United States General Accounting Office

GAO Briefing Report to Congressional Requesters

May 1998

# IDENTITY FRAUD

# Information on Prevalence, Cost, and Internet Impact is Limited

GAO/GGD-98-100BR

GAO

United States
General Accounting Office
Washington, D.C. 20548

General Government Division

B-279537

May 1, 1998

The Honorable Charles E. Grassley
Chairman
Special Committee on Aging
U.S. Senate

The Honorable Barbara B. Kennelly
Ranking Minority Member
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

The Honorable Gerald D. Kleczka
House of Representatives

This report summarizes the substance of our briefing today to your offices in response to your request that we provide information on various issues relating to identity fraud. Generally, identity fraud involves "stealing" another person's personal identifying information, e.g., Social Security number (SSN), date of birth, and mother's maiden name. Criminals use such information to fraudulently establish credit, run up debt, or to take over existing financial accounts. The methods used to obtain personal identifying information can range from basic street theft to sophisticated, organized crime schemes involving the use of computerized databases or the bribing of employees with access to personal information on customer or personnel records.

As agreed with your offices, this document provides information on (1) law enforcement's responsibilities for investigating identity fraud and the difficulties in tracking such crime; (2) statistics or other data showing the prevalence of identity fraud; (3) the costs of identity fraud; and (4) identity fraud and the Internet, including the status of self-regulation by computerized database services that collect and disseminate personal identifying information. Also, although not specifically related to identity fraud, we agreed with your offices to ask credit bureaus for revenue figures associated with selling personal identifying information and to discuss the effects on businesses or commerce if such sales were restricted.

In developing information on these issues, we conducted a literature search and contacted officials at various federal agencies, including the Federal Bureau of Investigation (FBI), the Secret Service, the Executive

Office for U.S. Attorneys, the Social Security Administration's (SSA) Office of the Inspector General, the Postal Inspection Service, the Internal Revenue Service's (IRS) Criminal Investigation Division, and the Federal Trade Commission. Also, we contacted state and/or local officials in Arizona and California, two states that have enacted identity-fraud legislation in recent years. Further, we interviewed representatives of the three largest credit bureaus (Equifax, Inc.; Experian Corporation; and Trans Union Corporation); the major credit-card companies; and various research, consumer interest, privacy rights, and other groups.

Our work generally consisted of (1) synthesizing information from existing studies, reports, or other publications and (2) interviewing relevant public and private sector officials, as previously indicated, to obtain available statistics, other applicable documentation, and testimonial evidence. We did not independently verify the accuracy of the statistical and other information provided to us by the various public and private entities. Appendix I provides more details about our objectives, scope, and methodology. We performed our work from November 1997 to March 1998, in accordance with generally accepted government auditing standards.

## Results in Brief

Identity fraud may be an element in a variety of financial crimes. No federal agency has overall or primary jurisdiction for the investigation of such fraud. Identity fraud is difficult to track because there is no standardized definition. Also, the scope or types of identity fraud can range from unauthorized use of a credit card to total takeover of a person's identity. Generally, the law enforcement officials we contacted told us that their respective agencies historically have not tracked identity fraud.

We found no comprehensive statistics on the prevalence of identity fraud, although we did obtain limited statistics from selected federal agencies. Several sections of the U.S. Code closely related to identity fraud appear to be section 1028 of title 18, which addresses fraud in connection with identification documents; section 1029 of title 18, which addresses fraud in connection with access devices (e.g., credit cards); and section 408 of title 42, which addresses misuse of SSNS in connection with fraud. The Executive Office for U.S. Attorneys provided data over the past 6 years for all 94 federal judicial districts that show the annual number of cases filed under these 3 statutes. For the most current year, 1997, the data show 387 cases involving code section 1028, 848 cases involving section 1029, and

305 cases involving section 406. However, this office's senior counsel advised us that these statistics do not capture cases prosecuted under other criminal statutes—such as mail fraud and bank fraud statutes—that involve elements of identity fraud.

A Secret Service official provided us arrest statistics for the agency's financial-crimes investigation cases considered to be directly associated with identity fraud. As reported by the Secret Service, arrests in these cases totaled 8,806, 8,686, and 9,455, respectively, for fiscal years 1995, 1996, and 1997.

Also, officials at SSA'S Office of the Inspector General told us that the agency's investigations of SSN misuse in connection with program fraud increased from 305 in fiscal year 1996 to 1,153 in fiscal year 1997. SSA officials said this increase was due, in part, to the agency's hiring of additional investigators. According to the Postal Inspection Service, another federal investigative agency, its arrests in fraud cases involving credit-card applications remained steady during fiscal years 1995 to 1997, while arrests involving change-of-address fraud—which involves the surreptitious diversion of a person's mail to addresses controlled by the criminals—more than doubled from 53 in fiscal year 1996 to 115 in fiscal year 1997. Also, Postal Inspection Service investigations show that identity fraud is perpetrated by organized criminal enterprises or groups and has a nationwide scope.

IRS Criminal Investigation Division officials told us IRS annually detects thousands of questionable refund schemes, many involving personal and business identity fraud. For 1993, for example, IRS reported detecting a total of 5,438 schemes that sought to obtain $137 million in refunds. The statistics that IRS reported for 1996 and 1997 were down considerably from the 1993 figures. However, for the first 9 months of 1997, the number of questionable refund schemes detected was higher than the 1996 total. We have previously reported that a major reason for the decrease in 1996 was because of a reduction in IRS staff.[1]

In the private sector, an official with Associated Credit Bureaus, Inc., told us that the occurrences of credit fraud appear to have increased. An official of Trans Union Corporation, one of the national credit bureaus, told us that two-thirds of all consumer inquiries to the company's Fraud Victim Assistance Department involve identity fraud. According to this official, the total number of inquiries increased from 35,235 in calendar

[1]Tax Administration: Earned Income Credit Noncompliance (GAO/T-GGD-97-105, May 8, 1997).

year 1992 to 522,922 in 1997. The official attributed this trend to company growth and outreach efforts to consumers as well as increasing occurrences of identity fraud.

Officials at VISA U.S.A., Inc., and MasterCard International, Inc., indicated that overall fraud losses from their member banks are in the hundreds of millions of dollars annually, but these losses constitute a small part (about 0.1 percent) of the banks' overall billing transactions processed. Nevertheless, an official from MasterCard told us that dollar losses relating to identity fraud represented about 96 percent of its member banks' overall fraud losses of $407 million in 1997.

A recent American Bankers Association survey of the bank-card industry reported that lost and stolen cards (excluding mail intercepts) represented the largest single source of fraud losses in 1996, which marked the sixth consecutive year of this trend. On average, nearly 113,000 lost and stolen credit cards and about 16,800 cases involving credit-card fraud were reported for each of the 10 large banks surveyed. The survey also noted that large banks had dollar losses averaging about $20 million per bank in 1996.

We found no comprehensive estimates of the costs of identity fraud. As previously mentioned, the two largest credit-card companies told us that their member banks' total fraud losses were several hundred million dollars each in 1997. A Secret Service official told us that actual losses—to the victimized individuals and institutions—associated with the agency's investigations of financial crimes involving identity fraud totaled $442 million in fiscal year 1995, $450 million in fiscal year 1996, and $745 million in fiscal year 1997. Moreover, officials at other federal law enforcement agencies we contacted said that identity fraud can be an element of various financial crimes. In this sense, the costs of identity fraud can be very high, even though not specifically quantifiable. Moreover, on an individual level, the "human" costs of identity fraud can be quite substantial. These costs include emotional costs, as well as various financial and/or opportunity costs. For example, the victims may be unable to obtain a job, purchase a car, or qualify for a mortgage.

