United States General Accounting Office

GAO

Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EST
Thursday, February 14, 2002

IDENTITY THEFT

Available Data Indicate Growth in Prevalence and Cost

Statement of Richard M. Stana, Director, Justice Issues

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
00FEB2002	N/A	-

Title and Subtitle IDENTITY THEFT Available Data Indicate Growth in Prevalence and Cost	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) U.S. General Accounting Office P.O. Box 37050 Washington, D.C. 20013	**Performing Organization Report Number** GAO-02-424t
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
I am pleased to be here today to discuss the preliminary results of our ongoing studyrequested by the Subcommittee and Senator Charles Grassleyto develop information on the extent or prevalence of identity theft and its cost to the financial services industry, victims, and the federal criminal justice system. Generally, identity theft involves stealing another persons personal identifying informationsuch as Social Security number (SSN), date of birth, and mothers maiden nameand then using the information to fraudulently establish credit, run up debt, or to take over existing financial accounts. Although not specifically or comprehensively quantifiable, the prevalence and cost of identity theft seem to be increasing, according to the available data we reviewed and many officials of the public and private sector entities we contacted. Given such indications, most observers agree that identity theft certainly warrants continued attention, encompassing law enforcement as well as prevention efforts. Various recently introduced bills, including S. 1055 (Privacy Act of 2001), have provisions designed to enhance such efforts. While the scope of our work did not include an evaluation of S. 1055, we did compile information that could be useful in discussing related issues, and my testimony today will offer perspectives on several identity theft-related provisions of the bill.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR
Number of Pages 14	

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to discuss the preliminary results of our ongoing study—requested by the Subcommittee and Senator Charles Grassley—to develop information on the extent or prevalence of identity theft and its cost to the financial services industry, victims, and the federal criminal justice system. Generally, identity theft 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 to take over existing financial accounts. Although not specifically or comprehensively quantifiable, the prevalence and cost of identity theft seem to be increasing, according to the available data we reviewed and many officials of the public and private sector entities we contacted. Given such indications, most observers agree that identity theft certainly warrants continued attention, encompassing law enforcement as well as prevention efforts. Various recently introduced bills, including S. 1055 (Privacy Act of 2001), have provisions designed to enhance such efforts. While the scope of our work did not include an evaluation of S. 1055, we did compile information that could be useful in discussing related issues, and my testimony today will offer perspectives on several identity theft-related provisions of the bill.

To obtain the most recent statistics on the incidence and societal cost of identity theft, we interviewed responsible officials and reviewed documentation obtained from the Department of Justice and its components, including the Executive Office for U.S. Attorneys (EOUSA) and the Federal Bureau of Investigation (FBI); the Department of the Treasury and its components, including the Secret Service and the Internal Revenue Service (IRS); the Social Security Administration's (SSA) Office of the Inspector General (OIG); the Postal Inspection Service; and the Federal Trade Commission (FTC). Also, we contacted representatives of the three national consumer reporting agencies (commonly referred to as "credit bureaus") and two payment card associations (MasterCard and Visa). Further, at our request and with the consent of the victims, FTC provided us with the names and telephone numbers of 10 victims to interview. According to FTC staff, the sample of 10 victims was selected to illustrate a range in the extent and variety of the identity theft activities reported by victims. The experiences of these 10 victims are not statistically representative of all victims.

Background

Since our earlier report in May 1998[1], various actions—particularly passage of federal and state statutes—have been taken to address identify theft. Later that year, Congress passed the Identity Theft and Assumption Deterrence Act of 19098 (the "Identity Theft Act").[2] Enacted in October 1998, the federal statute made identify 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. Under U.S. Sentencing Commission guidelines—even if (1) there is no monetary loss and (2) the perpetrator has no prior criminal convictions—a sentence of from 10 to 16 months incarceration can be imposed. Regarding state statutes, at the time of our 1998 report, very few states had specific laws to address identity theft. Now, less than 4 years later, a large majority of states have enacted identify theft statues.

