United States General Accounting Office

GAO

Report to Congressional Requesters

March 2002

IDENTITY THEFT

Prevalence and Cost Appear to be Growing

GAO-02-363

Contents

Tables

Abbreviations

ABA	American Bankers Association
BOP	Bureau of Prisons
CALPIRG	California Public Interest Research Group
CRA	consumer reporting agencies
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FTC	Federal Trade Commission
GAO	General Accounting Office
IACP	International Association of Chiefs of Police
OIG	Office of the Inspector General
SSA	Social Security Administration
SSA/OIG	Social Security Administration's Office of the Inspector General
SSN	Social Security number

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

March 1, 2002

The Honorable Dianne Feinstein
Chairwoman
The Honorable Jon Kyl
Ranking Minority Member
Subcommittee on Technology, Terrorism
and Government Information
Committee on the Judiciary
United States Senate

The Honorable Charles E. Grassley
United States Senate

This report responds to your request that we review and compile the latest statistics on the incidence and societal cost of identity theft. Generally, as noted in our May 1998 report,[1] identify theft or identity fraud 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 legislation—the Identity Theft and Assumption Deterrence Act of 1998 (the Identity Theft Act)[2]—which separately made identity theft a specific federal crime and recognized that victims include individuals, as well as financial institutions and other business entities. Also, since 1998, most states have enacted laws that criminalize identity theft.

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

- the extent or prevalence of identity theft;

[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").

- the cost of identity theft to the financial services industry,[3] including direct fraud losses, staffing of fraud departments, and effect on consumer confidence in online commerce;
- the cost of identity theft to victims, including victim productivity losses, out-of-pocket expenses, and cost of being denied credit; and
- the cost of identity theft to the federal criminal justice system.

To address these topics, we interviewed responsible officials and reviewed documentation obtained from relevant federal agencies—the Department of Justice and its components, including the Executive Office for U.S. Attorneys (EOUSA) and the Federal Bureau of Investigation (FBI); 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 and two payment card associations (MasterCard and Visa). Furthermore, at our request and with the consent of the victims, FTC provided us with the names and telephone numbers of a small cross section of victims (10 total) 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. We conducted our work from March 2001 to January 2002 in accordance with generally accepted government auditing standards. Appendix I presents more details about the scope and methodology of our work.

Results

No single hotline or database captures the universe of identity theft victims. Some individuals do not even know that they have been victimized until months after the fact, and some known victims may choose not to report to the police, credit bureaus, or established hotlines. Thus, it is difficult to fully or accurately quantify the prevalence of identity theft. Some of the often-quoted estimates of prevalence range from one-quarter to three-quarters of a million victims annually. Usually, these

[3]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 national consumer reporting agencies (commonly referred to as "credit bureaus"). We did not obtain information about losses involving other general-purpose cards (American Express, Diners Club, and Discover) nor losses involving merchant-specific cards issued by retail stores.

estimates are based on limited hotline reporting or other available data, in combination with various assumptions regarding, for example, the number of victims who do not contact credit bureaus, the FTC, the SSA/OIG, or other authorities. Generally speaking, the higher the estimate of identity theft prevalence, the greater the (1) number of victims who are assumed not to report the crime and (2) number of hotline callers who are assumed to be victims rather than "preventative" callers. We found no information to gauge the extent to which these assumptions are valid. Additionally, there are no readily available statistics on the number of victims who may have contacted their banks or credit card issuers only and not the credit bureaus or other hotlines.

Nevertheless, 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. The following presents summary information for each of the topics that we addressed. More detailed information is presented in appendixes II through V, respectively.

Prevalence of Identity Theft

As we reported in 1998, there are no comprehensive statistics on the prevalence of identity theft. Similarly, during our current review, various officials noted that precise, statistical measurement of identity theft trends is difficult due to a number of factors. Generally, federal law enforcement agencies 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, 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 noted that identity theft is not typically a stand-alone crime; rather, identity theft 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, while recognizing measurement difficulties, a number of data sources can be used as proxies or indicators for gauging the prevalence of such crime. These sources can include consumer complaints and hotline allegations, as well as law enforcement 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 agency data. Generally, in the view of consumer reporting agency officials, 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 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.[4] 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[5] for 2000 but was unable to provide information for any earlier year.[6] Also, due largely to increased public awareness about identity theft, the number of inquiries received by the fraud units of consumer reporting agencies is at an all-time high. However, an industry official opined that the number of inquiries is not a reasonable measure of the incidence of identity theft because virtually all individuals whose wallet or purse is lost or stolen will now call the consumer reporting agencies as a precautionary measure.

FTC data. From its establishment in November 1999 through September 2001, FTC's Identity Theft Data Clearinghouse received a total of 94,100 complaints from victims, including 16,784 complaints transferred to the FTC from the SSA/OIG. In the first month of operation, the Clearinghouse answered an average of 445 calls per week. By March 2001, the average number of calls answered had increased to over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls.

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

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

[6]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.

However, FTC officials noted that identity theft-related statistics may, in part, reflect enhanced consumer awareness and reporting.

SSA/OIG data. SSA/OIG has reported a substantial increase in call-ins of identity theft-related allegations to its Fraud Hotline in recent years. Allegations involving SSN misuse, for example, increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001. To some extent, the increased number of allegations may be due to additional Fraud Hotline staffing, which increased from 11 to over 50 personnel during this period. However, SSA/OIG officials attributed the trend in allegations partly to a greater incidence of identity theft. Also, irrespective of staffing levels, SSA/OIG data indicate that about 81 percent of all allegations of SSN misuse relate directly to identity theft.

Federal law enforcement data. Generally, although federal law enforcement agencies do not have information systems that facilitate specific tracking of identity theft cases, the agencies provided us 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 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] 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." (See app. II.)

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. 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/or incomplete

[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 credit cards; or financial institution fraud.

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 year 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.[8] Regarding actual losses, the 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.[9] Based on 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 $700 million in 1996 to about

[8]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 11 percent, the ABA's data should be interpreted with caution.

[9]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.

$1.0 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. Generally, the fraud losses are borne by the respective financial institution that issued the payment card.

To reiterate, regarding direct fraud losses involving payment cards, we contacted MasterCard and Visa only. We did not obtain information about losses involving other general-purpose cards (American Express, Diners Club, and Discover), which account for about 25 percent of the market. Also, we did not obtain information about losses involving merchant-specific cards issued by retail stores. Furthermore, we did not obtain information from various other entities, such as insurance companies and securities firms, which may incur identity theft-related costs.

Regarding staffing and cost of fraud departments, in its year 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.

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 1990's 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 year 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. Furthermore, 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.[10]

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.[11] 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. (See app. III.)

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 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 complaint data 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

[10]Federal Deposit Insurance Corporation, *Evolving Financial Products, Services, and Delivery Systems* (Feb. 14, 2001).

[11]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.

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 the names and telephone numbers of 10 victims, whom we contacted to obtain an understanding of their experiences. In addition to the types of harm mentioned above, several of the victims expressed 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. For instance, some victims reported being able to file a police report in their state of residence but were unable to do so in other 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 the spring of 2000) of 66 identity theft victims who had contacted these organizations.[12] 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 findings may not 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)." (See app. IV.)

Federal Criminal Justice System Costs

Regarding identity theft and any other type of crime, the federal criminal justice system incurs costs associated with investigations, prosecutions, incarceration, and community supervision.[13] Generally, we found that federal agencies do not separately maintain statistics on the person hours,

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

[13]As agreed with the requesters, this section of our report focuses on costs of identity theft to the federal government only and not to state or local governmental entities; although, since 1998, most states have enacted laws that criminalize identity theft.

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 workyear counts for white-collar crime cases—a category that covers financial crimes, including identity theft.

In response to our request, the FBI estimated that the average cost of an investigative matter 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. Nonetheless, the agency's Management and Organization Division made its "best estimate of the average cost" of a financial crimes investigation conducted by the Secret Service in fiscal year 2001. The resulting estimate was approximately $15,000. Secret Service officials noted that this estimate was for a financial crimes investigation and not specifically for an identity theft investigation. Also, the officials emphasized that, in the absence of specific guidelines establishing a standard methodology, average-cost figures provide no basis for making interagency comparisons.

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. Also, in commenting on a draft of this report, the Commissioner, SSA, said that SSA/OIG's priorities are appropriately targeted to SSA's program integrity areas and business processes rather than specifically on identity theft, which is investigated by many different federal and state agencies.

Regarding prosecutions, in fiscal year 2000, federal prosecutors dealt with 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. (See app. V.)

Concluding Observations

Since our May 1998 report, various actions—particularly passage of federal and state statutes—have been taken to address identity theft. The federal statute,[14] enacted in October 1998, 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. 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 as high as 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 identity theft statutes.

In short, federal and state legislation indicate that identity theft has been widely recognized as a serious crime across the nation. As such, a current focus for policymakers and criminal justice administrators is to ensure that relevant legislation is effectively enforced. Given the frequently cross-jurisdictional nature of identity theft crime, enforcement of the relevant federal and state laws presents various challenges, particularly regarding coordination of efforts. Although we have not evaluated them, initiatives designed to address these challenges include the following:

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

- After enactment of the 1998 Identity Theft Act, the Attorney General's Council on White Collar Crime established a Subcommittee on Identity Theft. Purposes of the Subcommittee are 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 representatives from various Justice, Treasury, and State Department components; SSA/OIG; the FTC; federal regulatory agencies, such as the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation; and professional organizations, such as the International Association of Chiefs of Police (IACP), the National Association of Attorneys General, and the National District Attorneys Association.

- Various identity theft task forces, with multiagency participation (including state and local law enforcement), have been established to investigate and prosecute cases. Such task forces enable law enforcement to more effectively pursue cases that have multijurisdictional elements, such as fraudulent schemes that involve illegal activities in multiple counties or states. At the time of our review, the Secret Service was the lead agency in 37 task forces across the country that were primarily targeting financial and electronic crimes, many of which may include identity theft-related elements.

- Also, under the 1998 Identity Theft Act, the FTC established a toll-free number for victims to call and is compiling complaint information in a national Identity Theft Data Clearinghouse. FTC's Consumer Sentinel Network makes this information available to federal, state, and local law enforcement. According to FTC staff, use of the Consumer Sentinel Network enables law enforcement to coordinate efforts and to pinpoint high-impact or other significant episodes of identity theft.

Furthermore, there is general agreement that, in addition to investigating and prosecuting perpetrators, a multipronged approach to combating identity theft must include prevention efforts, such as limiting access to personal information. In this regard, federal law enacted in 1999, the Gramm-Leach-Bliley Act,[15] directed financial institutions—banks, savings associations, credit unions, broker-dealers, investment companies, investment advisers, and insurance companies—to have policies, procedures, and controls in place to prevent the unauthorized disclosure

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

of customer financial information and to deter fraudulent access to such information. Prevention efforts by financial institutions are particularly important, given FTC data showing that a large majority of consumer complaints regarding identity theft involve financial services—new credit card accounts opened, existing credit card accounts used, new deposit accounts opened, and newly obtained loans.

Finally, given indications that the prevalence and cost of identity theft have increased in recent years, most observers agree that such crime certainly warrants continued attention from law enforcement, industry, and consumers.[16] Also, due partly to the growth of the Internet and other communications technologies, there is general consensus that the opportunities for identity theft are not likely to decline.

Agency Comments

On February 5, 2002, we provided a draft of this report for comment to the Departments of Justice and the Treasury, FTC, SSA, and the Postal Inspection Service. The various agencies either expressed agreement with the information presented in the report or provided technical comments and clarifications, which have been incorporated in this report where appropriate.

Also, the Commissioner, SSA, offered additional perspectives to clarify that the role of the SSA/OIG is to protect SSA's programs and operations from fraud, waste, and abuse. That is, the Commissioner noted that the SSA/OIG's priorities are appropriately targeted to SSA's program integrity areas and business processes. On the other hand, the Commissioner said that most identity theft allegations referred to SSA/OIG are not related to these areas and processes. The Commissioner commented that identity theft is a serious crime and that many federal and state agencies have a role in investigating such crime.

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of the 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

[16]Appendix VI lists contact points for reporting identity theft and seeking assistance.

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 or wish to discuss the matter further, please contact me at (202) 512-8777 or Danny R. Burton at (214) 777-5600. Other key contributors are acknowledged in appendix VII.

Richard M. Stana
Director, Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

In response to a request from Senator Dianne Feinstein, Chairwoman, and Senator Jon Kyl, Ranking Minority Member, Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary, and Senator Charles E. Grassley, we developed information on

- the extent or prevalence of identity theft;
- the cost of identity theft to the financial services industry, including direct fraud losses, staffing of fraud departments, and effect on consumer confidence in online commerce;
- the cost of identity theft to victims, including victim productivity losses, out-of-pocket expenses, and cost of being denied credit; and
- the cost of identity theft to the federal criminal justice system.

Scope and Methodology

The following sections discuss the scope and methodology of our work.

Extent or Prevalence of Identity Theft

To obtain information on the extent or prevalence of identity theft, we contacted private and public sector entities that could provide broad or national perspectives. For example, we contacted entities that operate call-in centers for receiving consumer complaints and hotline allegations, as well as federal law enforcement agencies responsible for investigating and prosecuting identity theft-related crimes. We did not canvass state and local law enforcement agencies.

In contacting each of the following entities, we obtained relevant statistics and discussed with responsible officials any qualifications or caveats associated with the data:

- The three national consumer reporting agencies—Equifax, Inc.; Experian Information Solutions, Inc.; and Trans Union, LLC. Each agency has a call-in center that receives complaints or allegations from consumers. In obtaining statistics from the three agencies, we agreed to report the information in a manner not specifically identifiable to the respective agency.
- The Federal Trade Commission (FTC), which operates a toll-free telephone hotline for consumers to report identity theft.
- The Social Security Administration's Office of the Inspector General, which operates a hotline to receive allegations of Social Security number misuse and program fraud.