Many of the officials we contacted said that Internet growth increases opportunities for criminal activity. While no one provided us any specific trend data, anecdotal evidence suggests that the Internet can be used for crimes relating to identity fraud. The federal law enforcement officials we

contacted recognized that Internet growth creates risks relating to identity fraud.

In recent years, concerns have been raised about such risks associated with computerized database services, an industry that is widely used by both public and private sector entities to locate or verify the identity of individuals. In 1997, with encouragement from the Federal Trade Commission, industry members adopted self-regulatory principles, which are to go into effect not later than December 31, 1998.

Regarding the amount of money credit bureaus earn from selling personal identifying information, an official with Associated Credit Bureaus, Inc., told us that members do not disclose revenue data, but aggregate figures are in the "tens of millions of dollars" annually. This official commented that restrictions on selling such information would have various adverse effects. He noted, for example, that restrictions would make it more difficult to authenticate a consumer's application data, thus increasing the creditor's risk of a fraudulent account being opened.

## Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to the Department of Justice, the Department of the Treasury, the Federal Trade Commission, the Postal Inspection Service, and the Social Security Administration. We received either written or oral comments during the period April 8 to 14, 1998.

We received written comments from the (1) Department of Justice, which indicated that the draft was reviewed by representatives of the Civil Division, Criminal Division, Executive Office for U.S. Attorneys, FBI, and Office of Justice Programs; (2) Postal Inspection Service; and (3) SSA. We received oral comments from (1) Treasury Department components, i.e., IRS and the Secret Service and (2) the Federal Trade Commission.

Generally, the various agencies provided technical comments and clarifications, which have been incorporated in this report where appropriate. Also, the Federal Trade Commission and SSA commented that the report could have a stronger emphasis on the human costs of identity fraud. We expanded our discussion of this topic in briefing sections I and IV.

We hope this information is helpful to you. And, as agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of issuance. We will then send copies of this briefing report to the Ranking Minority Member, Senate Special Committee on Aging; the Chairman, Subcommittee on Social Security, House Committee on Ways and Means; the Chairman and the Ranking Minority Member, Subcommittee on Social Security and Family Policy, Senate Committee on Finance; the Attorney General; the Director, FBI; the Under Secretary of the Treasury (Enforcement); the Director, U.S. Secret Service; the Commissioner of Internal Revenue; the Commissioner, Social Security Administration; the Chief Postal Inspector, U.S. Postal Inspection Service; the Chairman, Federal Trade Commission; the Director, Office of Management and Budget; and other interested parties. We will also make copies available to others on request.

Major contributors to this briefing report are listed in appendix II. If you have any questions about the information in this report, please call me on (202) 512-8777.

Richard M. Stana
Associate Director
Administration of Justice Issues

# Contents

**Abbreviations**

| | |
|---|---|
| FBI | Federal Bureau of Investigation |
| IRS | Internal Revenue Service |
| SSA | Social Security Administration |
| SSN | Social Security number |

# Introduction and Background

## GAO Identity Fraud

- Involves the use of personal identifying information to commit fraud
- Can range from unauthorized use of a credit card to comprehensive takeover of another person's identity
- Can result in the loss of assets or creditworthiness
- Can claim many victims

# Identity Fraud

There is no one universally accepted definition of identity fraud. Typically, identity fraud refers to the illegal use of personal identifying information—such as name, address, Social Security number (SSN), and date of birth—to commit financial fraud. Identity fraud can encompass a host of crimes, ranging from the unauthorized use of a credit card to a comprehensive takeover of another person's identity and financial accounts. In short, an identity thief can fraudulently use personal identifying information to take over a person's identity and open new accounts; apply for loans, credit cards, and social benefits; rent apartments and establish services with utility companies; and engage in many other types of fraudulent activities, which can result in the loss of assets or creditworthiness.

Identity fraud can claim many victims. Credit grantors, such as banks and retail merchants, can be victims because they finance the selling of goods and services that ultimately are not paid for. The individuals whose identities are stolen are victims too, even though they may be protected in some instances from personal financial loss—e.g., by insurance coverage or credit card maximum-loss and/or reimbursement provisions. Even if they have no out-of-pocket costs, individual victims can nonetheless suffer from injuries to their reputations and must undergo a sometimes very lengthy and agonizing process of clearing up their credit history. In the interim, these individuals may be unable to keep or find a job, obtain a home mortgage, or secure other time-critical loans, such as tuition loans for college-age children.

## GAO Briefing Objectives

To provide information on

- law enforcement responsibilities and tracking of identity fraud
- prevalence and costs of identity fraud
- identity fraud and the Internet
- credit bureau perspectives on selling personal identifying information

## Briefing Objectives

The objectives of this briefing report are to provide information on the following issues and questions related to identity fraud:

Law enforcement responsibilities and tracking. (1) What government agency, if any, has primary jurisdiction for investigating identity fraud crimes? (2) From the law enforcement viewpoint, what are the difficulties in tracking the extent of identity fraud; e.g., is such tracking feasible?

Prevalence of identity fraud. (1) How many identity-fraud cases occur in the United States every year? (2) By what percentage have identity-fraud claims increased over the last 5 years?

Costs of identity fraud. (1) How much does identity fraud cost federal and state governments, businesses, credit bureaus, and individuals?

Identity fraud and the Internet. (1) How has the growth of the Internet contributed to trends in the reported or estimated cases of identity fraud? (2) What is the extent or status of industry self-regulation regarding computerized database services ("individual reference services") that collect and disseminate personal identifying information about consumers?

Also, although not specifically related to identity fraud, we were asked to address two questions about selling personal identifying information: (1) How much money do credit bureaus earn from selling personal identifying information, such as SSNS and dates of birth? (2) How would businesses or commerce be affected if credit bureaus could not sell personal identifying information?

## GAO Scope and Methodology

- We contacted officials and obtained available documentation at
  - selected federal and state agencies;
  - national credit bureaus and credit-card companies; and
  - various research, consumer interest, privacy rights, and other groups
- We did not independently verify agency and company information

## Scope and Methodology

In developing information on the issues and questions, we conducted a literature search and contacted law enforcement or other officials of

- selected federal agencies, including the Federal Bureau of Investigation (FBI), the Executive Office for U.S. Attorneys, the Social Security Administration's (SSA) Office of the Inspector General, the Secret Service, the Internal Revenue Service's (IRS) Criminal Investigation Division, the Postal Inspection Service, and the Federal Trade Commission, and two states, Arizona and California, that have enacted identity fraud legislation in recent years;
- the three national credit bureaus (Equifax, Inc.; Experian Corporation; and Trans Union Corporation); three major credit-card companies (American Express Company; MasterCard International, Inc.; and VISA U.S.A., Inc.); and
- various research, consumer interest, privacy rights, and other groups.

Given the number and scope of the issues and questions, we did not undertake any detailed or comprehensive analyses of the information provided. Rather, our work generally consisted of (1) synthesizing information from existing studies, reports, or other publications and (2) interviewing relevant public and private sector officials, as indicated above, to obtain available statistics, other applicable documentation, and testimonial evidence. We did not independently verify the accuracy of the statistical and other information provided us by the various public and private entities. Appendix I provides more details about our objectives, scope, and methodology.

