate reports in some cases."[12] Consequently, the study recommended that "all law enforcement agencies be required to generate a report on identity theft complaints regardless of their subsequent decision on whether or not they will investigate the case."

[12]First interim report of the Sixteenth Statewide Grand Jury, *Statewide Grand Jury Report – Identity Theft in Florida*, in the Supreme Court of the State of Florida (Case No. SC 01-1095, Jan. 10, 2002). Members of the Sixteenth Statewide Grand Jury were empaneled by the Florida Supreme Court at the request of the state's governor to investigate and address identity theft-related issues as they occur in Florida.

Also, during our review, a federal official told us that a continuing priority of the Attorney General's Identity Theft Subcommittee[13] is to help educate local police departments about the critical first step of taking reports from victims of identity theft crime. In this regard, the Secret Service is developing a police training video with the cooperation of the FTC, Department of Justice, and the International Association of Chiefs of Police, which is anticipated to be completed by September 30, 2002. Among other purposes, the training video is to emphasize the importance of police reports in identity theft cases.

State Officials Cited Insufficient Resources as an Obstacle to More Fully Addressing Identity Theft

Officials in several of the 10 states included in our study told us that the level of resources being allocated to investigate and prosecute identity theft often is insufficient. This observation was voiced, for example, by a deputy district attorney in California (Los Angeles County), who told us that there are not enough investigators and prosecutors to handle the county's identity theft cases.

Similar comments were provided to us by a supervisor in the Consumer Fraud Division of the Illinois Cook County State's Attorney's Office, which reportedly is the second largest prosecutor's office in the nation, with over 900 assistant state's attorneys. In addition to noting that more prosecutors and support staff were needed to effectively combat identity theft, the supervisor commented that funds were needed for training local police agencies how to handle the more complex cases involving multiple victims, multiple jurisdictions, and voluminous documents.

Further, a chief deputy attorney in the Philadelphia District Attorney's Office commented that, given competing priorities and other factors, there is little incentive for police departments in Pennsylvania to allocate resources for investigating identity theft cases. This official said that police departments are more inclined to use their limited resources for investigating violent crimes and drug offenses rather than handling complicated identity theft cases that, even if successfully prosecuted, often lead to relatively light sentences. In explanation, the chief deputy attorney noted the following:

[13]As discussed in more detail later in this report, the subcommittee was established in 1999 to foster coordination of investigative and prosecutorial strategies and promote consumer education programs.

- Identity theft cases require highly trained investigators, require longer-than-usual efforts, and often end without an arrest.

- Also, under the state's identity theft statute, the first offense is a misdemeanor, although identity theft may be a "lesser included offense" with felony charges involving forgery and theft, given that the fact patterns of these crimes may overlap.

- Even when convictions are obtained, identity theft cases generally do not result in long sentences. For instance, to get a minimum prison term of 1 year for an economic crime in Pennsylvania, a defendant probably would have to steal approximately $100,000. In contrast, a felony drug case conviction involving more than 2 grams of cocaine or heroin—an amount with a street value of about $200—has a mandatory minimum sentence of 1 year of imprisonment.

Despite resource and other challenges, the chief deputy attorney said that the Philadelphia District Attorney's Office does handle identity theft cases. He estimated, for instance, that the office investigated about 100 to 200 identity theft cases in calendar year 2000, and he said these cases represented a "small fraction" of the total number of reported cases in Philadelphia.

State Officials Cited Jurisdiction Issues as an Obstacle to More Fully Addressing Identity Theft

According to many of the state and local officials we contacted, jurisdiction and venue problems are common in identity theft cases. The officials noted, for instance, that many identity theft cases present cross-jurisdictional issues, such as when a perpetrator steals personal information in one city and uses the information to conduct fraudulent activities in another city or another state. In this regard, an official in one state told us that law enforcement agencies sometimes tend to view identity theft as being "someone else's problem." That is, the police department in the victim's area of residence refer the victim to the police department in another county or state where the perpetrator used the personal information—and, in turn, the remote police department refers the victim back to the area-of-residence police department.

To help mitigate this type of problem, some of the states' identity theft statutes have provisions that permit multiple counties to have jurisdiction. For example, Arizona's identity theft statute has a provision that allows victims to file reports in any jurisdiction within the state where the theft or related activities arising from the theft occur. Thus, if a credit card is stolen in Phoenix and used in Tempe, the victim may file in either jurisdiction. Similarly, Florida modified its identity theft statute, effective

July 1, 2001, to specify that the crime of identity theft can be investigated and prosecuted in the county in which the victim resides or where any element of the crime occurred. Also, during our study, a Wisconsin Department of Justice official told us that consideration was being given to amending Wisconsin's identity theft law to permit prosecution of such crime in the jurisdiction of the victim's residence, in addition to any jurisdiction where the stolen personal identity information was fraudulently used.

Federal, State, and Local Law Enforcement Agencies Use Various Means to Promote Cooperation or Coordination in Addressing Identity Theft Crimes

Many federal, state, and local law enforcement agencies have roles in investigating and prosecuting identity theft. Federal agencies include, for example, the FBI, Secret Service, IRS (Criminal Investigation), Postal Inspection Service, and SSA/OIG, as well as U.S. Attorney Offices. However, most identity theft crimes fall within the responsibility of local investigators and prosecutors—such as city police departments or county sheriffs' offices and county district attorney offices, although state-level agencies, such as state attorney general offices, also have a role.

Generally, the prevalence of identity theft and the frequently multi- or cross-jurisdictional nature of such crime underscore the importance of having means for promoting cooperation or coordination among federal, state, and local law enforcement agencies. One such means is the establishment of law enforcement task forces with multi-agency participation. Other relevant means include a coordinating entity (the Attorney General's Identity Theft Subcommittee) and an information-sharing database (accessible via the FTC's Consumer Sentinel Network) established with federal leadership. However, as discussed in the following sections, there are opportunities for promoting greater awareness and use of the Consumer Sentinel Network.

Law Enforcement Task Forces that Address Identity Theft

The use of task forces is perhaps the most commonly used means for promoting cooperation or coordination among law enforcement agencies to address identity theft cases involving multiple jurisdictions. A main advantage of task forces, according to Secret Service officials, is that the pooling of resources and expertise results in more thorough investigations and better continuity from inception of the investigations through prosecution. The officials also noted that improved interagency relationships result in the sharing of investigative leads, bridging of jurisdictional boundaries, and avoiding duplication of efforts. Regarding the views of state officials, a California deputy attorney general, who was working on a task force that included federal and local law enforcement

agencies, told us that this approach simplified all aspects of multi-jurisdictional issues, particularly given that each agency has its own "go to" person.

Generally, task forces can have participating agencies from all levels of law enforcement—federal, state, and local—and may also have private sector representation. The following sections provide examples of task forces developed by federal (Secret Service) and state (California and Florida) leadership, respectively. The scope of our work did not include assessing the effectiveness of these task forces.

Secret Service Task Force Efforts

At the time of our review, the Secret Service was the lead agency in 38 task forces across the country that were primarily targeting financial and electronic crimes—categories of crimes that frequently have identity theft-related elements.[14] According to the Secret Service, electronic crimes task forces concentrate on crimes involving e-commerce, telecommunications fraud, and computer intrusions (hacking), as well as cases involving missing and exploited children. An identity theft-related example is an investigation initiated in December 2000 by the electronic crimes task force of the Secret Service's New York Field Office. According to Secret Service testimony presented in May 2001 at a congressional hearing:[15]

- The investigation, which was conducted jointly by the Secret Service and the New York Police Department, determined that the credit card accounts of many of the nation's wealthiest chief executive officers, as well as many other citizens, had been compromised.
- Using the Internet and cellular telephones, the perpetrators obtained the victims' credit card account numbers and then established fictitious addresses to conduct fraudulent transactions.
- Also, the perpetrators attempted to transfer approximately $22 million—from the legitimate brokerage and corporate accounts of the victims—into

[14]Of the 38 task forces, the Secret Service categorized 24 as being financial crimes task forces, 4 as West African organized crime task forces, 9 as electronic crimes task forces, and 1 as a violent crimes task force. According to Secret Service officials, investigations conducted by each the 38 task forces can include identity theft-related cases, although none of the 38 focuses solely or exclusively on such cases.

[15]Prepared statement of Mr. Bruce Townsend, Special Agent in Charge, Financial Crimes Division, U.S. Secret Service, for a hearing ("On-line Fraud and Crime: Are Consumers Safe?") before the Subcommittee on Commerce, Trade, and Consumer Protection; House Committee on Energy and Commerce (May 23, 2001).

fraudulently established accounts for conversion to the perpetrators' own use.

Table 3 presents an example of another Secret Service electronic crimes task force, which was first developed in 1995 by the agency's Washington (District of Columbia) Field Office and has subsequently grown to include a total of 32 participating law enforcement agencies and private sector entities.

Table 3: Participants in Electronic Crimes Task Force Developed by Secret Service's Washington Field Office

Task force participants	Number of agencies or entities
Federal law enforcement agencies: Bureau of Alcohol, Tobacco and Firearms; Customs Service; Defense Criminal Investigative Service; Department of Housing and Urban Development; Department of State; Drug Enforcement Administration; FBI; General Services Administration; Immigration and Naturalization Service; Metropolitan Washington Airports Authority; Postal Inspection Service; Secret Service; and SSA.	13
State and local law enforcement agencies: Bladensburg Police Department, Hyattsville Police Department, Fairfax County Police Department, Maryland State Police, Metropolitan Police Department, Montgomery County Police Department, Mount Rainier Police Department, Prince George's County Police Department, and Vienna Police Department.	9
Private sector entities: Allfirst Bank, Bank of America, Bell Atlantic, Cellular One, Chevy Chase Bank, Citibank, First Union Bank, MBNA, Target Department Stores, and Wachovia Bank.	10
Total number of law enforcement agencies and private sector entities	**32**

Source: Secret Service.