- Two Department of Justice law enforcement components—the Executive Office for U.S. Attorneys (EOUSA) and the Federal Bureau of Investigation (FBI).
- Three Department of the Treasury law enforcement components—the Internal Revenue Service (IRS), the Secret Service, and the Financial Crimes Enforcement Network (FinCEN).
- The Postal Inspection Service, a leading federal law enforcement agency that investigates the theft of mail or use of the mail to defraud individuals or financial institutions.

Cost of Identity Theft to the Financial Services Industry

In obtaining information on the cost of identity theft to the financial services industry, we focused on three categories—(1) direct fraud losses, (2) staffing and operating cost of fraud departments, and (3) consumer confidence in online commerce. Generally, the scope of our work focused primarily on obtaining information from banks, two payment card associations (MasterCard and Visa), and the national consumer reporting agencies. We did not obtain information about fraud losses involving other general-purpose cards (American Express, Diners Club, and Discover), nor losses involving merchant-specific cards issued by retail stores. Furthermore, we did not obtain information from various other entities, such as insurance companies and securities firms, which may incur identity theft-related costs.

Regarding direct fraud losses, we reviewed recent surveys of banks conducted by the American Bankers Association (ABA). For instance, one survey—Deposit Account Fraud Survey Report 2000—provided information about the percentages of total check fraud-related losses attributable to identity theft in 1999. However, we believe that the results from the ABA's Report 2000 should be interpreted with caution. Although the ABA surveyed a national probability sample of all commercial and savings banks, the overall response rate—that is, the number of completed questionnaires divided by the number of sent questionnaires—was only 11 percent. The response rates stratified by bank size were as follows:

- 10 percent for community banks (assets under $500 million), the large majority of all banks.
- 16 percent for mid-size banks (assets of $500 million to under $5 billion).
- 27 percent for regional banks (assets of $5 billion to under $50 billion).
- 65 percent for superregional/money center banks (assets of $50 billion or more).

Surveys with a low level of responses—particularly surveys with response rates lower than 50 percent—could be affected by nonresponse bias. In other words, if a survey has a low response rate, and if respondents are different in important ways from those who did not respond, the survey results could be biased. For instance, if banks with little or no fraud losses tend not to respond, then survey estimates about the percentage of banks nationwide that regard identify theft as a problem could be overstated. ABA staff did not conduct any follow-up analyses to find out whether the banks that responded were different from the banks that did not respond. ABA staff said that they were not concerned about the survey's response rate because they believed that the survey had adequate coverage of banking industry assets and losses by virtue of having a good representation of large banks (i.e., regional banks and superregional/money center banks). The ABA staff noted, for instance, that most assets and dollar losses in the banking industry are with larger banks.

Furthermore, regarding direct fraud losses, two major payment card associations (MasterCard and Visa) provided us with information on their identity theft-related fraud losses. As mentioned previously, we did not obtain information about direct fraud losses involving other general-purpose cards (American Express, Diners Club, and Discover), nor losses involving merchant-specific cards issued by retail stores. However, to obtain additional perspectives on direct fraud losses, we contacted the top 14 credit-card issuing banks.[1] Six of the banks provided us with information. Generally, the other eight banks (1) chose not to respond, partly because of concerns about the release and use of proprietary information,[2] or (2) asked that we seek to obtain the information from the Consumer Bankers Association.[3] However, citing definitional differences among financial institutions, the Consumer Bankers Association was

[1]Our selection of these 14 banks was based on dollar amounts of managed receivables (as of Dec. 31, 2000) presented in *The Nilson Report* (Oxnard, Cal.), a leading source of news and proprietary research on consumer payment systems. Managed receivables consist of credit card balances outstanding that are carried on the balance sheet, as well as such balances outstanding that are securitized (off the balance sheet), by the credit card issuer.

[2]Credit card issuers' participation in our study was voluntary because we do not have a legal right of access to any of their account or business information not publicly available.

[3]The Consumer Bankers Association (Arlington, Vir.) provides leadership and representation on retail banking issues. Member institutions are active in consumer finance (auto, home equity, credit cards, and education), electronic retail delivery systems, bank sales of investment products, small business services, and community development.

unable to provide us with information on identity theft-related fraud losses.

Regarding staffing and cost of fraud departments, we obtained information from the ABA's 2000 survey report and from the six banks, mentioned previously. Also, we contacted each of the three national consumer reporting agencies to discuss the staffing levels and the costs associated with the respective entity's fraud or victim assistance department.

Furthermore, regarding consumer confidence in online commerce, we conducted a literature search and reviewed relevant congressional hearings and testimony statements made by officials from FTC, the Department of Justice, and a major credit card issuer. Also, officials at five of the six banks we contacted offered comments about the impact of identity theft on consumer confidence in using e-commerce.

Cost of Identity Theft to Victims

In response to our inquiry, FTC staff provided us with statistical information on the types of nonmonetary harm (e.g., denied credit or other financial services) and monetary harm (e.g., out-of-pocket expenses) reported by identity theft victims. This information was based on complaints reported to the FTC's Identity Theft Data Clearinghouse during the period November 1999 through June 2001.

Furthermore, at our request and after obtaining the individuals' consent, FTC staff provided us with the names and telephone numbers of a small cross section of identity theft victims (10 total) to interview. According to FTC staff, the 10 victims were selected to illustrate the range in the types of identity theft activities reported by victims. The experiences of these 10 victims are not statistically representative of all identity theft victims.

Also, we reviewed and summarized information from a May 2000 report prepared by two nonprofit advocacy entities—the California Public Interest Research Group (CALPIRG) and the Privacy Rights Clearinghouse.[4] The report presented findings based on a survey (conducted in the spring of 2000) of 66 identity theft victims who had contacted these organizations.

[4]CALPIRG (Sacramento, Cal.) and Privacy Rights Clearinghouse (San Diego, Cal.), "Nowhere to Turn: Victims Speak Out on Identity Theft" (May 2000). The report is accessible at www.privacyrights.org/ar/idtheft2000.htm.

Cost of Identity Theft to the Federal Criminal Justice System

As agreed with the requesters' offices, to obtain estimates of the cost of identity theft to the criminal justice system, we focused on federal agencies only and did not attempt to quantify the cost of state and local law enforcement activities. Thus, our efforts focused on obtaining information about the cost associated with federal investigations, prosecutions, incarceration, and community supervision. Generally, we found that federal agencies do not maintain cost data specifically attributable to cases involving identity theft. Thus, as an alternative, we asked the agencies to provide us with average cost estimates based, for example, on white-collar crime cases—a category that covers financial crimes, including identity theft. Specifically, we contacted the following federal agencies:

- The FBI and the Secret Service were asked to provide data on the respective agency's average cost of investigating white-collar crimes. The SSA/OIG was asked to provide an estimate for investigating cases involving SSN misuse.
- EOUSA was asked to provide data on the average cost of prosecuting white-collar crimes.
- The federal Bureau of Prisons was asked to provide data on the average cost of incarcerating felons convicted of white-collar crimes.
- The Administrative Office of the United States Courts was asked to provide data on the average cost of supervising white-collar crime offenders in the community.

Appendix II: Prevalence of Identity Theft

This appendix presents information about the prevalence of identity theft, that is, the extent or incidence of such theft. Some individuals do not even know that they have been victimized until months after the fact, and some known victims may choose not to report to the police, credit bureaus, or established hotlines. Thus, it is difficult to fully or accurately quantify the prevalence of identity theft. Some of the often-quoted estimates of prevalence range from one-quarter to three-quarters of a million victims annually. Usually, these estimates are based on limited hotline reporting or other available data, in combination with various assumptions regarding, for example, the number of victims who do not contact credit bureaus, the FTC, the SSA/OIG, or other authorities. Generally speaking, the higher the estimate of identity theft prevalence, the greater the (1) number of victims who are assumed not to report the crime and (2) number of hotline callers who are assumed to be victims rather than "preventative" callers. We found no information to gauge the extent to which these assumptions are valid. Additionally, there are no readily available statistics on the number of victims who may have contacted their banks or credit card issuers only and not the credit bureaus or other hotlines.

As we reported in 1998, there are no comprehensive statistics on the prevalence of identity theft.[1] Similarly, during our current review, various officials noted that precise, statistical measurement of identity theft trends is difficult due to a number of factors. The Secret Service noted, for instance, that identity theft is not typically a stand-alone crime; rather, identity theft is almost always a component of one or more crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments. Nonetheless, while recognizing measurement difficulties, a number of data sources can be used as proxies or indicators for gauging the prevalence of such crime. These sources can include consumer complaints and hotline allegations as well as law enforcement investigations and prosecutions. Each of these various sources or measures seems to indicate that the prevalence of identity theft is growing. This appendix summarizes statistical and related information we obtained from

- the three national consumer reporting agencies (CRAs) that have call-in centers for reporting identity fraud or theft;

[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).

- the Federal Trade Commission (FTC), which maintains a database of complaints concerning identity theft;
- the Social Security Administration's Office of the Inspector General (SSA/OIG), which operates a hotline to receive allegations of SSN misuse and program fraud; and
- federal law enforcement agencies—Department of Justice components, Department of the Treasury components, and the Postal Inspection Service—responsible for investigating and prosecuting identity theft-related cases.

National Consumer Reporting Agencies

Statistics provided to us by the three national CRAs included the number and types of fraud alerts placed on consumers' credit files, as well as the number of inquiries (call volume) received by the fraud units of the CRAs. 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.

Due largely to increased public awareness about identity fraud, the number of inquiries received by the fraud units of CRAs is at an all-time high. For instance, a senior official of one CRA told us that his agency's fraud unit experienced an 84-percent increase in inquires from 1998 to 2000. Now, the CRA official opined, virtually all individuals whose wallet or purse is lost or stolen will call a CRA as a precautionary measure.

According to industry officials, individuals who suspect that they have been the victims of fraud will generally contact all three national CRAs rather than just one or two.[2] Thus, industry officials told us that there probably is a high degree of overlap in each CRA's respective fraud statistics. Also, the officials said that any large variations in reported statistics among the national CRAs are generally the result of different methods for classifying fraud-related inquiries.

In obtaining statistics from the three national CRAs, we agreed to report the information in a manner not specifically identifiable to the respective

[2]During our review, we noted that various Web sites—including those of two of the three national CRAs, 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 CRAs.

agency. Thus, in the following sections, we refer to the three sources as "Agency A," "Agency B," and "Agency C."

Agency A: Number of Files with Fraud Alerts

Agency A officials provided us with trend statistics on the number of individual credit files that had a 7-year fraud alert posted by the agency's fraud victim assistance division. Regarding the total number of consumers helped by this division, the officials said that the number of fraud alert postings is a better indicator than the number of consumer contacts with the division. The officials explained that:

- The number of consumer contacts may include some double counting. For instance, the same consumer may call or write the fraud victim assistance division more than once.
- In contrast, for any given time period, the agency will post a fraud alert only once to an individual consumer's file. Thus, there is no double counting in these statistics.

Furthermore, the officials noted that, based on the agency's best judgment and years of experience with 7-year fraud alert postings, the reasons for such postings can be grouped into three categories.

- About 50 percent of the postings are based on preventative calls from consumers rather than actual or verified instances of fraud. Generally, these consumers request a fraud alert from the standpoint of being "safe rather than sorry"—a preventative approach.
- Another 25 percent of the postings are based on credit card account takeovers. The agency does not define or consider these postings as involving "identity fraud."
- The remaining 25 percent of the postings are based on identity fraud. Most of these instances involve fraudulent credit card applications.

Using these groupings and estimated percentages, Agency A officials developed the 7-year fraud alert data presented in table 1. As indicated, the estimated number of consumers who had their credit files impacted by identity fraud increased about threefold in recent years—from an estimated 27,800 for calendar year 1995 to an estimated 89,000 for calendar year 2000. The most recent year's estimated number (89,000 consumer files in 2000) represents an increase of about 36 percent over the 1999 number (65,600).

Table1: Number of Files with Fraud Alerts Posted (Agency A), 1995 through 2000

Year fraud alert posted[a]	Expiration year of fraud alert	Number of files with fraud alert[b]	Reason for fraud alert: preventative (50 percent)	Reason for fraud alert: account takeover (25 percent)	Reason for fraud alert: identity fraud (25 percent)
1995	2002	111,287	55,600	27,800	27,800
1996	2003	172,319	86,200	43,100	43,100
1997	2004	168,992	84,500	42,200	42,200
1998	2005	191,321	95,700	47,800	47,800
1999	2006	262,410	131,200	65,600	65,600
2000	2007	356,001	178,000	89,000	89,000

Note: Agency A ran a special scan on the agency's national database to produce counts of the number of individual credit files that had a 7-year fraud alert posted. To array the count data, the agency sorted the counts by year of the alert's expiration. According to agency officials, most fraud alerts are posted for 7 years, unless the consumer requests a shorter period.

[a]We calculated these dates by subtracting 7 years from the expiration year shown in the next column.

[b]As noted in the table, Agency A officials determined these counts based on a special scan of the agency's national database. The agency used these counts (and the percentages indicated in the next three columns) to calculate the "reason" numbers shown in the respective column. We rounded the "reason" numbers to the nearest hundred.

Source: Consumer reporting agency (Agency A) data.