# Law Enforcement Responsibilities and Tracking

## GAO Federal Agencies' Responsibilities Regarding Identity Fraud

- No one federal agency has primary jurisdiction regarding identity fraud; rather, several have a role
  - Secret Service
  - FBI
  - SSA
  - IRS
  - Postal Inspection Service

## Federal Agencies' Responsibilities Regarding Identity Fraud

According to the law enforcement officials we interviewed, identity fraud can be an element in a variety of financial crimes, such as bank fraud, credit-card fraud, social program fraud, tax refund fraud, and mail fraud. Thus, while the Secret Service has primary jurisdiction for investigations involving credit-card fraud, we found that no federal agency has overall jurisdiction regarding identity fraud. Rather, various agencies can have a role in investigating identity fraud as an enabling crime that resulted in another crime for which they had jurisdiction. These agencies, in addition to the Secret Service's Financial Crimes Division, include the FBI, the Social Security Administration's Office of the Inspector General, the IRS' Criminal Investigation Division, and the Postal Inspection Service.

## GAO Selected Federal Statutes That Address Identity Fraud

- Fraud and related activity in connection with identification documents (18 U.S.C. 1028)
- Fraud and related activity in connection with access devices (18 U.S.C. 1029)
- Misuse of (with intent to deceive) a Social Security number (42 U.S.C. 408(a)(7))
- Various other statutes

While identity fraud may be an element of various types of financial crimes, at least three sections of the U.S. Code address identity fraud—18 U.S.C. 1028, 18 U.S.C. 1029, and 42 U.S.C. 408(a)(7).

Under section 1028, title 18 of the U.S. Code, it is a criminal offense (punishable by up to 15 years in prison, or a fine, or both) to, among other things, knowingly possess with intent to use unlawfully or transfer unlawfully five or more identification documents or false identification

documents. As used in this section, the term "identification document" is defined to mean a document (1) made or issued by or under the authority of the U.S. government, a state, a political subdivision of a state, or certain other governmental and quasi-governmental entities and (2) which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification.

Under section 1029, title 18 of the U.S. Code, it is a criminal offense (punishable by up to 15 years in prison, or a fine, or both) to, among other things, knowingly and with intent to defraud, traffic in or use one or more unauthorized access devices (such as credit cards) during any 1-year period and by such conduct obtain anything of value aggregating $1,000 or more during that period.

Under section 408(a)(7), title 42 of the U.S. Code, a penalty for up to 5 years in prison, or a fine, or both, can result from, among other things, falsely representing—with intent to deceive—a number as the Social Security account number assigned by the Commissioner of Social Security to him or to another person.

The above is not an all-inclusive listing of U.S. Code sections relating to identity fraud. For example, other statutory provisions that could involve elements of identity fraud include 18 U.S.C. 287 (false, fictitious or fraudulent claims), 18 U.S.C. 1341 (mail frauds and swindles), 18 U.S.C. 1342 (fictitious names or address), 18 U.S.C. 1343 (fraud by wire, radio, or television), and 18 U.S.C. 1344 (bank fraud).

## GAO Difficulties in Tracking Identity Fraud

- Scope of identity fraud makes it difficult to define and track
  - Agencies historically have not tracked identity fraud; rather, it has been viewed as an element of other crimes
- Some agencies are beginning to track certain types of identity fraud

Identity fraud is difficult to track. Generally, the law enforcement officials we contacted told us that their respective agencies historically have not tracked identity fraud for various reasons. One reason is the lack of a standardized definition of identity fraud. Another reason is that identity fraud cuts across the statistical categories tracked by law enforcement agencies because it is an element of many crimes. A third reason is the mere possession of another person's personal identifying information is not a crime in itself. Rather, the use of that information to deceive is a

crime. As a result, law enforcement classifies its cases according to how the information is illegally used, rather than by the possession of someone's personal identifying information. In reference to bank-fraud investigations, for example, FBI officials told us that

- identity fraud may be an element of any given bank-fraud investigation. But, the FBI'S inquiries will focus on the primary or core violations, that is, the bank-fraud violations. In conducting and developing investigations, FBI agents may not specifically include identity fraud among the list of charges. Even if the use of false identification documents is among the initial list of charges, there is a possibility that this charge could be dropped or negotiated away during the prosecutive process.

However, we found that two agencies—the Postal Inspection Service and the Secret Service—are attempting to track certain types of identity fraud. In fiscal year 1995, the Postal Inspection Service began tracking mail-theft cases involving fraudulent credit-card applications and change of addresses. In October 1997, also in reference to fraudulent credit-card activity, the Secret Service began tracking cases involving identity takeover. Later in this briefing, we present more details regarding the results of these tracking efforts.

GAO

## Selected State Legislation on Identity Fraud

- Two states have recently passed legislation making identity fraud a crime
  - Arizona (1996)
    - 89 court cases filed
  - California (1997)
    - no cases filed yet

We identified two states, Arizona and California, that have passed legislation criminalizing the act of taking the identity of another person.

Arizona Legislation. In 1996, Arizona passed legislation adding section 2708 to title 13, Arizona Revised Statutes. Under this new section, a person commits identity fraud by knowingly taking another person's name, birth date, or SSN without the consent of that person, with the intent of obtaining or using the person's identity for any unlawful purpose or for causing

financial loss to the person. Further, under Arizona's statute, taking the identity of another person is a class 5 felony, punishable with imprisonment of 1-1/2 years, plus a fine of not more than $150,000. According to an Arizona official, from the time of the 1996 enactment of the state's law to February 1998, 142 investigative cases have been forwarded by the police to county prosecutors, who have subsequently filed 89 court cases.

California Legislation. In 1997, California added section 530.5 to the California Penal Code. Section 530.5, which became effective January 1, 1998, makes it a public offense to (1) willfully obtain the personal identifying information of another person without the authorization of that person and (2) use that information to obtain, or attempt to obtain, credit, goods, or services in the name of another person without consent of that person. Under this law, "personal identifying information" is defined as the name, address, telephone number, driver's license number, SSN, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit-card number of an individual.

Conviction under section 530.5 is punishable by imprisonment in a county jail not to exceed 1 year, or a fine not to exceed $1,000, or both. According to a California official, at the time of our review, no cases had been filed under the new statute.

# Prevalence of Identity Fraud

## GAO Identity-Fraud Cases and Trends

- No comprehensive national statistics but some limited statistics from
  - five federal agencies: U.S. Attorneys, Secret Service, SSA, Postal Inspection Service, and IRS;
  - a national credit bureau and two major credit-card companies; and
  - American Bankers Association (bank-card industry survey)

We found no comprehensive national statistics on the prevalence of identity fraud collected by any organization in the public or private sectors. However, we did obtain limited statistics from five federal agencies, one of the three national credit bureaus, two major credit-card companies, and an American Bankers Association survey, which illustrate different ways that identity fraud is being reported:

- From the Executive Office for U.S. Attorneys, we obtained statistics on the number of cases filed under selected statutes related to identity fraud.
- From the Secret Service, we obtained arrest and cost statistics for financial crimes cases that agency officials considered to be directly associated with identity fraud.
- From the SSA, we obtained information on the number of investigations involving SSN misuse.
- From the Postal Inspection Service, we obtained information on the number of arrests in relevant types of mail-theft cases.
- From the IRS, we obtained information on certain questionable refund schemes.
- From a credit bureau, we obtained information on the volume of consumer inquiries relating to identity fraud.
- From two major credit-card companies, we obtained information on the amount of dollar losses relating to identity fraud by association members.
- From an American Bankers Association survey of the bank-card industry, we obtained information on credit-card fraud cases and dollar losses.

The following briefing charts respectively discuss each of these information sources, including the specific relevance of the information as an indicator of identity fraud.