Secret Service officials said that the agency's task forces generate cases that result in prosecutions in state and local courts as well as in federal courts. The officials estimated, for instance, that the majority (about 60 percent) of the Washington Field Office Task Force's cases had been prosecuted in state courts. Further, regarding the operations of Secret Service task forces in general, the officials noted that, while the Secret Service may have overall administrative responsibility, the role of "quarterback" regarding the investigative agenda often is a shared role. In explanation, the officials said that the task forces do get involved in cases important to the needs of local communities.

California: High-Technology Task Forces Address Identity Theft

In the mid-1990s, the California Attorney General's Office established five regional task forces in the state to facilitate multi-jurisdictional investigations and prosecutions of high-technology crimes, such as the

theft of chips and other computer components. The five high-technology task forces also are to address identity theft/fraud and its related crimes. One of the five is the Sacramento Valley High-Technology Crime Task Force, which was reorganized in October 1999 as a separate division within the Sacramento County Sheriff's Department. The task force includes participants from local, state, and federal agencies in the 34 counties of the eastern judicial district of the state of California. As of calendar year 2001, a total of 32 agencies or entities were represented, as table 4 shows.

Table 4: Participants in the Sacramento Valley High-Technology Crimes Task Force

Task force participants	Number of agencies or entities
Police departments: Davis, Folsom, Modesto, Isleton, Roseville, Sacramento, Turlock, West Sacramento, and Yuba.	9
Sheriff's departments: El Dorado, Merced, Placer, Sacramento, San Joaquin, Stanislaus, Sutter, and Tuolumne.	8
District attorney offices: Placer, Sacramento, and Yolo.	3
State agencies: Controller's Office, Department of Corrections, Department of Justice, Department of Motor Vehicles, Highway Patrol, Probation (Sacramento), and University of California (Davis).	7
Federal agencies: FBI, Forest Service, Postal Inspection Service, Secret Service, and U.S. Attorney's Office.	5
Total number of agencies and entities	**32**

Source: Sacramento Valley High-Technology Crimes Task Force.

According to its annual report for calendar year 2001, the Sacramento Valley High-Technology Crimes Task Force investigated 153 cases involving identity theft. Examples of these cases included the following:

- Detectives were called to the Sacramento International Airport to investigate a suspect who used stolen credit card information to purchase tickets for two other suspects. The investigation revealed 24 other victims whose credit cards had been stolen by one of the suspects from his place of employment.

- A suspect attempted to purchase items at a store using a manufactured fraudulent check. After being arrested, the suspect identified herself using another person's identity and was booked into jail using that name. However, an investigation determined the suspect's true identity and that she had written at least seven other fraudulent checks in the Sacramento area.

- A suspect used a victim's identity to open an account at a jewelry store and charge several items. Also, the suspect opened several other accounts in the victim's name and made purchases (some over the Internet) using these accounts. Further, the investigation found numerous names, credit information, SSNs, and driver's licenses—and documents with Internet Web sites, passwords, and personal identification numbers—indicating that the suspect had opened accounts using the personal information of the victims.

Florida: Statewide Initiative to Investigate and Prosecute Identity Theft Cases

Identity theft-related enforcement efforts in Florida are being led by the Florida Attorney General's Office of Statewide Prosecution and the Florida Department of Law Enforcement. In 2001, these agencies partnered to create a statewide task force initiative to target perpetrators of identity fraud. The initiative—called Operation LEGIT (law enforcement getting identity thieves)—has special agents and other personnel assigned from various regional offices of the Florida Department of Law Enforcement. Other task force participants can include local and federal law enforcement agencies, as indicated in the following examples of cases:[16]

- For more than 12 years, a Florida suspect assumed and lived under the identity of a California victim, who had lost his wallet (with his driver's license and other personal identification information) while vacationing in Daytona Beach in 1987. Since that time, the suspect had purchased and sold homes, opened bank accounts, obtained credit, established utility and phone service, and been arrested on at least three separate occasions. Based on a Florida warrant, the victim was wrongly arrested in California and held in jail for more than a week. Also, the victim has had civil judgments levied against him. The investigation that led to the suspect's arrest was initiated in May 2001 and was conducted by the Hernando County (Florida) Sheriff's Office, the Florida Department of Law Enforcement, the Office of Statewide Prosecution, and SSA/OIG.

- In July 2001, six suspects were charged with racketeering and multiple counts of identity theft that affected victims throughout Florida. The ringleader orchestrated the scheme from a Florida prison (Gulf County Correctional Facility), where he was serving a 9-year sentence for his involvement in a similar investigation that concluded in 1998, with victims throughout Florida and Georgia. Using the inmate telephone system and

[16]The examples are excerpts from news releases made by Florida's Office of Statewide Prosecution. Generally, the news releases noted that charges are merely accusations and arrested defendants are presumed innocent until and unless the charges are proven beyond a reasonable doubt.

the U.S. mail service, the ringleader obtained account and identity information of unsuspecting consumers. Accomplices used the compromised identities to commit credit card fraud, purchase vehicles, open fraudulent checking accounts, and apply for instant loans at furniture stores and other businesses across Florida. The organized scheme netted the ring more than $200,000 in stolen property. This case was investigated by the Florida Department of Law Enforcement, the Office of Statewide Prosecution, and SSA/OIG.

- In October 2001, six suspects were arrested for fraudulently obtaining nearly $300,000 in merchandise, after assuming the identities of 18 individuals from around the country. An employee of a children's clinic in Orlando obtained the SSNs and other identifying information of the 18 individuals, who had participated in a medical study concerning cystic fibrosis and whose children suffer from the disease. The employee passed the information to another person, who created false birth certificates and other documents that were used to obtain identity cards in the names of the victims through offices of the Florida Department of Motor Vehicles. The suspects used the false identities to obtain instant credit at electronic and furniture stores in Orange and Seminole Counties in Florida. The suspects purchased big-screen televisions, computers, and other high-cost items until the victims' credit lines were exhausted. The purchased items were later sold on the streets of Orlando (Florida) and Chicago (Illinois) for half their retail value, with the proceeds divided by the suspects. The investigation was conducted by the Orlando Police Department, the Florida Department of Law Enforcement, and the Office of Statewide Prosecution.

- In February 2002, a former resident of Daytona Beach was charged with obtaining personal identifying information (names, addresses, and SSNs) on various individuals and using the information to fraudulently purchase more than $35,000 worth of merchandise throughout east-central Florida. The suspect obtained the information from a Web site used legitimately by a variety of businesses and individuals for the purpose of finding and tracking others. As of February 2002, the then-ongoing investigation by the Florida Department of Law Enforcement revealed that the suspect had compromised the identities of victims in 12 states.

Identity Theft Subcommittee Formed to Have Coordination and Education Role

In early 1999, following passage of the federal Identity Theft Act in 1998, 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 and promote consumer education programs. 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 as state and local representation through the International Association of Chiefs of Police, the National Association of Attorneys General, and the National District Attorneys Association. Appendix III lists the membership of the subcommittee.

In response to our inquiries, the Chairman of the subcommittee said that, although there is no written charter or mission statement, the role and activities of the subcommittee are substantially as follows:

- Initially, to promote awareness and use of the federal Identity Theft Act, the subcommittee prepared guidance memorandums for field distribution to law enforcement and regulatory agencies. Also, the subcommittee helped to plan or support various identity theft-related educational presentations and workshops, with participants from the public and private sectors.

- Because so much of identity theft is a local matter, it was imperative that the subcommittee's membership include state and local representatives. Participation by the International Association of Chiefs of Police gives the subcommittee a channel to thousands of local law enforcement entities. A continuing priority of the subcommittee is to help educate local police departments about the critical first step of taking reports from victims of identity theft crime.

- Furthermore, the subcommittee continually promotes the availability of FTC's Consumer Sentinel Network as a tool for federal, state, and local law enforcement agencies to use.

The subcommittee Chairman also noted that, since the terrorist incidents of September 11, 2001, there has been more of a focus on prevention. For example, the American Association of Motor Vehicle Administrators attended a recent subcommittee meeting to discuss ways to protect against counterfeit or fake driver's licenses.

To obtain a broader understanding of the subcommittee's role, as well as ways to potentially enhance that role, we contacted the designated individuals who, respectively, represented six member organizations—FBI, National District Attorneys Association, Postal Inspection Service, Secret Service, Sentencing Commission, and SSA/OIG. Generally, the representatives commented that the subcommittee has been helpful in combating identity theft and has been functioning well, particularly

considering the fact that membership is a collateral duty for each representative. One member—representing the National District Attorneys Association—suggested that the subcommittee's role could be enhanced by having a formal charter or mission statement detailing each participant's role. However, the FBI and Secret Service representatives said that the informality of the subcommittee promotes member participation and also commented that additional directives could be counterproductive.

Opportunities for Law Enforcement to Use FTC Data to Aid in Investigations of Identity Theft

Since its establishment in 1999, FTC's Identity Theft Data Clearinghouse has been used for reporting statistical and demographic information about victims and perpetrators. While not immediate, the value of the Clearinghouse database as a law enforcement tool has been growing but has not reached its full potential. In conducting investigations, for example, relatively few law enforcement agencies have used FTC's Consumer Sentinel Network, which provides computer access to the Clearinghouse database. Further, centralized analysis of database information to generate investigative leads and referrals has been limited. Law enforcement's limited use of the Consumer Sentinel Network and the Clearinghouse database may be due to various reasons, including the relatively short operating history of the database. To promote greater awareness and use of the Network and the Clearinghouse database, FTC and Secret Service outreach efforts include conducting regional law enforcement training seminars and developing a training video for distribution to local law enforcement agencies across the nation.