Agency B: Number of Files with Security Alerts or Victim Statements

Agency B provides its customers two types of fraud alerts—a temporary or 90-day security alert and a 7-year victim statement. A security alert requests that a creditor ask for proof of identification before granting credit in that person's name. A victim statement provides telephone numbers supplied by the consumer and requests that creditors call the consumer before issuing credit in that person's name.

The officials explained that, if a consumer suspects a fraud-related problem, the individual is to initially call the agency's automated voice response system, which generates a 90-day security alert on the respective credit file. Agency B officials emphasized to us that most of these initial calls are not indicators that the individuals have been actual victims of fraud. Rather, the officials noted that consumers may take action to generate a 90-day security alert for a variety of reasons, such as

- reaction to a media story on identity fraud;
- a desire for added protection from identity fraud;
- suspicion of a relative, coworker, neighbor, or other person;
- an effort to get out of a legitimate debt or financial obligation; or
- a host of other reasons not related to fraud.

Also, after the 90-day security alert is generated, Agency B's policy is to provide the consumer a free copy of his or her credit file. This policy, according to Agency B officials, is to help ensure that the consumer has a better-informed basis for considering his or her situation and the need for any further action or assistance.

Upon receiving and reviewing the credit file copy, the consumer may then follow-up with the agency's call center and speak to a fraud specialist to discuss any suspicious entries on the file. In so doing, the consumer can choose to make a "victim statement," which will have the effect of extending the fraud alert from 90 days to 7 years.

Agency B officials told us that the most reliable indicator of the true incidence of identity fraud that the agency could provide is the number of 7-year victim statements placed on consumer credit files. Relevant statistics (see table 2) provided to us by Agency B indicate that the number of 7-year victim statements 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). Agency B officials pointed out that these numbers are relatively small compared with the numbers of initial calls that generated the 90-day security alerts. For the more recent 12-month period, for example, the number of 7-year victim statements (29,593) equates to about 2.5 percent of the initial calls that generated 90-day security alerts.

Table 2: Number of Files with Fraud Alerts Posted (Agency B), July 1999 through June 2001

Initial and follow-up calls from consumers	July 1999 through June 2000	July 2000 through June 2001	Percentage change
Initial calls that generated 90-day security alerts	1,033,180	1,198,272	+16.0
Some follow-up calls generated 7-year victim statements:			
Follow-up calls	81,041	73,096	-9.8
7-year victim statements	19,347	29,593	+53.0

Source: Consumer reporting agency (Agency B) data.

Agency C: Number of Files with Fraud Alerts

Agency C allows consumers to place temporary or 6-month fraud alerts on their credit files either by (1) using an automated voice response system and choosing the fraud option or (2) directly calling the fraud hotline and speaking with an operator at the agency's Consumer Services Center. Then, after the consumers have had the opportunity to receive and review a copy of their files, they have the option of requesting that a longer-term

fraud alert be placed on their files. The duration of such an alert can range from 2 to 7 years, at the discretion of the individual consumer.

An Agency C official told us that the most reliable metric of fraud, including identity theft, is the number of files with the longer-term (2- to 7-year) fraud alerts. The official said that, in 2000, approximately 92,000 consumers called Agency C to place longer-term fraud alerts on their files. However, the official said that Agency C had no comparative statistics available for earlier years and, thus, could not make any observations about trends in the number of such fraud alerts.

The official noted that many consumers who took action to have the longer-term fraud alerts placed on their files generally had some information—such as documentation from a credit grantor, a police report, or an affidavit—indicating that they were the victims of fraud. On the other hand, the official also noted that some consumers had no direct evidence that they were victims but were uncomfortable enough with the information on their credit files to request an extended (2- to 7-year) fraud alert. The official explained that Agency C does not require consumers to submit any particular type of evidence or information in order to have these longer-term fraud alerts placed on their files.

FTC Maintains a National Database of Identity Theft Complaints

The Identity Theft and Assumption Deterrence Act of 1998 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 (the FTC Clearinghouse) to gather information from any consumer who wishes to file a complaint or pose an inquiry concerning identity theft.[3] In November 1999, the first month of operation, the FTC Clearinghouse answered an average of 445 calls per week. By March 2001, the average number of calls answered had increased to over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls.

[3]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.

At a congressional hearing in September 2000, an FTC official testified that Clearinghouse data demonstrate that identity theft is a "serious and growing problem."[4] 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 be due solely or primarily to an increase in the incidence 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. As table 3 shows, five states accounted for about 44 percent of the total complaints.

Table 3: Number of Identity Theft Complaints FTC Received (Nov. 1999 through Sept. 2001) from Leading States

State	Number of complaints	Percentage
California	16,147	17.2
New York	8,219	8.7
Texas	6,775	7.2
Florida	6,309	6.7
Illinois	4,145	4.4
Subtotal	**41,595**	**44.2**
Remaining states and the District of Columbia	45,175	48.0
Other[a]	7,330	7.8
Total[b]	**94,100**	**100.0**

[a]Other refers to identity theft complaints made from U.S. territories and other countries, as well as complaints made by consumers who do not list their location.

[b]The total includes identity theft complaints forwarded from SSA/OIG to the FTC. The total does not include approximately 36,274 calls from consumers who were not identity theft victims but were seeking information about identity theft.

Source: FTC's Identity Theft Data Clearinghouse.

Furthermore, the FTC data for November 1999 through September 2001 showed that FTC received 500 or more identity theft complaints from each of 13 cities. Of these, New York City had the highest number of complaints (3,916), followed by Chicago (1,620), Los Angeles (1,487), Houston (1,282), Miami (941), Philadelphia (695), San Francisco (621), Las Vegas (572), Phoenix (570), District of Columbia (542), San Diego (539), Dallas (537), and Atlanta (517).

[4]FTC, prepared statement on Identity Theft, hearing before the House Committee on Banking and Financial Services (Sept. 13, 2000).

As table 4 shows, of the total identity theft complaints (94,100) reported to the FTC during November 1999 through September 2001, the majority of the victims (about 62 percent of the complaints) were unaware of the methods that the suspects had used to obtain the victims' personal information, and in another 18 percent of the cases, this type of information was not collected. Of the remaining 19,241 complaints, or about 20 percent of the 94,100 total complaints reported to the FTC for the 23-month period, the victims provided the FTC information about the various methods used by suspects. FTC data indicated that in cases where the identity theft victim knew how the identity theft had occurred, "access through relationship with victim" (e.g., family member, neighbor, or coworker) was the most prevalent method used by suspects to obtain personal information. Specifically, this method accounted for 10,101 complaints for which the victim reported one or more methods used to obtain his or her personal information.

Table 4: Identity Theft Complaints FTC Received (Nov. 1999 through Sept. 2001) and Categories of Methods Suspects Used to Obtain Personal Information

Method suspects used to obtain information	Number of complaints	Percent
Method not known	58,078	61.7
Information not collected (non-FTC data[a])	16,781	17.8
Method known	19,241	20.5
Total	**94,100**	**100.0**
Method-known cases (methods of obtaining personal information were reported):	**Number of complaints**	**Percent based on subtotal[c]**
Access through relationship with victim	10,101	52.5
Wallet or purse containing identification was lost or stolen	6,615	34.4
Mail theft or fraudulent address change filed	2,577	13.4
Application, financial, or employment records compromised	1,322	6.9
Burglary or break-in	686	3.6
Internet solicitation or purchase	462	2.4
Telephone or mail solicitation or purchase	132	0.7
Other	1,706	8.9
Information about method not provided[b]	572	3.0
Subtotal	**19,241[d]**	

[a]Non-FTC data refer to identity theft complaints forwarded from SSA/OIG to the FTC. In these complaints, information about the methods suspects used was not collected.

[b]In 572 cases, consumers said that they knew but did not specify how the suspects obtained the personal information.

[c]Percentages add to more than 100 percent because some victims reported that the suspect used multiple methods of obtaining the data.

[d]Details exceed 19,241 because some victims reported that the suspect used multiple methods of obtaining data.

Source: FTC data.

Additional information about the 10,101 cases involving "access through relationship with victim" is presented in table 5. As shown, in 4,629 of the 10,101 cases where the victim knew the suspect, the victim and the suspect were family members. However, table 5 further indicates that the 10,101 cases represent less than 11 percent of the total 94,100 complaints received by the FTC during November 1999 through September 2001.

Table 5: Relationship of Suspect to Victim in Identity Theft Complaints FTC Received (Nov. 1999 through Sept. 2001)

Relationship of suspect to victim	Number of complaints	Percent based on total 94,100 complaints
Family member	4,629	4.9
Roommate/cohabitant	1,137	1.2
Neighbor	1,003	1.1
Workplace coworker/employer/employee	836	0.9
Otherwise known	2,496	2.7
Total	**10,101**	**10.7**

Source: FTC data.

SSA/OIG Fraud Hotline Statistics

SSA/OIG operates a Hotline to receive allegations of fraud, waste, and abuse. According to SSA/OIG officials, until about mid-February 2001, Hotline staff had no procedures for specifically categorizing any incoming calls as involving identity theft allegations. Rather, in recent years, the allegations most likely to involve identity theft were recorded by Hotline staff as either (1) SSN misuse or (2) program fraud, which may contain elements of SSN misuse potential. SSA/OIG officials explained these two categories of allegations as follows:

- Allegations of "SSN misuse" included, for example, incidents wherein a criminal used the SSN of another individual for the purpose of fraudulently obtaining credit, establishing utility services, or acquiring goods. 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 or disabled often entailed some element of SSN misuse. For example, a criminal may have used the victim's SSN or other identifying information for the purpose of obtaining Social Security benefits. When Hotline staff received this type of allegation, it was to be classified in the appropriate program fraud category, which may also have SSN misuse potential.

As shown in table 6, the number of Fraud Hotline allegations in both of these categories increased substantially in recent years. That is, the number of SSN misuse allegations increased more than fivefold, from 11,058 in fiscal year 1998 to 65,220 in fiscal year 2001, and the number of allegations of program fraud with SSN misuse potential more than doubled, from 14,542 in 1998 to 38,883 in 2001. To some extent, the increased number of allegations may be due to additional Fraud Hotline staffing, which increased from 11 to over 50 personnel during this period. However, SSA/OIG officials attributed the trend in allegations partly to a greater incidence of identity fraud.

Table 6: SSA/OIG Fraud Hotline Statistics on Allegations of SSN Misuse and Program Fraud with SSN Misuse Potential

Fiscal year	Allegations of SSN misuse	Allegations of program fraud with SSN misuse potential
1998	11,058	14,542
1999	30,116	32,260
2000	46,840	36,881
2001	65,220	38,883

Source: SSA/OIG data.

As mentioned previously, for most of the years shown in table 7, SSA/OIG had no procedures for specifically categorizing incoming calls as involving identity theft allegations. However, in 1999, SSA's Office of the Inspector General analyzed a sample of SSN misuse allegations and determined that 81.5 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 SSN misuse allegations received by the SSA/OIG Fraud Hotline from October 1997 through March 1999. The analysis did not cover the other category presented in table 6, that is, allegations of program fraud with SSN misuse potential.

Recently, in about mid-February 2001, SSA/OIG implemented procedures to routinely and specifically determine which Fraud Hotline allegations of SSN misuse involve identity theft.[6] For example, as table 7 shows, for 7

[5]SSA, Office of the Inspector General, *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).

[6]The procedures do not cover allegations of program fraud with SSN misuse potential.

months (Mar. through Sept.) in 2001, the Fraud Hotline received 25,991 identity theft allegations, which are arrayed among 16 categories. As shown, the most prevalent identity theft category involved credit cards, which accounted for 9,488 allegations or almost 37 percent of the total identity theft allegations. The next highest identity theft category—about 4,600 employment-related allegations—usually involved illegal aliens, according to SSA/OIG officials.

Table 7: SSA/OIG Fraud Hotline Statistics on Allegations of SSN Misuse That Directly Involve Identity Theft (by Category), March through September 2001

Identity theft category	Number of allegations	Percentage
Credit card	9,488	36.5
Employment	4,637	17.8
Lost/stolen SSN information (wallet/purse)[a]	3,421	13.2
Bank fraud	2,765	10.6
Utility	2,761	10.6
Tax return	1,032	4.0
Medical care	548	2.1
Driver's license	496	1.9
Housing	224	0.9
Child support	171	0.7
Internet	157	0.6
Government loan	93	0.4
Bankruptcy	83	0.3
INS document	79	0.3
Birth certificate	24	0.1
Passport	12	0.0
Total	**25,991**	**100.0**

Note: According to the SSA/OIG, the identity theft categories reflect the most applicable primary allegation code assigned by the individual SSA program specialist who originally received the allegation. Also, the SSA/OIG noted that the accuracy of the categorizations cannot be confirmed until an allegation is investigated; only about 10 percent of all allegations are opened as investigative cases. Furthermore, the SSA/OIG noted that its identity theft codes do not include certain categories, such as counterfeit SSN cards, trafficking counterfeit SSN cards, trafficking legitimate SSN cards, and false statement to obtain SSN.

[a]The SSA/OIG began using this primary allegation code in June 2001. The SSA/OIG indicated that the code is used for reports of a lost or stolen SSN card where the caller is concerned that his or her SSN may be used fraudulently, but no information is provided to indicate that the SSN has in fact been misused and no loss has been suffered.

Source: SSA/OIG data.

During this 7-month period, the number of identity theft allegations per month increased about 40 percent, from 3,028 in March 2001 to 4,258 in September 2001.

Department of Justice Law Enforcement Components

Regarding Department of Justice law enforcement actions (e.g., number of investigations, arrests, and prosecutions), we obtained identity theft-related statistics from the Executive Office for U.S. Attorneys (EOUSA) and the Federal Bureau of Investigation (FBI).