GAO

# U.S. Attorneys: Cases Filed Under Statutes Related to Identity Fraud

| | Cases filed | | |
|---|---|---|---|
| Fiscal year | False identification documents (18U.S.C. 1028) | Unauthorized use of access devices (18U.S.C. 1029) | Misuse of SSNs (42 U.S.C. 408) |
| 1992 | 367 | 685 | 428 |
| 1993 | 384 | 804 | 447 |
| 1994 | 251 | 831 | 306 |
| 1995 | 332 | 964 | 344 |
| 1996 | 300 | 907 | 310 |
| 1997 | 387 | 848 | 305 |

Source: Data from Department of Justice.

## U.S. Attorneys: Cases Filed Under Statutes Related to Identity Fraud

For all types of federal crimes, the Department of Justice files about 40,000 criminal cases per year, according to the Senior Counsel, Executive Office for U.S. Attorneys. At our request, regarding three U.S. Code sections—sections 1028 and 1029 of title 18 and section 408 of title 42—the Executive Office for U.S. Attorneys provided us information showing the number of times each of the statutes was charged in a case in all federal judicial districts during fiscal years 1992 to 1997. Section 1028 deals with fraudulent activity in connection with identification documents; section 1029 deals with unauthorized use of access devices (e.g., credit cards); and section 408 deals with misuse of SSNS.

The number of times charges were filed under these U.S. Code sections includes all cases where the statute was used, although it may not have been the primary charge. In fiscal year 1997, the data show 387 cases involving code section 1028, 848 cases involving code section 1029, and 305 cases involving section 408. The Senior Counsel stated that these statistics do not reflect cases where the facts would reflect an identity fraud or have elements of such fraud but are prosecuted under mail fraud, wire fraud, and other statutes.

GAO

# Secret Service: Arrests and Costs Relating to Identity Fraud

- Financial crimes generally involve identity fraud, as reflected in arrests
- The 1997 increase in the costs of identity fraud is due to various reasons, such as a focus on high-dollar cases, better training of agents, and new opportunities for criminal activity presented by emerging technology

| Fiscal year | Total financial-crimes arrests | Financial-crimes arrests involving identity fraud | Costs of identity fraud (millions) |
|---|---|---|---|
| 1995 | 9,470 | 8,806 | $442 |
| 1996 | 9,220 | 8,686 | 450 |
| 1997 | 10,066 | 9,455 | 745 |

Source: Secret Service data.

## Secret Service: Arrests and Costs Relating to Identity Fraud

In response to our questions about the prevalence of identity fraud, a Secret Service official told us financial crimes generally involve identity fraud, which is reflected in the arrest statistics of the agency's Financial Crimes Division. For example, in fiscal year 1995, according to a Secret Service official, the Financial Crimes Division made a total of 9,470 arrests, of which 8,806 (93 percent) involved identity fraud. Similarly, the official reported that financial crimes arrests in fiscal year 1996 totaled 9,220, of which 8,686 (94 percent) involved identity fraud and that financial crimes arrests in fiscal year 1997 totaled 10,066, of which 9,455 (94 percent) involved identity fraud.

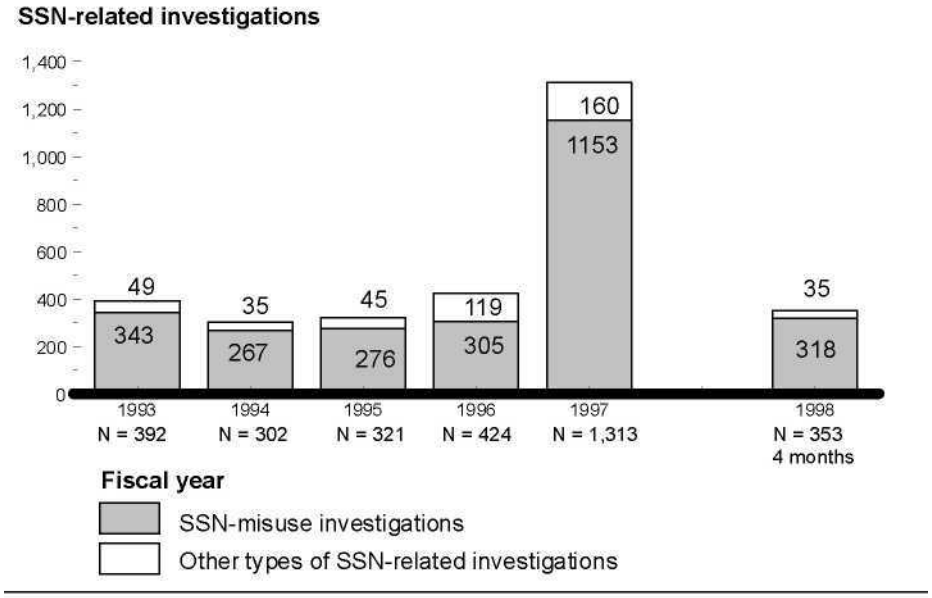
Also, according to a Secret Service official, the actual costs associated with these identity-fraud cases were $442 million, $450 million, and $745 million, respectively. The official explained that these figures represent the actual costs or losses to victimized individuals and financial institutions. Further, the official noted that the large increase from 1996 to 1997 is attributable to various reasons, such as the agency's efforts to focus on high-dollar cases, improved training for agents, and emerging technologies that create new opportunities for criminals.

Also, a Secret Service official told us that the agency has a lead role in 29 fraud-related task forces that have investigated numerous cases that involve identity fraud. The official noted that 12 of the 29 task forces focus primarily on organized criminal enterprises composed of an ethnic group widely engaged in fraudulent activities.

GAO

# Social Security Administration: SSN-Related Investigations

- SSN-related investigations usually involve identity fraud
- The number of SSN-related investigations has recently increased




Source: SSA data.

## Social Security Administration: SSN-Related Investigations

Officials at SSA'S Office of the Inspector General told us that the agency's SSN-related investigations consist of various categories that usually involve identity fraud. According to SSA officials, the largest category, "SSN misuse" investigations in connection with program fraud, almost always involves identity fraud. The number of SSN misuse investigations increased from 305 in fiscal year 1996 to 1,153 in 1997. SSA officials said this increase was due, in part, to the hiring of additional investigators after SSA became an independent agency in March 1995.

The officials told us that four other types or categories of SSN-related investigations are not restricted to but also involve identity fraud; these categories cover (1) counterfeiting of SSN cards, (2) trafficking in counterfeit cards, (3) trafficking in and selling SSN data, and (4) trafficking in legitimate SSN cards. The number of investigations in these four categories increased from 119 in fiscal year 1996 to 160 in fiscal year 1997. SSA officials said this increase was also due, in part, to the hiring of additional investigators.

## GAO Postal Inspection Service: Arrests

- Theft or diversion of mail contributes significantly to identity fraud
- Two arrest categories reflect identity-fraud cases
  - credit-card application fraud: arrests have stabilized
  - change-of-address fraud: arrests have increased over the past 2 years and continue to climb in fiscal year 1998

At our request, in reference to mail theft, diversions, or other misuse, the Postal Inspection Service's Office of Criminal Investigations provided us an overview of its investigative activities and its perspectives regarding the extent of identity fraud. According to the Postal Inspection Service

- the theft or diversion of mail contributes significantly to the problems of identity fraud. Nearly all mail-theft cases in which a financial transaction

device (e.g., credit card) or document is stolen can lead to a legitimate person's credit history and name being assumed.