FTC Established the Identity Theft Data Clearinghouse in 1999

The federal Identity Theft Act of 1998 required 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, in November 1999, FTC established the Identity Theft Data Clearinghouse to gather information from any consumer who wishes to file a complaint or pose an inquiry concerning identity theft. Consumers can call a toll-free telephone number (1-877-ID-THEFT) 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, the Clearinghouse received a total of 94,100 complaints from identity theft victims. This total includes 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 had increased to

over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls.

From its inception, the Clearinghouse database has been used to report statistical and demographic information about victims and perpetrators. For example, regarding identity theft complaints received in calendar year 2001, an FTC official testifying at a March 2002 congressional hearing summarized database information partly as follows:[17]

"The Clearinghouse database has been in operation for more than two years. … While not comprehensive, information from the database can reveal information about the nature of identity theft activity. For example, the data show that California has the greatest overall number of victims in the FTC's database, followed by New York, Texas, Florida, and Illinois. On a per capita basis, per 100,000 citizens, the District of Columbia ranks first, followed by California, Nevada, Maryland and New York. The cities with the highest numbers of victims reporting to the database are New York, Chicago, Los Angeles, Houston, and Miami.

"Eighty-eight percent of victims reporting to the FTC provide their age. The largest number of these victims (28%) were in their thirties. The next largest group includes consumers from age eighteen to twenty-nine (26%), followed by consumers in their forties (22%). Consumers in their fifties comprised 13%, and those age 60 and over comprised 9%. Minors under 18 years of age comprised 2% of victims. …

"Thirty-five percent of the victims had not yet notified any credit bureau at the time they contacted the FTC; 46% had not yet notified any of the financial institutions involved. Fifty-four percent of the victims had not yet notified their local police department of the identity theft. By advising the callers to take these critical steps, we enable many victims to get through the recovery process more efficiently and effectively."

Centralized Analysis of Clearinghouse Data to Generate Investigative Leads and Referrals is Increasing

In addition to providing a basis for reporting statistical and demographic information about identity theft victims and perpetrators, another primary purpose of the Clearinghouse database is to support law enforcement. Since May 2001, one Secret Service special agent, working with an FTC attorney, an investigator, and a paralegal, has been involved in centrally analyzing Clearinghouse data to generate investigative leads and referrals. Specifically, according to FTC staff:

[17]Prepared statement of the FTC, *Identity Theft: the FTC's Response*, before the Subcommittee on Technology, Terrorism and Government Information, Senate Judiciary Committee (Mar. 20, 2002).

- The team uses intelligence software to analyze Clearinghouse data to generate investigative leads.

- These leads are then further developed using criminal investigative resources provided by the Secret Service and research and analytical tools provided by the FTC.

- When the case leads have been comprehensively developed, they are referred to federal, state, or local law enforcement officers in the field. These officers participate in financial, high-tech, or economic crimes task forces and are well equipped to handle the cases.

The pace of developing and sending out investigative leads has picked up since FTC and the Secret Service jointly initiated their efforts in May 2001. For instance, 10 investigative referrals were made to regional law enforcement during the last 6 months of calendar year 2001, whereas 19 referrals were made in the first 5 months of 2002. One of the 29 referrals involved 10 individuals with the same address. In response to our inquiries in May 2002, Secret Service officials said that the 29 referrals were still being worked and, thus, the results or outcomes were yet to be determined.

Relatively Few Law Enforcement Agencies Use the Consumer Sentinel Network to Access FTC's Identity Theft Data Clearinghouse

In addition to receiving referrals based on centralized analysis of Clearinghouse data, federal, state, and local law enforcement agencies nationwide can use desktop computers to access Clearinghouse data to further support ongoing cases or develop new leads. Specifically, through FTC's Consumer Sentinel Network—which is a secure, encrypted Web site—law enforcement agencies can access Clearinghouse data and use search tools tailored for identity theft investigations. For instance, an investigator may scan consumer complaints matching certain criteria to determine if there is a larger pattern of criminal activity. FTC does not charge a fee for use of the Consumer Sentinel Network. However, each law enforcement agency must enter into a confidentiality agreement (pledging to abide by applicable confidentiality rules) with FTC.

As of May 24, 2002, a total of 46 federal agencies had signed user agreements with FTC, facilitating access to Identity Theft Data Clearinghouse information via the Consumer Sentinel Network. These agencies include the FBI, Secret Service, Postal Inspection Service, SSA/OIG, and some U. S. Attorney Offices. Further, relatively few of the nation's over 18,000 state and local law enforcement agencies have signed agreements with FTC to use the Consumer Sentinel Network to access the Identity Theft Data Clearinghouse. Specifically, as of May 24, 2002, a total

of 306 state and local law enforcement agencies had entered into such agreements. Of this total, the number of users varied from 1 law enforcement agency in each of 5 states (Delaware, Hawaii, Idaho, New Hampshire, and New Mexico) and 2 agencies in each of 8 other states (Arizona, Arkansas, Kansas, Massachusetts, Nebraska, Oregon, South Dakota, and Wyoming) to 17 agencies in Texas and 45 agencies in California. Even at the high end of this range, the extent of access is not comprehensive. For example:

- In Texas, the Houston Police Department and the Harris County Sheriff's Office—jurisdictions that encompass about 22 percent of the state's population—are not users of the Consumer Sentinel Network. As stated previously, in reference to number of identity theft victims, Houston is among the top five cities nationally. Overall, less than 1 percent of the state's law enforcement agencies have entered into confidentiality agreements with FTC.

- Although California has the largest number of users (45 agencies), the list of subscribers does not include the city police departments in Los Angeles, Sacramento, or San Jose. As mentioned previously, over 8,000 cases of identity theft were reported to the Los Angeles Police Department in calendar year 2001.

According to FTC staff, the number of Consumer Sentinel member agencies continually increases, particularly in response to outreach activities such as regional law enforcement training. Appendix IV gives a full listing of the 352 agencies that had entered into user agreements with FTC, as of May 24, 2002.

FTC staff provided us query statistics showing external law enforcement usage of the Consumer Sentinel Network and the Identity Theft Data Clearinghouse for January 2001 through March 2002. During this 15-month period, the number of external law enforcement queries about identity theft complaints totaled 7,946—an average of about 530 per month—and ranged from 378 in December 2001 to 783 in January 2002. FTC staff noted that these usage statistics do not reflect centralized analysis of identity theft complaint data, conducted jointly by the Secret Service and FTC.

Reasons for Limited Law Enforcement Use of Consumer Sentinel Network and Clearinghouse Database

Various reasons may explain law enforcement's relatively limited use of the Consumer Sentinel Network and the Identity Theft Data Clearinghouse database. Department of Justice officials said, for instance, that many state and local agencies may have an insufficient number of computers and support personnel, in addition to being challenged by competing

priorities. Also, FTC staff and Secret Service officials noted that the availability of the Clearinghouse database as an aid for law enforcement agencies is still relatively new. As such, some potential users are unaware of this investigative resource, despite ongoing outreach efforts.

Further, regarding usefulness of database information for law enforcement purposes, we asked whether any examples of federal, state, or local success stories had been presented or discussed at any of the monthly meetings of the Attorney General's Identity Theft Subcommittee. In response, the head of the subcommittee told us that none of the meetings had included such examples—neither examples involving field agencies that used the Consumer Sentinel Network to develop cases nor examples involving the results of investigative leads or referrals that were based on centralized analysis of Clearinghouse data.

One state's deputy attorney general, in replying to our inquiry about the usefulness of the Consumer Sentinel Network and the Clearinghouse database, said that, as a practical matter, a local investigator with numerous outstanding cases on his or her desk will not be using the FTC system to obtain more cases. Rather, this state official suggested, for example, that FTC could use the system to generate periodic reports to alert law enforcement of specific problems within their respective jurisdictions and facilitate the coordination of investigative resources for the maximum benefit.

FTC staff acknowledged that Sentinel members appear to use the Clearinghouse database to bolster the cases they have under investigation more often than to initiate new cases. However, the FTC staff told us that they are continuously looking for ways to make the Clearinghouse database more efficient and user friendly. The staff noted, for example, that FTC has established an e-mail address to take requests for specific searches from Sentinel members and, thereby, FTC can use its internal search tools to query the Clearinghouse database and provide more comprehensive results to requesters. Also, the staff noted that FTC expects to implement an "alert" function before the end of fiscal year 2002. According to the staff:

- The alert function will enable a Clearinghouse user (e.g., police officer) to flag or annotate one or more particular complaints relating to an investigation that the user is conducting. If and when another user executes a query that retrieves one of the flagged complaints, this second user will get a pop-up message box asking him or her to contact the first

user before proceeding.

- Thus, two police officers, who likely are from different jurisdictions but are looking at the same complaint records, can avoid duplicating investigatory efforts or inadvertently impeding each other's investigations.

Also, the staff noted that FTC has plans to implement (by the end of fiscal year 2002) a report listing the suspect locations most frequently reported in the database.[18] Further, in response to requests from Sentinel members, the FTC will soon begin testing a program to provide Sentinel members access to electronic batches of Clearinghouse data—for example, all complaint information reported by victims in a given city during a specified period of time. According to FTC staff, Sentinel members will be able to run the batched data through their own intelligence or link analysis software and also combine the data with their own investigative information for more impact.

Moreover, FTC staff said that additional steps are being taken to increase law enforcement agencies' awareness and use of the Consumer Sentinel Network and the Clearinghouse database. The staff noted, for example, that training sessions for law enforcement agencies were conducted in Washington, D.C., in March 2002, in Des Moines, Iowa, and Chicago, Illinois, in May 2002, and that additional sessions are planned for San Francisco, California, in June 2002, and for Dallas, Texas, in August 2002. Also, as mentioned previously, the Secret Service is developing a police training video with the cooperation of the FTC, Department of Justice, and the International Association of Chiefs of Police, which is anticipated to be completed by September 30, 2002. According to FTC staff and Secret Service officials, the training video will briefly discuss the availability of the Consumer Sentinel Network and the Identity Theft Data Clearinghouse, in addition to emphasizing the importance of police reports in identity theft cases.

These planned initiatives appear to be steps in the right direction. If implemented effectively, the initiatives should help to ensure that more law enforcement agencies are aware of existing data that can be used to combat identity theft. Nonetheless, concerted and continued outreach efforts will be needed to promote broad awareness and use of the

[18]Further, as discussed in appendix V, FTC and the Department of Defense have agreed to establish Soldier Sentinel, an online system designed specifically to collect consumer and identity theft complaint information from members of the armed forces and their families.

Consumer Sentinel Network and the Clearinghouse database by all levels of law enforcement.

SSA/OIG Actions to Resolve SSN Misuse and Other Identity Theft-Related Allegations

As mentioned previously, SSA/OIG's fraud hotline annually receives tens of thousands of allegations, most of which involve either (1) SSN misuse or (2) program fraud with SSN misuse potential. In these 2 categories, SSA/OIG received approximately 62,000 allegations in fiscal year 1999, and the agency opened investigative cases on 4,636 (about 7 percent) of these allegations. About three in four of the investigative cases involved program fraud-related allegations. Generally, SSA/OIG concentrates its investigative resources on this category of allegations because the protection of Social Security trust funds is a priority. SSA/OIG statistics for investigative cases opened in fiscal year 1999 indicate that a total of 1,347 cases had resulted in criminal convictions or other judicial actions, as of April 30, 2002. During our review, the SSA Inspector General told us that his office does not have enough investigators to address all of the SSN misuse allegations received on the agency's fraud hotline. However, FTC staff noted that, starting in February 2001, FTC began to routinely upload information from SSA/OIG's fraud hotline about these allegations into FTC's Identity Theft Data Clearinghouse, thereby making the information available to law enforcement agencies via the Consumer Sentinel Network.

SSA/OIG Concentrates Its Investigative Resources on Allegations of Program Fraud with SSN Misuse Potential

Within the categories of SSN misuse and program fraud with SSN misuse potential, SSA/OIG received a total of 62,376 allegations in fiscal year 1999, a greater number (83,721) in fiscal year 2000, and an even higher number (104,103) in fiscal year 2001. According to SSA/OIG officials, allegations are reviewed by supervisory personnel to determine which should be further pursued. The review criteria, among others, include considerations of the credibility of the alleged information, the actual or potential dollar-loss amounts involved, the severity of other effects on SSA programs, and the prosecutive merits of the allegation, as well as considerations of current workloads and the availability of investigative resources.

Most allegations of identity theft made to SSA/OIG do not result in criminal investigations being opened. Of the two categories of allegations, however, SSA/OIG generally concentrates its investigative resources on allegations of program fraud with SSN misuse potential because the protection of Social Security trust funds is a priority. In fiscal year 1999, for example, SSA/OIG opened investigative cases on 12 percent of the allegations categorized as program fraud with SSN misuse potential and 3 percent of the allegations categorized as SSN misuse (see table 5). In other

words, although the total numbers of allegations received in each category were similar, program fraud-related allegations were about four times more likely to result in investigative cases being opened.

Table 5: Allegations Received by SSA/OIG and Investigative Cases Opened, Fiscal Year 1999

Allegation type	Number of allegations received	Number of investigative cases opened	Percentage of allegations investigated
SSN misuse	30,116	868	3
Program fraud with SSN misuse potential	32,260	3,768	12
Total	**62,376**	**4,636**	**7**

Source: SSA/OIG data.

Investigations of Allegations Have Produced Convictions and Other Judicial Actions

In response to our inquiry regarding the results of SSA/OIG criminal investigations, the agency provided us statistics for applicable cases opened in fiscal year 1999 that resulted in criminal or other judicial actions. As table 6 shows, as of April 30, 2002, SSN misuse cases (768) accounted for 57 percent of the 1,347 investigations involving SSN misuse or program fraud with SSN misuse potential that were opened in fiscal year 1999 and resulted in criminal or other judicial actions.

Table 6: Results, as of April 30, 2002, of SSA/OIG Investigations Opened in Fiscal Year 1999

Results category	Description of category	Number of investigations resulting in criminal or other judicial actions			Percentage of total number
		SSN misuse	Program fraud with SSN misuse potential	Total	
Individual convicted and sentenced	These cases involved accused individuals who were tried, found guilty, and sentenced.	338	339	677	50
Alien apprehended and deported	These cases involved the taking into custody of an illegal alien or undocumented immigrant, who used the SSN of another person.	423	31	454	34
Fugitive felon apprehended	These cases involved individuals who were receiving Social Security benefits and who were also the subjects of outstanding warrants. SSA/OIG coordinated with the U.S. Marshals Service or state or local law enforcement to apprehend the fugitive.	0	137	137	10
First-time offender handled by pretrial diversion program	These cases involved first-time offenders who were placed on probation for 12 to 18 months.	7	72	79	6
Total		**768**	**579**	**1,347**	**100**
Percentage of total		**57**	**43**	**100**	

Note: Data represent criminal investigations that were opened in fiscal year 1999 by SSA/OIG and that were closed with a criminal or other judicial actions as of April 30, 2002. Other criminal investigations may have resulted in civil monetary penalties or administrative action or may have been closed with no action.

Source: SSA/OIG data.

SSA/OIG officials said that investigations of SSN misuse allegations produce convictions or other criminal results because SSN misuse generally is tied to other white-collar or financial crimes that can have identity theft-related elements. On the other hand, the officials said that many investigations of program fraud cases may be closed with administrative actions, which can include suspension of benefit payments.

SSA/OIG Allegation Information Is Now Being Added to FTC's Database

In recent years, the number of SSN misuse allegations received by the SSA/OIG has grown faster than the number of program fraud-related allegations. That is, SSN misuse allegations constitute a growing proportion of these two categories of allegations, increasing from 48 percent in fiscal year 1999, to 56 percent in fiscal year 2000, and to 63 percent in fiscal year 2001. During our review, the SSA Inspector General

told us that, given limited resources and competing priorities, his office investigates relatively few allegations of SSN misuse. Consequently, the Inspector General said that many credible allegations of identity theft that have the potential to produce criminal convictions or other judicial actions are not addressed.

Starting in February 2001, FTC began routinely uploading SSA/OIG information about SSN misuse allegations into FTC's Identity Theft Data Clearinghouse. This enhancement of the Clearinghouse database makes the SSA/OIG allegation information available to law enforcement agencies via the Consumer Sentinel Network. However, as discussed previously, relatively few law enforcement agencies use the Network, and centralized analysis of Clearinghouse data to generate investigative leads and referrals has been limited.

Conclusions

Comprehensive results—such as number of prosecutions and convictions—under the federal Identity Theft Act and relevant state statutes are not available. However, examples of actual cases illustrate that identity theft often is a component of other white-collar or financial crimes, and these cases often have fact-pattern elements involving more than one jurisdiction. Moreover, the prevalence of identity theft and the frequently multi- or cross-jurisdictional nature of such crimes underscore the importance of leveraging available resources and promoting cooperation or coordination among all levels of law enforcement.

Our review indicates that there are opportunities for law enforcement to make greater use of existing data to combat identity theft. In particular, the Consumer Sentinel Network potentially can provide all law enforcement agencies across the nation with access to FTC's Identity Theft Data Clearinghouse database to support ongoing investigations. In addition to complaint information reported by identity theft victims directly to FTC, the Clearinghouse database now routinely incorporates identity theft-related information received by SSA/OIG. However, despite outreach efforts to date, relatively few state and local law enforcement agencies have signed Consumer Sentinel confidentiality agreements with FTC. Also, although the number is increasing, few investigative leads and referrals have been generated by centralized analysis of database information. Given the growing prevalence of identity theft, continued and concerted emphasis is warranted regarding the availability and use of the Consumer Sentinel Network and the Clearinghouse database as law enforcement tools.

Recommendation for Executive Action

We recommend that the Attorney General have the Identity Theft Subcommittee promote greater awareness and use of the Consumer Sentinel Network and the Identity Theft Data Clearinghouse by all levels of law enforcement—federal, state, and local.

Agency Comments

On June 5, 2002, we provided a draft of this report for comment to the Departments of Justice and the Treasury, FTC, and SSA. The Department of Justice generally agreed with the substance of the report and recommendation that the Identity Theft Subcommittee promote greater awareness and use of the Consumer Sentinel Network and the Identity Theft Data Clearinghouse by all levels of law enforcement. Further, Justice noted several actions that it has taken or will take to directly address the recommendation. These actions include, for example, regional training seminars cosponsored by Justice, FTC, and the Secret Service that have specific components about the Consumer Sentinel and the identity theft database. Justice noted that five training seminars have been or are planned for this fiscal year and that additional seminars are being considered for fiscal year 2003. Also, Justice said that the state and local law enforcement representatives on the Identity Theft Subcommittee will be consulted regarding additional mechanisms for informing police departments and sheriffs' offices about the Consumer Sentinel. Further, Justice cited its efforts to inform the public about identity theft and ensure that courts are meting out appropriate criminal sanctions. The full text of Justice's comments is reprinted in appendix VI.

The Secret Service, a component agency of the Department of the Treasury, said that the draft report accurately presented the agency's positions. Also, the Secret Service commented that the agency's liaison to the FTC attended 33 speaking engagements from May 2001 to May 2002 to promote the Identity Theft Data Clearinghouse and that a similar schedule is anticipated for the next 12 months. Furthermore, the Secret Service noted that the FTC—in conjunction with the Secret Service liaison, Justice, and the International Association of Chiefs of Police—plans to sponsor at least six training seminars in fiscal year 2003.

Justice and the Secret Service also provided various technical comments and clarifications, which have been incorporated in this report where appropriate. Similarly, the FTC and SSA provided technical comments and clarifications, which have been incorporated where appropriate.

In sum, we believe that the ongoing and planned efforts cited by the Department of Justice and the Secret Service are responsive to the recommendation that we make in this report.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies to interested congressional committees and subcommittees; the Attorney General; the Secretary of the Treasury; the Chief Postal Inspector, U.S. Postal Inspection Service; the Commissioner, SSA; and the Chairman, FTC. We will also make copies available to others on request.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or Danny R. Burton at (214) 777-5600. Other key contributors are acknowledged in appendix VII.

Sincerely yours,

Richard M. Stana
Director, Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

In response to a request from Representative Sam Johnson, we developed information on the following topics:

- Law enforcement results (such as examples of prosecutions and convictions) under the federal Identity Theft and Assumption Deterrence Act of 1998 (the "Identity Theft Act").
- Law enforcement results under state statutes that, similar to the federal act, provide state and local law enforcement officials with the tools to prosecute and convict identity theft criminals.
- The means used to promote cooperation or coordination among federal, state, and local law enforcement agencies in addressing identity theft crimes that span multiple jurisdictions.
- Actions taken by the Social Security Administration's Office of the Inspector General (SSA/OIG) to resolve Social Security number (SSN) misuse and other identity theft-related allegations received during fiscal year 1999.

Scope and Methodology

The following sections discuss the scope and methodology of our work in addressing the respective topics.

Law Enforcement Results under the Federal Statute

To determine what have been the law enforcement results under the federal Identity Theft Act,[1] we contacted various federal agencies responsible for investigating and prosecuting this type of crime. Specifically, we interviewed responsible officials and reviewed documentation obtained from the Department of Justice's Criminal Division, the Executive Office for United States Attorneys (EOUSA), the Federal Bureau of Investigation (FBI), the Postal Inspection Service, the Secret Service, and SSA/OIG. We reviewed available statistics on number of investigations and prosecutions and obtained examples of actual investigations and prosecutions under the federal statute.

Also, we conducted a literature search to identify studies, reports, or other products—including congressional testimony statements—giving examples of cases or other results under the federal Identity Theft Act. In

[1]The relevant section of this legislation is codified at 18 U.S.C. § 1028(a)(7) ("fraud and related activity in connection with identification documents and information").

February 2002, we conducted a search of the LexisNexis database.[2] Our search was designed to retrieve only those identity theft cases that specifically mentioned the federal statute—that is, cases that cited 18 U.S.C. § 1028(a)(7). We summarized the results of selected cases prosecuted under this statute. Our summary (see app. II) is not intended to be a comprehensive listing of all federal prosecutions under the 1998 federal statute.

Law Enforcement Results under State Statutes

We contacted the Federal Trade Commission (FTC) to determine which states had enacted specific laws related to identity theft. To determine the availability of any national overview information regarding law enforcement results under the states' identity theft laws, we reviewed the offense categories included in the FBI's Uniform Crime Reporting (UCR) Program,[3] and we contacted the National Association of Attorneys General, the National District Attorneys Association, and the International Association of Chiefs of Police.

For more detailed inquiries, we selected 10 states—Arizona, California, Florida, Georgia, Illinois, Michigan, New Jersey, Pennsylvania, Texas, and Wisconsin. We judgmentally selected these states on the basis of having the highest incidences of reported identity theft or the longest-standing applicable statutes. Specifically, with one exception (New York), we selected each state that had more than 2,500 complaints reported to FTC during November 1999 through September 2001 (see table 8). Also, some of the first states to enact identity theft laws were Arizona (1996), California (1997), and Wisconsin (1997). As indicated in table 7, the 10 states we selected represent about 51 percent of the total number of complaints received by the FTC during November 1999 through September 2001.

[2]LexisNexis provides a researchable database service, which includes legal documents (federal and state laws, regulatory information, and court decisions), news, public records, and business information via on-line, hardcopy print, and CD-ROM formats.

[3]The UCR Program is a nationwide, cooperative statistical effort of nearly 17,000 city, county, and state law enforcement agencies voluntarily reporting data on crimes brought to their attention. According to the FBI, during 2000, law enforcement agencies active in the UCR Program represented nearly 254 million U.S. inhabitants, or 94 percent of the total population as established by the Bureau of the Census.

Table 7: Number of Identity Theft Complaints Received by FTC (Nov. 1999 through Sept. 2001) for Selected States

State	Number of complaints	Percentage
States with more than 2,500 complaints[a]:		
California	16,147	17.2
Texas	6,775	7.2
Florida	6,309	6.7
Illinois	4,145	4.4
Michigan	3,038	3.2
Pennsylvania	2,979	3.2
New Jersey	2,827	3.0
Georgia	2,770	2.9
States with longest-standing statutes[b]:		
Arizona	2,049	2.2
California (included above)		
Wisconsin	1,016	1.1
Subtotal	48,055	51.1
Other states and the District of Columbia	38,715	41.1
Other locations or not reported[c]	7,330	7.8
Total	**94,100**	**100.0**

[a]The only other state with more than 2,500 complaints was New York, which accounted for 8,219 complaints during November 1999 through September 2001. However, given the terrorist events of September 11, 2001, and the ongoing recovery efforts, we did not include New York in our case study of selected states. In addition, at the time we initiated our review, New York did not have a specific statute making identity theft a crime.

[b]Mississippi possibly enacted the nation's first identity theft statute (Miss. Code Ann. § 97-19-85), even though it was titled as a "false pretenses" statute rather than specifically labeled as an "identity theft" statute. Originally enacted in 1993, the statute was amended in 1998 to include additional identifiers and increase punishment from a misdemeanor to a felony.

[c]This category includes complaints from (1) victims who did not report their location and (2) victims who reported from other locations, such as Guam, Puerto Rico, the U.S. Virgin Islands, and Canada.

Source: FTC Identity Theft Data Clearinghouse. Also, note "b" is based on our analysis of the Mississippi statute and a follow-up discussion with an official in the Mississippi Attorney General's Office.

In each of the 10 selected states, we attempted to contact officials in the state's attorney general's office and in at least one local jurisdiction (e.g, a county district attorney's office). We developed a structured data collection instrument and distributed it to each of these officials. The instrument was used to obtain information about the respective state's specific identity theft statute, implementation activities, relevant investigative and prosecutorial units, reports or records of statistical results, examples of actual cases, and observations on the usefulness or effectiveness of the statute. With the exception of Arizona, the attorney

general's office in each of the 10 selected states responded to our inquiries. Also, at least one local official in each of the 10 states except Georgia responded to our inquiries. Given the limited distribution of our data collection instrument, the observations of the respondents cannot be viewed as being representative of the entire law enforcement community in the respective state. Table 8 lists the agencies we contacted in each of the 10 selected states.

Table 8: State and Local Agencies Contacted in 10 States

State	State agency	Local agency
Arizona	Assistant Attorney General, Attorney General's Office[a]	Special Assistant Law Enforcement Liaison, Maricopa County Attorney's Office Sergeant, Document Crimes Detail, Phoenix Police Department
California	Deputy Attorneys General (2), Special Crimes Unit, Attorney General's Office	Deputy District Attorney, High Technology Crimes Unit, Los Angeles County District Attorney's Office Detective Supervisor, Identity Theft & Credit Card Squad, Los Angeles Police Department, Principal Criminal Attorney, Sacramento County District Attorney's Office
Florida	Special Counsel, Office of Statewide Prosecution, Florida Department of Legal Affairs	Attorney, Dade County State Prosecutor's Office
Georgia	Assistant Attorney General, Attorney General's Office	Deputy District Attorney, Fulton County District Attorney's Office[a]
Illinois	Supervisor, Attorney General - Cook County State's Attorney's Office[b]	
Michigan	Assistant Attorney General, Chief of High Tech Crime Unit, Attorney General's Office	Deputy Prosecutor, Warrants & Investigations Unit, Oakland County Office of the Prosecuting Attorney
New Jersey	Deputy Attorney General, Attorney General's Office	Sergeant, Atlantic County Prosecutor's Office
Pennsylvania	Chief Deputy Attorney General, Attorney General's Office	Chief Deputy Attorney, Economic & Cyber Crime Unit, Philadelphia District Attorney's Office
Texas	Assistant Attorney General, Internet Bureau, Attorney General's Office	Assistant District Attorney, Dallas County District Attorney's Office
Wisconsin	Special Agent, Wisconsin Department of Justice	Deputy District Attorney, Dane County District Attorney's Office

[a]Did not respond to our inquiries.

[b]The Cook County State's Attorney's Office of the Illinois Attorney General's Office was able to provide both a state and local perspective on identity theft enforcement efforts.

Source: GAO summary.

Means Used to Promote Cooperation or Coordination among Federal, State, and Local Law Enforcement Agencies in Addressing Identity Theft

Our literature search and discussions with federal and state law enforcement officials indicated that three principal means are used to promote cooperation or coordination among all levels of law enforcement in addressing identity theft crimes—law enforcement task forces with multi-agency participation, the Attorney General's Identity Theft Subcommittee, and FTC's Consumer Sentinel Network and Identity Theft Data Clearinghouse database. We obtained examples of task forces established by federal (Secret Service) and state (California and Florida) leadership, respectively. The scope of our work did not include assessing the effectiveness of these task forces.

Regarding the Identity Theft Subcommittee, we interviewed the Chairman—a leadership role vested in the Fraud Section of the Department of Justice's Criminal Division—to obtain an overview of the subcommittee's role, membership, activities, and accomplishments. For the most part, in studying the subcommittee's role, we relied on testimonial rather than documentary evidence. According to the Chairman, there are no minutes of the subcommittee's monthly meetings because the subcommittee is not an "advisory" entity as defined in applicable sunshine laws. Also, the Chairman said that the subcommittee has not produced any annual reports of its activities.