EOUSA Data

For fiscal years 1996 through 2000, EOUSA provided us with statistics on the number of cases filed under federal statutes related to identity fraud. As indicated in table 8:

- The number of cases filed under 18 U.S.C. § 1028 reflect year-to-year increases and more than doubled from 314 cases in 1996 to 775 cases in 2000.
- The number of cases filed under 18 U.S.C. § 1029 reflect a general decrease, and the most recent figure—703 cases in 2000—is considerably lower than the 924 cases filed in 1996.
- The number of cases filed under 42 U.S.C. § 408 reflect a general increase. The number of cases filed increased substantially in 1998, when compared with the previous 2 years. And, the number of cases filed in 2000 was more than double the number filed in 1996.

Table 8: U.S. Attorney Cases Filed Under Statutes Related to Identity Fraud

Fiscal year	18 U.S.C. § 1028 (Identification documents)	18 U.S.C. § 1029 (Access devices)	42 U.S.C. § 408 (SSN misuse)
1996	314	924	310
1997	404	864	308
1998	550	752	576
1999	568	675	558
2000	775	703	694

Source: EOUSA data.

Also, in reference to table 8, EOUSA staff made the following clarifying comments:

- A given case may be counted under more than one of the three U.S. Code sections because a defendant could have been charged with multiple offenses. However, in table 8's statistics for case filings, there is no double counting of multiple charges of the same Code section, nor of filings under the subsections of that section. For instance, if a defendant was charged with two counts of violations under 18 U.S.C. § 1028(a)(7) in one case, the relevant statistics would still appear as only one case under the 18 U.S.C. § 1028 column in table 8.

- EOUSA has only limited statistical information available at the subsection level or the sub-subsection level for offenses charged under title 18 of the U.S. Code. Except for certain firearms statutes, the case management system requests that cases be recorded under the U.S. Code section only, not under the subsection or the sub-subsection, although this additional information sometimes is provided. Thus, these "subsection-level or sub-subsection-level statistics" have great potential for underreporting. Also, cases involving identity theft or identity fraud are charged under a variety of different statutes, and many criminals who commit identity theft are charged under statutes relating to these defendants' other crimes. With these significant limitations or caveats in mind, EOUSA data indicated that, of the 568 cases filed under 18 U.S.C. § 1028 in fiscal year 1999, the number of cases with at least one charge of a violation of subsection (a)(7) recorded in the EOUSA data base was 24 cases. And, for fiscal year 2000, of the 775 cases filed under 18 U.S.C. § 1028, the number of cases with at least one charge of a violation of subsection (a)(7) recorded in the EOUSA data base was 68 cases.

FBI Data

At the time of our review, FBI officials told us that the agency did not have the capability to determine the number of statistical accomplishments (e.g., arrests and convictions) that have resulted from 18 U.S.C. § 1028(a)(7). The officials noted, however, that the agency was in the process of developing a system to track the number of cases that included identity theft as a component.

Moreover, regarding case statistics that were presently available, the FBI officials offered the following contextual considerations:

- Even if accomplishments from investigative cases could be isolated or tracked to the 1998 act, these cases would not necessarily be an accurate reflection on this law. For instance, an open issue would be to determine if these cases would have been prosecuted using other equally beneficial statutes or not at all.
- Cases involving identity theft or identity fraud typically are classified by the crimes committed using the stolen fraudulent identity—classified, for example, as bank fraud, wire fraud, or mail fraud. In other words, an individual may not always be charged with identity theft but instead be charged with the substantive violations carried out using the stolen identity.
- As other possibilities, a prosecutor may allow an individual who was charged with identity theft to plead guilty to other criminal conduct charges.

With these considerations in mind, the FBI provided us with statistics showing the agency's accomplishments under identity theft-related statutes. Table 9 summarizes the statistics for fiscal years 1996-2001. As indicated, much of the FBI's enforcement activities involved bank fraud cases, which is an area of longstanding responsibility for the FBI.

Table 9: FBI Accomplishments Under Identity Theft-Related Statutes, Fiscal Years 1996 through 2001

Statute	1996	1997	1998	1999	2000	2001[a]
18 U.S.C. § 1028 (Identification documents)						
Indictments and informations[b]	33	33	22	55	99	49
Arrests	24	17	20	28	40	43
Convictions	33	27	17	21	50	29
18 U.S.C. § 1029 (Access devices)						
Indictments and informations[b]	90	95	114	96	125	39
Arrests	38	60	78	69	90	35
Convictions	60	80	77	105	74	35
18 U.S.C. § 1014 (Loan and credit applications)						
Indictments and informations[b]	311	290	235	189	206	94
Arrests	58	62	72	38	85	38
Convictions	304	242	170	146	121	50
18 U.S.C. § 1344 (bank fraud)						
Indictments and informations[b]	1,225	1,159	1,305	1,492	1,481	626
Arrests	311	468	579	691	645	311
Convictions	1,121	896	983	1,047	1,112	449
42 U.S.C. § 408 (SSN misuse)						
Indictments and informations[b]	85	75	97	119	98	40
Arrests	25	15	40	48	62	22
Convictions	61	50	62	64	68	23
15 U.S.C. § 1644 (fraudulent use of credit cards)						
Indictments and informations[b]	11	1	1	1	1	1
Arrests	2	0	1	0	0	2
Convictions	5	2	2	0	0	1

[a]Fiscal year 2001 numbers are as of April 10, 2001.

[b]Generally, an indictment is an accusation presented in writing by a grand jury, charging a person for some criminal offense, whereas an information is presented by a competent public officer on his or her oath of office.

Source: FBI data.

Department of the Treasury Law Enforcement Components

Regarding Department of the Treasury law enforcement actions, we obtained identity theft-related statistics from the Internal Revenue Service (IRS), the Secret Service, and the Financial Crimes Enforcement Network (FinCEN).

IRS: Many Questionable Refund Schemes Involve Identity Theft

According to the IRS, many questionable refund schemes involve an element of identity theft or identity fraud. However, IRS emphasized that not all questionable refund schemes involve this element. For instance, IRS noted that many false returns are filed by the true taxpayer using false income documents (e.g., W-2s, W-2Gs, and Forms 4852 and 1099) with inflated income and/or withholding.

IRS-Criminal Investigation does not routinely keep statistics as to how many questionable refund schemes and questionable returns involve some element of identity theft or identity fraud. Thus, IRS told us that it is difficult to determine the specific number of schemes, refunds, claims, and dollar losses that are solely attributable to identity theft or fraud.

With these caveats in mind and in response to our request, IRS-Criminal Investigation's Office of Refund Crimes developed statistics to reflect its "best effort to show the prevalence of identity fraud." That is, for calendar years 1996 through 2000, IRS provided us with statistics covering all questionable refund schemes that IRS classified as involving a "high frequency" of identity theft or identity fraud—schemes very likely to have elements of this type of crime (see table 10). In 2000, for example, IRS detected a total of 3,085 such schemes, consisting of 35,185 questionable tax returns that claimed a total of $783 million in refunds. According to IRS officials, the agency's detection efforts in that year prevented payment of $757 million.

Table 10: Questionable Refund Schemes Detected by IRS

Dollars in millions

Calendar year	Questionable refund schemes	Questionable returns detected	Refunds claimed	Refunds stopped
1996	2,458	24,919	$82	$69
1997	2,857	30,936	108	95
1998	2,810	31,155	98	77
1999	2,406	31,532	689	667
2000	3,085	35,185	783	757
Total	**13,616**	**153,727**	**$1,760**	**$1,665**

Source: IRS, Criminal Investigation.

Secret Service Data

According to the Secret Service, the vast majority of financial crimes involve the use of some sort of false identification, the use of another individual's personal or financial identifiers, or the assumption of a false or fictitious identity. In explanation, Secret Service officials noted the following:

- Broadly speaking, from the perspective of law enforcement, identity theft can involve either "account takeover" or "identity takeover." That is, such theft involves the use of personal information to (1) make unauthorized use of existing credit or other financial accounts or (2) establish new accounts, apply for loans, etc. Generally, the personal information often sought by criminals is information required to obtain goods and services on credit. Primary types of this information include names, dates of birth, and SSNs. With the proliferation of computers and increased use of the Internet, many identity thieves have used information obtained from company databases and Web sites.
- Identity theft is not typically a "stand alone" crime. Rather, identity theft is almost always a component of one or more crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments. In many instances, an identity theft case encompasses several different types of fraud.

In further response to our inquiry, Secret Service officials said that they believe that identity theft continues to occur at a seemingly increasing pace. The officials cautioned, however, that the incidence of identity theft is difficult to measure on the basis of available statistics (such as number of investigations or arrests) for a variety of reasons. Among others, the reasons cited were lack of reporting by victims, classification of identity theft in other crime categories (e.g., theft or forgery) or perhaps as a civil

matter, and different levels of law enforcement (federal, state, and local) having concurrent jurisdiction with respect to many aspects of identity theft. Given these limitations, the officials suggested that any assessment of overall trends regarding identity theft perhaps should be based on statistics from FTC—the agency designated to be the primary point of contact for victims.

Nonetheless, we obtained available statistics from the Secret Service regarding its identity-theft related cases for fiscal years 1998-2000 (see table 11). In interpreting these data, Secret Service officials noted that, in recent years, the agency has moved away from investigating "street crime" level offenders in the identity theft spectrum to targeting individuals and groups engaged in the systematic, large-scale pursuit of profits through the commission of various types of identity theft. That is, the agency is now focusing on high-dollar, community-impact cases that merit federal interest. Case statistics for fiscal years 1998-2000 reflect this shift in focus, according to Secret Service officials, who noted the following:

- The number of arrests decreased 28 percent from 1998 to 2000, and the number of cases closed dropped 37 percent.
- On the other hand, the average actual losses to victims in closed cases rose 71 percent from 1998 to 2000. The average fraud losses prevented rose 48 percent from 1998 to 1999 and rose an additional 101 percent from 1999 to 2000.

Table 11: Secret Service Data on Identity Theft-Related Arrests, Cases Closed, and Dollar Losses in Fiscal Years 1998 through 2000

Data category	1998	1999	2000
Arrests	4,421	3,814	3,163
Cases closed[a]	8,489	7,071	5,379
Average actual losses to victims in cases closed[b]	$26,922	$38,078	$46,119
Average fraud losses prevented in cases closed[c]	$73,382	$108,476	$217,696

Note: In compiling these data, the Secret Service defined identity theft as any case related to the investigation of false, fraudulent, or counterfeit identification; stolen, counterfeit, or altered checks or Treasury securities; stolen, altered, or counterfeit credit cards; or financial institution fraud.

[a]Cases can be closed for a variety of reasons, such as completion of judicial action, declination to prosecute by the Office of the United States Attorney, or a determination that insufficient evidence exists to identify or charge a suspect.

[b]As defined by the Secret Service, "actual losses" are the amounts of money, goods, or services that were obtained by the criminal or group of criminals through the commission of the crime.

[c]As defined by the Secret Service, "fraud losses prevented" is the difference between potential losses and actual losses. The Service defined "potential losses" as the amounts of money, goods, or services that the criminal or group of criminals was trying to obtain through the commission of the crime.

Source: Secret Service data.

FinCEN Data

In April 1996, financial institutions were required to begin filing suspicious activity reports (SAR) to assist law enforcement in detecting and prosecuting violations of money laundering and other financial crimes.[7] Recently, to "provide insights into the patterns of criminal financial activity associated with identity theft," FinCEN analyzed SARs filed during the period April 1996 through November 2000—a total of 490,595 filings. Of this total, FinCEN's analysis indicated that 1,030 SARs reported identity y theft. Analysis of these 1,030 SARs, according to FinCEN's June 2001 report, confirms "industry perceptions of increases in both the incidence of identity theft-based fraud and SAR reporting about the phenomenon."[8] Specifically, FinCEN noted the following:

- During January through December 1997, the first full year of required SAR reporting, 44 instances of identity theft—fewer than 4 per month—were reported.
- Recently, during January through November 2000, there were 617 SARs filed that reported identity theft, an average of 56 SARs per month.

Also, in its report, FinCEN noted—but did not elaborate or provide related statistics—that advanced technology (particularly the Internet) is proving to be a "powerful facilitator" of identity theft.

Postal Inspection Service

The Postal Inspection Service is a leading federal law enforcement agency in the investigation of identity takeovers, a crime that frequently begins with the theft of mail or use of the mail to defraud individuals or financial institutions. In its fiscal year 2000 annual report, the Postal Inspection Service noted that identity theft is a growing trend:

"Inspection Service identity theft investigations increased by 67 percent since last year. Identity theft occurs when mail is stolen for the personal information it contains, which criminals use to fraudulently order credit cards, checks or other financial instruments. Mail theft may go unreported—the thief looks for mail containing items such as a credit card payment, copies personal identifiers and credit card and bank account information, and

[7]The SAR system replaced a "criminal referral reporting" system that had been used since 1984.