- Identity-fraud crimes most often are synonymous with the compromise of a person's credit history. About 2 years ago, the Service began tracking its investigations involving the submission of fraudulent credit applications that result in the issuance of a credit card. More recently, the Service began to track criminal activity associated with change-of-address fraud, which involves the surreptitious diversion of a legitimate person's mail to addresses controlled by criminals, such as private mail boxes at Commercial Mail Receiving Agencies. These two arrest categories (credit-card application fraud and change-of-address fraud) most closely measure the Postal Inspection Service's activity regarding identity-fraud cases.
- Regarding the first category, fraud involving credit-card applications, the Service has seen a stabilized pattern of activity over the last 3 fiscal years, 1995 to 1997. During the first 4 months of fiscal year 1998, arrests in this category totaled 48, down from the total of 59 arrests for the first 4 months of fiscal year 1997.
- However, arrests in the other category (change-of-address fraud) have more than doubled in recent years, from 53 in fiscal year 1996 to 115 in 1997. Moreover, during the first 4 months of fiscal year 1998, arrests in this category totaled 54, up from the total of 33 arrests for the first 4 months of fiscal year 1997.

## GAO Postal Inspection Service: Organized Crime Involved in Identity Fraud

- Criminal enterprises involved in identity fraud are nationwide in scope
- Identity-fraud activity is used to finance drug trafficking
- Crime rings have caused losses in the millions of dollars
- Postal Inspection Service has responded to the threat by forming task forces with other law enforcement agencies

## Postal Inspection Service: Organized Crime Involved in Identity Fraud

Investigations conducted by the Postal Inspection Service show that organized criminal activity involving identity fraud has a nationwide scope. To illustrate, the following is a paraphrased description of selected case summaries presented in a 1997 report.[1]

- Investigations of criminal enterprises consume many Inspection Service resources. For theft of mail and related offenses, arrests were made in various cities across the United States, including Atlanta, Boston, Chicago, Jacksonville, Houston, Miami, New Orleans, Newark, New York, Philadelphia, San Francisco, and Tampa.
- Mail theft and credit-card fraud activity frequently support drug trafficking. Large amounts of money may be obtained through such fraud.
- A sophisticated crime ring involving the theft of identities of credit-worthy individuals, and the subsequent use of fraudulently obtained credit cards, was investigated in New York. Losses to the card-issuing banks were over $1.8 million.
- The Postal Inspection Service has combined its resources with other law enforcement agencies to form task forces in 10 U.S. cities. Postal inspectors participating in a task force in Florida assisted in arresting 32 people suspected of working in a credit-card fraud ring responsible for losses of at least $1.5 million.

An official of the Postal Inspection Service told us that often the illegally diverted mail in identity-fraud schemes is sent to private mail boxes located at Commercial Mail Receiving Agencies rented by the criminals.

[1]U.S. Postal Service, Office of Inspector General, Semiannual Report to Congress (fiscal year 1997, Vol.1), Oct. 1, 1996 - Mar. 31, 1997, p. 25-26.

# GAO IRS: Questionable Refund Schemes Detected

- Questionable refund schemes have a high frequency of identity fraud
- A major reason for the decrease in schemes detected in 1996 was a reduction in IRS staff

| Calendar year | Total questionable schemes | Questionable returns detected | Refunds claimed (millions) | Refunds stopped (millions) |
|---|---|---|---|---|
| 1993 | 5,438 | 77,840 | $137 | $102 |
| 1994 | 5,344 | 77,781 | 161 | 117 |
| 1995 | 4,487 | 62,309 | 132 | 83 |
| 1996 | 2,458 | 24,919 | 82 | 69 |
| 1997 (9 months) | 2,470 | 24,780 | 88 | 79 |

Source: IRS data.

## IRS: Questionable Refund Schemes Detected

IRS Criminal Investigation Division officials told us IRS annually detects thousands of questionable refund schemes, many of which involve personal and business identity fraud. For example, the officials described one scheme whereby an individual fraudulently used the actual SSNS of 1,000 students to file refund-due tax returns.

For calendar years 1993 through 1997, IRS provided us statistics covering all questionable refund schemes that IRS classified as involving a "high frequency" of identity fraud. In 1993, for example, IRS detected a total of 5,438 schemes, consisting of 77,840 questionable tax returns that claimed a total of $137 million in refunds. According to IRS officials, the agency's detection efforts prevented payment of $102 million of the claimed refunds.

The number of schemes detected—and the related statistics—decreased after 1995. For instance, the number of questionable schemes detected in 1996 was 2,458, down considerably from the 4,487 schemes detected in 1995. However, for the first 9 months of 1997, the number of questionable refund schemes detected was higher than the 1996 total. We have previously reported that a major reason for the decrease in 1996 was a reduction in IRS staff.[2]

[2]Tax Administration: Earned Income Credit Noncompliance (GAO/T-GGD-97-105, May 8, 1997).

# GAO Three National Credit Bureaus' Fraud Units: Overview

- The three national credit bureaus have fraud units and toll-free number access
- One bureau tracks some fraud; the other two may begin, depending on the costs

| National Credit Bureaus | When was fraud unit created? | When was toll-free number available? | Has fraud unit grown since inception? | Does the unit track fraud statistics? |
|---|---|---|---|---|
| Equifax | 1992 | 1994 | ■ | □ |
| Experian | 1995 | 1995 | ■ | □ |
| Trans Union | 1992 | 1994 | ■ | ■ [a] |

■ Yes □ No

[a]Some data are tracked.

Source: Data from Associated Credit Bureaus, Inc.

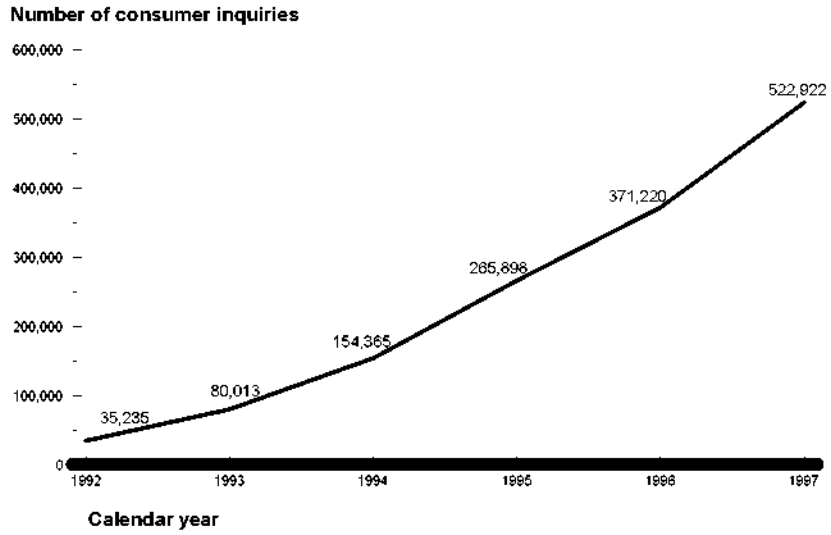
## Three National Credit Bureaus' Fraud Units: Overview

The Vice President of Associated Credit Bureaus, Inc., provided us overview information on the fraud units of the three national credit bureaus—Equifax, Inc.; Experian Corporation; and Trans Union Corporation. The overview information covered, for example, the year that the respective fraud unit was created and the year that a toll-free number was available to consumers. According to this official, all of the fraud units have increased their staffing levels in recent years due to various reasons, including more referrals from the creditor community and a greater incidence of credit fraud.

Also, this official commented that one national bureau does track some fraud statistics, but the other two national bureaus do not. He added that, the three bureaus may be willing to consider the feasibility of systematically and consistently tracking various forms of fraud, including identity fraud, if the value of such an effort outweighs the costs.

# GAO A Credit Bureau: Identity-Fraud Inquiries

- Constitute about two-thirds of consumer inquiries to Trans Union Corporation
- Upward trend due to company growth, improved outreach, and increasing identity fraud




Source: Data from Trans Union Corporation.