To obtain a broader understanding of the subcommittee's role, as well as ways to potentially enhance that role, we contacted the designated individuals who, respectively, represented six member organizations—FBI, National District Attorneys Association, Postal Inspection Service, Secret Service, Sentencing Commission, and SSA/OIG. Various representatives offered suggestions for ways to potentially enhance the subcommittee's role. These suggestions do not necessarily reflect the consensus views of either the full subcommittee or the seven representatives we contacted.

Also, the structured data collection instrument that we distributed to law enforcement officials in the 10 selected states included a question about the role, usefulness, and effectiveness of the Identity Theft Subcommittee. As previously mentioned, given the limited distribution of the data collection instrument, the observations of the respondents cannot be viewed as being representative of the entire law enforcement community in the respective state.

Regarding the Consumer Sentinel Network and the Identity Theft Data Clearinghouse database, we interviewed responsible FTC staff and reviewed available documentation, including law enforcement usage

statistics for January 2001 through March 2002. We reviewed the list of federal, state, and local law enforcement agencies that, as of May 24, 2002, had entered into user agreements with FTC, pledging to abide by applicable confidentiality rules when using the Consumer Sentinel Network to access the Clearinghouse database.

Regarding usefulness of database information for law enforcement purposes, we asked the Identity Theft Subcommittee Chairman for examples (if any) of federal, state, or local success stories that had been presented or discussed at the subcommittee's monthly meetings. We discussed with FTC staff the extent to which Clearinghouse data have been centrally analyzed to generate investigative leads and referrals. Further, we inquired about FTC's plans for making the Clearinghouse database more useful for law enforcement purposes.

Also, the structured data collection instrument that we distributed to law enforcement officials in the 10 selected states included a question about the usefulness of the Consumer Sentinel Network and the Clearinghouse database. To reiterate, given the limited distribution of the data collection instrument, the observations of the respondents cannot be viewed as being representative of the entire law enforcement community in the respective state.

SSA/OIG Actions to Resolve SSN Misuse and Other Identity Theft-Related Allegations

To obtain information about actions taken to resolve SSN misuse and other identity theft-related allegations, we contacted officials from the various components of SSA/OIG, including officials from the Office of Investigations, the Office of Executive Operations, as well as the Counsel to the Inspector General. We focused primarily on allegations received during fiscal year 1999. However, to provide a trend perspective and more currency, an official from the SSA/OIG's Office of Executive Operations provided us annual allegation data for fiscal years 1998 through 2001.

To determine the criteria used to establish which allegations are selected for criminal investigation, we spoke with staff from the Office of Investigation's Allegation Management Division, which operates SSA/OIG's fraud hotline. Also, officials from SSA's Office of Executive Operations provided us statistical information detailing the number of criminal investigations that resulted from program fraud-related allegations and the number that resulted from SSN misuse allegations that did not involve SSA programs. Information was also provided on how many of these criminal investigations produced a criminal result, such as a fugitive felon being apprehended or an individual being convicted and sentenced.

Appendix II: Examples of Cases Prosecuted under the Federal Identity Theft Act

This appendix summarizes selected federal cases prosecuted under the Identity Theft and Assumption Deterrence Act of 1998. The relevant section of this legislation is codified at 18 U.S.C. § 1028(a)(7)("fraud and related activity in connection with identification documents and information"). The cases summarized in this appendix are not intended to be a comprehensive listing of all federal prosecutions under the 1998 federal statute. As mentioned in appendix I, we identified these cases by conducting a search of the LexisNexis database in February 2002. Our search was designed to retrieve only those identity theft cases that specifically mentioned the federal statute—that is, cases that cited 18 U.S.C. § 1028(a)(7).

The following summaries of five cases prosecuted in U.S. district courts illustrate that identity theft generally is not a stand-alone crime. Rather, identity theft typically is a component of one or more other white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or mail fraud.

Illinois, Northern District, Eastern Division

In early 2001, a defendant was charged in a six-count indictment with bank fraud (counts 1, 2, and 3), possession of a counterfeit check (count 4), interstate transportation of a counterfeit check (count 5), and use of another person's SSN with intent to commit a state felony (count 6). In May 2001, the defendant pleaded guilty to counts 1 and 6 pursuant to a written plea agreement, and the remaining counts were dismissed. The district court sentenced the defendant to concurrent 46-month prison terms for offense conduct under the Identity Theft Act, 18 U.S.C. § 1028(a)(7)—using another person's SSN with intent to commit a crime—and under 18 U.S.C. § 1344 (bank fraud). *U.S. v. Burks*, No. 01-3313, 2002 U.S. App. Lexis 2387 (7th Cir. Feb. 11, 2002).

Michigan, Western District, Southern Division

This was a consolidated case involving three separate actions, in which three plaintiffs each alleged liability against the defendant car dealership, whose salesman/employee committed criminal acts. Specifically, the salesman/employee wrongly obtained credit reports for the plaintiffs, without their consent, and then used the reports to secure financing for car sales or leases for applicants with bad credit histories. The salesman/employee was convicted on a federal fraud criminal charge under 18 U.S.C. § 1028(a)(7). Also, the plaintiffs established liability against the dealership for intentional violation of the Fair Credit Reporting Act. *Benjamin Adams v. Berger Chevrolet, Inc.*, No. 1:00-CV-225, 1:00-CV-226, and 1:00-CV-228, 2001 Dist. Lexis 6174 (W.D. Mich. May 7, 2001).

North Carolina, Eastern District

A defendant was charged with stealing mail from residential mailboxes, using information from personal checks to create counterfeit checks and fraudulent driver's licenses, and negotiating the counterfeit checks at numerous banks in North Carolina using the fraudulent licenses as identification. The defendant pled guilty to

- one count of using false identification documents, 18 U.S.C. § 1028(a)(7);
- five counts of producing false identification documents, 18 U.S.C. § 1028(a)(1); and
- three counts of possession of stolen mail, 18 U.S.C. § 1708.

The defendant was sentenced to a term of 63 months of imprisonment. *U.S. v. Hooks*, No. 99-4754, 2000 U.S. App. Lexis 2388 (4th Cir. Sept. 14, 2000).

Ohio, Southern District

In May 2000, following a bench trial, the district court found a defendant guilty of the following violations

- using the identification of another with intent to commit unlawful activity, 18 U.S.C. § 1028(a)(7);
- possessing false identification with intent to defraud the United States, 18 U.S.C. § 1028(a)(4);
- furnishing false information to the Commissioner of Social Security, 42 U.S.C. § 408(a)(6);
- fraud and misuse of an entry document, 18 U.S.C. § 1546, and
- making a false statement to an agency of the United States, 18 U.S.C. § 1001.

The court sentenced the defendant to 6 months of imprisonment, plus 3 years of supervised release. *U.S. v. Balde*, No. 00-4070, 2001 U.S. App. Lexis 23741 (6th Cir. Oct. 26, 2001).

Wisconsin, Eastern District

A defendant pleaded guilty to using another person's SSN to commit fraud, 18 U.S.C. § 1028(a)(7); using unauthorized credit cards, 18 U.S.C. § 1029(a)(2); and issuing a false SSN, 42 U.S.C. § 408(a)(7)(B).

The defendant was sentenced to 36 months of imprisonment. *U.S. v. Lippold*, No. 00-2868, 2001 U.S. App. Lexis 15126 (7th Cir. July 2, 2001).

Appendix III: Identity Theft Subcommittee Membership

This appendix presents a membership overview (see table 9) of the Identity Theft Subcommittee, which was established by the U.S. Attorney General's White Collar Crime Council in 1999, following passage of the Identity Theft and Assumption Deterrence Act of 1998.

Table 9: List of Federal Agencies and National Organizations Represented on the Identity Theft Subcommittee

Participating agencies and organizations
Federal agencies
Department of Justice:
Executive Office for United States Attorneys
Federal Bureau of Investigation
Fraud Section Criminal Division[a]
Immigration and Naturalization Service
Office of Consumer Litigation
Office of Policy and Legislation, Criminal Division
Tax Division
U.S. Trustees Program
Department of State:
Bureau of Diplomatic Security
Department of the Treasury:
Internal Revenue Service
Office of Enforcement
Treasury Inspector General for Tax Administration
Secret Service
Federal Trade Commission
Postal Inspection Service
Sentencing Commission
Social Security Administration, Office of the Inspector General
Regulatory agencies:
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency
National organizations:
International Association of Chiefs of Police
National Association of Attorneys General
National District Attorneys Association

[a]A Deputy Chief of the Fraud Section serves as chair of the subcommittee.

Source: U.S. Department of Justice, Criminal Division.

As table 9 indicates, in addition to federal law enforcement and regulatory agencies, subcommittee membership has state and local representation through three national organizations:

- **International Association of Chiefs of Police**. The association's goals, among others, are to advance the science and art of police services; develop and disseminate improved administrative, technical, and operational practices and promote their use in police work; and foster cooperation and exchange of information and experience among police administrators.

- **National Association of Attorneys General**. A goal of the association—whose membership includes the attorneys general and chief legal officers of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and associated territories—is to promote cooperation and coordination on interstate legal matters in order to foster a responsive and efficient legal system for state citizens.

- **National District Attorneys Association**. A purpose of the association is to promote the continuing education of prosecuting attorneys by various means, such as arranging seminars and fostering periodic conventions or meetings for the discussion and solution of legal problems affecting the public interest in the administration of justice. Among other sources, training is offered at the National Advocacy Center—located on the campus of the University of South Carolina in Columbia—which is a joint venture of the association and the U.S. Department of Justice.

Appendix IV: Law Enforcement Agencies with Access to Identity Theft Data Clearinghouse Via Consumer Sentinel

In response to a provision in the Identity Theft and Assumption Deterrence Act of 1998, FTC established the Identity Theft Data Clearinghouse in November 1999 to gather information from any consumer who wishes to file a complaint or pose an inquiry concerning identity theft. Federal, state, and local law enforcement agencies may access the Clearinghouse database via a secure link in FTC's Consumer Sentinel Network.

The Consumer Sentinel Web site was initially established in 1997 to track telemarketing or mass-market fraud complaints received by FTC. With the passage of the Identity Theft Act, FTC added a link in the Consumer Sentinel to allow law enforcement agencies access to the Identity Theft Data Clearinghouse database. In order to gain access to the secure Web site, agencies must sign a confidentiality agreement. Only domestic law enforcement agencies are permitted to have access to the detailed information in the Clearinghouse database. Other domestic government agencies, consumer reporting agencies, and private entities are permitted limited access to overall or aggregate information. Also, at *www.consumer.gov/sentinel*, the general public can view macro-level information (e.g., overall statistics by states or cities) that FTC maintains on general fraud and identity theft matters.

As of May 24, 2002, a total of 352 law enforcement agencies (46 federal and 306 state and local) had entered into agreements with FTC to have access to the Identity Theft Data Clearinghouse via the secure link in the Consumer Sentinel. The following is a list of the 352 agencies.

Federal Agencies: 46

Air Force Judge Advocate General
Army Legal Assistance
Army Judge Advocate General
Coast Guard
Commodity Futures Trading Commission
Consumer Product Safety Commission
Customs Service
Department of Defense Criminal Investigative Service
Department of Justice, Consumer Litigation, Civil Division
Department of Justice, Fraud Section, Criminal Division
Federal Bureau of Investigation
Federal Deposit Insurance Corporation, Inspector General
Federal Trade Commission
Food and Drug Administration

General Services Administration, Inspector General
Internal Revenue Service, Criminal Investigations
Marine Corps, Office of Legal Assistance
Navy Judge Advocate General
Nuclear Regulatory Commission, Inspector General
Postal Inspection Service
Probation Office, District of Massachusetts
Secret Service
Small Business Administration, Inspector General
Social Security Administration Inspector General
State Department, Bureau of Diplomatic Security,
    Criminal Investigations Division
Treasury IG for Tax Administration
U.S. Attorney Offices
    California, Eastern District
    California, Southern District
    Colorado
    Florida, Northern District
    Iowa, Southern District
    Louisiana, Middle District
    Minnesota
    Missouri, Western District
    New Hampshire
    New York, Eastern District
    New York, Southern District
    New York, Western District
    North Carolina, Eastern District
    Oregon
    Pennsylvania, Eastern District
    Pennsylvania, Western District
    Washington D.C.
    Washington, Eastern District
    West Virginia, Southern District
U.S. Trustees, Executive Office

State and Local Agencies: 306

Alabama: 3

Attorney General
Homewood Police Department
Mountain Brook Police Department

Alaska: 3

Division of Banking, Securities, and Corporations
State Troopers
Division of Insurance

Arizona: 2

Attorney General
Corporation Commission

Arkansas: 2

Conway Arkansas Police Department
Insurance Fraud Investigation Division

California: 45

Attorney General
Arcadia Police Department
Anaheim Police Department
Bakersfield Police Department
Beverly Hills Police Department
Chino Police Department
Claremont Police Department
Clayton Police Department
Coronado Police Department
Davis Police Department
Department of Corporations
Fresno Police Department
Glendora Police Department
Huntington Beach Police Department
La Mesa Police Department
Los Angeles City Attorney
Los Angeles County District Attorney

Los Angeles County Sheriff
Marin County District Attorney, Consumer Protection Unit
Merced County District Attorney's Office
Monterey County District Attorney
Morro Bay Police Department
Napa County District Attorney
Napa Sheriff's Office
Novato Police Department
Orange County District Attorney
Orange County Sheriff
Palo Alto Police Department
Placer County Sheriff's Department
Pomona Police Department
Riverside County District Attorney
Roseville Police Department
Sacramento County District Attorney's Office
Sacramento County Sheriff
San Bernardino County District Attorney
San Carlos Police Department
Santa Cruz Sheriff Office
San Diego District Attorney
San Diego Police Department
San Francisco Police Department
San Luis Obispo County District Attorney
Santa Barbara County District Attorney
Signal Hill Police Department
Solano County District Attorney
Ventura County District Attorney

Colorado: 7

Attorney General
Bureau of Investigation
District Attorney 4th Judicial District
District Attorney 8th Judicial District
Douglas County Sheriff
Jefferson County Sheriff
Pueblo County District Attorney

Connecticut: 5

Attorney General
Department of Banking
Department of Consumer Protection
Naugatuck Police Department
New Britain Police Department

Delaware: 1

New Castle Police Department

District of Columbia: 2

Corporation Counsel
Department of Insurance and Securities

Florida: 17

Attorney General
Altamonte Springs Police Department
City of Panokee Police Department
Comptroller Department of Banking and Finance
Coral Gables Police Department
Davie Police Department
Daytona Beach Police Department
Department of Law Enforcement
Fort Lauderdale Police Department
Miami-Dade Police Department, High-Tech Crime Squad
Office of Statewide Prosecution
Office of the State Attorney, 10th Judicial Circuit
Office of the State Attorney, 13th Judicial Circuit
Orange County Consumer Fraud Unit
Palm Beach County Sheriff
Panama City Police Department
Stuart Police Department

Georgia: 5

Attorney General
Bureau of Investigation
College Park Police Department

DeKalb County Solicitor General
Governor's Office of Consumer Affairs

Hawaii: 1

Office of Consumer Protection

Idaho: 1

Attorney General

Illinois: 10

Attorney General
Bloomington Police Department
Cook County State's Attorney's Office
Flossmoor Police Department
Minier Police Department
Ogle County State's Attorney's Office
Orlando Park Police Department
Schaumburg Police Department
Securities Department
Will County State's Attorney

Indiana: 8

Attorney General
Bartholomew County Sheriff
Brown County Sheriff
Fishers Police Department
Fountain City Prosecuting Attorney
Indianapolis Police Department
Martin County Sheriff
Tipton Police Department

Iowa: 5

Le Mars Police Department
Manson Police Department
Marshalltown Police Department
Newton Police Department
Polk County Attorney's Office

Kansas: 2

Johnson County District Attorney
Securities Commissioner

Kentucky: 4

Attorney General
Berea Police Department
Bowling Green Police Department
Public Service Commission

Louisiana: 4

Department of Justice
State Police
Lafayette Parish Sheriff's Office
Union Parish Sheriff

Maryland: 9

Attorney General
Baltimore City Police Department
Baltimore County Police Department
Hartford County State's Attorney's Office
Howard County Consumer Affairs
Hyattsville Police Department
Montgomery County Consumer Affairs
Montgomery County States Attorney
Talbot County Sheriff

Massachusetts: 2

Attorney General
Boston Police Department Intelligence Unit

Michigan: 9

Attorney General
Burton Police Department
Genesee County Sheriffs Department
Houghton City Police Department
Houghton County Sheriff

Lansing Police Department
Livingston County Sheriff's Office
Meridan Township Police Department
South Lyon Police Department

Minnesota: 8

Attorney General
Department of Commerce
State Patrol
Brooklyn Center Police Department
Edina Police Department
Maplewood Police Department
Oak Park Heights Police Department
Ramesy County Attorney's Office

Missouri: 7

Attorney General
Manchester Police Department
Secretary of State, Securities Division
St. Charles Police Department
St. Francois County Sheriff
St. Peters Police Department
Taney County Sheriff

Montana: 3

Attorney General
State Auditor
Department of Administration, Office of Consumer Protection

Nebraska: 2

Attorney General
Department of Banking and Finance

Nevada: 3

Attorney General
Elko Police Department
Secretary of State

New Hampshire: 1

Attorney General

New Jersey: 12

Attorney General
Cape May County Prosecutor
Clifton Township Police Department
Dover Turnpike Police Department
Jefferson Township Police
Marlboro Township Police Department
Maywood Police Department
Middlesex County Prosecutor
Moorestown Township Police Department
Piscataway Township Police Department
Somerset County Department of Consumer Affairs
Union County Prosecutor

New Mexico: 1

Securities Division

New York: 8

Attorney General
Cheektowaga Police Department
Clinton County District Attorney
Lancaster Village Police Department
Nassau County District Attorney
Rockland County Sheriff
Rouses Point Police Department
State Police

North Carolina: 11

Chowan County Sheriff's Office
Department of Justice
Gaston County Police Department
Hickory Police Department
Nash County Sheriff Office
Mooresville Police Department
Mt. Gilead Police Department
Raleigh Police Department
Pinehurst Police Department
Union County Sheriff's Office
Winston-Salem Police Department

Ohio: 10

Attorney General
Beachwood Police Department
Brunswick Police Department
Cheviot Police Department
Clayton Police Department
Division of Securities
Findlay Police Department
Mentor-on-the-Lake Police Department
Wickliffe Police Department
Willoughby Police Department

Oklahoma: 3

Attorney General
Purcell Police Department
Portland Police Bureau

Oregon: 2

Douglas County Sheriff Office
Medford Police Department

Pennsylvania: 10

Attorney General
Allegheny County Police Department
Duryea Police Department
Easttown Township Police Department
Lower Allen Township Police Department
Lower Makefield Township Police Department
Philadelphia Police Department
West Whiteland Township Police Department
Wyomissing Police Department
York Police Department

Rhode Island: 3

Attorney General
Securities Division
State Police

South Carolina: 5

Charleston Police Department
City of North Charleston Police Department
Myrtle Beach Police Department
Real Estate Commission
Secretary of State

South Dakota: 2

Attorney General
South Dakota Securities Commission

Tennessee: 11

Bartlett Police Department
Bristol Police Department
Franklin Police Department
La Vergne Police Department
Marshall County Sheriff's Office
Millington Police Department
Munford Police Department

Regulatory Authority
Rutherford County Sheriff's Office
Smyrna Police Department
Tipton County Sheriff's Office

Texas: 17

Attorney General
Allen Police Department
Coppell Police Department
Copperas Cove Police Department
Dallas County District Attorney's Office
Dallas Police Department
Department of Public Safety
Department of Insurance
Fort Bend County Sheriff Office
Garland Police Department
Grapevine Police Department
Missouri City Police Department
North Richland Hills Police Department
Richardson Police Department
San Antonio Police Department
Travis County District Attorney
Wichita Falls Police Department

Utah: 5

Attorney General
Cedar City Police Department
Department of Commerce, Consumer Protection Division
Midvale City Police Department
Utah County Attorney's Office

Vermont: 4

Attorney General
Caledonia County Sheriff's Department
Essex Police Department
Rutland County Sheriff

Virginia: 10

Attorney General
Alexandria Police Department
Arlington County Police Department
Fairfax City Dept. of Telecom and Consumer Services
Fredricksburg Police Department
Lynchburg Police Department
State Police
Virginia Beach Commonwealth Attorney
Virginia Beach Police Department
William and Mary Police Department

Washington: 7

Attorney General
Grays Harbor County Sheriff
Lynnwood Police Department
Mount Vernon Police Department
Poulsbo Police Department
Securities Division
Tumwater Police Department

Wisconsin: 10

Attorney General, Department of Justice
Department of Financial Institutions
Department of Agriculture, Trade, and Consumer Protection
Greenfield Police Department
Monona Police Department
Monroe Police Department
New Berlin Police Department
River Falls Police Department
University of Wisconsin- Madison Police Department
Waukesha County Sheriff

Wyoming: 2

Attorney General
District Attorney 1st District

Appendix V: Military-Related Identity Theft Cases and Plans for Soldier Sentinel System

This appendix (1) gives examples of identity theft cases that have a military connection, for example, cases that affect uniformed personnel and (2) discusses plans for establishing Soldier Sentinel, an online system designed specifically to collect consumer and identity theft complaint information from members of the armed forces and their families.

Examples of Military-Related Identity Theft Cases

Due to various factors, members of the armed services may be more susceptible than the general public to identity theft. For instance, given their mobility, service members may have bank, credit, and other accounts in more than one state and even overseas. At times, service members may be deployed to locations far away from family members, which can increase dependence on credit cards, automatic teller machines, and other remote-access financial services. For these same reasons, while any victim of identity theft can face considerable problems, the rigors of military life can compound problems encountered by uniformed personnel and family members who are victimized.

We found no comprehensive or centralized data on the number of military-related identity theft cases. For instance, in response to our inquiry, an official with the Defense Criminal Investigative Service[1] told us the agency's case information system cannot specifically isolate and quantify the number of identity theft cases. However, in conducting a literature search, we found various examples of military-related identity theft cases, including the following:

- One case involved over 100 victims, each a high-ranking military official. In this case, according to multi-agency task force results reported by the Social Security Administration's Office of the Inspector General (SSA/OIG) for fiscal year 2000, two perpetrators used the Internet to obtain the names and SSNs of the military officials. Then, the perpetrators used the personal information to fraudulently obtain credit cards. According to the SSA/OIG, the case culminated with the perpetrators being incarcerated and ordered to pay restitution of over $287,000 to the companies that were victimized by the scheme.

- Another case, reported in January 2002 by the Army News Service, involved a perpetrator who was caught trying to cash a $9,000 check drawn on the bank account of a Navy retiree. During the subsequent

[1]The Defense Criminal Investigative Service is the investigative arm of the Department of Defense's Office of the Inspector General.

investigation, the perpetrator's laptop computer was found to contain several thousand military names, SSNs, and other information. The common link among the military veterans on the list was that, in accordance with a once-common practice, they all had filed their military discharge form (Department of Defense Form 214) with their local county courthouse in order to ensure always being able to have a certified copy available to receive Veterans Administration benefits. The Form 214 contains an individual's SSN and birth date, and the document becomes a public record after being filed; some courthouses have even put this information online. Now, according to the news story, the military's transition counselors are advising soldiers to not file discharge forms with county courthouses but rather to safeguard any documents that have personal identification information.

- In a recent (April 17, 2002), press release, the Defense Criminal Investigative Service announced the arrest of a suspect for alleged violations involving one count of identity theft and one count of using a false SSN. Between November 1999 and October 2001, the suspect allegedly assumed the SSN of four different persons. The suspect represented himself as a major with the U.S. Army and conducted fraudulent schemes to obtain a 2001 Nissan truck, a 2002 Mercedes Benz, and a 2002 Jaguar. In addition to the Defense Criminal Investigative Service, two other federal law enforcement agencies (the FBI and the SSA/OIG) and one local agency (St. Tammany Parish Sheriff's Office, Louisiana) participated in the investigation. Prosecution of the case is to be handled by the U.S. Attorney's Office, Eastern District of Louisiana.

Plans to Establish the Soldier Sentinel System

In January 2001, FTC and the Department of Defense announced the signing of a memorandum of understanding to create an online system (Soldier Sentinel) designed specifically to collect consumer and identity theft complaints from the members of the armed forces and their families. Among other purposes, the system is to provide the military community a convenient way to file complaints directly with law enforcement officials. Also, the Department of Defense and its component services are to use the data collected to shape consumer education and protection policies at all levels within the military.

Plans call for Soldier Sentinel to mirror the FTC's Consumer Sentinel system, which provides secure, password-protected access to a consumer complaint database and other tools designed to allow law enforcement to share data about fraud. Also, the Soldier Sentinel agreement allows the Department of Defense and the component services to collect, share, and analyze specific service-related information.

In April 2002, FTC staff told us that the Soldier Sentinel was not yet operational but was anticipated to be online during the summer of 2002.

Appendix VI: Comments from the Department of Justice

U.S. Department of Justice

Washington, D.C. 20530

JUN 19 2002

Mr. Richard M. Stana
Director, Justice Issues
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Stana:

On June 5, 2002, the General Accounting Office (GAO) provided the Department of Justice copies of its draft report entitled "IDENTITY THEFT: Greater Awareness and Use of Existing Data Are Needed" and requested its comments on the substance of the report. The Department generally agrees with the substance of the GAO draft report and its recommendation to promote greater use of available information sources to combat identity theft. We are providing additional information concerning our efforts to address this issue.

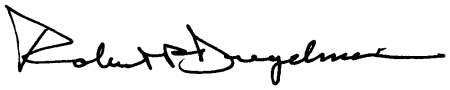
In its draft report, the GAO recommends "that the Attorney General have the Identity Theft Subcommittee promote greater awareness and use of the Consumer Sentinel Network and the Clearinghouse database by all levels of law enforcement – federal, state and local." The Department agrees that the Subcommittee should continue its efforts to facilitate the dissemination of information about Consumer Sentinel and the database to all levels of law enforcement. On an ongoing basis, the Subcommittee is continuing to do so through training programs for federal prosecutors at the National Advocacy Center, information bulletins on the Department of Justice's intranet, and regular meetings of other interagency working groups that the Department chairs. The Subcommittee also will consult with state and local law enforcement representatives on the Subcommittee to identify additional mechanisms for informing police departments and sheriffs' offices about Consumer Sentinel. In addition, the Federal Trade Commission (FTC), the U.S. Secret Service, and the Department have already been conducting a series of regional training conferences on identity theft this year in five locations around the country, and are exploring the idea of conducting an expanded series of regional training seminars on identity theft in calendar year 2003.

In this regard, the Department also notes that in the regional training seminars cosponsored with the FTC and the Secret Service, it has included specific training about Consumer Sentinel and the identity theft database and has advocated that law enforcement agencies make full use of existing multiagency task forces that address identity theft. While many smaller police departments and sheriff's offices may not have their own computers to maintain Internet access to Consumer Sentinel, their participation in these multiagency task forces can enable them to make use of Consumer Sentinel and the identity theft database in identity theft investigations.

Further, as part of its efforts to inform the public about identity theft and ensure that courts are meting out appropriate criminal sanctions for offenses involving identity theft, the Department recently has taken two significant steps. First, on May 2, 2002, Attorney General Ashcroft announced a nationwide "sweep" of federal identity theft prosecutions. In that sweep, 73 criminal prosecutions were brought against 135 individuals in 24 districts, including 25 new prosecutions in the 24 hours preceding the announcement. Further details are set forth in the prepared remarks of the Attorney General at http://www.usdoj.gov/ag/speeches/2002/050202agidtheftranscript.htm. Second, also on May 2, 2002, the Attorney General announced that the Department would seek legislation to increase criminal sentences in identity theft-related federal cases, including a new provision for aggravated identity theft and expansion of the existing provisions of 18 U.S.C. § 1028(a)(7). On May 22, 2002, Senator Feinstein introduced this proposal as S. 2541.

We believe that these efforts will address the GAO recommendation. If you should have any questions concerning the Department's comments you may contact Vickie L. Sloan, Director, Audit Liaison Office, Justice Management Division on 202-514-0469.

Sincerely,



Robert F. Diegelman
Acting Assistant Attorney General
for Administration

Appendix VII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Richard M. Stana, (202) 512-8777
Danny R. Burton (214) 777-5600

Staff Acknowledgments

In addition to the above, David P. Alexander, Shirley A. Jones, Jan B. Montgomery, Tim Outlaw, Robert J. Rivas, and Richard M. Swayze made key contributions to this report.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548