[8]FinCEN, *The SAR Activity Review—Trends, Tips & Issues*, Issue 2 (June 2001), p. 14.

reseals the envelope and returns it to the mailstream, often undetected. Checks and credit cards may then be ordered in the victim's name. Private mailboxes at commercial receiving agencies … are often rented so the crook can receive the fraudulently obtained cards and checks anonymously."[9]

Also, in its 2000 annual report, the Postal Inspection Service mentioned various initiatives to address identity theft:

"Credit card theft and identity theft are becoming increasingly intertwined as crimes involving the U.S. Mail. The U.S. Postal Inspection Service's Credit Card Mail Security Initiative has brought various federal law enforcement agencies and credit card industry representatives together since 1992 to discuss loss and theft issues and develop solutions. Many of the identity theft issues related to credit card losses are currently being addressed by members of the initiative. …

"On November 6, 1999, President Clinton announced the Know Fraud initiative, a partnership of several leading private and government agencies, including the U.S. Postal Inspection Service, to educate consumers about how to protect themselves from telemarketing and mail fraud. … Although work continues on the first Know Fraud initiative, plans are underway for a second one to launch in early 2001. Focusing on identity theft, the goal of the new effort is to deliver to every home in America prevention information that will raise awareness of this growing trend and provide consumers with protective tactics."[10]

According to the Postal Inspection Service, the "Know Fraud" initiative is "the largest consumer protection effort ever undertaken, with postcards sent to 123 million addresses across America, arming consumers with common sense tips and guidelines …"

Postal Inspection Service arrest statistics indicate that the agency has increased its focus on identity theft-related crime in recent years (see table 12). For instance, whereas the annual number of arrests was relatively constant during fiscal years 1996 through 1999, the year 2000 total (1,722 arrests) represents an increase of about 36 percent over the previous year. Furthermore, the total for partial-year 2001 (9 months) is higher than the year 2000 total.

[9] *2000 Annual Report of Investigations of the United States Postal Inspection Service* (Nov. 2000), p. 9.

[10] *2000 Annual Report of Investigations of the United States Postal Inspection Service* (Nov. 2000), pp. 9, 40-41.

Table 12: Postal Inspection Service Identity Theft-Related Arrests, Fiscal Years 1996 through 2001

Fiscal year	Number of arrests
1996	1,287
1997	1,226
1998	1,122
1999	1,267
2000	1,722
2001 (through June 30, 2001)	1,752

Source: Postal Inspection Service data.

Appendix III: Cost of Identity Theft to the Financial Services Industry

According to industry data, the dollar value of goods and services purchased by consumers in the United States was $6.8 trillion in the year 2000. General purpose credit cards—American Express, Diners Club, Discover, MasterCard, and Visa—were used to pay for 20.4 percent of these consumption expenditures.[1] MasterCard and Visa comprised about 76 percent of the U.S. card market share, based on first quarter 2001 data. Also, as members of the MasterCard and Visa associations, much of the banking industry engaged in issuing credit cards, as well as offering checking accounts.

This appendix discusses identity theft and the financial services industry in reference to three categories or aspects of cost—direct fraud losses, staffing and operating cost of fraud departments, and consumer confidence in online commerce (i.e., e-commerce through the Internet).

Direct Fraud Losses

Regarding identity theft-related direct fraud losses incurred by the financial services industry, we obtained information from (1) the American Bankers Association (ABA); (2) the two leading payment card associations, MasterCard and Visa; and (3) six credit card-issuing banks.[2]

ABA Check Fraud Survey

In its 2000 bank industry survey on check fraud, the ABA reported that total check fraud-related losses in 1999—considering both actual losses ($679 million) and loss avoidance ($1.5 billion)—against commercial bank accounts reached $2.2 billion, which was twice the amount in 1997.[3] Regarding actual losses, the report noted that the 1999 figure ($679 million) was up almost 33 percent from the 1997 estimate ($512 million).

[1]Checks were used to pay for 51.3 percent of total consumption expenditures, cash was used for 16.7 percent, other proprietary cards for 4.1 percent, and "other" (such as money orders) for 7.6 percent. (Details add to 100.1 percent due to rounding.)

[2]As discussed in appendix I, these banks are among the top 14 credit-card issuing banks in terms of managed receivables. Of the top-issuing group of 14 banks, we were able to arrange in-person or telephone interviews with officials of 6 banks.

[3]ABA, *Deposit Account Fraud Survey Report 2000*, p. 9. ABA conducted its survey between February and June 2000 and received responses (completed survey forms) from 542 commercial banks. According to the ABA, the reported loss figures represent extrapolations to the industry level. ABA defined "loss avoidance" as the amount of losses avoided as a result of the banks' prevention systems and procedures.

In 1999, according to ABA data shown in table 13, the percentages of total check fraud-related losses attributable to identity theft ranged from 56 percent at community banks to 5 percent at superregional/money center banks. To restate, at the high end of this range, community banks reported that 56 percent of their check fraud-related losses could be attributed to identity theft; and at the low end of the range, superregional/money center banks reported that 5 percent of their check fraud-related losses could be attributed to identity theft. As previously mentioned, the ABA reported that check fraud-related losses totaled $2.2 billion in 1999. However, the ABA's report did not specifically disaggregate this total among the bank-size categories shown in table 13.

Table 13: Percentages of Banks' Total Check Fraud-Related Losses Attributable to Identity Theft, 1999

Banks (by size based on assets)	Identity theft losses as a percentage of total check fraud-related losses
Community banks (assets under $500 million)	56
Mid-size banks (assets of $500 million to under $5 billion)	18
Regional banks (assets of $5 billion to under $50 billion)	6
Superregional/money center banks (assets of $50 billion or more)	5
All sizes combined	29

Note: ABA defined identity theft as losses due to account takeovers (or true name fraud). As indicated in appendix I, the overall response rate for ABA's survey was 11 percent. The response rates by bank size were as follows: community banks (10 percent), mid-size banks (16 percent), regional banks (27 percent), and superregional/money center banks (65 percent). Surveys with a low level of responses—particularly surveys with response rates lower than 50 percent—could be affected by nonresponse bias. Thus, the results from ABA's survey should be interpreted with caution.

Source: ABA, *Deposit Account Fraud Survey Report 2000*, p. 19.

In the same report, banks surveyed by the ABA between February and June 2000 identified the leading threats against deposit accounts anticipated in the next 12 months. The leading threat category cited by the surveyed banks involved counterfeit checks, and this category was closely followed by concerns regarding debit cards, identity theft (true name fraud), and the Internet. The percentages of surveyed banks that ranked identity theft among the top three threats against deposit accounts, as shown in table 14, ranged from a low of 48.4 percent of community banks to a high of 75.8 percent of regional banks.

Table 14: Percentage of Banks that Regard Identity Theft (True Name Fraud) as One of the Top Three Threats Against Deposit Accounts

Banks (by size based on assets)	Percentage of surveyed banks
Community banks (assets under $500 million)	48.4
Mid-size banks (assets of $500 million to under $5 billion)	60.2
Regional banks (assets of $5 billion to under $50 billion)	75.8
Superregional/money center banks (assets of $50 billion or more)	63.6

Note: ABA defined identity theft as losses due to account takeovers (or true name fraud). As indicated in appendix I, the overall response rate for ABA's survey was 11 percent. The response rates by bank size were as follows: community banks (10 percent), mid-size banks (16 percent), regional banks (27 percent), and superregional/money center banks (65 percent). Surveys with a low level of responses—particularly surveys with response rates lower than 50 percent—could be affected by nonresponse bias. Thus, the results from ABA's survey should be interpreted with caution.

Source: ABA Data.

Two Major Payment Card Associations: Fraud Losses Involving Identity Theft

MasterCard and Visa are separate associations owned by numerous financial institutions that issue payment cards (credit cards and debit cards) bearing the MasterCard name and the Visa name, respectively. As such, MasterCard and Visa rarely receive complaints of fraud directly from consumers. Rather, the fraud-related statistics that MasterCard and Visa report represent an aggregation of data reported by each association's members. Association members report fraud-related statistics in various categories, such as account takeovers, fraudulent applications, lost cards, stolen cards, never-received cards, counterfeit cards, and mail order/telephone order fraud.

Regarding these various categories, MasterCard and Visa use very similar (although not identical) definitions regarding which of these categories constitute identity theft, as opposed to other types of fraud. According to a MasterCard official, the identity theft-related categories are account takeovers and some portion of fraudulent applications. A Visa official said that two categories—account takeovers and fraudulent applications—are considered by Visa to be identity theft because the other forms of fraud do not necessarily require the "stealing" of another person's identifying information.[4]

[4]In contrast to these relatively narrow definitions, the Secret Service, as a lead federal enforcement agency for identity theft, defines this crime more broadly to encompass virtually all categories of payment card fraud.

In response to our inquiry, MasterCard and Visa officials provided us with information on their respective association's fraud-related dollar losses for calendar years 1996 through 2000. However, the officials considered this information to be proprietary and requested that we aggregate the data in our reporting rather than present association-specific data. We agreed. The associations' aggregated data are presented in table 15. As indicated, for domestic (U.S.) operations, the associations' identity theft-related fraud losses—defined as involving account takeovers and fraudulent applications—rose from $79.9 million in 1996 to $114.3 million in 2000, an increase of about 43 percent. Much of this increase is reflected in the account-takeover losses, which increased more than twofold, from $33.0 million in 1996 to $68.2 million in 2000. An official of one association said that this increase probably could be attributed to "inconsistencies in reporting among member banks." The official added that consumers are not really at risk because a zero liability policy protects them from financial loss.

Table 15: MasterCard and Visa Fraud Losses, Calendar Years 1996 through 2000

Dollars in millions					
Fraud losses by category	**1996**	**1997**	**1998**	**1999**	**2000**
Identity theft-related losses:					
Account takeovers[a]	$33.1	$32.4	$34.4	$39.8	$68.2
Fraudulent applications[b]	46.8	36.9	37.2	43.4	46.1
Subtotal	**$79.9**	**$69.3**	**$71.6**	**$83.3**	**$114.3**
Additional fraud losses[c]	620.3	590.4	663.9	700.8	898.9
Total fraud losses	**$700.2**	**659.7**	**735.5**	**784.1**	**$1,013.2**
Identity theft-related losses as a percentage of total fraud losses	11.4%	10.5	9.7	10.6	11.3
Total fraud losses as a percentage of associations' U.S. members' sales volume	**0.104%**	**0.084%**	**0.081%**	**0.074%**	**0.082%**

[a]A Visa official said that the account takeover category may include some miscellaneous fraud losses reported by Visa member banks; thus, the dollar losses attributed to account takeovers may be somewhat overstated.

[b]According to a MasterCard official, the fraudulent applications category can have components that do not involve identity theft.

[c]Additional fraud losses include categories such as lost and stolen cards, never-received cards, counterfeit cards, and mail order/telephone order fraud.

Source: MasterCard and Visa data for domestic (U.S.) operations.

Furthermore, table 15 shows that the associations' identity theft-related losses as a percentage of total fraud losses were relatively constant at about 9 to 10 percent during 1996 through 2000. In further perspective, for most of these years, table 15 shows that the associations' total fraud losses represented less than 1/10th of 1 percent of U.S. member banks' sales

volume. Generally, the fraud losses are borne by the financial institution that issued the payment card. In some instances, although reportedly rare, retail merchants may bear such losses if the merchants do not follow proper procedures for verifying use of the card.

To reiterate, regarding direct fraud losses involving payment cards, we contacted MasterCard and Visa only. We did not obtain information about losses involving other general-purpose cards (American Express, Diners Club, and Discover), which account for about 25 percent of the market. Also, we did not obtain information about losses involving merchant-specific cards issued by retail stores. Furthermore, we did not obtain information from various entities, such as insurance companies and securities firms, which may incur identity theft-related costs.

An official of one of the associations told us that identity theft is not perceived to be one of the biggest fraud-related problems faced by member banks. The official said that many banks have experience in dealing with identity fraud, including using new technology to detect where such fraud may be taking place. Additionally, to help reduce the incidence of fraud, the official noted that the association provides guidance or recommendations for member banks and merchants to follow, as well as a number of specific computer models and authorization and verification systems that help reduce fraud and identity theft.

Selected Credit Card-Issuing Banks

Officials of six credit card-issuing banks that we contacted said their financial institutions track fraud in several categories. But, we found some inconsistency among these institutions on the definition of credit card fraud associated with identity theft. For example, some financial institutions did not consider "friendly fraud" or "family fraud"[5] in their fraud losses to be related to identity theft. However, two categories of identity theft-related fraud used by all six banks were (1) fraudulent applications and (2) account takeovers. Five of the six banks had data on identity theft losses involving fraudulent applications and account takeovers. These losses ranged from 18 percent to 42 percent of the

[5]Friendly or family fraud could occur when there is an unauthorized use of a credit card or personal information by an acquaintance, friend, or family member. Friends or family members sometimes apply for credit in the victim's name or take over existing accounts in cases of death or disability without notifying the financial institution. In these cases, financial institutions are usually able to recover their losses or shift the responsibility for existing accounts.

respective bank's overall fraud losses.[6] However, bank officials acknowledged that identity theft could also be associated with lost or stolen payment cards or other categories of losses—and, thus, the reporting of losses for only two categories (fraudulent applications and account takeovers) may understate total identity theft-related losses.

Officials from one of the six banks said that the amount of losses is not large, and the bank considered these losses to be within an acceptable level of risk. Also, the officials noted that the bank experienced more fraud from unauthorized use—that is, use of lost or stolen cards and forged checks—than from account takeovers and fraudulent applications.

Officials from a second bank said that their bank's largest source of credit card fraud was from lost or stolen credit cards. The officials added that the next most common form of fraud involved counterfeit credit cards—a type of fraudulent activity that occurred worldwide and often was perpetrated by organized crime rings. The third most common form of fraud—and more difficult to detect—was account takeover. The root cause of identity theft associated with account takeover, according to these bank officials, involved the misuse of SSNs acquired from another source. Also, this bank reported having experienced an increase in the number of cases of friendly fraud—that is, incidents whereby a victim's family member or acquaintances obtained or tried to obtain credit in the victim's name. For example, in a divorce situation, a spouse may have opened an account in his or her partner's name without consent.

Officials from a third bank said that the growth of fraud losses was correlated to business growth. However, the officials noted that the bank's losses associated with identity theft had remained relatively constant during the last few years.

Officials at a fourth bank said that the bank does not normally track identity theft. Rather, the bank tracked the number of fraudulent applications denied due to the suspicion of fraud. Regarding this category, the bank officials did not consider the number of incidents to be significant in relationship to the bank's overall customer base; however, the officials noted that cases often occurred in "waves." Moreover, the

[6]The sixth bank did not provide us with data reflecting identity theft losses as a percentage of overall fraud losses.

officials said that they were concerned with larger losses, which resulted from fraudulent activities perpetrated by organized crime rings.

At a fifth bank, officials said that roughly 90 percent of the bank's identity theft cases involved fraudulent applications, and the remainder represented account takeovers. The officials explained that, when the bank focuses on combating one form of fraudulent activity, other or replacement manifestations often begin to appear. For instance, the officials noted that fraud had increased from credit cards not received in the mail. In addition, the officials said they believed that fraudulent activity associated with organized crime rings was on the rise.

At the sixth bank, officials provided no additional information about the institution's fraud losses.

Staffing and Cost of Fraud Departments

The following sections discuss the staffing and cost of the fraud departments of banks and CRAs. The sections present information based on (1) ABA's 2000 bank industry survey on check fraud, (2) responses from officials of various banks we contacted, and (3) our interviews with officials of the three national CRAs.

ABA Data: Fraud-Related Operating Expenses of Banks

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 as a direct function of bank size. For instance, as table 16 shows for check fraud-related operating expenses (not including actual losses) in 1999,

- over two-thirds (69.5 percent) of the 446 community banks that responded to ABA's survey each incurred less than $10,000 for such expenses;
- about one-third (32.0 percent) of the 103 responding mid-size banks each incurred such expenses ranging from $50,000 to $249,999;
- about one-fourth (24.2 percent) of the 33 responding regional banks each incurred such expenses ranging from $500,000 to $999,999. Another one-fourth of the regional banks each incurred such expenses ranging from $1 million to $4.9 million; and
- about one-fourth (27.3 percent) of the 11 responding superregional/money center banks each incurred more than $10 million for such expenses.

Table 16: Amount of Expenses Per Bank Devoted to Prevention, Detection, Investigation, and Prosecution of Check Fraud, 1999

Expenses per bank	Community banks (assets under $500 million)	Mid-size banks (assets of $500 million to under $5 billion)	Regional banks (assets of $5 billion to under $50 billion)	Superregional/ money center banks (assets of $50 billion or more)
Less than $10,000	69.5%	24.3%	—	—
$10,000 to $49,999	9.6	21.4	—	—
$50,000 to $249,999	1.3	32.0	21.2%	—
$250,000 to $499,999	—	4.9	18.2	—
$500,000 to $999,999	—	—	24.2	18.2%
$1 million to $4.9 million	—	1.0	24.2	27.3
$5 million to $9.9 million	—	—	—	9.1
$10 million or more	—	—	—	27.3
Do not know	19.5	16.5	12.1	18.2
Totals[a]	**99.9%**	**100.1%**	**99.9%**	**100.1%**
Number of banks responding	446	103	33	11

[a]Percentages do not add to 100.0 percent due to rounding.

Source: ABA, *Deposit Account Fraud Survey Report 2000*, p. 60.

Fraud Departments of Selected Banks

The six banks discussed earlier also responded to our questions about fraud department staffing. Bank officials expressed concern about the growing sophistication of identity thieves, and the officials indicated that their respective banks had taken a number of proprietary steps for preventing, detecting, and responding to fraud. The officials told us that fraud department staffing had increased over the last few years, both in relationship to the growth in business portfolios and to address increasing fraud losses. However, the officials said that they could not specifically quantify the fraud department costs associated with identity theft. Rather, the information provided to us can be summarized as follows:

- At four of the six banks, officials reported that fraud department staffing had expanded, with designated or specialized staff devoted to dealing with fraud prevention. The officials noted that their respective bank's fraud prevention procedures were dynamic and proprietary.
- At a fifth bank, officials told us that about 30 percent of the fraud unit's employees were associated with addressing identity theft. The officials added that the unit's staffing had increased over the last 5 years, in line with the bank's portfolio growth. However, the officials also said they had witnessed an increase in fraudulent applications—concurrent with an

increase in Web site usage—and had taken additional preventative steps to address such applications.

- At the sixth bank, officials told us that fraud department staffing had remained relatively stable over the last 5 years.

Moreover, in addition to fraud department staffing, various bank officials indicated that there were other indirect costs associated with addressing identity theft. Examples of such costs included the following:

- To assist in correcting credit bureau files, banks devote resources to communicating with customers and CRAs.
- Banks use resources in cooperating with law enforcement agents who investigate identity theft crimes. And, expenses are incurred in attempts to locate perpetrators, bill them, and collect owed amounts.
- Banks may incur lost opportunity costs in not being able to extend credit to legitimate customers.

Fraud-Assistance Staffing at the Three National CRAs

Officials from each of the three national CRAs told us that the number of fraud-assistance staff—that is, staff to answer telephone calls and correspondence from individuals who believed that they may have been the victims of fraud—had increased in recent years. In obtaining staffing information from the three national CRAs, we agreed to report the information in a manner not specifically identifiable to the respective agency. Thus, in the following sections, we refer to these sources as "Agency A," "Agency B," and "Agency C." Of the three, Agency A and Agency C had a call center devoted specifically to fraud assistance. Agency B's call center handled both fraud-related and nonfraud-related matters, such as various types of consumer inquiries and disputes.

Agency A: Fraud-Assistance Staffing Has Doubled

An Agency A official said that the number of staff in the agency's fraud assistance department doubled in recent years, increasing from 50 in 1997 to 103 in 2001. In discussing the reasons for this increase, the official explained that greater public awareness of identity theft has resulted in a much larger volume of calls from consumers to the CRA. Now, the official opined, virtually any person who has a wallet or purse stolen will call a CRA as a protective measure against becoming a fraud victim.

Moreover, the official said that Agency A's operating policy is to have a sufficient number of fraud-assistance staff available so that consumers will be able to speak with someone when they first telephone. In contrast, the official noted that the other two CRAs have an automated response system

for handling the initial telephone inquiries from consumers. Thus, the official said that Agency A has a greater number of fraud-assistance staff than the other two CRAs.

According to this official, Agency A's staffing costs for the fraud assistance department were about $3.3 million in 2000. Adding administrative costs to the staffing costs, the official said that the department's total operating costs for the year exceeded $4 million.

Agency B: Fraud-Assistance Staffing Has Increased

Agency B officials provided us with information that was more general or less specific than that provided by Agency A. That is, the officials said that:

- Agency B's fraud-assistance staffing has increased in recent years and remained relatively steady at 30 to 40 fraud specialists in 2000 and 2001.
- The annual cost of maintaining a staff of fraud-assistance specialists is in the range of "several million dollars."

Also, in discussing Agency B's automated response system for handling initial inquiries, the officials said that the system has the advantage of being available to consumers 24 hours a day, 7 days a week. The officials explained Agency B's system as follows:

- When a consumer telephones the CRA, the automated system gives a menu of various options, one of which is a fraud-assistance option. If a consumer selects this option, Agency B automatically places a 90-day security alert on the consumer's file.
- In addition to being provided a credit file report, the consumer is given a toll-free telephone number that the consumer can call to discuss—with Agency B fraud-assistance staff—the report and any related fraud concerns. In calling and discussing his or her situation, the consumer may choose to make a "victim statement," which will have the effect of extending the fraud alert to a period of 7 years. Upon adding the victim statement, an updated credit report will be sent to the consumer, and two more reports will be provided at 45-day intervals.

According to these officials, another advantage of Agency B's automated response system for handling a consumer's initial inquiry is that the credit file reports give the consumer a basis for subsequently having a more informed discussion with the agency's fraud-assistance staff. Finally, the officials noted that the free reports—which total over 1 million annually—represent a significant but easily overlooked cost of identity fraud to CRAs.

Agency C: Fraud-Assistance Staffing Has Increased

An Agency C official provided us with information on the approximate costs and hotline staffing levels for the fraud component of the agency's Consumer Services Center. The official told us that the number of fraud operators at the Consumer Services Center had increased in the 1990's but has remained relatively constant at about 30 to 50 individuals since 1997. The official said that the cost of salaries for these operators has been approximately $900,000 per year, with annual adjustments to reflect inflation and merit increases. Also, the official noted that other administrative expenses—such as computer costs, rent payments, etc.—would raise the cost higher. However, the official did not quantify these expenses.

In describing Agency C's inquiry process, the official explained that consumers could place temporary or 6-month fraud alerts on their credit files by (1) using the agency's main automated toll free number and choosing the fraud option or (2) directly calling the fraud hotline and speaking with a fraud operator. According to this official:

- After temporary fraud alerts have been initiated, the consumers are automatically opted out of preapproved offers of credit.
- Additionally, the consumers receive free copies of their credit files. Upon reviewing their credit files, the consumers can contact a fraud operator and place a longer-term (2- to 7-year) fraud alert on their files.

Consumer Confidence in Online or E-Commerce

The following sections present (1) overview information about Internet fraud, (2) credit industry views regarding identity theft and consumer confidence in using e-commerce, and (3) statistical data showing continued growth in e-commerce.

Overview: Internet Fraud

In addition to facilitating e-commerce, Internet technology can also increase the potential of exposing individuals to identity theft and other fraudulent activities or schemes. Generally, the term "Internet fraud" refers to any scheme that uses one or more components of the Internet—such as Web sites, message boards, e-mail, or chat rooms—to conduct fraudulent transactions, present fraudulent solicitations to prospective victims, or transmit the proceeds of fraud to financial institutions or others connected with the scheme. According to Internet Fraud Watch, which

was created in 1996 to enable the National Fraud Information Center[7] to offer consumers advice about promotions in cyberspace and to route reports of suspected Internet and online fraud to the appropriate government agencies:

"While scams online are both new and old, free standing and combinations, the Internet itself creates a whole new set of problems and opportunities for law enforcement and for criminals. There are millions of people online, with thousands of new users every day. … [T]here are now more e-mails sent every day than regular mail, including junk mail. Once a consumer goes online, he or she is bombarded with unsolicited commercial e-mail (spam) advertising everything from legitimate services to fraudulent investment schemes. Web sites abound offering both legitimate and fraudulent products and services."[8]

At a congressional hearing in September 2000, an FTC official testified, in part, as follows:

"The Internet has dramatically altered the potential occurrence and impact of identity theft. First, the Internet provides access to identifying information through both illicit and legal means. The global publication of identifying details that previously were available only to a select few increases the potential for misuse of that information. Second, the ability of the identity thief to purchase goods and services from innumerable e-merchants expands the potential harm to the victim through numerous purchases. The explosion of financial services offered on-line, such as mortgages, credit cards, bank accounts and loans, provides a sense of anonymity to those potential identity thieves who would not risk committing identity theft in a face-to-face transaction."[9]

Recently, at a congressional hearing in May 2001, a Department of Justice official testified partly as follows:

"Internet fraud, in all of its forms, is one of the fastest-growing and most pervasive forms of white-collar crime. … Regrettably, criminal exploitation of the Internet now encompasses a

[7]The National Fraud Information Center was established in 1992 by the National Consumers League, a nonprofit consumer organization, to address telemarketing fraud by improving prevention and enforcement.

[8]Phillip C. McKee, III, Internet Fraud Watch Coordinator, "Remarks to the Annual Conference of the American Society of Travel Agents" (Oct. 8, 1999).

[9]FTC, prepared statement on Identity Theft for a hearing before the House Committee on Banking and Financial Services, (Sept. 13, 2000).

wide variety of securities and other investment schemes, online auction schemes, credit-card fraud, financial institution fraud, and identity theft. …

"A January 2001 study by Meridien Research … reports that with the continuing growth of e-commerce, payment-card fraud on the Internet will increase worldwide from $1.6 billion in 2000 to $15.5 billion by 2005. The Securities and Exchange Commission staff reports that it receives 200 to 300 online complaints a day about Internet-related securities fraud. Foreign law enforcement authorities also regard Internet fraud as a growing problem. Earlier this year, the European Commission reported that in 2000, payment-card fraud in the European Union rose by 50 percent to $553 million in fraudulent transactions, and noted that fraud was increasing most in relation to remote payment transactions, especially on the Internet. Similarly, the International Chamber of Commerce's Commercial Crime Service reported that nearly two-thirds of all cases it handled in 2000 involved online fraud."[10]

Industry Views: Payment Card Association and Selected Banks

At the May 2001 congressional hearing, a Senior Vice President from Visa—a major credit card association testified, in part, as follows:[11]

"Electronic commerce is vital to the U.S. economy and to the prospects for our continued economic growth. … There is no doubt that electronic commerce is a large, growing and permanent new channel for the sale of goods and services to consumers. The Department of Commerce estimates, for example, that online retail sales grew from less than $5.2 billion in the fourth quarter of 1999 to almost $8.7 billion in the same quarter one year later. Sales projections for the electronic commerce market range from $35 billion to $76 billion by the year 2002. By any measure, this counts as explosive growth …

"Visa has taken steps to promote consumer confidence in this new channel of commerce. These steps include … [a] zero liability policy for unauthorized use of our payment cards. … This zero liability policy applies to online transactions a well as offline transactions. Customers are protected online in exactly the same way as when they are using their cards at a store, ordering from a catalog by mail, or placing an order over the phone. In case of a problem, Visa provides 100 percent protection against unauthorized card use, theft, or loss.

[10]Statement of Mr. Bruce Swartz, Deputy Assistant Attorney General, Criminal Division, Department of Justice, at 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).

[11]Statement of Mr. Mark MacCarthy, Senior Vice President, Public Policy, Visa U.S.A. Incorporated, at 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).

If someone steals a payment card number from one of our cardholders while the cardholder is shopping, online or offline, our customers are fully protected—they pay nothing for the thief's fraudulent activity."

During our review, of the six credit card-issuing banks we contacted, five responded to our questions about the impact of identity theft on consumer confidence in using e-commerce. These responses can be summarized as follows:

- One of the five banks had recently conducted a focus group to assess the issue of consumer confidence in using e-commerce. Bank officials told us that most of the focus group participants expressed no concern about identity theft or fraud in conducting online banking or e-commerce transactions. In the credit card issuer's experience, individuals over age 55 were more leery of online banking and e-commerce and were not as familiar with the technology.
- A second bank's officials told us that many of the bank's customers had an irrational fear of using e-commerce, or using credit cards for Internet transactions. The officials explained that, when fraud occurs, many customers were absolutely convinced the Internet was the root cause of the compromised information and the subsequent fraud, regardless of whether or not the Internet was actually used in the fraudulent transaction.
- A third bank had conducted focus groups on fraud and found that the largest concern voiced was identity theft. However, according to bank officials, this concern was not a major barrier to using e-commerce.
- At the fourth and fifth banks, officials did not have any information about consumers' fears of identity theft from using online banking services or engaging in e-commerce transactions. However, officials from one of these banks noted that there was little basis in fact for such concerns. The officials explained that information transmitted to and from financial institutions for banking and other online transactions is encrypted; and, while there have been instances in which such information has been compromised, its misuse for identity theft purposes has been rare.

Steady Growth of E-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. Furthermore, in 1995, only 130 banks and thrifts had a Web site; but, the number had grown to 4,600 by 2000. Similarly, 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.[12]

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.[13] 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. In short, as more consumers become familiar with online products and services, e-commerce is likely to gain greater acceptance as a channel of commerce, and usage can be expected to increase further.

[12]Federal Deposit Insurance Corporation, *Evolving Financial Products, Services, and Delivery Systems* (Feb. 14, 2001).

[13]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.

Appendix IV: Cost of Identity Theft to Victims

Victims of identity theft may experience a range of costs that encompass nonmonetary harm as well as monetary losses. This appendix presents information about both of these cost categories.

FTC Data on the Cost of Identity Theft to Victims

As mentioned previously, from its establishment in November 1999 through September 2001, the FTC Clearinghouse received a total of 94,100 complaints from identity theft victims. In response to our request, FTC staff provided us with information about the nonmonetary harm and the monetary losses (out-of-pocket expenses) reported by the complainants.

The extent of the harm reported to the FTC depends upon the victims' knowledge at the time that they call the FTC. Victims call the FTC at all stages of their experience with identity theft. Some victims call shortly after they discover the theft of their identities, while others may not hear about the FTC's hotline and not call until months after they discover the crime. In addition, some victims discover the misuse of their identity soon after the misuse begins, while others do not discover it until years later. Moreover, the thieves may continue to misuse identities long after victims contact the FTC. For these reasons, the amount of harm that the victims are aware of and report at the time that they call the FTC may not be the full extent of the harm they have experienced or will experience.

FTC Data on Nonmonetary Harm Reported by Identity Theft Complainants

As table 17 shows, of the 94,100 identity theft complaints reported to the FTC during November 1999 through September 2001, about 14 percent involved reports of nonmonetary harm. By far the most prevalent type of nonmonetary harm cited by consumers—mentioned in over 7,000 complaints—was "denied credit or other financial services." The second leading type of nonmonetary harm—cited in about 3,500 complaints—was "time lost to resolve problems." In nearly 1,300 complaints, identity theft victims alleged that they had been subjected to "criminal investigation, arrest, or conviction."

Table 17: Nonmonetary Harm Reported by Identity Theft Complainants to FTC (Nov. 1999 through Sept. 2001)

Nonmonetary harm	Number of complaints	Percent
Did the consumer report any nonmonetary harm?		
No	63,959	68.0
Information not collected (non-FTC data[a])	16,784	17.8
Yes	13,357	14.2
Totals	**94,100**	**100.0**
If yes, what was the harm?	Number of complaints	Percent based on subtotal[c]
Denied credit or other financial services[b]	7,376	55.2
Time lost to resolve problems	3,489	26.1
Harassed by debt collector or creditor	2,968	22.2
Criminal investigation, arrest, or conviction	1,281	9.6
Civil suit filed or judgment entered	819	6.1
Denied employment or loss of job	580	4.3
Other	3,780	28.3
Total	**13,357[d]**	

Note: According to FTC staff, most identity theft victims can be assumed to have received a negative or inaccurate credit report and, by itself, such a report is not a harm and is not included in this analysis. Rather, a negative or inaccurate credit report may result in various types of harm, such as the victim being denied credit, having to spend time to resolve problems, etc.

[a]Non-FTC data refer to identity theft complaints forwarded from the SSA/OIG to the FTC. In these complaints, information about nonmonetary harm to victims was not collected.

[b]Denied credit or other financial services includes being denied a loan, being denied a credit card, being denied a checking or savings account, having a credit card rejected, having a telephone or utilities cut off or new service denied, or having checks refused for payment (bounced).

[c]Percentages add to more than 100 percent because an identity theft complainant may allege more than one type of nonmonetary harm.

[d]Details add to more than 13,357 because an identity theft complainant may allege more than one type of nonmonetary harm.

Source: FTC data.

FTC Data on Monetary Losses Reported by Identity Theft Complainants

As table 18 shows, FTC data indicated that 2,633 complaints received from November 1999 through September 2001 involved dollar amounts that victims reported as having been lost or paid as out-of-pocket expenses as a result of identity theft. While most financial institutions do not hold victims liable for fraudulent debts, victims may incur significant expenses in trying to restore their good names and financial health. According to FTC staff, for example, victims routinely incur costs for document copies, notary fees, certified mail, and long-distance calls. Some consumers have

tax refunds or other benefits withheld pending resolution of the identity theft crime. In addition, some consumers have hired attorneys. Other consumers reported that they chose to pay the fraudulent debt because of difficulties encountered in trying to have the debt absolved.

The FTC Clearinghouse had no data regarding direct out-of-pocket monetary losses (if any) for 77,063 (about 82 percent) of the 94,100 complaints received during November 1999 through September 2001. Also, for another 14,404 complaints, FTC data indicated that the individual victims reported zero dollar losses, that is, no out-of-pocket expenses. On the other hand, the data indicated that hundreds of complaints—2,633 in total during the 23-month period—reported at least some out-of-pocket expenses, with 207 of the complaints each alleging losses above $5,000 and another 203 complaints each alleging losses above $10,000. Out-of-pocket expenses may increase after victims report to the FTC and take further steps to resolve identity theft-related problems.

Table 18: Monetary Losses Reported by Identity Theft Complainants to FTC (Nov. 1999 through Sept. 2001)

Dollar amount of losses	Number of complaints	Percent
No data[a]	77,063	81.9
Zero dollar losses reported	14,404	15.3
Dollar losses reported:		
$1 – 100	502	0.5
$101 – 500	653	0.7
$501 – 1,000	399	0.4
$1,001 – 5,000	669	0.7
$5,001 – 10,000	207	0.2
Over $10,000	203	0.2
Subtotal	**2,633**	**2.8**
Total	**94,100**	**100.0**

[a]At the time they contacted the FTC, most complainants provided no information about the amount of out-of-pocket expenses, if any, they had incurred.

Source: FTC data.

Summary of Our Contacts with Victims

From its database of identity theft victims, after obtaining permission from the individuals, FTC staff provided us with the names and telephone numbers of 10 victims, whom we contacted to obtain a direct or first-hand understanding of their experiences. As presented in table 19:

- In all 10 cases, the perpetrator used the victim's personal information to engage in identity takeover activities. Varying by case, such fraudulent activities ranged from the opening of new charge accounts and cellphone accounts to obtaining employment and filing tax returns in the victim's name. Also, in 2 of the 10 cases, the perpetrator engaged in account takeover activities; that is, the perpetrator made charges on existing accounts.
- Nine of the 10 victims reported experiencing both nonmonetary and monetary harms. Regarding nonmonetary harm, various victims reported being harassed by collection agencies, expending time to clear their names, having difficulty obtaining credit, and losing productivity at work. Furthermore, one victim reportedly was the subject of an arrest warrant, based on speeding tickets issued to the perpetrator, and another victim was taken into police custody for a drug-related search stemming from the perpetrator's activities. Regarding monetary harm, the victims generally reported that out-of-pocket expenses were relatively low. However, two victims reported losing a job and wages (with losses of about $6,000 and $2,500 per victim, respectively), and two victims reported an inability to obtain tax refunds ($1,000 and $814, respectively).

Table 19: Summary of GAO's Interviews of Identity Theft Victims

Victim	For what fraudulent activities did the perpetrator use the victim's personal information?	What were the types of harm experienced by the victim?
1	Identity takeover activities: Opened 12 to 18 charge accounts. Obtained housing. Obtained utility services. Obtained fraudulent identification. Opened cellphone account.	Nonmonetary harm: Harassed by collection agency. Reappearance of charges after they had been removed. Expended time (about 200 hours over 10 months) to clear name. Monetary harm: Incurred out-of-pocket expenses ($100 to $200). Lost job and wages (about $6,000).
2	Identity takeover activities: Attempted to open charge account. Account takeover activities: Made charges on existing account.	Nonmonetary harm: Expended time (about 40 hours over 4 to 6 weeks) to clear name. Monetary harm: Incurred out-of-pocket expenses (less than $20).
3	Identity takeover activities: Opened charge accounts. Obtained housing. Purchased car. Wrote bad checks. Obtained employment and owed back taxes.	Nonmonetary harm: Expended time (about 3 months in worktime equivalent over 6 years) to clear name. Experienced difficulty obtaining credit. Monetary harm: Harassed by collection agencies. Incurred out-of-pocket expenses (about $20). Could not claim tax refund ($1,000).

Victim	For what fraudulent activities did the perpetrator use the victim's personal information?	What were the types of harm experienced by the victim?
4	Identity takeover activities: Opened charge accounts. Attempted to obtain car loan. Wrote bad checks. Obtained fraudulent identification. Opened cellphone account.	Nonmonetary harm: Expended time (between 150 and 200 hours over 6 weeks) to clear name. Monetary harm: Incurred out-of-pocket expenses (between $20 and $30 for notaries, faxes, etc.).
5	Identity takeover activities: Violated traffic laws (3 speeding tickets). Opened charge accounts. Wrote bad checks. Obtained employment and filed tax return. Obtained utility services. Obtained fraudulent identification. Attended college classes.	Nonmonetary harm: Arrest warrant issued for victim based on perpetrator's speeding tickets. Went to court to contest speeding ticket. Expended hundreds of hours over last 6 years. Experienced difficulty obtaining credit. Monetary harm: Could not obtain IRS tax refund ($814).
6	Identity takeover activities: Opened 10 charge accounts. Wrote bad checks. Made fraudulent identification. Account takeover activities: Used existing credit accounts.	Nonmonetary harm: Harassed by retailers over bad checks. Expended time (missed 3 days of work in 2 months). Had lower productivity at work. Monetary harm: Purse was stolen. Incurred out-of-pocket expenses for notaries and incidentals ($20).
7	Identity takeover activities: Opened about 20 charge accounts.	Nonmonetary harm: Experienced difficulty obtaining credit (rejected for credit 10 times). Expended time (about 48 hours over 2-½ years) to clear name. Experienced difficulty purchasing a car. Monetary harm: Incurred several hundred dollars in out-of-pocket expenses on notaries, faxes, etc.
8	Identity takeover activities: Filed for income tax refunds. Was arrested three times in victim's name.	Nonmonetary harm: Expended time (about 30 hours over 1-½ years) to clear name. Taken to police station for car to be searched for drugs.
9	Identity takeover activities: Obtained fraudulent identification. Opened bank account. Opened multiple charge accounts. Purchased car. Obtained prescription medication. Obtained employment and was fired from employment. Received unemployment benefits. Was evicted three times from housing.	Nonmonetary harm: Experienced difficulty obtaining credit. Experienced difficulty obtaining employment. Experienced difficulty purchasing a car. Experienced difficulty obtaining housing due to perpetrator's eviction history. Expended hundreds of hours over 6 years attempting to clear name. Monetary harm:

Victim	For what fraudulent activities did the perpetrator use the victim's personal information?	What were the types of harm experienced by the victim?
	Used victim's name during auto accident. Was arrested twice in victim's name.	Lost job and wages ($2,500). Incurred out-of-pocket expenses (about $50).
10	Identity takeover activities: Obtained fraudulent identification. Opened multiple charge accounts. Received traffic violation in victim's name.	Nonmonetary harm: Experienced difficulty obtaining credit. Expended 15 to 20 hours over last 3 years attempting to clear name. Monetary harm: Incurred out-of-pocket expenses (about $59).

Note: According to FTC staff, the 10 victims were selected to illustrate a range in the number of types of identity theft activities reported by victims. The experiences of these 10 victims are not statistically representative of all identity theft victims.

Source: GAO's summary of telephone interviews with 10 identity theft victims FTC selected.

In addition to the types of harm presented in table 19, several of the victims expressed to us feelings of "invaded privacy" and "continuing trauma" that likely would affect their lives for quite some time. In particular, such "lack of closure" was cited if elements of the crime involved more than one jurisdiction and/or if the victim had no awareness of any arrest being made. For instance, two victims reported being able to file a police report in their state of residence but were unable to do so in other states where the perpetrators committed fraudulent activities using the stolen identities. Also, 2 of the 10 victims told us they were aware that the perpetrator had been arrested.