## A Credit Bureau: Identity-Fraud Inquiries

A Trans Union official told us that the total number of consumer inquiries to Trans Union each year can be classified into three categories, with each having about one-third of the total inquiries. According to the Trans Union official, all inquiries in two of the three categories involve identity fraud. One category is what Trans Union calls "true person fraud." This category covers incidents whereby someone assumes a "true" person's identity and applies for credit using that identity. A second category is account takeover fraud, which covers incidents involving fraudulent access to an existing account. The final or third category is labeled "precautionary." This category, according to the Trans Union official, consists of inquiries from consumers who would rather be safe than sorry.

According to a Trans Union official, the total number of consumer inquiries to the company's Fraud Victim Assistance Department has increased significantly over time, rising from 35,235 in 1992 to 522,922 in 1997. The Trans Union official attributed this upward trend to various factors, including company growth and outreach efforts to consumers as well as increasing occurrences of identity fraud.

The other two national credit bureaus were unable to provide us information about consumer inquiries relating to identity fraud.

## GAO VISA: Perspectives on Identity-Fraud Prevalence

- In 1997, U.S. fraud losses of VISA member banks totaled $490 million or about 0.1% of billing transactions ($505 billion)
  - fraudulent applications accounted for about 5% of fraud losses
  - account takeovers accounted for about 6% of fraud losses
- Losses from fraudulent applications have declined due to antifraud efforts

Source: Data from VISA U.S.A., Inc.

## VISA: Perspectives on Identity-Fraud Prevalence

According to an official we contacted at VISA U.S.A., Inc., within the credit-card business, there is no standardized or industrywide definition of identity fraud. In response to our inquiries about the prevalence or significance of identity fraud, the VISA official told us that

- VISA member banks' fiscal year 1997 fraud losses in the United States totaled $490 million, or about 0.097 percent of the banks' business volume, as measured by the value of billing transactions processed ($504.9 billion).
- VISA has six categories of fraud losses, each of which could have elements of identity fraud. Of the six categories, "fraudulent applications" most closely involve identity fraud. For fiscal year 1997, this category represented about 5 percent of VISA member banks' total fraud losses in the United States.
- Another of the six categories is "account takeovers," a category that VISA began using in fiscal year 1997. Generally, this type of fraud could be considered mail theft, in that one person may steal another's mail, which could include a credit-card application. The thief may then request a change of address. For fiscal year 1997, the account takeover category represented about 6 percent of VISA member banks' total fraud losses.
- The fraudulent applications component of 1997 fraud losses is about 19.5 percent lower than for fiscal year 1996. VISA attributes this decline in losses to its antifraud efforts, which include development of fraud detection and avoidance programs as well as close cooperation with law enforcement.

## GAO MasterCard: Perspectives on Identity-Fraud Prevalence

- In 1997, worldwide fraud losses of Mastercard member banks totaled $407 million or about 0.11% of billing transactions ($365 billion)
- Of the total fraud losses, about 96% involved identity fraud
- MasterCard considers identity-fraud losses to be a significant part of overall fraud losses

Source: Data from MasterCard, Inc.

## Mastercard: Perspectives on Identity-Fraud Prevalence

In response to our inquiries about the prevalence or significance of identity fraud, an official at MasterCard International, Inc., commented substantially as follows:

- In calendar year 1997, MasterCard member banks' fraud losses worldwide totaled $407 million, which represented about 0.11 percent of the banks' billing transactions processed ($365 billion).
- About 96 percent of the $407 million total fraud losses involved identity fraud-related categories, such as account takeovers, fraudulent applications, counterfeit cards, and lost and stolen cards.

In summary, in terms of dollar losses, the MasterCard official said that identity fraud losses are a significant part of overall fraud losses. Another MasterCard official noted that identity fraud can have long-term negative impacts on consumers' purchasing power and, in turn, on business. Therefore, according to this official, MasterCard has taken steps in recent years to educate merchants about ways to perform identity checks.

## GAO American Bankers Association: Survey of Bank-Card Industry

- Loss/theft of credit cards (excluding mail intercepts) was the biggest single source of fraud losses (66 percent of cases and 49 percent of dollar losses) in 1996
- Counterfeiting, fraudulent applications, mail intercept, and account takeover had the proportionately greater dollar loss per case
- For large banks, the average number of stolen cards was 112,720; the average number of fraud cases was 16,801

Source: Data from American Bankers Association.

## American Bankers Association: Survey of Bank-Card Industry

The American Bankers Association surveyed the bank-card industry in 1997 and reported on various aspects of credit-card fraud, along with other issues. The survey covered banks of various sizes based on asset portfolios—community (58 banks), medium (11 banks), and large (10 banks).[3] According to the American Bankers Association's report, which presented information on the bank-card industry's 1996 financial fraud losses:

- For the sixth consecutive year, lost and stolen credit cards (excluding mail intercepts) was the biggest single source of fraud loss for all size banks in terms of both case volume and dollar losses. Counterfeit credit cards rose significantly for community banks while fraudulent applications became a more significant issue for medium banks.
- The average number of stolen credit cards reported for each of the 10 large banks surveyed was 112,720. The average number of credit-card fraud cases in 1996 for each large bank was 16,801. Certain credit-card fraud categories have a larger dollar impct than other categories. Among cases involving credit-card fraud at large banks, counterfeiting, fraudulent applications, intercept in mail, and account takeover accounted for 23 percent of the cases but 44 percent of the dollar losses. Lost and stolen credit cards made up 66 percent of the fraud cases but 49 percent of the dollar losses.

[3]According to an official of the American Bankers Association, community banks have less than $50 million in credit-card outstandings or less than 50,000 credit-card accounts with balances (58 banks); medium banks have $50 million to $749 million in credit-card outstandings or 50,000 to 749,000 credit-card accounts with balances (11 banks); and large banks have $750 million or greater in credit-card outstandings or 750,000 or more credit-card accounts with balances (10 banks).

# Costs of Identity Fraud

## GAO Identity-Fraud Costs Are Difficult to Determine

- No comprehensive or agreed-upon way to estimate economic costs
- Some sectors report relatively low costs
- Costs could be high if identity fraud is an element of many financial crimes
- Human costs can be substantial

We did not find any comprehensive estimates of the costs of identity fraud—to either the federal or state governments, businesses, credit bureaus, or individuals. Some information is available, but difficulties in estimating costs are compounded by limited tracking of the prevalence of identity fraud and lack of agreement on a definition of such fraud.

In 1997, the Federal Reserve Board reported that (1) fraud involving use of sensitive identifying information is often not tracked separately from other

types of fraud and (2) although anecdotal information seems to suggest that this type of fraud is increasing, these losses likely play a relatively small role in overall fraud losses and pose no significant threat to insured depository institutions.[1]

The American Bankers Association reported in its 1997 survey of the bank-card industry that credit-card fraud losses for 10 large banks averaged about $20 million per bank in 1996. Also, a Secret Service official told us that actual losses—to the victimized individuals and financial institutions—associated with the agency's investigations of financial crimes involving identity fraud totaled $745 million in fiscal year 1997. Other law enforcement officials said that identity fraud can be an element of various financial crimes and the costs can be substantial.

On an individual level, the "human" costs of identity fraud should be acknowledged. Emotional costs are associated with identity-fraud incidents as well as the time and effort required to repair a compromised credit-history. One Secret Service field agent told us that victims of identity fraud feel they have been violated. Although not easily quantified, the financial and/or opportunity costs to victims can also be substantial. For example, the victims may be unable to obtain a job, purchase a car, or qualify for a mortgage.

[1]Board of Governors of the Federal Reserve System, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud, (Mar. 1997).