Prevalence of Identity Theft

As we reported in 1998, there are no comprehensive statistics on the prevalence of identity theft or identity fraud. Similarly, during our current review, various officials noted that precise, statistical measurement of identity theft trends is difficult for number of reasons. Generally, federal law enforcement agencies do not have information systems that specifically track identity theft cases. For example, while the amendments of 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 because docketing staff are asked to record cases under only the U.S. Code section, not the subsection or the sub-subsection. Also, the FBI and the Secret Service said that identity theft is not typically a stand-alone crime; rather, it is almost always a component of one or more white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments.

Nonetheless, a number of data sources can be used as proxies for gauging the prevalence of identity theft. These sources can include consumer complaints and hotline allegations, as well as law enforcement

[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).

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

investigations and prosecutions of identity theft-related crimes such as bank fraud and credit card fraud. Each of these various sources or measures seems to indicate that the prevalence of identity theft is growing.

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

According to the consumer reporting agency officials that we talked with, the most reliable indicator of the incidence of identity theft is the number of 7-year fraud alerts placed on consumer credit files. Generally, fraud alerts constitute a warning that someone may be using the consumer's personal information to fraudulently obtain credit. Thus, a purpose of the alert is to advise credit grantors to conduct additional identity verification or contact the consumer directly before granting credit. One of the three consumer reporting agencies that we contacted estimated that its 7-year fraud alerts involving identity theft increased 36 percent over 2 recent years—from about 65,600 in 1999 to 89,000 in 2000.[3] A second agency reported that its 7–year fraud alerts increased about 53 percent in recent comparative 12-month periods; that is, the number increased from 19,347 during one 12-month period (July 1999 through June 2000) to 29,593 during the more recent period (July 2000 through June 2001). The third agency reported about 92,000 fraud alerts for 2000 but was unable to provide information for any earlier year.[4]

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

The Identity Theft Act requires the FTC to "log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief" that one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired. In response to this requirement, in November 1999, FTC established the Identity Theft Data Clearinghouse (FTC Clearinghouse) to gather information from any consumer who wishes to file a complaint or pose an inquiry concerning

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

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

identity theft.[5] In November 1999, the first month of operation, the FTC Clearinghouse responded to an average of 445 calls per week. By March 2001, the average number of calls answered had increased to over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls.

At a congressional hearing in September 2000, an FTC official testified that Clearinghouse data demonstrate that identity theft is a "serious and growing problem."[6] More recently, during our review, FTC staff cautioned that the trend of increased calls to FTC perhaps could be attributed to a number of factors, including increased consumer awareness, and may not necessarily be attributed to an increase in the incidence of identity theft.

SSA/OIG: An Increasing Number of Fraud Hotline Allegations

SSA/OIG operates a fraud hotline to receive allegations of fraud, waste, and abuse. In recent years, SSA/OIG has reported a substantial increase in calls related to identity theft. For example, allegations involving SSN misuse increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001. However, the increased number of allegations may be due partly to additional fraud hotline staffing, which increased from 11 to over 50 personnel during this period. SSA/OIG officials attributed the trend in allegations partly to a greater incidence of identity theft. Also, irrespective of staffing levels, a review performed by SSA/OIG of a sample of 400 allegations of SSN misuse indicated that up to 81 percent of all allegations of SSN misuse related directly to identity theft.

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

Although federal law enforcement agencies do not have information systems that specifically track identity theft cases, the agencies provided us with case statistics for identity theft-related crimes. Regarding bank fraud, for instance, the FBI reported that its arrests increased from 579 in 1998 to 645 in 2000—and was even higher (691) in 1999. The Secret Service reported that, for recent years, it has redirected its identity theft-related efforts to focus on high-dollar, community-impact cases. Thus, even

[5] On November 1, 1999, FTC established a toll-free telephone hotline (1-877-ID-THEFT) for consumers to report identity theft. Information from complainants is accumulated in a central database (the Identity Theft Data Clearinghouse) for use as an aid in law enforcement and prevention of identity theft.

[6] FTC, prepared statement on "Identity Theft," hearing before the Committee on Banking and Financial Services, U.S. House of Representatives (Sept. 13, 2000).

though the total number of identity theft-related cases closed by the Secret Service decreased from 8,498 in fiscal year 1998 to 7,071 in 2000, the amount of fraud losses prevented in these cases increased from a reported average of $73,382 in 1998 to an average of $217,696 in 2000.[7] IRS reported on the extent of questionable refund schemes involving a "high frequency" of identity fraud, that is, cases very likely to have elements of identity fraud. Regarding such cases, for a 5-year period (calendar years 1996 to 2000), IRS reporting detecting fraudulent refund claims totaling $1.76 billion—and that 83 percent ($1.47 billion) of this total occurred in 1999 and 2000. The Postal Inspection Service, in its fiscal year 2000 annual report, noted that identity theft is a growing trend and that the agency's investigations of such crime had "increased by 67 percent since last year."

Cost of Identity Theft to the Financial Services Industry

We found no comprehensive estimates of the cost of identity theft to the financial services industry.[8] Some data on identity theft-related losses—such as direct fraud losses reported by the American Bankers Association (ABA) and payment card associations—indicated increasing costs. Other data, such as staffing of the fraud departments of banks and consumer reporting agencies, presented a mixed and, in some instances, incomplete picture. For example, one consumer reporting agency reported that staffing of its fraud department had doubled in recent years, whereas another agency reported relatively constant staffing levels. Furthermore, despite concerns about security and privacy, the use of e-commerce has grown steadily in recent years. Such growth may indicate greater consumer confidence but may also have resulted from an increase in the number of people who have access to Internet technology.

Regarding direct fraud losses, in its 2000 bank industry survey on check fraud, the ABA reported that total check fraud-related losses against commercial bank accounts —considering both actual losses ($679 million) and loss avoidance ($1.5 billion)—reached an estimated $2.2 billion in 1999, which was twice the amount in 1997.[9] Regarding actual losses, the

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

[8] Generally, regarding the financial services industry, the scope of our work focused primarily on obtaining information from banks, two payment card associations (MasterCard and Visa), and the three national consumer reporting agencies.

report noted that the 1999 figure ($679 million) was up almost 33 percent from the 1997 estimate ($512 million). However, not all check fraud-related losses were attributed to identity theft, which the ABA defined as account takeovers (or true name fraud). Rather, the ABA reported that, of the total check fraud-related losses in 1999, the percentages attributable to identity theft ranged from 56 percent for community banks (assets under $500 million) to 5 percent for superregional/money center banks (assets of $50 billion or more) and the average for all banks was 29 percent.

The two major payment card associations, MasterCard and Visa, use very similar (although not identical) definitions regarding which categories of fraud constitute identity theft. Generally, the associations consider identity theft to consist of two fraud categories—account takeovers and fraudulent applications.[10] On the basis of these two categories, the associations' aggregated identity theft-related losses from domestic (U.S. operations) rose from $79.9 million in 1996 to $114.3 million in 2000, an increase of about 43 percent. The associations' definitions of identity theft-related fraud are relatively narrow, in the view of law enforcement, which considers identity theft as encompassing virtually all categories of payment card fraud. Under this broader definition, the associations' total fraud losses from domestic operations rose from about $760 million in 1996 to about $1.1 billion in 2000, an increase of about 45 percent. However, according to the associations, the annual total fraud losses represented about 1/10th of 1 percent or less of U.S. member banks' annual sales volume during 1996 through 2000.

Regarding staffing and cost of fraud departments, in its 2000 bank industry survey on check fraud, the ABA reported that the amount of resources that banks devoted to check fraud prevention, detection, investigation, and prosecution varied according to bank size. For check fraud-related operating expenses (not including actual losses) in 1999, the ABA reported that over two-thirds of the 446 community banks that responded to the survey each spent less than $10,000, and about one-fourth of the 11 responding superregional/money center banks each spent $10 million or more for such expenses.

[9] ABA, *Deposit Account Fraud Survey Report 2000*. The ABA defined "loss avoidance" as the amount of losses avoided as a result of the banks' prevention systems and procedures. Because the overall response rate by banks to the survey was only 11 percent, the ABA's data should be interpreted with caution.

[10] Other fraud categories that the associations do not consider to be identity-theft related include, for example, lost and stolen cards, never-received cards, counterfeit cards, and mail order/telephone order fraud.

One national consumer reporting agency told us that staffing of its Fraud Victim Assistance Department doubled in recent years, increasing from 50 individuals in 1997 to 103 in 2001. The total cost of the department was reported to be $4.3 million for 2000. Although not as specific, a second agency reported that the cost of its fraud assistance staffing was "several million dollars." And, the third consumer reporting agency said that the number of fraud operators in its Consumer Services Center had increased in the 1990s but has remained relatively constant at about 30 to 50 individuals since 1997.

Regarding consumer confidence in online commerce, despite concerns about security and privacy, the use of e-commerce by consumers has steadily grown. For example, in the 2000 holiday season, consumers spent an estimated $10.8 billion online, which represented more than a 50 percent increase over the $7 billion spent during the 1999 holiday season. Further, in 1995, only one bank had a Web site capable of processing financial transactions; but, by 2000, a total of 1,850 banks and thrifts had Web sites capable of processing financial transactions.[11]The growth in e-commerce could indicate greater consumer confidence but could also result from the increasing number of people who have access to and are becoming familiar with Internet technology. According to an October 2000 Department of Commerce report, Internet users comprised about 44 percent (approximately 116 million people) of the U.S. population in August 2000. This was an increase of about 38 percent from 20 months prior.[12] According to Commerce's report, the fastest growing online activity among Internet users was online shopping and bill payment, which grew at a rate of 52 percent in 20 months.

Cost of Identity Theft to Victims

Identity theft can cause substantial harm to the lives of individual citizens—potentially severe emotional or other nonmonetary harm, as well as economic harm. Even though financial institutions may not hold victims liable for fraudulent debts, victims nonetheless often feel "personally violated" and have reported spending significant amounts of time trying to resolve the problems caused by identity theft—problems such as bounced

[11] Federal Deposit Insurance Corporation, *Evolving Financial Products, Services, and Delivery Systems* (Washington, D.C.: Feb. 14, 2001).

[12] Department of Commerce, *Falling Through the Net: Toward Digital Inclusion* (Oct. 2000). This report was the fourth in a series of studies issued by Commerce on the technological growth of U.S. households and individuals.

checks, loan denials, credit card application rejections, and debt collection harassment.

For the 23-month period from its establishment in November 1999 through September 2001, the FTC Identity Theft Data Clearinghouse received 94,100 complaints from victims, including 16,781 identity theft complaints contributed by SSA/OIG. The leading types of nonmonetary harm cited by consumers were "denied credit or other financial services (mentioned in over 7,000 complaints) and "time lost to resolve problems" (mentioned in about 3,500 complaints). Also, in nearly 1,300 complaints, identity theft victims alleged that they had been subjected to "criminal investigation, arrest, or conviction." Regarding monetary harm, FTC Clearinghouse data for the 23-month period indicated that 2,633 victims reported dollar amounts as having been lost or paid as out-of-pocket expenses as a result of identity theft. Of these 2,633 complaints, 207 each alleged losses above $5,000; another 203 each alleged losses above $10,000.

From its database of identity theft victims, after obtaining the individuals' consent, FTC provided us with the names and telephone numbers of 10 victims. We contacted the victims to obtain an understanding of their experiences. In addition to the types of harm mentioned above, several of the victims expressed to us feelings of "invaded privacy" and "continuing trauma." In particular, such "lack of closure" was cited when elements of the crime involved more than one jurisdiction and/or if the victim had no awareness of any arrest being made. Some victims told us of filing police reports in their home state but not being able to do so in the states where the perpetrators committed fraudulent activities using the stolen identities. Only 2 of the 10 victims told us they were aware that the perpetrator had been arrested.

In a May 2000 report, two nonprofit advocacy entities—the California Public Interest Research Group (CALPIRG) and the Privacy Rights Clearinghouse—presented findings based on a survey (conducted in spring 2000) of 66 identity theft victims who had contacted these organizations.[13] According to the report, the victims spent 175 hours, on average, actively trying to resolve their identity theft-related problems. Also, not counting legal fees, most victims estimated spending $100 for out-of-pocket costs. The May 2000 report stated that these finding may not

[13] CALPIRG (Sacramento, CA) and Privacy Rights Clearinghouse (San Diego, CA), "Nowhere to Turn: Victims Speak Out on Identity Theft" (May 2000).

be representative of the plight of all victims. Rather, the report noted that the findings should be viewed as "preliminary and representative only of those victims who have contacted our organizations for further assistance (other victims may have had simpler cases resolved with only a few calls and felt no need to make further inquiries)."

Later, at a national conference, the Director of Privacy Rights Clearinghouse expanded on the results of the May 2000 report. For instance, regarding the 66 victims surveyed, the Director noted that one in six (about 15 percent) said that they had been the subject of a criminal record because of the actions of an imposter.[14] .Further, the Director provided additional comments substantially as follows:

- Unlike checking for credit report inaccuracies, there is no easy way for consumers to determine if they have become the subject of a criminal record.
- Indeed, victims of identity theft may not discover that they have been burdened with a criminal record until, for example, they are stopped for a traffic violation and are then arrested because the officer's checking of the driver's license number indicated that an arrest warrant was outstanding.

Federal Criminal Justice System Costs

Regarding identify theft and any other type of crime, the federal criminal justice system incurs costs associated with investigations, prosecutions, incarceration, and community supervision.[15] Generally, we found that federal agencies do not separately maintain statistics on the person hours, portions of salary, or other distinct costs that are specifically attributable to cases involving identity theft. As an alternative, some of the agencies provided us with average cost estimates based, for example, on work year counts for white-collar crime cases—a category that covers financial crimes, including identity theft.

[14] Beth Givens, Director, Privacy Rights Clearinghouse, "Identity Theft: The Growing Problem of Wrongful Criminal Records," paper presented at the SEARCH National Conference on Privacy, Technology and Criminal Justice Information (Washington, D.C.: June 2000).

[15] As agreed with the requesters, our study focused on the costs of identity theft to the federal government only and no to state or local government entities; although, since 1998, most states have enacted laws that criminalize identity.

In response to our request, the FBI estimated that the average cost to investigate white-collar crimes handled by the agency's white-collar crime program was approximately $20,000 during fiscal years 1998 to 2000, based on budget and workload data for the 3 years. However, an FBI official cautioned that the average cost figure has no practical significance because it does not capture the wide variance in the scope and costs of white-collar crime investigations. Also, the official cautioned that—while identity theft is frequently an element of bank fraud, wire fraud, and other types of white-collar or financial crimes—some cases (including some high-cost cases) do not involve elements of identity theft.

Similarly, Secret Service officials—in responding to our request for an estimate of the average cost of investigating financial crimes that included identity theft as a component—said that cases vary so much in their makeup that to put a figure on average cost is not meaningful. SSA/OIG officials responded that the agency's information systems do not record time spent by function to permit making an accurate estimate of what it costs the OIG to investigate cases of SSN misuse.

Regarding prosecutions, in fiscal year 2000, federal prosecutors handled approximately 13,700 white-collar crime cases, at an estimated average cost of about $11,400 per case, according to EOUSA. The total cases included those that were closed in the year, those that were opened in the year, and those that were still pending at yearend. EOUSA noted that the $11,400 figure was an estimate and that the actual cost could be higher or lower.

According to Bureau of Prisons (BOP) officials, federal offenders convicted of white-collar crimes generally are incarcerated in minimum-security facilities. For fiscal year 2000, the officials said that the cost of operating such facilities averaged about $17,400 per inmate.

After being released from BOP custody, offenders are typically supervised in the community by federal probation officers for a period of 3 to 5 years. For fiscal year 2000, according to the Administrative Office of the United States Courts, the cost of community supervision averaged about $2,900 per offender—which is an average for "regular supervision" without special conditions, such as community service, electronic monitoring, or substance abuse treatment.

Observations on Identity Theft and Legislative Proposals

Given indications that the prevalence and cost of identity theft have increased in recent years, most observers agree that such crime is serious and warrants continued attention from law enforcement, industry, and consumers. Since our May 1998 report, various actions—particularly passage of federal and state statutes—have been taken to address identity theft. A current focus for policymakers and criminal justice administrators is to ensure that relevant legislation is effectively enforced. Along these lines, we identified several initiatives—including coordinating committees, multijurisdictional task forces, and information clearinghouses—that might help define the dimensions of the problem and help focus limited enforcement resources.

Moreover, there is general agreement that, in addition to investigating and prosecuting violations of these laws, a multipronged approach to combating identity theft must include prevention efforts, such as limiting access to personal information. As you know, at the request of this Subcommittee and others, we have ongoing work looking at government agencies' use of SSNs and whether better safeguards or protections are needed. Prevention efforts can be particularly important, given the personal toll that this crime seems to exact on its victims and how difficult it is to investigate and prosecute perpetrators.

Although the scope of our work for today's testimony did not include an evaluation of various legislative proposals designed to combat identity theft, we did compile information that offers perspectives on various provisions of S. 1055 that are designed to address some aspects of the crime. For example, a major component of identity theft is acquiring personal identifiers—such as SSNs, which are used in some states as driver's license numbers—to build false identities. According to a 1999 study by the U.S. Sentencing Commission,[16] driver's licenses and SSNs are two of the most commonly misused identification means. In fact, the Commission's study reported that driver's licenses and SSNs are the identification means most frequently used to generate or "breed" other fraudulent identifiers. A provision (title II, section 205) of S. 1055 would prohibit the use of SSNs on driver's licenses or motor vehicle registration documents. In 1992, California enacted a law specifying that the SSN collected on a driver's license application shall not be displayed on the driver's license, including any magnetic tape or strip used to store data on

[16] U.S. Sentencing Commission, *Identity Theft Final Report* (Washington, D.C.: Dec. 15, 1999).

the license. More recently, in November 2001, Ohio passed a law prohibiting the display of an SSN on a person's driver's license unless the person requests that the number be displayed. According to the American Association of Motor Vehicle Administrators, most states either prohibit display of the SSN on the face of the license or give the applicant the option to choose whether to display it.

Another potential source of personal identifiers for identity thieves is the personal financial information sold by financial institutions to non-affiliated third parties. The Gramm-Leach-Bliley Act of 1999[17] (GLBA) established the "opt-out" standard currently in effect. That is, unless an exception applies under the current standard, a financial institution must give consumers notice and the opportunity to opt-out before the financial institution can disclose private financial information to non-affiliated third parties. Generally, to implement the opt-out standard, financial institutions are required by law to send consumers an opt-out notice informing them of their right to prohibit its disclosure. In addition, financial institutions have to provide consumers an initial notice and customers an annual notice to inform them of the institution's information policies and practices. These requirements for federally regulated financial institutions became effective July 1, 2001. Limited data are available about the response to and effectiveness of such notices. However, another provision (title III, section 302) of S. 1055 would impose a stricter standard if the financial institution seeks to sell the information. Specifically, that provision would amend GLBA to provide consumers an "opt-in" standard, whereby a bank would need prior consent of the customers before selling personal financial information to non-affiliated third parties.

Resource levels and competing priorities can limit any one level of government's capacity, including the federal government's capacity, to address identity theft crimes. Another provision (title VI, section 601) of S. 1055 would empower state attorneys general to enforce this act. Regarding precedent for such a provision, although GLBA does not have a similar provision, the act's legislative history indicates that earlier versions of the House and Senate bills included similar state enforcement authority, which was dropped in conference. In further reference to precedent, however, one example of an enacted provision is in the antitrust context. State attorneys general have the authority to bring civil actions on behalf

[17] Public Law 106-102 (1999).

of resident consumers who have been injured as a result of violations of federal antitrust laws.

In a similar vein, resource constraints and dollar threshold levels have limited the numbers and types of cases that federal law enforcement agencies have investigated. One type of case that has not often been investigated involves SSN misuse. Currently, SSA/OIG devotes a majority of its investigative resources to program integrity priority areas rather than SSN misuse cases. SSN misuse allegations increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001. Title II, section 207 of S. 1055 would give SSA the authority to impose civil monetary penalties for SSN misuse. It is not clear how the SSA/OIG would carry out this new authority or how many additional resources it would require and at what cost.

In sum, while legislative and other actions have been taken in recent years to address identity theft, incidence and cost data indicate that more can and should be done. The provisions contained in S. 1055 and other proposed legislation are aimed at enhancing the prevention and enforcement tools available to law enforcement, industry, and consumers. These legislative proposals deserve careful attention and analysis.

Madam Chairwoman, this concludes my prepared statement. I would be pleased to answer any questions that you or other members of the subcommittee may have.

Contacts and Acknowledgments

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