Consumer Advocacy Report on the Cost of Identity Theft to Victims

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 the spring of 2000) of 66 identity theft victims who had contacted these organizations.[1] The May 2000 report noted that victims of identity theft "face extreme difficulties attempting to clear the damaged credit, or even criminal record, caused by the thief." According to the report, the following findings illustrate the obstacles that victims encounter when trying to resolve their identity theft cases:

- The victims spent 175 hours, on average, actively trying to resolve their identity theft-related problems. Less than half (45 percent) of the

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

respondents believed that their cases had been fully resolved; these respondents reported an average of 23 months to reach resolution. The other survey respondents (55 percent) reported that their unresolved cases had already been open, on average, for 44 months.

- Not counting legal fees, victims reported spending between $30 and $2,000 on costs related to their identity theft. The average reported loss was $808, but most victims estimated spending $100 for out-of-pocket costs.
- The majority (76 percent) of the surveyed cases involved "true name fraud"—which occurred, for instance, when the imposter opened new credit accounts in the name of the victim. The number of fraudulent new accounts opened per victim ranged from 1 to 30, and the average was 6 new accounts.

The May 2000 report stated that these findings may not 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.[2] Furthermore, 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.

[2]Beth Givens, Director, Privacy Rights Clearinghouse, "Identity theft: The Growing Problem of Wrongful Criminal Records," presented at the SEARCH National Conference on Privacy, Technology and Criminal Justice Information, in Washington, D.C. (June 1, 2000).

Additional Observations

In an April 2001 advisory letter to national banks, the Office of the Comptroller of the Currency (OCC) made the following observations about the cost of identity theft:

"This growing crime has a devastating effect on financial institution customers and a detrimental impact on the banks. Four of the top five consumer complaints regarding identity theft involve financial services—new credit card accounts opened, existing credit card accounts used, new deposit accounts opened, and newly obtained loans. Banks absorb much of the economic losses from bank fraud associated with the theft of their customers' identities. Individuals who become victims of identity theft also pay, at a minimum, out-of-pocket expenses to clear their names and may spend numerous hours trying to rectify their credit records."[3]

Also, in congressional testimony in May 2001, an experienced New York City police detective characterized the cost of identity theft to victims as follows:

"Over the past five years, there has been a significant increase in crimes where criminals compromise personal identification data of victims, in order to commit identity theft. The information that falls into criminal hands includes name, date of birth, Social Security Number, banking account number, and other personal and financial information.

"Victims of identity theft, like other crime victims, are made to feel personally violated. This is especially true in light of the vicious cycle of event that typically follows the perpetration of this crime. Imagine for a moment, a recently married couple just starting out in their life together. They work hard and save enough money to make a down payment on their first new home only to be denied a mortgage because of a negative payment history reflected in a credit report—information that they knew nothing about. The trauma of this type of fraud causes its innocent victims is unimaginable. Moreover, once the crime is discovered and reported, victims are left to fend for themselves in attempting to clear their credit history and good name.

"Our unit has successfully conducted numerous investigations where perpetrators have used the personal information to not only obtain credit cards and personal loans, but also to purchase cars and homes. Although we in law enforcement garner some sense of

[3]Comptroller of the Currency, Administrator of National Banks, OCC Advisory Letter (AL 2001-4), Subject: Identity Theft and Pretext Calling (Apr. 30, 2001), pp. 2-3.

satisfaction when we make arrests for these crimes, it is not enough when compared to the amount of time and energy a victim spends trying to undo the work of these criminals."[4]

[4]Testimony of Detective Michael Fabozzi, New York City Police Department, hearing on "Protecting Privacy and Preventing Misuse of Social Security Numbers" before the Subcommittee on Social Security, House Committee on Ways and Means (May 22, 2001).

Appendix V: Cost of Identity Theft to the Federal Criminal Justice System

This appendix presents information about the cost of identity theft to the federal criminal justice system—that is, the cost associated with investigations, prosecutions, incarceration, and community supervision. 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 18 U.S.C. §1028(a)(7) and other criminal statutes that may be applicable to identity theft and fraud. Thus, as an alternative, some of the agencies provided us with average cost estimates based, for example, on white-collar crime cases—a category that covers financial crimes, including identity theft.

Cost of Investigations

Various Justice Department law enforcement agencies (e.g., the FBI), Treasury Department agencies (e.g., the Secret Service), and the Postal Inspection Service are responsible for investigating possible federal criminal violations in which identity theft or fraud is a factor. Also, the SSA's Office of the Inspector General (OIG) may investigate possible identity theft and fraud cases where misuse or abuse of Social Security numbers (SSNs) is involved. Three of these agencies—the FBI, the Secret Service, and SSA/OIG—responded to our request for cost-related information, as discussed in the following sections.

FBI: Cost of Investigations

In response to our inquiry regarding the cost of investigating identity theft crimes, the FBI provided us with an estimate based on budget and workload data for the agency's white-collar crime program for fiscal years 1998 to 2000. For this 3-year period, the FBI estimated that approximately $20,000 was the average cost of an investigative matter handled by the agency's white-collar crime program. However, an FBI official noted that the agency does not have cost data related specifically to identity theft cases, and the official told us that the average-cost figure ($20,000) was not very meaningful given the following caveats:

- Using available data, the average cost of an investigative matter can be calculated in a number of different ways, none of which is perfect. Due to such imperfections, the validity of the $20,000 figure is highly questionable. For instance, the average cost figure does not capture the wide variance in the scope and costs of white-collar crime investigations. Some cases can be of short duration and involve only one FBI agent, whereas other cases can be very complicated, be ongoing for several years, and involve many agents.

- Also, it is questionable methodology for the FBI to apply the average cost of its white-collar crime investigations in general to identity theft cases specifically. Identity theft is rarely a stand-alone crime; that is, identity theft is frequently an element of bank fraud, wire fraud, and other types of white-collar or financial crimes. On the other hand, some white-collar or financial crimes, including some high-cost cases, may not involve elements of identity theft. However, the FBI's information systems are not sufficiently code to isolate identity theft-related budget and workload data within the white-collar crime program.

Secret Service: Cost of Investigations

We asked the Secret Service for an estimate of the average cost of investigating financial crimes that included identity theft as a component. The Secret Service responded that the agency does not track costs on a per-case basis and noted that the nature and variety of factors regularly present in common investigative scenarios do not lend themselves to accurate "average cost" tracking. The agency explained that variants affecting cost include, but are not limited to, the number of personnel assigned, the use of technical and surveillance assets, transcription and translation services, case-related travel (domestic and foreign), task force expenses, expenditures for investigative information and evidence, expenditures associated with undercover activities, and trial preparation. In summary, the Secret Service responded that its cases vary so much in their makeup that to put a figure on average cost is not meaningful.

Nonetheless, recognizing these caveats, the Secret Service's Management and Organization Division made its "best estimate of the average cost" of a financial crimes investigation conducted by the Secret Service in fiscal year 2001. The resulting estimate was approximately $15,000. Secret Service officials noted that this estimate was for a financial crimes investigation and not specifically for an identity theft investigation. Also, the officials emphasized that, in the absence of specific guidelines establishing a standard methodology, average-cost figures provide no basis for making interagency comparisons.

SSA/OIG: No Estimate of Cost

We asked SSA/OIG for an estimate of the average cost of investigating cases involving SSN misuse. 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 to work these types of cases. Furthermore, the officials commented substantially as follows:

- Identity theft poses greater costs to the public and to financial institutions than to law enforcement.
- The cost of identity theft to law enforcement is a moving target. The cost can be small or large, depending on what priority SSN misuse is given in any law enforcement organization.
- In fact, SSA/OIG probably could dedicate its entire workforce to SSN misuse cases and still not scrape the surface of this issue.

Finally, the SSA/OIG officials noted that the SSA/OIG's appropriations for fiscal year 2001 totaled about $69 million; however, the officials reiterated the impracticality of estimating how much of this amount was used for investigating cases of SSN misuse.

Cost of Prosecutions

Executive Office for U.S. Attorneys (EOUSA) officials said that the agency's timekeeping system could not specifically isolate the cost of prosecuting identity theft cases. The officials noted, however, that such cases generally are categorized as white-collar crimes, as are other types of financial crimes. According to EOUSA:

- U.S. Attorney Offices handled a total of 13,720 white-collar crime cases in fiscal year 2000. This total includes all white-collar crime cases that U.S. Attorney Offices dealt with in any manner during the year. That is, the total includes cases that were closed in the year, cases that were opened in the year, and cases that were still pending at yearend.
- The total cost associated with the 13,720 white-collar crime cases handled was $157 million in fiscal year 2000. Thus, the estimated average annual cost of prosecuting a white-collar crime case was $11,443.

EOUSA emphasized that this figure was derived using a broad, inexact methodology. Furthermore, EOUSA emphasized that the figure was only an estimate and that the actual cost could be higher or lower.

Cost of Incarceration

According to Bureau of Prisons (BOP) officials, federal offenders convicted of white-collar crimes generally are incarcerated in minimum-security correctional facilities. For fiscal year 2000, BOP officials told us that the cost of operating such facilities averaged $47.68 daily per inmate. Thus, on a monthly (30 days per month) and an annual basis (365 days per year), the respective cost figures would be $1,430 per inmate and $17,403 per inmate.

Cost of Community Supervision

Federal probation officers are responsible for the community supervision of federal offenders released from prison, as well as those placed on probation in lieu of a prison sentence. Each offender under supervision is assigned to a designated probation officer, whose responsibilities include (1) enforcing the conditions of supervision; (2) reducing the risk the offender poses to the community; and (3) providing the offender with access to treatment, such as substance abuse aftercare and mental health services.[1] Offenders are typically supervised in the community for a period of 3 to 5 years.

In response to our inquiry, AOUSC provided us average daily cost data covering all federal offenders under supervision. The average daily cost reported for fiscal year 2000 ranged from $8.02 for regular supervision to $31.46 for supervision that involved electronic monitoring and substance abuse treatment. An AOUSC official told us that white-collar offenders—including those who committed identity theft and do not need contract services—probably would fall into the regular supervision category. For this category, the average daily cost of $8.02 equates to about $2,900 annually per offender. According to AOUSC, regular supervision cost is based on the national average salary and benefits of a U.S. probation officer, plus additional costs associated with management, administrative support, training, and overhead (e.g., automation, space, telephone service, and travel).

[1]Title 18, section 3583 of the U.S. Code provides for inclusion of a term of supervised release after imprisonment. Section 3603 specifies the duties of probation officers.

Appendix VI: Contact Points for Reporting Identity Theft and Seeking Assistance

Name	Address	Telephone, Web page, or e-mail
Credit bureaus		
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241	1-800 525 6285 www.equifax.com
Experian	P.O. Box 9532 Allen, TX 75013	1-888 397 3742 www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834	1-800 680 7289 www.transunion.com
Advocacy sources		
Privacy Rights Clearinghouse	3100 5th Ave., #B San Diego, CA 92103	1-619 298 3396 www.privacyrights.org
Identity Theft Resource Center	P.O. Box 26833 San Diego, CA 92196	1-858 693 7935 www.idtheftcenter.org
U.S. Public Interest Research Group	218 D St., SE Washington, D.C. 20003	1-202 546 9707 uspirg@pirg.org
Federal agencies		
Federal Trade Commission	Identity theft Data Clearinghouse 600 Pennsylvania Ave., NW Washington, D.C. 20580	1-877 438 4338 (toll free) www.consumer.gov/idtheft
Department of Justice		www.usdoj.gov/criminal/fraud/idtheft.html
Federal Bureau of Investigation	Call local field office	www.ifccfbi.gov (for Internet fraud)
Internal Revenue Service Department of the Treasury	Taxpayer Advocates Office	1-877 777 4778 www.treas.gov/irs/ci
Postal Inspection Service	Call local post office	www.usps.gov/websites/depart/inspect
U.S. Secret Service Department of the Treasury	Call local field office	www.treas.gov/usss/financial_crimes.htm
Office of the Inspector General Social Security Administration	Fraud Hotline P.O. Box 17768 Baltimore, MD 21235	1-800 269 0271
Other sources		
State law on identity theft	State attorney general's office for your state	www.naag.org
Victim report	Your local police	
Compromised credit cards	Your credit card issuer or local bank (also follow the four steps listed below)	Contact information is often found on your most recent monthly credit card statement
Compromised checking accounts	The bank that holds your account	Contact information is often found on your most recent monthly checking account statement

To report identity theft, follow the steps below as listed in the Identity Theft FTC Web site: (www.ftc.gov/opa/2002/02/idtheft.htm).

1. Contact the fraud departments of each of the three credit bureaus and report the thefts.

2. For fraudulently accessed accounts, contact the security department of the appropriate creditor or financial institution.

3. File a report with your local police or the police in the community where the identity theft took place. Get the report number or copy of the report in case the bank, credit card company, or others need proof of the crime.

4. Call the ID Theft Clearinghouse toll free at 1-877.438.4338 to report the theft. The Identity Theft Hotline and the ID Theft Web site (www.consumer.gov/idtheft) give you one place to report the theft to the federal government and receive helpful information.

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, Kay E. Brown, Heather T. Dignan, Nancy M. Eibeck, William Falsey, Debra R. Johnson, Shirley A. Jones, Harry Medina, Robert J. Rivas, Ronald J. Salo, and Donovan Wilson 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 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
P.O. Box 37050
Washington, D.C. 20013

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

Visit GAO's Document Distribution Center

GAO Building
Room 1100, 700 4th Street, NW (corner of 4th and G Streets, NW)
Washington, D.C. 20013

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm,
E-mail: fraudnet@gao.gov, or
1-800-424-5454 or (202) 512-7470 (automated answering system).

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