# Identity Fraud and the Internet

## GAO The Growth of the Internet Creates Identity-Fraud Risks

- The Internet creates risks by providing access to personal identifying information
- Internet Fraud Watch had no specific trend data
- Law enforcement had no specific trend data but recognizes the risks

Many of the officials we contacted said that Internet growth, which enhances the availability and accessibility of personal identifying information, obviously creates greater risks or opportunities for criminal activity, including identity fraud. However, in February 1998, the Director of the Internet Fraud Watch,[1] testified that no one, including the Internet

[1]The Internet Fraud Watch was created in 1996 by the National Consumers League to operate in tandem with the League's National Fraud Information Center.

Fraud Watch, knows the full extent of Internet fraud.[2] According to the Director's testimony, the Internet Fraud Watch received a total of 1,152 reports of possible Internet fraud in 1997, which represented a threefold increase over 1996. Also, regarding the 1997 reports, the Director listed the top 10 types of Internet fraud. In reviewing this list, we found no specific mention of identity fraud-related crimes or scams. However, additional testimony at the February 1998 hearing included anecdotal information illustrating that the Internet can be used for identity fraud-related crime.

Further, although the federal law enforcement officials we contacted had no specific trend data, they recognized that Internet growth creates identity fraud-related risks. Secret Service officials told us, for example, that numerous instances of identity fraud have been perpetrated using the Internet. These officials opined that, without effective encryption measures, Internet-related identity fraud will increase.

Also, at an earlier congressional hearing (September 1997), an FBI official testified that:

"Technological advances have also facilitated 'identity theft,' the availability and misuse of electronic account and personal information. Identity theft poses significant risks to financial institutions and individuals alike. The Internet is also engendering other bank-related frauds."[3]

[2]Statement of Susan Grant, Director, National Fraud Information Center, in a hearing on Fraud on the Internet: Scams Affecting Consumers, held by the Permanent Subcommittee on Investigations, Governmental Affairs Committee, U.S. Senate, Feb. 10, 1998.

[3]Statement of Charles L. Owens; Chief, Financial Crimes Section, FBI; in a hearing on Financial Instrument Fraud held by the Subcommittee on Financial Services and Technology; Committee on Banking, Housing, and Urban Affairs; U.S. Senate; Sept. 16, 1997.

## GAO Status of Self-Regulation in the "Individual Reference Services" Industry

- Federal Trade Commission encouraged the industry to develop self-regulatory principles
  - no distribution of certain personal identifiers to the general public
  - industry members to undergo annual compliance reviews
- Principles go into effect not later than December 31, 1998

## Status of Self-Regulation in the "Individual Reference Services" Industry

Computerized database services—frequently referred to as "individual reference services" or "look-up services"—are used widely by both public and private sector entities to locate or verify the identity of individuals. These services—which collect and disseminate personal identifying information—have raised privacy rights issues as well as concerns about increased risks of identity fraud.

In 1997, the Federal Trade Commission began working with industry representatives (the Individual Reference Services Group) to encourage adoption of a self-regulatory framework. The results of this effort are presented in a December 1997 report to Congress.[4] As reported, the Individual Reference Services Group developed and agreed to implement a set of self-regulatory principles. Among other things, the principles prohibit distributing certain nonpublic information (e.g., SSN, mother's maiden name, and date of birth) to the general public.[5] Also, industry members agreed to undergo an annual compliance review by a third party.

The self-regulatory principles are to go into effect not later than December 31, 1998. Thus, at the time of our inquiry, a Federal Trade Commission official told us it was too soon to measure or determine the effectiveness of the principles. However, the official said that the principles show promise because they contain provisions not normally seen in other self-regulating efforts.

[4]Federal Trade Commission, Individual Reference Services - A Report to Congress, Dec. 1997.

[5]The principles do not restrict the sale of this information obtained from public sources, such as state departments of motor vehicles, according to an official at the Federal Trade Commission.

# Perspectives on Selling Personal Identifying Information

GAO Selling Personal Identifying Information: No Prohibition; Millions of Revenue Dollars

- Credit bureaus are not statutorily prohibited from selling personal identifying information
- The proposed Personal Information Privacy Act of 1997 (H.R. 1813) would prevent credit bureaus from selling lists with personal identifying information
- Credit bureau aggregate revenues are in the tens of millions of dollars annually

## Selling Personal Identifying Information: No Prohibition; Millions of Revenue Dollars

According to the Federal Trade Commission, credit bureaus are not statutorily prohibited from releasing or selling noncredit-related, consumer-identifying information. Such information—commonly referred to as "credit header" information in reference to the top portion of a credit-history report—typically consists of an individual's name, aliases, birth date, SSN, and current and previous addresses. In a March 1997 report to the Congress, the Board of Governors of the Federal Reserve System also noted that consumer reporting agencies are not restricted from selling this header information.[1]

The proposed Personal Information Privacy Act of 1997, H.R. 1813, which was introduced in the 105th Congress, is intended to protect consumers' privacy by preventing credit bureaus from selling any identifying information of the consumer except the name, address, and telephone number if listed in a telephone directory. The bill would also prohibit the use of SSNS for commercial purposes without the prior written consent of the consumer. Further, H.R. 1813 would restrict the release of SSNS by state Departments of Motor Vehicles.

In response to our inquiry about how much revenue is earned from the selling of personal identifying information, an official with Associated Credit Bureaus, Inc., told us that pricing strategies are proprietary and members do not share revenue data on specific product lines. However, the official stated that aggregate revenues are in the "tens of millions of dollars" annually.

[1]Board of Governors of the Federal Reserve System, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud (Mar. 1997), submitted pursuant to section 2422 of the Economic Growth and Regulatory Paperwork Reduction Act of 1996.

## GAO Restriction on Sale of Personal Identifying Data Could Affect Business/Commerce

- Such information is widely used for many purposes
- "Instant credit" is said to fuel the economy
- Credit bureaus say that verifying the accuracy of account information would be more difficult if sale of personal identifying information is restricted

## Restriction on Sale of Personal Identifying Data Could Affect Business/Commerce

The scope of our work did not permit a comprehensive or quantitative answer to the question of how businesses or commerce would be affected if personal identifying information could not be sold. Quite obviously, however, personal identifying information has a market value, and such information is widely used for many purposes within both the public and private sectors. The insurance industry, for instance, accesses databases of personal identifying information to investigate potentially fraudulent claims. Also, credit grantors in the retail industry use such information to confirm the identity of credit applicants. Some observers say that the resulting "instant credit" plays a significant role in the continuing robustness of the economy. Law enforcement agencies also use this information in the investigation and prosecution of financial crimes.

An official with Associated Credit Bureaus, Inc., told us that some proposals to limit the availability of SSNS and other personal identifying information would make it more difficult to authenticate a consumer's application data, thus increasing the risk of a fraudulent account being opened.

# Objectives, Scope, and Methodology

By letters dated February 26, 1998, September 30, 1997, and June 23, 1997, respectively, the Chairman, Senate Special Committee on Aging; the Ranking Minority Member, Subcommittee on Social Security, House Committee on Ways and Means; and Representative Gerald D. Kleczka asked us to review various issues related to identity fraud. Specifically, our review focused on the following issues and questions:

Law enforcement responsibilities and tracking. (1) What government agency, if any, has primary jurisdiction for investigating identity-fraud crimes? (2) From the law enforcement viewpoint, what are the difficulties in tracking the extent of identity fraud; e.g., is such tracking feasible?

Prevalence of identity fraud. (1) How many identity-fraud cases occur in the United States every year? (2) By what percentage have identity-fraud claims increased over the last 5 years?

Costs of identity fraud: (1) How much does identity fraud cost the federal and state governments, businesses, credit bureaus, and individuals?

Identity fraud and the Internet: (1) How has the growth of the Internet contributed to trends in the reported or estimated cases of identity fraud? (2) What is the extent or status of industry self-regulation regarding computerized database services ("individual reference services") that collect and disseminate personal identifying information about consumers?

Also, although not specifically related to identity fraud, we were asked to address two questions about the selling of personal identifying information: (1) How much money do credit bureaus earn from selling personal identifying information, such as SSNs and dates of birth? (2) How would businesses or commerce be affected if credit bureaus could not sell personal identifying information?

## Overview of Our Scope and Methodology

To address these issues and questions, we conducted a literature search; and we contacted federal law enforcement officials and officials of (1) other relevant federal agencies; (2) two states, Arizona and California, that have enacted identity-fraud statutes in recent years; (3) credit bureaus and credit-card companies; and (5) various research, consumer interest, privacy rights, and other groups. See table I.1 at the end of this appendix for a list of the public and private sector entities we contacted.

Given the number and scope of the issues and questions, we did not undertake any detailed or comprehensive analyses of the information provided. Rather, our work generally consisted of (1) synthesizing information from existing studies, reports, or other publications and (2) interviewing relevant public and private sector officials, as previously indicated, to obtain available statistics, other applicable documentation, and testimonial evidence. We did not independently verify the accuracy of the statistical and other information provided us by the various public and private entities.

## Literature Search

We conducted a literature search to identify published articles, reports, studies, and other documents dealing with the various issues. Some of the more recent, relevant materials we identified are the following:

- Board of Governors of the Federal Reserve System, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud, March 1997.
- Federal Trade Commission, Individual Reference Services - A Report to Congress, December 1997.
- Fraud on the Internet: Scams Affecting Consumers, hearing before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, February 10, 1998.
- U.S. Public Interest Research Group, Theft of Identity II: Return to the Consumer X-Files, September 1997.

## Federal Agencies Contacted

Within the Department of Justice, we contacted the Executive Office for U.S. Attorneys to obtain statistics regarding the number of cases filed under selected statutes related to identity fraud. That office provided us data for fiscal years 1992 through 1997 for all federal judicial districts. Also, we contacted the Federal Bureau of Investigation to determine whether it had any investigation statistics or other information regarding identity fraud.

Within the Department of the Treasury, we contacted the Internal Revenue Service's Criminal Investigation Division and obtained statistics on questionable refund schemes detected from January 1, 1993, through September 30, 1997. Also, we contacted the U.S. Secret Service to determine whether it had any investigation statistics or other information regarding identity fraud.

We contacted the Social Security Administration's Office of the Inspector General to obtain statistics on investigations involving (1) misuse of Social Security numbers and (2) other types of identity fraud-related cases. The Office of the Inspector General provided us relevant investigation statistics covering fiscal years 1993 through 1997, plus the first 4 months of fiscal year 1998.

We contacted the Postal Inspection Service to obtain arrest statistics for mail theft or mail diversion cases involving identity fraud. The Inspection Service provided us statistics for two relevant categories—credit-card application fraud and change-of-address fraud. However, trend data are limited in that the Service could not provide us arrest data in both categories for periods before fiscal year 1996. Also, we reviewed the agency's recent semiannual reports, which presented case summaries of investigations showing that organized criminal activity involving identity fraud has a nationwide scope.

We contacted the Federal Trade Commission to obtain its views on related issues. In particular, however, we were interested in the Commission's views on questions regarding identity fraud and the Internet.

## State and Local Government Agencies Contacted

To determine which states had enacted identity-fraud laws, we contacted the Council of State Governments (Washington, D.C.) and the National Conference of State Legislatures (Denver, CO). We then contacted officials in Arizona and California, the two states identified as having enacted applicable laws in recent years. In so doing, among other inquiries, we asked about the availability of any state or local data showing the prevalence or costs of identity fraud.

## Credit Bureaus Contacted

We contacted the three national credit bureaus—Equifax, Inc.; Experian Corporation; and Trans Union Corporation—to obtain information on related issues. Similarly, we contacted Associated Credit Bureaus, Inc., a trade association with membership consisting of 661 credit reporting agencies and more than 650 mortgage reporting and collection services companies.

## Credit-Card Companies Contacted

We contacted the three largest credit card companies—American Express Company; MasterCard International, Inc.; and VISA U.S.A., Inc.—to obtain information on related issues. According to an industry representative,

based upon the total number of credit and debit cards issued worldwide, the two largest companies are VISA (1 billion cards) and MasterCard (850 million cards), followed by American Express (40 million cards) and Discover (35 million cards).

## Other Groups Contacted

Also, as table I.1 shows, we contacted various research, consumer interest, privacy rights, and other groups. Generally, we asked for relevant information regarding all of the issues.

**Table I.1: Organizations Contacted by GAO**

| |
|---|
| **Federal government agencies:** |
| Board of Governors of the Federal Reserve System (Washington, D.C.) |
| Department of Justice (Washington, D.C): |
| —Executive Office for U.S. Attorneys |
| —Federal Bureau of Investigation |
| Department of the Treasury (Washington, D.C): |
| —Internal Revenue Service |
| —Secret Service |
| Federal Trade Commission (Washington, D.C.) |
| Social Security Administration (Baltimore, MD) |
| U.S. Postal Inspection Service (Washington, D.C.) |
| State and local government agencies: |
| Arizona: |
| —Arizona State Legislature (Phoenix, AZ) |
| —Arizona Law Library (Phoenix, AZ) |
| —Association of Arizona County Attorneys |
| California: |
| —Anaheim Police Department (Anaheim, CA) |
| —Los Angeles County District Attorney's Office |
| —Los Angeles City Housing Authority Police Department |
| Council of State Governments (Washington, D.C.) |
| National Conference of State Legislatures (Denver, CO) |
| Credit bureaus: |
| Associated Credit Bureaus, Inc. (Washington, D.C.) |
| Equifax, Inc. (Atlanta, GA) |
| Experian Corporation (Orange, CA) |
| Trans Union Corporation: |
| —Fraud Victim Assistance Department (Fullerton, CA) |
| —Department of Consumer Relations (Cleveland, OH) |

(continued)

**Federal government agencies:**

—Office of General Counsel (Chicago, IL)

Credit-card companies:

American Express Company (Los Angeles, CA) (New York, NY)

MasterCard International, Inc. (Huntington Beach, CA)

VISA U.S.A., Inc. (McLean, VA)

Research, consumer interest, privacy rights, and other groups:

American Bankers Association (Washington, D.C.)

American Prosecutors Research Institute (Alexandria, VA)

California Public Interest Research Group (Sacramento, CA)

Center for Law and Public Interest (Los Angeles, CA)

Electronic Privacy Information Center (Washington, D.C.)

International Association of Chiefs of Police (Alexandria, VA)

International Association of Financial Crimes (Novato, CA)

National Consumer Law Center (Boston, MA)

National White Collar Crime Center (Richmond, VA)

Privacy Rights Clearinghouse (San Diego, CA)

U.S. Public Interest Research Group (Washington, D.C.)

# Major Contributors to This Report

| | |
|---|---|
| General Government Division, Washington, D.C. | Danny R. Burton, Assistant Director<br>David P. Alexander, Senior Social Science Analyst<br>Michael H. Little, Communications Analyst |
| Office of the General Counsel, Washington, D.C. | Ann H. Finley, Senior Attorney |
| Dallas Field Office | Ronald J. Salo, Evaluator-in-Charge |
| Los Angeles Field Office | Daniel R. Garcia, Senior Evaluator<br>Carla D. Brown, Evaluator |

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov