# USE AND MISUSE OF SOCIAL SECURITY NUMBERS

## HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JULY 10, 2003

**Serial No. 108–35**

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

93–570 WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

## COMMITTEE ON WAYS AND MEANS

BILL THOMAS, California, *Chairman*

PHILIP M. CRANE, Illinois
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHIL ENGLISH, Pennsylvania
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY C. HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin
ERIC CANTOR, Virginia

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
EARL POMEROY, North Dakota
MAX SANDLIN, Texas
STEPHANIE TUBBS JONES, Ohio

Allison H. Giles, *Chief of Staff*
Janice Mays, *Minority Chief Counsel*

---

## SUBCOMMITTEE ON SOCIAL SECURITY

E. CLAY SHAW, JR., Florida, *Chairman*

SAM JOHNSON, Texas
MAC COLLINS, Georgia
J.D. HAYWORTH, Arizona
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

ROBERT T. MATSUI, California
BENJAMIN L. CARDIN, Maryland
EARL POMEROY, North Dakota
XAVIER BECERRA, California
STEPHANIE TUBBS JONES, Ohio

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

# CONTENTS

# USE AND MISUSE OF SOCIAL SECURITY NUMBERS

**THURSDAY, JULY 10, 2003**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 1:18 p.m., in room B–318, Rayburn House Office Building, Hon. E. Clay Shaw, Jr. (Chairman of the Subcommittee) presiding.

[The advisory and revised advisory announcing the hearing follow:]

# *ADVISORY*

## FROM THE COMMITTEE ON WAYS AND MEANS

## SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
July 02, 2003
SS–3

CONTACT: (202) 225–1721

# Shaw Announces Hearing on Use and Misuse of Social Security Numbers

Congressman E. Clay Shaw, Jr. (R–FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on both the use and misuse of Social Security numbers. **The hearing will take place on Thursday, July 10, 2003, in room B–318 Rayburn House Office Building, beginning at 10:00 a.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

**BACKGROUND:**

The Social Security number (SSN) was originally created in 1936 to track workers' earnings for benefit purposes. Use of the SSN by both government agencies and the private sector has exploded over the decades as automation of record keeping and other business processes encouraged use of this simple, unique number that virtually every American possesses. As a result, many have called it a *de facto* national identifier, though it was never intended as such.

Today, even the most routine transactions may involve sharing of SSNs. Banks, schools, stores, and other businesses often use SSNs as account numbers. The SSN is used to help compile information from many different public and private sources for use in everything from tracking down criminals to issuing credit. Additionally, SSNs are easily found on display to the general public on employee badges, licenses, or court documents. In short, SSNs are the key to an individual's financial and other personal information, but their confidentiality is not well protected.

Use of the SSN as a personal identifier has produced some beneficial results for the public, including reduction in government waste from program fraud, enhanced collection of child support, and better law enforcement. Unfortunately, widespread utilization and public exposure of SSNs have also made them an invaluable tool for identity thieves. According to the Identity Theft Resource Center, an estimated 700,000 people of all ages, races, and economic backgrounds were victims of identity theft last year. The harm inflicted can be devastating difficulty obtaining credit, harassment by debt collectors, or even arrest because of the crimes of the identity thief. Worse yet, according to the Federal Bureau of Investigation, terrorists have utilized Social Security number fraud and identity theft to obtain employment, access secure locations, and finance their activities all of which threaten our national security.

The Social Security Administration (SSA) serves as the front line of defense in ensuring SSN integrity. It is responsible for accurately assigning SSNs and ensuring the wages earned and Social Security benefits claimed on that number are only those of the number holder. The SSA's Inspector General (IG) has long criticized the agency's failure to verify the authenticity of identification documents, and last year SSA began verifying supporting immigration records before issuing SSN cards. In

addition, despite the agencies efforts to reduce wage-reporting discrepancies—including outreach to employers 2 to 3 percent of wage items, equaling about $50 billion, will remain unmatched after wage processing is complete, according to the SSA.

In announcing the hearing, Chairman Shaw stated: "The Social Security number was originally intended to ensure American's hard-earned wages were properly credited to their record, so that they could receive their due benefits at retirement. Today, however, use and misuse of these numbers is rampant. The Federal Government requires the use of Social Security numbers and, therefore, has the responsibility to ensure they are assigned accurately, exchanged only when necessary, and protected from indiscriminant disclosure. We must stem the tide of attacks on Social Security number privacy. As in previous Congresses, I remain committed to pursuing bipartisan legislation to protect the privacy and integrity of Social Security numbers."

**FOCUS OF THE HEARING:**

The Subcommittee will examine the widespread use and misuse of the SSN in the public and private sectors and the effects of such use and misuse, as well as the integrity of the SSA's Social Security number issuance and wage crediting process.

**DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:**

**Please Note:** Due to the change in House mail policy, any person or organization wishing to submit a written statement for the printed record of the hearing should send it electronically to *hearingclerks.waysandmeans@mail.house.gov*, along with a fax copy to (202) 225–2610, by the close of business, Thursday, July 24, 2003. Those filing written statements who wish to have their statements distributed to the press and interested public at the hearing should deliver their 200 copies to the Subcommittee on Social Security in room B–316 Rayburn House Office Building, in an open and searchable package 48 hours before the hearing. The U.S. Capitol Police will refuse sealed-packaged deliveries to all House Office Buildings.

**FORMATTING REQUIREMENTS:**

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. Due to the change in House mail policy, all statements and any accompanying exhibits for printing must be submitted electronically to *hearingclerks.waysandmeans@mail.house.gov*, along with a fax copy to (202) 225–2610, in Word Perfect or MS Word format and MUST NOT exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. Any statements must include a list of all clients, persons, or organizations on whose behalf the witness appears. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers of each witness.

Note: All Committee advisories and news releases are available on the World Wide Web at http://waysandmeans.house.gov.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

* * * NOTICE—CHANGE IN TIME * * *

# *ADVISORY*

FROM THE COMMITTEE ON WAYS AND MEANS

## SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
July 08, 2003
SS–3 Revised

CONTACT: (202) 225–1721

## Change in Time for Hearing on Use and Misuse of Social Security Numbers

Congressman E. Clay Shaw, Jr. (R–FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee hearing on use and misuse of Social Security numbers, previously scheduled for Thursday, July 10, 2003, at 10:00 a.m., in room B–318 Rayburn House Office Building, **will now be held at 1:00 p.m. or immediately following the completion of the full Committee informal mark up of the Singapore and Chilean Free Trade Agreements**.

All other details for the hearing remain the same. (See Subcommittee Advisory No. *SS–3*, dated July 3, 2003).

---

Chairman SHAW. I am sorry. We are a few minutes late starting, but we had a busy morning with our Committee. Good afternoon. Today, the Subcommittee will examine the use and misuse of Social Security Numbers (SSNs). Using the SSN as a personal identifier has proven both a blessing and a curse. On one hand, the public is served when governmental agencies can use the number in matching information from other sources to reduce program waste, fraud and abuse, or when law enforcement agencies employ SSNs to help track down criminals or deadbeat dads. On the other hand, easy access to these numbers and their widespread use has provided a new tool for identity thieves. Worse yet, terrorists use SSN fraud and identity theft to assimilate themselves into our society, as did those responsible for the September 11th attacks. Identity theft continues to threaten our national security. Identity theft is the fastest growing white collar crime, and no one is immune, but the public is increasingly recognizing the vulnerabilities of SSNs and is working to protect them. Businesses are taking steps on their own to move away from using SSNs and several States have passed legislation, including Texas just last week, to protect SSNs from public display.

The Social Security Administration (SSA) serves as the front line of defense in ensuring the integrity of SSNs from the moment they are issued throughout the number holder's lifetime and even after his or her death, a responsibility the SSA takes very seriously. It is also responsible for ensuring the wages earned and Social Security benefits claimed on that number are only those of the number holder. As our witnesses will tell us, while the agency has taken

steps to improve the number assignment process, there is still more to do to prevent people from fraudulently obtaining and using SSNs. However, protecting the privacy and accuracy of SSNs is not the SSA's responsibility alone. Employers and individuals have a responsibility for submitting correct information to the SSA or correcting erroneous information. The Internal Revenue Service (IRS) has responsibility for imposing appropriate penalties on employers who submit erroneous wage reports to the SSA. The Bureau of Citizenship and Immigration Services must better coordinate with the SSA in verifying eligibility for a SSN and acting on information regarding earnings reported to nonwork numbers. Lastly, every public agency that uses and shares SSNs has the responsibility to protect their privacy.

The Subcommittee has been working on a bipartisan basis to protect the privacy of SSNs and prevent identity theft since the 106th Congress, when it first approved the Social Security Number Privacy and Identity Theft Prevention Act of 2000 (H.R. 4857). In the 107th Congress I, along with Ranking Member Matsui and 80 other Members of Congress, reintroduced a similar bill. Mr. Kleczka, of our full Committee, has also been very active in this regard. Consideration of this legislation was rightly preempted by necessary congressional response to 9/11 attacks. In coming days, Mr. Matsui and I will again introduce bipartisan legislation to restrict the sale and public display of SSNs, establish penalties for violations, limit dissemination of SSNs by credit reporting agencies, make it more difficult for businesses to deny services if a customer refuses to provide their SSN, and improve the integrity of the SSN assignment process. Congress must act this session to protect the very number it requires each of us to obtain and use throughout our lifetime. Providing for uses of SSNs that benefit the public while protecting these numbers from being used by criminals or even terrorists is a complex balancing act, as we found out in previous Congresses. We can make significant progress toward this goal by ensuring SSNs are assigned accurately, exchanged only when necessary, and protected from indiscriminate disclosure. I look forward to hearing from each of our witnesses, and thank them in advance for sharing with us their experiences and their recommendations. I understand Mr. Matsui is otherwise engaged this afternoon, and he has asked Mr. Cardin to sit in for him. The gentleman from Maryland.

[The opening statement of Chairman Shaw follows:]

**Opening Statement of The Honorable E. Clay Shaw, Jr., Chairman, and a Representative in Congress from the State of Florida**

Good afternoon. Today, the Subcommittee will examine the use and misuse of Social Security numbers.

Using the Social Security number as a personal identifier has proved both a blessing and a curse. On one hand, the public is served when government agencies can use the number in matching information from other sources to reduce program waste, fraud and abuse, or when law enforcement agencies employ Social Security numbers to help track down criminals or deadbeat dads. On the other hand, easy access to these numbers and their widespread use has provided a new tool for identity thieves. Worse yet, terrorists use Social Security number fraud and identity theft to assimilate themselves into our society, as did those responsible for the September 11th attacks. Identity theft continues to threaten our national security.

Identity theft is the fastest growing white collar crime, and no one is immune. But the public is increasingly recognizing the vulnerabilities of Social Security num-

bers and is working to protect them. Businesses are taking steps on their own to move away from using Social Security numbers, and several States have passed legislation, including Texas just last week, to protect SSNs from public display.

The Social Security Administration serves as the front line of defense in ensuring the integrity of Social Security numbers from the moment they are issued, throughout the number-holder's lifetime, and even after his or her death—a responsibility the SSA takes very seriously. It is also responsible for ensuring the wages earned and Social Security benefits claimed on that number are only those of the number-holder. As our witnesses will tell us, while the agency has taken steps to improve the number assignment process, there is still more to do to prevent people from fraudulently obtaining and using Social Security numbers.

However, protecting the privacy and the accuracy of Social Security numbers is not the Social Security Administration's responsibility alone. Employers and individuals have a responsibility for submitting correct information to the Social Security Administration, or correcting erroneous information. The Internal Revenue Service has responsibility for imposing appropriate penalties on employers who submit erroneous wage reports to the Social Security Administration. The Bureau of Citizenship and Immigration Services must better coordinate with the Social Security Administration in verifying eligibility for a Social Security number and acting on information regarding earnings reported to non-work numbers. Lastly, every public agency that uses and shares Social Security numbers has the responsibility to protect their privacy.

This Subcommittee has been working on a bipartisan basis to protect the privacy of Social Security numbers and prevent identity theft since the 106th Congress when it first approved the *Social Security Number Privacy and Identity Theft Prevention Act of 2000*. In the 107th Congress, I, along with Ranking Member Matsui and 80 other Members of Congress reintroduced a similar bill. Consideration of this legislation was rightly preempted by necessary Congressional response to the September 11th attacks.

In coming days, Mr. Matsui and I will again introduce bipartisan legislation to restrict the sale and public display of Social Security numbers, establish penalties for violations, limit dissemination of Social Security numbers by credit reporting agencies, make it more difficult for businesses to deny services if a customer refuses to provide their Social Security number, and improve the integrity of the Social Security number assignment process. Congress must act this session to protect the very number it requires each of us to obtain and use throughout our lifetime.

Providing for uses of Social Security numbers that benefit the public while protecting these numbers from being used by criminals, or even terrorists, is a complex balancing act. We can make significant progress toward this goal by ensuring Social Security numbers are assigned accurately, exchanged only when necessary, and protected from indiscriminant disclosure.

I look forward to hearing from each of our witnesses, and thank them in advance for sharing with us their experiences and their recommendations.

---

Mr. CARDIN. Thank you, Chairman Shaw. Let me thank you for holding this hearing. I also want to thank you for your leadership on this very important issue. I also want to acknowledge Mr. Matsui and Mr. Kleczka for the work they have done on identity fraud and the use of SSNs. Mr. Chairman, it is noteworthy to point out this is our ninth hearing on this subject, and it is a commitment that we have to take action in this area. As you pointed out, identity theft is considered one of the fastest growing crimes in the United States, with an average of an estimated 700,000 people being affected last year. It can ruin an individual's good name and destroy their credit rating. It even has affected the credit ratings of their young children. While credit issuers have been willing to refund fraudulent charges, victims are still faced with the effects of poor credit, the time commitments of restoring their ratings with multiple credit bureaus and credit issuers and the fear and anxiety associated with knowing someone is using their personal information to charge goods and services.

As a result of identity theft, victims have been turned down for jobs, mortgages and other important extensions of credit. So, therefore this is a very important subject, and we need to take action. As you pointed out, it even goes beyond the immediate problems of individuals that have found that the criminal elements, including terrorists, have used the identity of other people through SSNs in order to carry out their activities. We have a dilemma, the SSN is basically a national identifier. We have used it. We can't guarantee the confidentiality of that number, and therefore it can be used for identity theft. I am looking forward to the testimony from the U.S. General Accounting Office (GAO) and the Inspector General, who have been extremely helpful to us in coming forward with suggestions on how we can protect the confidentiality or use of the SSNs and how we can protect against identity theft. The bottom line is we need to take action in this area. The Chairman has indicated that he will be filing legislation shortly with Mr. Matsui. I can assure you we want to move forward as quickly as possible in a bipartisan way in order to try to help our people against this growing element of crime. Thank you, Mr. Chairman.

Chairman SHAW. Thank you, Mr. Cardin. I would like to just point out I think that we share jurisdiction with two other committees with regard to this legislation. Our Committee has moved forward in the past but we need to bring the other committees along with us in order to have a complete comprehensive bill rather than just picking and choosing the small portions of which our Committee has jurisdiction. Any other Members have an opening statement? The record will remain open. Without objection, they will be included in the transcript. On our first panel are two old friends of this Committee, Barbara Bovbjerg, who is the Director of Education, Workforce, and Income Security Issues from the GAO, and she is accompanied by Dan Bertoni, I believe that is the correct pronunciation, who is the Deputy Director. From the SSA, we have the Honorable James Huse, who is the Inspector General. As you all well know, we have your full statement which will be made a part of the record. We invite you to summarize as you see fit. Ms. Bovbjerg.

**STATEMENT OF BARBARA D. BOVBJERG, DIRECTOR, EDUCATION, WORKFORCE, AND INCOME SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY DAN BERTONI, DEPUTY DIRECTOR**

Ms. BOVBJERG. Thank you, Mr. Chairman, and Members of the Subcommittee. I am pleased to be here again today—I don't think it has been nine times for me, but it has been a number—to discuss issues associated with the integrity and use of the SSN. Although the SSN was originally created as a means to track workers' earnings and their eligibility for Social Security benefits, today the number is used for many non-Social Security purposes in both the public and private sectors. The wide use of SSNs causes concern because these numbers are among the personal identifiers most often sought by identity thieves. Today, I will present results of our completed and ongoing work on a variety of issues associated with the SSN. I would like to focus first on public and private sector use of the SSN and then, second, on the role of the SSA in preventing

the proliferation of false identities. My testimony is based on a report we did for this Subcommittee on government uses of the SSN and on ongoing work that focuses on private sector uses and on SSA's role in assigning SSNs and verifying them for others. I have so much material today that is relevant to this hearing and some visual aids to illustrate my points, I would ask to speak longer than the usual 5 minutes. I hope that will be acceptable to the Subcommittee. I will try not to prey on your good nature for very much longer.

Let me speak first about public and private uses. We reported last year that Federal, State, and county agencies rely extensively on the SSN. Although government agencies told us of various steps they take to safeguard the SSNs they use, we found that key protections are not uniformly in place at any level of government. We also found that some Federal agencies and many of the State and county agencies we surveyed, including courts in all the three levels of government, maintain public records that contain SSNs. Public records are documents routinely made available to the public for inspection such as marriage licenses or property transactions. For customer service reasons, some public officials told us they were considering making such records available on their websites. Because such actions would create new opportunities for identity thieves to gather SSNs from public records on a broad scale, we are beginning work for this Subcommittee to examine the extent to which SSNs in public records are already accessible on the Internet. Although we are not far along enough in this work to report the results today, I can assure you that we have already found SSNs in several public websites.

With regard to the private sector, we are finding that companies too are increasingly using SSNs, often collecting them from customers as a condition for providing service. For example, consumer reporting agencies (CRAs) build and maintain credit histories around an individuals' name, address, and SSN. The CRAs obtain SSNs from individuals who seek credit and from information resellers and public records. Some businesses aggregate information, including SSNs, from various public and private sources for resale. They obtain data from public records like bankruptcy proceedings, tax liens, and voter registration rolls—and from private compilations like telephone directories. These businesses combine and resell this information to a variety of customers. The ones we contacted told us that to comply with current law they generally limit their services to customers who establish accounts with them and with whom they have contracts that restrict the extent to which the data purchased can be redisclosed.

Despite protections such as these, large databases of information still represent a vulnerability for Americans. In the course of our work we have identified numerous instances in which the public and private databases have been compromised and personal data, including SSNs, stolen. Such cases illustrate the vulnerability of these databases to criminal misuse. Let me turn now to the role of the SSA in preventing the proliferation of false identities. This Subcommittee asked us to examine two aspects of the SSA role: SSA's assignment of new SSNs, a process called enumeration, and SSA's verification of SSNs for State driver's licensing agencies. Our

review of SSA's enumeration process found that SSA has begun to implement important new policies and procedures to prevent the inappropriate assignment of SSNs to noncitizens. For example, SSA has required staff to verify identity information and immigration status with the U.S. Department of State and the U.S. Department of Homeland Security prior to issuing an SSN. The SSA has also begun implementation of a program called Enumeration at Entry, where an applicant's information is vetted by the Department of Homeland Security and the Department of State before the applicants enter the United States. In addition, the SSA has created a special center in Brooklyn, New York to focus solely on enumeration and verification.

These three initiatives all hold promise of improved enumeration accuracy. However, the enumeration process overall still has vulnerabilities that could result in fraudulent use of Social Security cards and SSNs. I am speaking specifically of replacement Social Security cards and policies regarding SSNs for children under the age of 1. Let me turn to those now. As to replacement cards, SSA policy currently allows individuals to obtain up to 52 replacement cards a year. That is one a week. Of the 18 million cards SSA issued last year, 12.4 million, or almost 70 percent, were replacements. While SSA requires noncitizens to provide the same identity and immigration information that they need to obtain an original card when they get a replacement, citizens can use things like health insurance cards or church memberships when they apply for replacements. The ease of obtaining replacements creates the potential that these cards can be accumulated and sold to those not eligible for their own cards. This is an obvious vulnerability that should be better controlled.

With regard to enumerating young children, although SSA revised its policies to require that field staff obtain verification of birth records for most U.S.-born individuals applying for enumeration, agency policy requires only visual inspection of a birth certificate for children under the age of 1. Although such visual inspection can identify false documents, and indeed we found an instance where an alert Social Security field office staff member did identify a false birth certificate, we were able ourselves to create false documents and enumerate two nonexistent infants; the documents we used to do this are shown in the exhibit on your right. It is the left board, and I believe you have that in your packets in front of you. We have full names and other identifying information blacked out for security reasons. To support our applications for these cards, we used fake documents that you see on the left under the heading, "counterfeit documents." We used birth certificates and certificates of baptism for both of the applications we made. In one we used an employer identification card. In the other we also used a State driver's license to provide identification for the so-called parents who were applying for this infant's card. We created these documents with inexpensive, commercially-available software. You see the results on the right. We received one card already, and the written assurance below is that the other card is in the mail. After receiving these cards for children who do not exist we could have passed them to someone who is not eligible for a SSN. We wouldn't do that, but it is a clear vulnerability that SSA needs to address.

Let me now move on to SSA's verification of information for State driver's licensing agencies. Since driver's licenses are a widely accepted form of identification, the agencies that issue such licenses can be focal points for identity fraud. The SSA has a verification service in place that allows State agencies to verify the name, date of birth, and SSN of driver's license applicants. In our work for this Subcommittee and the House Judiciary Committee, we have found that 25 States have used the SSA service, but they have not all used it regularly. Most of them use the online verification method, but a few use only the batch method, which takes longer but costs less to use. States that don't use either verification method told us they were concerned about start-up costs and system performance. Indeed, there are 10 States awaiting improvement to the online verification system's capacity before they can be allowed to use it. Others already using the system have scaled back their use because of capacity problems.

In addition to the capacity problems the system has experienced, we also identified a key weakness in the batch method that exposes States to a higher risk of fraud. Unlike the online method, batch does not match verification requests against SSA's death records. As a result, the batch method will verify the name and SSN of a dead person as an accurate record. We observed this ourselves and again we have prepared a visual to illustrate—the one on the right. Our undercover investigators were able to obtain licenses in two States that use the batch verification method. We presented counterfeit identity documents that contain the name, data of birth, and SSN of a dead person to motor vehicle agencies in these States. In one instance, you can see we presented a fake birth certificate, a military identification, and a Social Security card. In another, we presented only the fake Social Security card and a fake driver's license from another State. In both instances, we received the driver's licenses you see before you on the right. The ease with which our staff were able to obtain these licenses suggests that the batch method must change and must change immediately to protect the State driver's licensing system. Our report on this topic will be issued in September and is likely to contain recommendations to improve SSA's verification systems, both online and batch.

In conclusion, let me say that SSNs are used for many beneficial purposes, but as we all know SSNs are also used for illegal financial gain and for immigration fraud. While most uses are for the benefit of the taxpayer and to ease the provision of various services such as granting credit, this personal information is not always adequately protected. Further, those who would live in the United States illegally have sought not just stolen SSNs, but their own Social Security cards and driver's licenses—fraudulently obtained, of course. The SSA has an important role to play both in limiting the issuance of SSNs only to those who are eligible to have them and to verifying personal information for State driver's licensing agencies. While progress is being made on both these fronts, we have demonstrated the vulnerabilities that remain. We look forward to continuing work with this Subcommittee to strengthen needed protections to ensure that false identities are not readily available to those who would harm the United States and its people. That con-

cludes my statement, Mr. Chairman. I really appreciate the extra time, and I am here to answer any questions.

[The prepared statement of Ms. Bovbjerg follows:]

**Statement of Barbara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues, U.S. General Accounting Office; accompanied by Dan Bertoni, Deputy Director**

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss ways to better protect Social Security Numbers (SSNs) to help prevent the proliferation of false identities whether for financial misuse or for assuming an individual's identity. Although the Social Security Administration (SSA) originally created SSNs as a means to track worker's earnings and eligibility for Social Security benefits, over time the SSN has come to be used for a myriad of purposes. As you know, SSNs are a key piece of information in creating false identities. Allegations of SSN misuse include, for example, incidents where a criminal uses the SSN of another individual for the purpose of fraudulently obtaining credit, acquiring goods, violating immigration laws, or fleeing the criminal justice system.

Although Congress has passed a number of laws to protect the security of personal information, the continued use of and reliance on SSNs by private and public sector entities and the potential for misuse underscores the importance of identifying areas that can be further strengthened. Accordingly, you asked us to talk about the uses of SSNs and ways that the integrity of the SSN may be preserved. My remarks today will focus on describing (1) public and private sector use and display of SSNs, and (2) SSA's role in preventing the proliferation of false identities. My testimony is based on a report we did for this subcommittee on government uses of the SSN,[1] ongoing work that focuses on private sector SSN uses, and work we are completing on SSA's enumeration process and the agency's verification of SSNs for state driver licensing.

In summary, public and some private sector entities rely extensively on SSNs. We reported last year that federal, state and county government agencies rely extensively on the SSN to manage records, verify eligibility of benefit applicants, collect outstanding debt, and conduct research and program evaluations. SSNs are also displayed on a number of public record documents that are routinely made available to the public. To improve customer service, some state and local government entities are considering placing more public records on the Internet. In addition, some private sector entities have come to rely on the SSN as an identifier, using it and other information to accumulate information about individuals. This is particularly true of entities that amass public and private data, including SSNs, for resale. Certain laws have helped to restrict the use of SSN and other information by these private sector entities to specific purposes. However, as a result of the increased use and availability of SSN information and other data, more and more personal information is being centralized into various corporate and public databases. Because SSNs are often the identifier of choice among individuals seeking to create false identities, to the extent that personal information is aggregated in public and private sector databases it becomes vulnerable to misuse.

As the agency responsible for issuing SSNs and maintaining the earnings records and other personal information for millions of SSN holders, SSA plays a unique role in helping to prevent the proliferation of false identities. Following the events of September 11, 2001, SSA formed a task force to address weaknesses in the enumeration process and developed major new initiatives to prevent the inappropriate assignment of SSNs to non-citizens, who represent the bulk of new SSNs issued by SSA's 1,300 field offices. For example, SSA now requires field staff to independently verify the identity information and immigration status of *all* non-citizen applicants with the Department of Homeland Security (DHS), prior to issuing an SSN. However, some SSA field staff are relying exclusively on the DHS verification system, while neglecting other standard practices for visually inspecting documents. SSA's automated system for assigning SSNs also does not prevent the issuance of an SSN if staff by-pass required verification steps. Other areas remain vulnerable and could be targeted by those seeking fraudulent SSNs. These include SSA's process for assigning social security numbers for children under age one and issuing replacement social security cards. In addition to its enumeration process, SSA provides a service to states to verify the SSNs of individuals seeking driver's licenses. We found that

[1] U.S. General Accounting Office, Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards, GAO–02–352 (Washington D.C.: May 31, 2002).

fewer than half the states have used SSA's service and the extent to which they regularly use the service varies widely across states. Factors such as cost, problems with system reliability, and state priorities and policies determine whether or not states use SSA's service. We also identified a weakness in SSA's verification service that exposes some states to fraud by those who would use the SSN of a deceased individual.

**BACKGROUND**

The Social Security Act of 1935 authorized the Social Security Administration to establish a recordkeeping system to help manage the Social Security program, and resulted in the creation of the SSN. Through a process known as "enumeration," unique numbers are created for every person as a work and retirement benefit record for the Social Security program. Today, SSNs are generally issued to most U.S. citizens and are also available to, non-citizens lawfully admitted to the U.S. with permission to work. Lawfully admitted non-citizens may also qualify for a SSN for nonwork purposes when a federal, state, or local law requires an SSN to obtain a particular welfare benefit or service. SSA is required to verify information from such applicants regarding their age, identity, foreign citizenship, and immigration status. Most of the agency's enumeration workload involves U.S. citizens who generally receive SSNs via SSA's birth registration process handled by hospitals. However, individuals seeking SSNs can also apply in-person at any of SSA's field locations, through the mail, or via the Internet.

The uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies' and businesses' own purposes. In addition, the boom in computer technology over the past decades has prompted private businesses and government agencies to rely on SSNs as a way to accumulate and identify information for their databases. As such, SSNs are often the identifier of choice among individuals seeking to create false identities. Law enforcement officials and others consider the proliferation of false identities to be one of the fastest growing crimes today. In 2002, the Federal Trade Commission received 380,103 consumer fraud and identity theft complaints, up from 139,007 in 2000.[2] In 2002, consumers also reported losses from fraud of more than $343 million. In addition, identity crime accounts for over 80 percent of social security number misuse allegations according to the SSA.

**PUBLIC AND PRIVATE SECTOR USES AND DISPLAY OF SSNS**

As we reported to you last year, federal, state, and county government agencies use SSNs.[3] When these entities administer programs that deliver services and benefits to the public, they rely extensively on the SSNs of those receiving the benefits and services. Because SSNs are unique identifiers and do not change, the numbers provide a convenient and efficient means of managing records. They are also particularly useful for data sharing and data matching because agencies can use them to check or compare their information quickly and accurately with that from other agencies. In so doing, these agencies can better ensure that they pay benefits or provide services only to eligible individuals and can more readily recover delinquent debts individuals may owe. In addition to using SSNs to deliver services or benefits, agencies also use or share SSNs to conduct statistical research and program evaluations. Moreover, most of the government departments or agencies we surveyed use SSNs to varying extents to perform some of their responsibilities as employers, such as paying their employees and providing health and other insurance benefits.

Many of the government agencies we surveyed in our work last year reported maintaining public records that contain SSNs. This is particularly true at the state and county level where certain offices such as state professional licensing agencies and county recorders' offices have traditionally been repositories for public records that may contain SSNs. These records chronicle the various life events and other activities of individuals as they interact with the government, such as birth certificates, professional licenses, and property title transfers. Generally, state law governs whether and under what circumstances these records are made available to the public, and they vary from state to state. They may be made available for a number of reasons, including the presumption that citizens need key information to ensure that government is accountable to the people. Certain records maintained by federal, state, and county courts are also routinely made available to the public. In

[2] Identity theft records broken out of consumer fraud totaled per year: 31,117(2000), 86,198(2001), and 161,819(2002).

[3] U.S. General Accounting Office, Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards, GAO–02–352 (Washington D.C.: May 2002).

principle, these records are open to aid in preserving the integrity of the judicial process and to enhance public trust and confidence in the judicial process. At the federal level, access to documents generally has its grounding in common law and constitutional principles. In some cases, public access is also required by statute, as is the case for papers filed in a bankruptcy proceeding. As with federal courts, requirements regarding access to state and local court records may have a state common law or constitutional basis or may be based on state laws.

Although public records have traditionally been housed in government offices and court buildings, to improve customer service, some state and local government entities are considering placing more public records on the Internet. Because such actions would create new opportunities for gathering SSNs from public records on a broad scale, we are beginning work for this subcommittee to examine the extent to which SSNs in public records are already accessible via the Internet.

In our current work, we found that some private sector entities also rely extensively on the SSN. Businesses often request an individual's SSN in exchange for goods or services. For example, some businesses use the SSN as a key identifier to assess credit risk, track patient care among multiple providers, locate bankruptcy assets, and provide background checks on new employees. In some cases, businesses require individuals to submit their SSNs to comply with federal laws such as the tax code. Currently, there is no law that prohibits businesses from requiring a person's SSN as a condition of providing goods and services. If an individual refuses to give his or her SSN to a company or organization, they can be refused goods and services unless the SSN is provided.

To build on previous work we did to determine certain private sector entities use of SSNs, we have focused our initial private sector work on information resellers and consumer reporting agencies (CRAs).[4] Some of these entities have come to rely on the SSN as an identifier to accumulate information about individuals, which helps them determine the identity of an individual for purposes such as employment screening, credit information, and criminal histories. This is particularly true of entities, known as information resellers, who amass personal information, including SSNs. Information resellers often compile information from various public and private sources.[5] These entities provide their products and services to a variety of customers, although the larger ones generally limit their services to customers that establish accounts with them, such as entities like law firms and financial institutions. Other information resellers often make their information available through the Internet to persons paying a fee to access it.

CRAs are also large private sector users of SSNs. These entities often rely on SSNs, as well as individuals' names and addresses to build and maintain credit histories. Businesses routinely report consumers' financial transactions, such as charges, loans, and credit repayments to CRAs. CRAs use SSNs to determine consumers' identities and ensure that incoming consumer account data is matched correctly with information already on file.

Certain laws such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Driver's Privacy Protection Act have helped to limit the use of personal information, including SSNs, by information resellers and CRAs. These laws limit the disclosure of information by these entities to specific circumstances. In our discussion with some of the larger information resellers and CRAs, we were told that they have to take specific actions to adhere to these laws, such as establishing contracts with their clients specifying that the information they obtain will be used only for accepted purposes under the law.

The extensive public and private sector uses of SSNs and availability of public records and other information, especially via the Internet, has allowed individuals' personal information to be aggregated into multiple databases or centralized locations. In the course of our work, we have identified numerous examples where public and private databases have been compromised and personal data, including SSNs, has been stolen. In some instances, the display of SSNs in public records and easily accessible websites provided the opportunity for identity thieves. In other instances, databases not readily available to outsiders have had their security breached by employees with access to key information. For example, in our current work, we identified a case where two individuals obtained the names and SSNs of 325 high-ranking United States military officers from a public Website, then used

[4] U.S. General Accounting Office, Social Security: Government and Commercial Use of the Social Security Number is Widespread, GAO/HEHS–99–28 (Washington, D.C.: Feb. 16, 1999.)

[5] The information compiled may include public records of bankruptcy, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registration, and professional licenses. Private data sources include information from telephone directories and copyrighted publications.

those names and identities to apply for instant credit at a leading computer company. Although criminals have not accessed all public and private databases, such cases illustrate that these databases are vulnerable to criminal misuse.

## SSA HAS A ROLE IN PREVENTING SSNS FROM BEING USED TO CREATE FALSE IDENTITIES BUT SOME AREAS REMAIN VULNERABLE

Because SSA is the issuer and custodian of SSN data, SSA has a unique role in helping to prevent the proliferation of false identities. Following the events of September 11, 2001, SSA began taking steps to increase management attention on enumeration and formed a task force to address weaknesses in the enumeration process. As a result of this effort, SSA has developed major new initiatives to prevent the inappropriate assignment of SSNs to non-citizens. However, our preliminary findings to date identified some continued vulnerabilities in the enumeration process including SSA's process for issuing replacement Social Security cards and assigning SSNs to children under age one. SSA is also increasingly called upon by states to verify the identity of individuals seeking driver licenses. We found that fewer than half the states have used SSA's service and the extent to which they regularly use the service varies widely. Factors such as costs, problems with system reliability, and state priorities have affected states use of SSA's verification service. We also identified a key weakness in the service that exposes some states to inadvertently issuing licenses to individuals using the SSNs of deceased individuals. We plan to issue reports on these issues in September that will likely contain recommendations to improve SSA's enumeration process and its SSN verification service.

### SSA's Enumeration Process Helps Prevent the Proliferation of False Identities, but Additional Actions are Needed to Safeguard the Issuance of SSNs

SSA has increased document verifications and developed new initiatives to prevent the inappropriate assignment of Social Security numbers (SSNs) to non-citizens who represent the bulk of all initial SSNs issued by SSA's 1,300 field offices. However, in some key areas, weaknesses remain. SSA has increased document verifications by requiring independent verification of the documents and immigration status of *all* non-citizen applicants with the issuing agency—namely the Department Homeland Security (DHS) and Department of State (State Department) prior to issuing the SSN. However, in our audit work, we found that many field offices are relying heavily on DHS's verification service, while neglecting standard, in-house practices for visually inspecting and verifying identity documents. We also found that while SSA has made improvements to its automated system for assigning SSNs, the system is not designed to prevent the issuance of an SSN if field staff by-pass essential verification steps. SSA also has begun requiring foreign students to show proof of their full-time enrollment, but does not require field staff to verify with the school the students' enrollment or their authorization to work. Consequently, SSNs for non-citizen students may still be improperly issued.

SSA has also undertaken other new initiatives to shift the burden of processing non-citizen applications from its field offices. SSA recently piloted a specialized center in Brooklyn, New York, which focuses exclusively on enumeration and utilizes the expertise of DHS document examiners and SSA's OIG investigators. However, the future of this pilot project and DHS' participation has not yet been determined. Meanwhile, in late 2002, SSA began a phased implementation of a long-term process to issue SSNs to non-citizens at the point of entry into the United States, called "Enumeration at Entry" (EAE). EAE offers the advantage of using State Department and DHS expertise to authenticate information provided by applicants for subsequent transmission to SSA who then issues the SSN. Currently, EAE is limited to immigrants age 18 and older who have the option of applying for an SSN at one of the 127 State posts worldwide that issue immigrant visas. SSA has experienced problems with obtaining clean records from both the State Department and DHS, but plans to continue expanding the program over time to include other non-citizen groups, such as students and temporary visitors. The agency also intends to evaluate the initial phase of EAE in conjunction with the State Department and DHS. However, this evaluation has not yet been planned or scheduled.

While SSA has embarked on these new initiatives, it has not tightened controls in two key areas of its enumeration process that could be exploited by individuals seeking fraudulent SSNs. One area is the assignment of SSNs to children under age one. Prior work by SSA's Inspector General identified the assignment of SSNs to children as an area prone to fraud because SSA did not independently verify the authenticity of various state birth certificates. Despite the training and guidance provided to field office employees, the OIG found that the quality of many counterfeit documents was often too good to detect simply by visual inspection. Last year,

SSA revised its policies to require that field staff obtain independent third party verification of the birth records for U.S.-born individuals age one and older from the state or local bureau of vital statistics prior to issuing an SSN card.[6] However, SSA left in place its policy for children under age one and continues to require only a visual inspection of documents, such as birth records.

SSA's policies relating to enumerating children under age one expose the agency to fraud. During our fieldwork, we found an example of a non-citizen who submitted a counterfeit birth certificate in support of an SSN application for a fictitious U.S. born child under age one. In this case, the SSA field office employee identified the counterfeit state birth certificate by comparing it with an authentic one. However, SSA staff acknowledged that if a counterfeit out-of-state birth certificate had been used, SSA would likely have issued the SSN because of staff unfamiliarity with the specific features of the numerous state birth certificates. Further, we were able to prove the ease with which individuals can obtain SSNs by exploiting SSA's current processes. Working in an undercover capacity our investigators were able to obtain two SSNs. By posing as parents of newborns, they obtained the first SSN by applying in-person at a SSA field office using a counterfeit birth certificate and baptismal certificate. Using similar documents, a second SSN was obtained by our investigators who submitted all material via the mail. In both cases, SSA staff verified our counterfeit documents as being valid. SSA officials told us that they are re-evaluating their policy for enumerating children under age one. However, they noted that parents often need an SSN for their child soon after birth for various reasons such as for income tax purposes. They acknowledge that a challenge facing the agency is to strike a better balance between serving the needs of the public and ensuring SSN integrity.

In addition to the assignment of SSNs to children under the age of one, SSA's policy for replacing Social Security cards also increases the potential for misuse of SSNs. SSA does not limit the number of replacement cards individuals can receive. Of the 18 million cards issued by SSA in FY2002, 12.4 million, or 69 percent, were replacement cards. More than 1 million of these cards were issued to non-citizens. In several of the field offices we visited, replacement cards represented 70 percent of the total enumeration workload. While SSA requires non-citizens applying for a replacement card to provide the same identity and immigration information as if they were applying for an original SSN, SSA's evidence requirements for citizens are much less stringent. Citizens applying for a replacement card need not prove their citizenship; they may use as proof of identity such documents as a driver's license, passport, employee identification card, school identification card, church membership or confirmation record, life insurance policy, or health insurance card. The ability to obtain numerous replacement SSN cards with less documentation creates a condition for requestors to obtain SSNs for a wide range of illicit uses including selling them to non-citizens. These cards can be sold to individuals seeking to hide or create a new identity, perhaps for the purpose of some illicit activity. SSA told us the agency is considering limiting the number of replacement cards with certain exceptions such as for name changes, administrative errors, and hardships. However, they cautioned that while support exists for this change within the agency, some advocacy groups oppose such a limit.

Field staff we interviewed told us that despite their reservations regarding individuals seeking excessive numbers of replacement cards, they were required under SSA policy to issue the cards. Many of the field office staff and managers we spoke to acknowledged that the current policy weakens the integrity of SSA's enumeration process.

*SSA's Verification of Driver Licenses Applicants Helps Prevent Fraudulent Documents, but Vulnerabilities Still Exist*

The events of September 11th, 2001 focused attention on the importance of identifying people who use false identity information or documents, particularly in the driver licensing process. Driver licenses are a widely accepted form of identification that individuals frequently use to obtain services or benefits from federal and state agencies, open a bank account, request credit, board an airplane, and carry on other

[6] Most U.S.-born individuals receive a SSN through a process SSA refers to as Enumeration-at-Birth (EAB). Under EAE parents can apply for a SSN for their newborn child at the hospital as part of the birth registration process. Under this process hospitals send birth registration information to a state or local bureau of vital statistics where it is put into a database. SSA accepts the data captured during the birth registration process as evidence of age, identity, and citizenship, and assigns the child an SSN without further parental involvement. The appropriate bureau of vital statistics forwards SSA the required information, usually by electronic means. Once SSA receives the required information, it performs edits, assigns the SSN and issues the card.

important activities of daily living. For this reason, driver licensing agencies are points at which individuals may attempt to fraudulently obtain a license using a false name, social security number (SSN), or other documents such as birth certificates to secure this key credential.

Given that most states collect SSNs during the licensing process, SSA is uniquely positioned to help states verify the identity information provided by applicants. To this end, SSA has a verification service in place that allows state driver licensing agencies to verify the SSN, name, and date of birth of customers with SSA's master file of SSN owners. States can transmit requests for SSN verification in two ways. One is by sending multiple requests together, called the "batch" method, to which SSA reports it generally responds within 48 hours. The other way is to send an individual request on-line, to which SSA responds immediately.

Twenty-five states have used the batch or on-line method to verify SSNs with SSA and the extent to which they use the service on a regular basis varies. About three-fourths of the states that rely on SSA's verification service used the on-line method or a combination of the on-line and batch method, while the remaining states used the batch method exclusively. Over the last several years, batch states estimated submitting over 84 million batch requests to SSA compared to 13 million requests submitted by on-line users. States' use of SSA's on-line service has increased steadily over the last several years. However, the extent of use has varied significantly, with 5 states submitting over 70 percent of all on-line verification requests and one state submitting about one-third of the total.

Various factors, such as costs, problems with system reliability, and state priorities affect states' decisions regarding use of SSA's verification service. In addition to the per-transaction fees that SSA charges, states may incur additional costs to set up and use SSA's service, including the cost for computer programming, equipment, staffing, training, and so forth. Moreover, states' decisions about whether to use SSA's service, or the extent to which to use it, are also driven by internal policies, priorities, and other concerns. For example, some of the states we visited have policies requiring their driving licensing agencies to verify all customers' SSNs. Other states may limit their use of the on-line method to certain targeted populations, such as where fraud is suspected or for initial licenses, but not for renewals of in-state licenses. The non-verifying states we contacted expressed reluctance to use SSA's verification service based on performance problems they had heard were encountered by other states. Some states cited concerns about frequent outages and slowness of the on-line system. Other states mentioned that the extra time to verify and resolve SSN problems could increase customer waiting times because a driver license would not be issued until verification was complete.

Indeed, weaknesses in SSA's design and management of its SSN on-line verification services have limited its usefulness and contributed to capacity and performance problems. SSA used an available infrastructure to set up the system and encountered capacity problems that continued and worsened after the pilot phase. The capacity problems inherent in the design of the on-line system have affected state use of SSA's verification service. Officials in one state told us that they have been forced to scale back their use of the system because they were told by SSA that their volume of transactions were overloading the system. In addition, because of issues related to performance and reliability, no new states have used the service since the summer of 2002. At the time of our review, 10 states had signed agreements with SSA and were waiting to use the on-line system and 17 states had received funds from Department of Transportation for the purpose of verifying SSNs with SSA. It is uncertain how many of the 17 states will ultimately opt to use SSA's on-line service. However, even if they signed agreements with SSA today, they may not be able to use the service until the backlog of waiting states is addressed. More recently, SSA has made some necessary improvements to increase system capacity and to refocus its attention to the day-to-day management of the service. However, at the time of our review, the agency still has not established goals for the level of service it will provide to driver licensing agencies.

In reviewing SSA's verification service, we identified a key weakness that exposes some states to issuing licenses to applicants using the personal information of deceased individuals. Unlike the on-line service, SSA does not match batch requests against its nationwide death records. As a result, the batch method will not identify and prevent the issuance of a license in cases where an SSN name and date of birth of a deceased individual is being used. SSA officials told us that they initially developed the batch method several years ago and they did not design the system to match SSNs against its death files. However, in developing the on-line system for state driver licensing agencies, a death match was built into the new process. At the time of our review, SSA acknowledged that it had not explicitly informed states about the limitation of the batch service.

Our own analysis of one month of SSN transactions submitted to SSA by one state using the batch method identified at least 44 cases in which individuals used the SSN, name, and date of birth of persons listed as deceased in SSA's records to obtain a license or an identification card.[7] We forwarded this information to state investigators who quickly confirmed that licenses and identification cards had been issued in 41 cases and were continuing to investigate the others. To further assess states' vulnerability in this area, our own investigators working in an undercover capacity were able to obtain licenses in two batch states using a counterfeit out-of-state license and other fraudulent documents and the SSNs of deceased persons. In both states, driver licensing employees accepted the documents we submitted as valid. Our investigators completed the transaction in one state and left with a new valid license.[8] In the second state, the new permanent license arrived by mail within weeks. The ease in which they were able to obtain these licenses confirmed the vulnerability of states currently using the batch method as a means of SSN verification. Moreover, states that have used the batch method in prior years to clean up their records and verify the SSNs of millions of driver license holders, may have also unwittingly left themselves open to identity theft and fraud.

**CONCLUSIONS**

The use of SSNs by both public and sector entities is likely to continue given that it is used as the key identifier by most of these entities and there is currently no other widely accepted alternative. To help control such use, certain laws have helped to safeguard such personal information, including SSNs, by limiting disclosure of such information to specific purposes. To the extent that personal information is aggregated in public and private sector databases, it becomes vulnerable to misuse. In addition, to the extent that public record information becomes more available in an electronic format, it becomes more vulnerable to misuse. The ease of access the Internet affords could encourage individuals to engage in information gathering from public records on a broader scale than they could before when they had to visit a physical location and request or search for information on a case-by-case basis.

SSA has made substantial progress in protecting the integrity of the SSN by requiring that the immigration and work status of every non-citizen applicant be verified before an SSN is issued. However, without further system improvements and assurance that field offices will comply fully with the new policies and procedures this effort may be less effective than it could be. Further, as SSA closes off many avenues of unauthorized access to SSNs, perpetrators of fraud will likely shift their strategies to less protected areas. In particular, SSA's policies for enumerating children and providing unlimited numbers of replacement cards may well invite such activity, unless they too are modified.

State driver license agencies face a daunting task in ensuring that the identity information of those to whom they issues licenses is verified. States effectiveness verifying individual's identities is often dependent on several factors, including the receipt of timely and accurate identity information from SSA. Unfortunately, design and management weaknesses associated with SSA's verification service have limited its effectiveness. States that are unable to take full advantage of the service and others that are waiting for the opportunity to use it remain vulnerable to identity crimes. In addition, states that continue to rely primarily or partly on SSA's batch verification service still risk issuing licenses to individuals using the SSNs and other identity information of deceased individuals. This remains a critical flaw in SSA's service and states' efforts to strengthen the integrity of the driver license.

GAO is preparing to publish reports covering the work I have summarized within the next several months, which will include recommendations aimed at ensuring the integrity of the SSN. We look forward to continuing to work with this Subcommittee on these important issues. I would be happy to respond to any questions you or other members of the Subcommittee may have.

**CONTACTS AND ACKNOWLEDGMENTS**

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director, or Dan Bertoni, Assistant Director, Education, Workforce, and Income Security at (202) 512–7215. Individuals making key contributions to this testimony include Mindy Bowman, Alicia Cackley, Tamara Cross, Patrick

[7] SSA's death records may contain inaccuracies because SSA records all reports of death but only verifies those involving benefit payments.

[8] This state does not use SSA's batch verification process for initial licenses, but only for license renewals. Therefore, the use of the deceased person's SSN will not be caught by the system when the state ultimately verifies it using the batch method.

DiBattista, Melissa Hinton, Jason Holsclaw, George Scott, Jacquelyn Stewart, and Tony Wysocki.

Chairman SHAW. Very good. We appreciate your testimony. Mr. Huse.

**STATEMENT OF THE HONORABLE JAMES G. HUSE, JR., INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION**

Mr. HUSE. Thank you, Mr. Chairman, Mr. Matsui, and Members of the Subcommittee. As always—and I have probably been here nine times—it is a pleasure to be here to assist you in your important work involving the SSN and its protection. In the interest of brevity and since you have accepted my full written testimony, I will summarize the major points that I have in that testimony. This Subcommittee and the Office of the Inspector General have been fighting SSN misuse and identity theft together for quite a few years now, beginning when I was Acting Inspector General at Social Security. So, now I am pleased to be here today and to see that the Subcommittee's continuing and tenacious dedication to stopping and reversing what is now a long-standing upward trend in SSN misuse and identity theft has never wavered. I come in support of legislation to strengthen protection for the SSN, our national identifier. We as a government remain ill-equipped to afford it the protection it needs and deserves. We need to protect the SSN at three stages: upon issuance, during the life of the number holder, and following the number holder's death. Perhaps the most important step we can take in preventing SSN misuse is to limit the SSNs' easy availability. Any meaningful legislation designed to protect the SSN must strictly limit the number's availability on public documents. The financial industry relies on the SSN and no one is suggesting that we change the way legitimate business is conducted in the United States. The use of the SSN as a student or patient identification number, as part of a car rental contract or to rent a video must be curtailed.

Finally, I respect and support the SSA's strict privacy regulations. The information SSA stores on each of us is personal and is entitled to all of the protections we can provide. However, there are times when that privacy must be abridged for the greater good. Following September 11th, and again during last year's sniper attacks in the Washington, D.C. area, it became necessary to share with appropriate law enforcement authorities information stored by SSA to permit those authorities to conduct their investigations and, more importantly, to prevent additional lives from being lost. On both occasions, I asked the Commissioner of Social Security to use the ad hoc authority vested in the Commissioner by SSA's regulations to permit me to share SSA information with our law enforcement partners. I now ask this Subcommittee for statutory authority that would enable the Inspector General to make such disclosures when necessary to protect human lives without prior formal authorization from the Commissioner. When lives are at stake, we cannot waste precious moments in order to sustain some bureaucratic modality.

Before I close, I would like to emphasize one part of my discussion. While the SSN is issued by SSA, the responsibility for protecting its integrity reaches far beyond the agency's boundaries. The SSA has come very far and is willing to do more, yet other Federal, State and local jurisdictions as well as the private sector must each also do their part. With everyone's participation we can protect the SSN and ultimately our homeland. Mr. Chairman, I thank you for your continuing commitment to these critical issues. I might add to sharpen all of this, that this very morning in California, we, along with the Los Angeles Police Department and other local police departments, made a raid and have arrested three suspects while one suspect remains at large. We also seized computers, printers, books of templates of every conceivable kind of identification, SSNs, lists of SSNs, birth certificates, driver's licenses, the seals to make driver's licenses, doctor's certificates, and infant footprints. Now what do you think they were going to do with those? This is a serious matter. It goes on every day. Thank you, Mr. Chairman.

[The prepared statement of Mr. Huse follows:]

**Statement of The Honorable James G. Huse, Jr., Inspector General, Social Security Administration**

Good Morning Mr. Chairman, Mr. Matsui, and members of the Subcommittee. As always, it is a pleasure to be here to assist you in your important work. We have been fighting Social Security number (SSN) misuse and identity theft together for quite a number of years now, starting when I was Acting Inspector General of the Social Security Administration's (SSA) Office of the Inspector General. On March 30, 2000, I testified before this Subcommittee about SSA program integrity issues in general. On that occasion, I expressed my appreciation that the Subcommittee had recognized the importance of confronting SSN misuse, and looked forward to separate hearings that you promised to hold on the issue.

Five weeks later, on May 9, 2000, I returned and reported at length on the misuse of SSNs in many areas, including identity theft. I explained that my office could not possibly investigate every instance of identity theft that involved an SSN. I testified that we were working vigorously on the audit side to identify and eliminate weaknesses in SSA's enumeration process, and just as vigorously on the investigative side to stop SSN misuse crimes that had a direct impact on SSA's programs and operations.

In the year that followed, even as we worked to tighten controls over the issuance of SSNs and fought to deter and punish SSN misuse, identity theft continued to increase. It became apparent that under existing law, we could not do enough to stop criminals from obtaining SSNs, and did not have sufficient enforcement tools to deter them from doing so.

So on May 22, 2001, I returned to this Subcommittee asking for its help. I asked for legislation that would severely restrict the use of SSNs in the private and public sector, and that would criminalize the sale of SSNs. I asked for an administrative safety net in the form of Civil Monetary Penalty authority for those instances of SSN misuse that could not be criminally prosecuted. And I pledged my office's unwavering support of the Subcommittee's efforts to prevent SSN misuse and, by extension, identity theft.

The Subcommittee's response was swift. H.R. 2036, which provided all of the relief I had requested and more, was an important step forward. Tragically, before we could take that step forward, we all took an enormous step back. September 11, 2001 stopped us all in our tracks, and H.R. 2036 understandably took a temporary back seat to more pressing Congressional responsibilities.

But it was a very short time before we collectively realized that H.R. 2036 and September 11 shared more common ground than we had ever contemplated. We had always seen SSN misuse as a bureaucratic problem for the government and a financial problem for the private sector and the citizenry. As our investigative offices were besieged with requests from the FBI for assistance in the September 11 investigation, we quickly came to realize that SSN misuse and identity theft threatened not only credit ratings and government records, but lives as well.

Shortly after the attacks on New York and Washington, I again came before this Subcommittee and testified about individuals seeking to assimilate themselves into our society for nefarious purposes. The assimilation process begins with the use of an SSN whether obtained legally or fabricated. Without it, I explained, it would be all but impossible to function in our society for any extended period. H.R. 2036, which *had* been an important piece of legislation eight weeks earlier, had become a critical one. Unfortunately, despite the best efforts of this Subcommittee and my office, the 107th Congress adjourned before that Bill became law.

Then just last week, Treasury Secretary John Snow called upon Congress to take additional steps to help stem what he correctly terms "the growing menace of identity theft." While the Secretary's focus was on the harm identity theft visits upon consumers, this Subcommittee knows the damage is much broader than that.

So, I am pleased to be here today, and to see that the Subcommittee's continuing and tenacious dedication to stopping and reversing what is now a long-standing upward trend in SSN misuse and identity theft has never wavered. As you well know, the use of the SSN in American society has expanded to the breaking point. Created in 1935 to track workers' earnings and pay them retirement benefits, its use has increased so dramatically that it has become a part of more government functions and financial transactions than we could ever count. It is our national identifier, and while it serves its purpose well, we as a government remain ill-equipped to afford it the protection it needs and deserves.

I have previously testified as to the need to protect the SSN at three stages: upon issuance, during the life of the number-holder, and following the number-holder's death. This three-tiered approach remains critical.

At Stage One, my office is doing more work than ever, working closely with this Subcommittee and SSA to strengthen controls over the enumeration process, ensure the integrity of identification documents, and make it as difficult as possible to obtain an SSN from the Federal government fraudulently. If we cannot accomplish this much—ensuring that the government is not an unwitting accomplice to identity theft and other SSN-related crimes—then we will have failed before we have begun. But I can testify today with confidence that this is not the case. Together with you and with SSA, we have made important strides in reducing enumeration vulnerabilities, and that effort continues. Still, legislation is sorely needed to limit the number of replacement Social Security cards an individual can obtain, and to require better cross-verification of records in the enumeration at birth process, to ensure that SSNs are not inappropriately issued in this important program. Excellent progress has been made in the enumeration arena, and we remain dedicated to even further improvements. At present, SSA is drafting two regulations to tighten the issuance of SSNs to non-workers and foreign students.

Similarly, Stage Three, following the death of the number-holder, is an area in which we are working hard to ensure that, through timely reporting, appropriate cross-matching, and better controls, the SSNs of deceased individuals are not recycled for inappropriate purposes.

But it is at Stage Two where we have focused the majority of our efforts, and where we have made the most progress. In the last several years, we have conducted numerous audits and made sweeping recommendations to SSA to improve the SSN misuse problem in the earnings reporting process, and most importantly, to improve controls over SSN misuse as it pertains specifically to Homeland Security. Further, over the last six months, we have led the President's Council on Integrity and Efficiency community in conducting an audit in assessing their respective Agency's practices in the use of SSNs. The final report noted that despite safeguards to prevent improper access, as well as disclosure and use of SSNs by external entities, many agencies remain at risk.

As I stated, the SSN was never intended for the uses to which it is now put millions of times every day. The Identity Theft and Assumption Deterrence Act of 1998 and the Internet False Identification Prevention Act of 2000 provided law enforcement with the initial tools necessary to punish SSN misuse as it relates to identity theft. But each SSN begins and ends at SSA, and true stewardship over that number must reside in the Act that created it, the Social Security Act. That stewardship must focus not only on punishment and deterrence, but also on prevention.

Perhaps the most important step we can take in preventing SSN misuse is to limit the SSN's easy availability. Any meaningful legislation designed to protect the SSN must strictly limit the number's availability on public documents. As long as criminals can walk into the records room of a courthouse or local government building and walk out with names and SSNs culled from public records, we can never reverse the trend. Any meaningful legislation must also specifically prohibit the sale of SSNs—including one's own SSN—on the open market. As long as criminals can buy a list of names and SSNs in an Internet auction, we will continue to be plagued

by the consequences. And legislation, if it is to be meaningful, must limit the use of the SSN to appropriate and valid transactions.

The financial industry relies on the SSN, and no one is suggesting that we change the way legitimate business is conducted in the United States. But the use of the SSN as a student or patient identification number, as part of a car rental contract or to rent a video, must be curtailed. Secretary Snow commented, "Secure, reliable information is the lifeblood of all financial services, among which consumer credit is fundamental. It is not an overstatement to suggest that preserving the integrity and availability of consumer credit in this economy is preserving prosperity itself." This is why I have testified that Congress should consider requiring the cross-verification of SSNs through both governmental and private sector systems of records to identify and address anomalies in SSA's files, and in data bases at various levels of government and the financial sector. Only in such a way can we combat and limit the spread of false of identification and SSN misuse. In fact, SSA has taken initial steps toward implementing provisions of the Patriot Act. This Act requires the Treasury Department to develop a system for domestic financial institutions to verify the identities of foreign nationals seeking to open accounts with information held by Government agencies.

If we can implement these changes, all of which come down to the acceptance of the fact that the SSN has become our national identifier and the application of common sense, criminals will have a far more difficult time obtaining an SSN from SSA *or* from other sources, and we will be able to better focus on enforcement.

The Identity Theft legislation I discussed earlier provides criminal penalties, but those penalties were designed for broader crimes involving Social Security cards and/or SSNs, not for SSN misuse itself. Meaningful legislation that is focused solely on SSN misuse must provide meaningful criminal penalties in the Social Security Act, must provide enhanced penalties for those few SSA employees who betray the public trust and assist criminals in obtaining SSNs, and must provide an administrative safety net in the form of Civil Monetary Penalties to allow for some form of relief when criminal prosecution is not available for SSN misuse and other Social Security-related crimes.

Finally, I respect and support SSA's strict privacy regulations. The information SSA stores on each of us is personal, and is entitled to all of the protections we can afford it. I have learned, however, through a series of unfortunate events, that there are times when that privacy must be abridged for the greater good. Following September 11th, and again during last year's sniper attacks in the Washington, D.C. area, it became necessary to share with appropriate law enforcement authorities information stored by SSA to permit those authorities to conduct their investigations and, more importantly, prevent additional lives from being lost. On both occasions, I asked the Commissioner of Social Security to use the *ad hoc* authority vested in the Commissioner by SSA regulations to permit me to share SSA information with our law enforcement partners. I now ask this Subcommittee for *statutory* authority that would enable the Inspector General to make such disclosures when necessary to protect human lives without prior formal authorization from the Commissioner. When lives are at stake, we cannot waste precious moments.

Before I close, I would like to emphasize one part of my discussion. While the SSN is issued by SSA, the responsibility for protecting its integrity reaches far beyond this Agency's walls. While SSA has come very far and is willing to do more, other Federal, State and local jurisdictions, as well as the private sector must each do their part. With everyone's participation, we can protect the SSN and ultimately our homeland.

I thank you for your continuing commitment to these critical issues, and would be happy to answer any questions.

---

Chairman SHAW. Thank you, Mr. Huse. What is the criminal penalty for supplying fraudulent documents in order to obtain a Social Security card—SSN? Or is there State law that you are familiar with that would do the same thing with regard to getting a driver's license that you are aware of?

Mr. HUSE. The answer to your question is, there are Federal statutes that cover those crimes, and State statutes also. There is a strong law enforcement remedy for all of this criminal activity. What there isn't, though, is an elastic enough charge or felony

charge for Social Security misuse in and of itself, which oftentimes is the common denominator through all of these levels of government and the crimes that have been established. If we had a strong, simple Social Security misuse felony, it would cut through a lot of this criminal justice activity.

Chairman SHAW. Let's take the examples that are up on the board. If one were to go in to the Social Security office and give them a birth certificate, a baptismal certificate and some other type of picture identification such as the one you use up there with the United Airlines employee type of identification, in order to obtain a SSN—these documents are fraudulent—what would be the criminal penalty that this person is liable for?

Mr. HUSE. There is a Federal criminal statute that covers this type of criminal activity. However, if I sold my SSN to Barbara to use illegally, there is no crime for the actual sale. I can't be charged for that. So, these are some of the aspects of this that we are trying to get in a specific SSN misuse felony.

Chairman SHAW. I am just talking about the individual who goes in and tries.

Mr. HUSE. It is a crime, and we can charge them.

Chairman SHAW. Is it a felony?

Mr. HUSE. It is a felony crime.

Chairman SHAW. Five years?

Mr. HUSE. Five to 10.

Chairman SHAW. Five to 10. Thank you.

Mr. HUSE. I would also add that in the Federal system there are also the sentencing guidelines.

Chairman SHAW. Are the prosecutors prosecuting these cases? Many of our courts I know in south Florida, are overworked so much, and the question of whether you are going to be prosecuted even for a felony can depend upon the severity of the felony because of short-handedness within the prosecutor's offices themselves, the right to speedy trial, overcrowded dockets, those type of things. Are these cases being prosecuted?

Mr. HUSE. Some of them are. I think the prosecutors try to do the right thing. They triage cases just like everybody else. There are those cases, as you just pointed out, that are not prosecuted, perhaps because the dollar amount is minimal, or the urgency, or there is no terrorism nexus, or what have you. Those cases usually fall out. That is why we are asking for this civil money penalty, a provision that would allow us to sanction those people who aren't prosecuted. They would still have to pay a substantial fine, and in that way perhaps we can do something about the proliferation of this crime.

Chairman SHAW. Mr. Cardin.

Mr. CARDIN. Thank you, Mr. Chairman. Let me again thank our witnesses for their testimony. The SSN is supposed to be the identification number for the Federal Government for Social Security purposes. Yet it is used as an identification number by a lot of different organizations and groups. I have my health insurance card, which my membership number is identical to my SSN. I am sure that is not unusual. Until 2 or 3 years ago, our U.S. House of Representatives identification cards included, mandatorily, our SSNs. So, I guess my question is, how important is it for us to try

to protect the confidentiality of an individual SSN? You point out that you can go on the Internet and probably find the SSNs of most of us in some documents that are probably public today. If you couldn't find it there you, probably with a little effort, could find out our SSNs. How much is that a contributing factor to identity theft? Should we be much more vigilant about protecting the use of the SSN as a way to protect against identity theft? How major is this? How much effort should we put behind keeping these numbers confidential or for use only by the SSA?

Ms. BOVBJERG. It couldn't hurt to quit giving people your SSN when you don't know what they are going to do with it. The Privacy Act (P.L. 93–579) requires all levels of government, not just the Federal Government, when they ask for your SSN, to tell you whether you are required to give it, and for what purpose it is to be used. This is not a provision of the Privacy Act that is followed very routinely. We have made a recommendation to the Office of Management and Budget to take some action to inform government agencies, particularly State and local governments, that this provision applies to them. I think as an individual it is probably also important to ask why Blockbuster Video or someone like that is asking you for your SSN and how it will be used, or to simply not give it to them. You are really also asking to put the genie back in the bottle.

Mr. CARDIN. I don't think people think about this. If they are asked to give their SSN they give their SSN because it is there, it is on the form. They don't think twice about it. Unless we develop policy nationally that prevents the use of the SSN for nongovernmental purposes or provide additional protection for the individual to make that judgment, it seems to me it is not going to happen.

Mr. HUSE. I agree with everything our distinguished witness from the GAO said, but I would add that that is 50 percent of the issue. The other 50 percent is for those numbers that are already out there. I believe there is also a governmental obligation to ensure that there is due diligence on the data that is stored by all of these entities in matching those records with the true records of government at all of the levels, but including the Federal level—to ensure that there is an attempt to make positive identification occur. I think that is the other half of the identity theft problem. I think we are doing a lot of work on the front end in trying to get the integrity in the system that issues numbers, but we are not doing enough on the back end to verify that data and to make sure that anomalies in it are rooted out and given to appropriate law enforcement authorities at the local, State, county and Federal level to deal with. This is a universal problem, it is way beyond just the SSA.

Mr. CARDIN. I agree with your point. I guess my point is, how do you put this all together? Would it make it a lot easier if these numbers weren't so readily available? I guess the answer is, it wouldn't hurt and certainly it would make it more difficult for identity theft. Unless we are prepared also to be very aggressive on the use of identity, and the verification of identity, and all the other issues there would still be a significant problem out there?

Mr. HUSE. I think you are at a point where, as Barbara said, you can't put it back in the bottle. I think we have to accept the status quo.

Mr. CARDIN. Why? I am not sure I agree with that. Unless we are willing to take action on who can use SSNs, and how they are to release and protect them, I agree with you. I guess my point is, that is one area that we could control here from Washington. It may cause disruptions and maybe it is not worth all the disruptions it causes, but I am trying to get a sense as to how important it would be to restrict the availability of SSNs. What I am getting from you is, that would certainly help us in reducing the amount of identity theft.

Mr. HUSE. The answer is yes.

Ms. BOVBJERG. If I could just add briefly, you have already done things that have helped. Certainly the Drivers Protection Act of 1993 (P.L. 103–322) helped enormously to prevent motor vehicle records that had SSNs on them from being sold in bulk. There are other things that have occurred over the last 10 years that have made the SSN, particularly in government, more secure. So, I think there are things that you already have done that have helped.

Mr. CARDIN. Why should my health insurance company require to use my SSN?

Ms. BOVBJERG. They want to know that you are you. It is a unique identifier. They want to distinguish you.

Mr. CARDIN. Well.

Mr. HUSE. From another person with a similar name.

Mr. CARDIN. Is that a responsibility of government, or the private insurance industry?

Ms. BOVBJERG. The government did not provide it to the insurance company.

Mr. CARDIN. No, but we provide the SSN. Thank you, Mr. Chairman.

Chairman SHAW. Mr. Collins.

Mr. COLLINS. No questions.

Chairman SHAW. Mr. Brady.

Mr. BRADY. Thank you, Mr. Chairman, for holding this hearing. Thank you to the witnesses for being here. It is very helpful. Reading the testimony in advance, I wanted to focus on defining the problem a little better. It seems like there are widely varying estimates of how big a problem identity theft is. I am wondering between thefts used for financial fraud that are—sometimes we identify them because of complaints, those used for illegal immigration purposes, those used for national security access. Do you think we really know how big the problem of identity theft is in America right now?

Mr. HUSE. I don't think we do. The numbers that come to us from the financial sector are those that they choose to share with us. All of the credit card entities have huge insurance bonds that mask a lot of the activity. By this I mean that they assume a lot of this is risk. In the context of the national security dimension, I think we do get good information, and it has really been emerging since 9/11, as to how important it is for someone that comes into this country to do ill, to be able to get underneath our radar by obtaining whatever requisite identification we need—principally the

driver's license because that is the one that allows you to move around as someone who has some kind of status. I think, to use a metaphor, this is the tip of the iceberg. We just see the top from the hysteria that we hear and the reporting. I think the problem is far bigger than we even know.

Mr. BRADY. Thank you. Ms. Bovbjerg.

Ms. BOVBJERG. I agree, we don't know. We have reported to Mr. Johnson in the past, that it is difficult to get statistics on this. I have brought Federal Trade Commission (FTC) statistics that said in calendar-year 2002, 380,000 consumer fraud and identity theft complaints came to their hotline. How many of those are SSN-related is unclear. They certainly don't get at the point that Mr. Huse made about the criminal immigration fraud, the terrorism side of identity theft. They also reported losses of more than $340 million. We know that not all of these losses get reported, so indeed this figure is lower than actual losses.

Mr. BRADY. Those aren't the answers I wanted to hear, but I think it is what we all know in the room—that it is the tip of the iceberg on this issue, and leads to the follow-up question, how successful are we in catching and prosecuting those who steal identities for various reasons? Do we have any numbers on how many prosecutions occur each year, and if I steal someone's identity for whatever reason, what are the chances that I will get caught—other than being a Member of Congress, we are likely to get caught—but still in the most part, how successful are we?

Mr. HUSE. I would say we are as successful there as we are with a number of issues when we talk about the criminal justice system. We know what we know. We have statistics, and I don't have them at my finger tips but we will supply them to you later, from what we do and the rest of Federal law enforcement. The U.S. Department of Justice garners the statistics from across the country. I don't think we really get at the universe of identity fraud through the criminal justice system. I think we probably, to use my metaphor from before, I think we are just getting at the surface of it. It is one of those crimes that has become provocative enough to warrant our attention. A lot of it goes on unnoticed. Some of it is because a victim has to discover that they have been violated. That is the part we don't really know yet.

[The information follows:]

Social Security Administration
Baltimore, Maryland 21235
*May 5, 2004*

The Honorable Kevin Brady
House of Representatives
Washington, D.C. 20515

Dear Mr. Brady:

During the Ways and Means Social Security Subcommittee hearing on July 10, 2003, you asked then Inspector General James Huse some questions related to the prosecution of identity theft cases. I would like to take the opportunity to respond to each of your questions in turn.

First, you asked how successful we are in catching and prosecuting those who steal identities for various reasons. It is important to note that the Social Security Administration (SSA) Office of the Inspector General (OIG) is responsible for investigating and referring for prosecution a small portion of the overall universe of identity theft cases—those that relate to Social Security disability benefits, earnings or

other fraud issues that concern SSA programs generally. With regard to these cases, the SSA OIG has been instrumental in successfully apprehending and referring violators for prosecution.

Second, you asked whether we have any numbers on how many identity theft prosecutions occur each year. As previously stated, the SSA OIG has statistics on the number of identity theft prosecutions relating to Social Security fraud, but not the number of identity theft prosecutions that occur nationwide as the result of investigations conducted by other federal, state and local entities. Between FY 2001 and FY 2003, the SSA OIG investigated over 1800 allegations of identity theft related to SSA's programs. These cases resulted in over 1100 convictions.

Finally, you asked how likely it is that someone will get caught for stealing an identity. Identity theft is often referred to as a crime that entails minimal risk. According to the Federal Trade Commission, the incidence of identity theft continues to rise. Through its investigations of Social Security-related identity theft allegations, and its referral process, the SSA OIG is making a significant contribution to the fight against identity theft. It is clear that more work needs to be done. We look forward to working cooperatively with other agencies and the Social Security Subcommittee in furtherance of this effort.

Sincerely,

Patrick P. O'Carroll, Jr.
*Acting Inspector General*

---

Mr. BRADY. Sure. Ms. Bovbjerg.

Ms. BOVBJERG. I am leaving the criminal justice statistics up to Mr. Huse.

Mr. HUSE. I didn't even answer them.

Mr. BRADY. I think really you did. I think the point you made earlier about more flexible criminal justice penalties and charges I think are real important. Mr. Chairman, I conclude with that. I think your bill on Social Security theft and response is an excellent approach. Perhaps we ought to find a way to better define this problem as well as better identify how successful we are because then we can at least start measuring our improvement against that. I yield back the balance of my time. Thank you.

Chairman SHAW. Mr. Pomeroy.

Mr. POMEROY. Mr. Chairman, I want to commend you for not just this hearing, but your long-standing work on this important issue. I would ask Ms. Bovbjerg whether there are some systems' investments that we need to make at SSA that will address some of the concerns your report notes. How do we get to where we need to go in terms of bringing a greater measure of security in the areas that you cite? Obviously the replacement cards, I suppose, if you don't issue—you don't allow 52 in a year would be a good start perhaps, but more specifically what recommendations you might have in that area, and the children's cards, the batch systems, what specifically do you think we ought to—how should we respond?

Ms. BOVBJERG. We are still thinking about recommendations in those areas. We will be issuing a report to the Subcommittee in September. We have been discussing these things with the SSA, and I know they have a concern about replacement cards and reducing the number permitted, thinking that, maybe 52 is too many, and certainly I think 52 is too many. The SSA raises the point about the homeless person who comes in regularly for his card, he needs it for benefits. The SSA doesn't want to cut that person off from his benefits. On the other hand, perhaps that person needs

something more than a replacement card if he is coming in to SSA offices that often. We are thinking about what would be a reasonable approach to fixing that problem. I think we have thought, particularly with regard to verification for enumeration that there might be some things that ought to be done, perhaps having SSA's staff have a means to acknowledge in the SSA system that they have done the third party verification. That is, the new SSN number could be issued. Things like that. These are recommendations that we are still thinking about, that we are discussing with the SSA. We don't want to recommend something that is not feasible. I think there are some things that can be done to strengthen the verification process.

Mr. POMEROY. Is your investigation also evaluating what legitimate private uses are occurring with SSNs as a national identifier in trying to find ways that put in place protections but on the other hand don't unduly disrupt existing systems that depend upon this identifier?

Ms. BOVBJERG. We are trying to look at that balance. In the work that we are doing for this Subcommittee on the private sector, we are asking certain parts of the private sector how they are using the number, how do they obtain it, what safeguards they have, because some companies have really thought about this a lot and are attempting to grapple with the safeguard issue. We will be reporting back in the fall on this. We are still in the middle of our work.

Mr. POMEROY. Mr. Huse.

Mr. HUSE. I just wanted to say that I think I can speak for Commissioner Barnhart here, too, that her interest in this is as strong as my own. The SSA does have a regulation moving through the vetting process now that will restrict the number of replacement cards available to an individual during the course of the year. It markedly reduces the number down from 52 to 2 in a given year, and 10 over the course of a lifetime, which I think is far more reasonable. That is going through the vetting process in the executive branch before it is issued as a regulation. So, it is there. I only answered that so that you understand that the SSA is not static on this issue. It is just a question of the process.

Ms. BOVBJERG. Your office too?

Mr. HUSE. My office too.

Mr. POMEROY. Do you have a feel for as we move to address identity theft it is going to significantly curtail commercial use of SSNs?

Mr. HUSE. I think it will. It will probably also spur the private sector to look to the promise in new technology for identification that takes us away from the number and its universal use now to biometrics and other more facile uses of identification. I think by drawing the line now, we are saying, that the continued use of the SSN will become too expensive for you, it would be better to try another way. The information technology will require this in any case.

Mr. POMEROY. Thank you. Thank you, Mr. Chairman.

Chairman SHAW. Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman. Mr. Huse, I asked you a question I think before on one of your nine appearances. I

wonder if you could give me an update on where we are with the regulatory process on the issuance of SSNs for nonwork purposes and for foreign students as well as those who are issued to foreigners. I have got a question along those lines. I believe you testified before with reference to the illegals that were allowed to have work permits in Dallas, that if they were issued a work permit they were allowed to get a SSN. What kind of documentation do they use to get that, one; and two, you said it was for life, good for life. Is that still true?

Mr. HUSE. Once a number is issued, it is valid for life.

Mr. JOHNSON. Well, then, what is this deal about you all issuing different kinds of SSNs for temporary work permits or students or people who are in the country temporarily from foreign countries? Is there such a thing? You were talking about different colors, I think.

Mr. HUSE. I never understood how complex this was until I took this office.

Mr. JOHNSON. It is, but you know the currency was counterfeited all over the world and we came up with coloration to take care of that. It isn't working, but it is still—well, it isn't. They keep changing it. It is an effort to stop the counterfeit process. I wonder why we don't do that with the Social Security card?

Mr. HUSE. The nonwork card, for example, was required as a means to provide legitimate visitors to this country with the ability to get a driver's license and be insured and to——

Mr. JOHNSON. They don't have to have a Social Security card to get a driver's license.

Mr. HUSE. Well, in some States you do need an SSN to get a driver's license. It is the underpinning of the driver's license system.

Mr. JOHNSON. That is not the purpose of the number. So, we are misusing it when we use it that way.

Mr. HUSE. The nonwork number, because there were these requirements, the SSA came up with this as a service. Now that was curtailed after September 11th. Commissioner Barnhart notified the governors of our States that the SSA would no longer do that. There were court challenges to that decision and the SSA has gone back to it temporarily, but it is under scrutiny now.

Mr. JOHNSON. So, what you are saying is the States use the SSN as verification to get a driver's license?

Mr. HUSE. They do. It is the underpinning of our driver's license system. That is why I used to use the term de facto national identifier for the SSN. If you notice over the time I have been here I have dropped that "de facto." If this is truly the case, that the number is underneath even the driver's license, we can't call it a de facto number, it is the national identifier until something changes.

Mr. JOHNSON. Do we legislate against that? I see driver's licenses being used as fake identification, too.

Mr. HUSE. The driver's license is probably the most counterfeited identification we have. In any case there is a lot of scrutiny on the uses of the nonwork number. There are foreign visitors to this country, students that obtain the appropriate visas that are in this country to be educated that for Citizenship and Immigration Services, if I got this right.

Mr. JOHNSON. I know what you are talking about. When you issue a SSN are you verifying it by one document or several documents? It seems to me if there is a fraudulent effort out there to obtain them, I don't know where they get them all from. Do they just make up the numbers or are they buying them or what?

Mr. HUSE. Thieves steal genuine numbers, thieves make up counterfeit numbers out of thin air and then create a myriad of identification from that. Between the two, all of this migrates into databases, and that is why I suggest that verification of these records is a way to root out SSN misuse.

Mr. JOHNSON. The IRS is your primary enforcement agency right now?

Mr. HUSE. It is.

Mr. JOHNSON. It seems to me that—how are they verifying the authenticity of the SSN? I know there is a lot of mismatches. How are we fixing that and are your computers being updated as we speak?

Mr. HUSE. There are efforts to do that. Our work and the work of the GAO have suggested system fixes to Social Security, and they have those in their queue to do along with their own systems enhancements. Those are under way. Are they done yet? No, they are not finished.

Mr. JOHNSON. We talked about this at least 2 years ago. Where are we with reference to that issue?

Mr. HUSE. We are moving toward the goal line, but it is not done yet.

Mr. JOHNSON. Can you see the goal line?

Mr. HUSE. Well, some things you take on faith.

Mr. JOHNSON. More than 100 yards away. Thank you very much. Thank you, Mr. Chairman.

Chairman SHAW. Mr. Becerra.

Mr. BECERRA. Thank you, Mr. Chairman. Before I begin my questions, I want to thank the Chairman for continuing to press on this issue. I know he has had legislation in the past, and I hope we are able to move something. I am sure it is going to be a bipartisan piece of legislation. I thank the Chairman for his efforts on this particular subject. To our witnesses, thank you again for being here. A couple of questions. First, with regard to the maintenance or the integrity of the SSN itself, the war on terrorism, the need for more security, it is becoming more and more important now that we check and verify. Now, I recall before 9/11, the SSA was already having problems trying to find the resources to take care of this massive work. Can you tell us what kind of monies you have post-9/11, or let's just focus on this year's budget, what kind of moneys you have in addition to what you already had to try to deal with this issue of identity theft.

Mr. HUSE. First of all, we do have built into our 2004 budget request appropriate funding to do some more significant work with——

Mr. BECERRA. How much are you asking for?

Mr. HUSE. Let me look back and get a dollar. The total appropriation we have asked for is $90 million, but in there, there is about an $8 million increase over current appropriations. We were looking to build out this SSN misuse capacity.

Mr. BECERRA. Let me make sure. Of the $90 million that you are asking for, $8 million of it would focus on the identity theft issue or all $90 million would focus on the identity theft issue?

Mr. HUSE. The $90 million covers all of our responsibilities, which is beyond just this particular mission. What we were looking for in the $90 million is $2 million, a modest amount to develop what we call SSN misuse teams that we have. The teams will include auditors, investigators and——

Mr. BECERRA. That is $2 million. Keep going.

Mr. HUSE. That is the only growth we asked for.

Mr. BECERRA. That's $2 million for a country the size of the United States?

Mr. HUSE. Well, we——

Mr. BECERRA. I suspect the folks that are forging these documents could give you more than $2 million off their profits just of what they have made.

Mr. HUSE. Now, I need to be careful here, because my role in relation to all of this is the integrity to the SSN business process itself. The whole issue that you speak to is a massive universe that involves——

Mr. BECERRA. That is very true.

Mr. HUSE. The whole government.

Mr. BECERRA. Outline for us what moneys you are getting for your particular role within the Inspector General's office, and perhaps we could ask, Mr. Chairman, for the SSA to break down the monies it is requesting to deal specifically with the identity theft issue so we have a sense. I am almost positive what we will find is that you all need more resources, and we should know that now so that when you come back and testify for the 10th or 11th time, we won't be asking why you haven't made more progress along the yardage markers to get closer to the goal line. Another question for you. Do government administrators or employees today at any level of government, whether Federal, State, local, or any business employees that you are aware of, undergo any training for identification verification to know when a document is real or fraudulent?

Mr. HUSE. They do. Even Social Security field employees get training in the identification of——

Mr. BECERRA. Without going further, because I want to make sure I get all my questions in, if you could provide us or provide my office with the literature, whatever you have in writing that says what the training is——

Mr. HUSE. I would be glad to.

Mr. BECERRA. If you know what other State or local governments do as well, because I guess one of the problems is we have a lot of folks who aren't trying or doing much of an effort to figure out if these are authentic documents or identification cards or not.

Mr. HUSE. Sure.

Mr. BECERRA. If someone asks for a replacement Social Security card—I lost my card, I write to the SSA and say I need to get another one, I can get one; right?

Mr. HUSE. Right away.

Mr. BECERRA. If a year later I write back and say, you know what, I lost it again.

Mr. HUSE. You would get it again.

Mr. BECERRA. If I say, you know what, I ripped it up. I lost it. Can I get another one?

Mr. HUSE. You can, and that goes on and on and on.

Mr. BECERRA. Does that trigger within SSA any thought that perhaps this individual is misusing the SSN?

Mr. HUSE. It does now, because we analyze the enumeration process, and where there are clusters of these, some are referred to us for an investigative look, where there is suspicion, which can't be——

Mr. BECERRA. So, we are doing something?

Mr. HUSE. Yes. Yes, we are.

Mr. BECERRA. Thank you, Mr. Chairman.

Chairman SHAW. The replacement card has the same number, doesn't it?

Mr. HUSE. Yes.

Chairman SHAW. Your concern with the replacement card is they are just handing them off to their buddies.

Mr. HUSE. Correct. We have, in some instances, where people get hundreds of these in a year, or almost 100 in a year.

Now, some people may be generationally used to the fact that they think they have to have this card at all times. Some of us get older, and we forget, misplace them and we think we have to get another one, and that is a service. That is a service some people believe they have to have, so a lot of these really aren't criminal, but when you see 80 or 90 a year, you begin to wonder, and those we are now——

Mr. BECERRA. I'd think you would begin to wonder before 80 or 90.

Chairman SHAW. Mr. Collins.

Mr. COLLINS. Maybe we ought to flag those and send them to them in bulk. I was just looking at some information the Subcommittee provided for us on mismatched records to see where the Social Security matches information with the IRS weekly about, and that is W–E–E–K–L–Y, not W–E–A–K–L–Y, about discrepancies. Interesting figures that no match letters were sent out to employers for employers to actually verify the employee, that it went from 110,000 to 950,000 letters last year, representing 10 million mismatches. Now, to go back to what Mr. Johnson was talking about, the immigration bill, and you talked about earlier, the raid that you all were successful with this morning in California where you apprehended three and one is on the loose. A lot of the cards or the material they had there to create cards will be part or a large part of this mismatch?

Mr. HUSE. There is absolutely no doubt that there is a demand for counterfeit identification documents brought on by our undocumented worker population in this country. That is fact.

Mr. COLLINS. A driver's license or most any kind of identification that has a SSN on it also has a photo on it. Any thoughts toward a photo? You get a SSN as an infant, but once you reach legal age, some age——

Mr. HUSE. There is no plan to do that. In fact, at the present time the SSA does not require a photograph for any of Social Security's services, including any of the insurance programs. Your num-

ber is the key that unlocks those benefits. In addition, there is not any biometrics involved.

Mr. COLLINS. It is also becoming a key to a lot of other folks too, using it in a wrong pattern. What can an individual—what has the Administration done to assist an individual in how to be more responsible or protective of their SSN?

Mr. HUSE. I can speak to what we, at SSA, and what I know from the FTC, and they have done extensive outreach work and activity in their communications arena to apprise people of the issues involved and the personal responsibility to protect your number, what to do when something happens to you, when you detect someone else has used your number and what remedies to take, and those are very understandable brochures and mailings. We have a fraud hotline at SSA that provides these answers to hundreds of people that call in with these problems. The FTC does the same thing. We also tell people in the process of getting their statement on Social Security every year, which is very important, that is a critical document, just like your monthly credit card statements, that you should review it carefully to be sure that the wages and earnings that are posted on it track with your recollection of your earnings history, because if there are differences there, that is almost a sure sign there has been a compromise of your identity. The other thing that SSA has advised people for some time now is to cease the practice of putting your SSN on private checks, and that is just not necessary. You shouldn't put your phone number either. This is just a desire by businesses to gather some data on folks that they don't really need to have.

Mr. COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman SHAW. You had a follow-up on—go ahead and then we will go to Ms. Tubbs Jones.

Mr. JOHNSON. Thank you. I would just like to ask, in the military, they ask you for your SSN. That is why we used to put them on the checks. I don't anymore.

Mr. HUSE. I remember, too.

Mr. JOHNSON. That, and phone number. That as well.

Mr. HUSE. So, they could get your officer's club bill to you.

Mr. JOHNSON. That is so you would pay them. That's right. I would like to ask a question real quick. Kids that get—when you give a baby a SSN, he isn't going to work. Why does he need one? The IRS asks you to do that, didn't they?

Mr. HUSE. They did.

Mr. JOHNSON. They use it, and it is if that is where how much of the fraud do you know what percentage of the fraud is in young kids?

Mr. HUSE. Well, the fraud that happens with the young children is when parents of young children get earned income credits for the purpose for——

Mr. JOHNSON. Kids get earned income credits?

Mr. HUSE. No. The parents do for the number of children they have, depending upon the level of the parent's income. That is a type of fraud. We can get you some information on that.

Mr. JOHNSON. Well, why isn't it possible to give a child a number that is not a SSN, that the IRS can use until they get of work-

ing age? We have child labor laws too. They are not supposed to work under a certain age.

Mr. HUSE. Like many things in government, this was a process that emerged out of a need to prevent fraud in filing income tax returns, where people claimed——

Mr. JOHNSON. It has turned around on us and we are having fraud develop in the Social Security regime. Then we maybe need to look at that again.

Mr. HUSE. That could be a possible area for adjustment. I know of the time in my youth you didn't get a number until you went to work.

Mr. JOHNSON. That's right. Thank you. Thank you, Mr. Chairman.

Mr. COLLINS. That may be part of the problem with the $10 billion of fraud that we have with the earned income tax credit each year.

Chairman SHAW. Ms. Tubbs Jones.

Ms. TUBBS JONES. Thank you. Do you have any indication that there is more abuse by earned income tax credit people filing than there is abuse of fraud in businesses across the country?

Mr. HUSE. No.

Ms. TUBBS JONES. Thank you. Let me go on. I heard you earlier raise the question that or say that there is no way you could prosecute Ms.—I don't know how to pronounce your name.

Ms. BOVBJERG. Bovbjerg.

Ms. TUBBS JONES. Thank you—for selling her SSN to you.

Mr. HUSE. You could prosecute her, but you couldn't prosecute me if I sold my number to her.

Ms. TUBBS JONES. Why not?

Mr. HUSE. There is no penalty for me to sell my genuine SSN.

Ms. TUBBS JONES. Oh, absolutely. There is a penalty for theft and deception and fraud.

Mr. HUSE. I meant in the Social Security Act (1935, 49 Stat. 620).

Ms. TUBBS JONES. I want you to be clear on that, because there is a law that covers that conduct.

Mr. HUSE. I believe there is a law on the books for just about every particular aspect of this, but it is sorting through those to get to the right penalty that makes it very difficult.

Ms. TUBBS JONES. Let me tell you the reason I raise the question with you, sir, is I am a former judge and a former prosecutor, prosecuted cases for Cuyahoga County for 8 years with 300 and some assistants, and the thing I worry about is us always trying to create another crime to prosecute conduct that can be prosecuted under existing law, and I just wanted the record to be clear that there is a law that you can be prosecuted for engaging in that conduct.

Mr. HUSE. I am sure.

Ms. TUBBS JONES. Let me ask you also. You said that you have been here nine times. My first time meeting you, it is nice to meet you. Have you, in the nine times that you have been here, requested sufficient dollars to be able to do the type of work that the SSA needs to do to adequately protect the people of the United States and their numbers?

Mr. HUSE. Yes, I think I have done that.

Ms. TUBBS JONES. So, the $2 million you asked for is sufficient to cover the needs of the SSA to help deal with this issue?

Mr. HUSE. To clarify, that was to add to what we already have received through the support of this Subcommittee and the House Committee on Appropriations over time. We have come some distance in the last 8 years from a very small organization to a very respected law enforcement organization. Most of which has occurred through the good will of this Subcommittee, and the Committee on Appropriations.

Ms. TUBBS JONES. I think you are being generous to the Subcommittee, and to yourself, to say that you have asked for enough money, because if you had asked for enough money, hopefully we would be further along than we are; and I don't mean to be accusatory, but I am just suggesting to you that prosecuting white-collar crime costs much more money. It costs many more law enforcement folks. It costs a lot more time than prosecuting a robbery or a burglary, and so the reality is that in order to be able to do some of the things that you really need to do to protect the people of the United States and their SSNs, you probably haven't asked for enough money, and you may be thinking that, well, they are probably not going to give it to me anyway, so I am not going to ask for it, but I would suggest to you that perhaps that might be, you might ratchet up that request so that if all of us, as Members of Congress, are sincere about trying to alleviate this problem for the people of the United States, we would put our money where our mouth is. That is all I am saying to you.

Mr. HUSE. I would say thank you, then. I will take your counsel.

Ms. TUBBS JONES. I appreciate it. Let me also, just one more area, Mr. Chairman. Commissioner, you say on page 5 that I asked the Commissioner of Social Security to use the ad hoc authority vested in the Commissioner by SSA regulations to permit me to share SSA information with our law enforcement partners. Can you tell me what that ad hoc authority is, please, sir?

Mr. HUSE. Well, it is authority that allows the Commissioner to disclose SSA information if not prohibited by Federal law.

Ms. TUBBS JONES. Why then, if you have that extraordinary authority under the ad hoc authority vested in the Social Security administrator, do you need statutory authority to enable the Inspector General to make such disclosures when necessary to protect human lives without formal authorization from the Commissioner?

Mr. HUSE. Well, this authority, because it is extraordinary, is a special and time-consuming process. Often the emergency is very time-restricted, where even seconds count, and that is the reason for this proposal in a simple statement.

Ms. TUBBS JONES. Under that authorization, what would be the circumstances upon which you would want this legislation to authorize the Commissioner to receive the—to be able to give up my SSN?

Mr. HUSE. It is actually the data that is in, they would be extremely limited to those, and it would be based—it is a discretionary authority. It would be based on my judgment, which I would have to answer for, as I do now to the Commissioner.

Ms. TUBBS JONES. So, if you can do it already, I guess my problem is in the name of terrorism, we have caused so many of the rights of the people of the United States to be abridged, and I am all for going after the terrorists and I am all for law enforcement having what they need to do their job and just for background, I am a former judge and I used to issue search warrants all of the time. I just fear the process of enlarging opportunities to give away a number that we are worried about giving away and we can't control government, so forth and so on, in the name of saving lives, per se. I would just suggest that it would be a good idea when we go through this process that we are real clear if we give away that authority that if he already has it in an ad hoc authority, maybe we might change the process but not expand it.

Mr. HUSE. That is what we seek in this legislation. The same restrictions would apply. We are merely moving the process from the Commissioner to the Inspector General, who, like the Commissioner, is Presidentially appointed and confirmed by the Senate. This proposal would just move the process into the law enforcement function in Social Security. The same rules would apply.

Ms. TUBBS JONES. There may be some advantage of having some oversight. That is why the law enforcement has to go to the judges to get search warrants, but I don't want to argue with you about it. What I would like to see, though, is the proposal that you have for the change in that authority. I thank you very much for your time, sir.

Mr. HUSE. Thank you.

Ms. BOVBJERG. Could I add something to that, please? Ms. Tubbs Jones, the Chairman has asked GAO to look at Social Security's policy with regard to sharing information with law enforcement. We are comparing it to the terms of the Privacy Act and to the policies of other Federal agencies. In this work, we are really looking at the balance between the privacy associated with the personal data that the SSA maintains and the needs of law enforcement, and of course we have been working with Mr. Huse and his office on that. We will be reporting out in September.

Ms. TUBBS JONES. I would be interested in hearing from you as well, and I would say the same thing to you, to you and anyone else looking at that area, that in the name of terrorism, we have abridged a whole bunch of rights. Let's think about it before we—especially to an area that has given us so much dilemma so far. Thank you, Mr. Chairman.

Chairman SHAW. Mr. Becerra asked for another follow-up question.

Mr. BECERRA. Thank you, Mr. Chairman. Quickly, if either of you, any of the three of you could respond to this, the breeder documents, I think at the end of the day we all recognize that as much integrity as we may put into the SSA's process for issuing cards, if the breeder documents that are used to obtain the SSN and card are fraudulent, that are very good fraudulent numbers or cards, identifiers, then we are still in the same place we were before. So, how—what can we do? Is there a carrot-or-stick approach that we can use to get the underlying State or local authorities who issue identifiers that are used often to obtain a SSN or any other private sector industries or businesses that issue identifies that are also

used, health care, health insurance card, for example, which is often used or accepted by some as an identification card. How can we make sure that those breeder cards or identity cards can be made more authentic? How can we provide the integrity in that process?

Ms. BOVBJERG. Well, third-party verification is really important. What we observed in the case of the driver's licenses, was that the third-party verification wasn't looking in the right place, so it was incomplete. In the other case, the SSN they weren't checking. There wasn't a verification of the birth record to see that the child didn't exist.

Mr. BECERRA. On that point, say the two faulty Social Security cards you got were verified by the SSA, so even if you take a State driver's license from whatever State and ask the State administrator, can you verify if this is a true identifier for you, is it an authentic State driver's license, someone might say, yeah, because it is such a great fake, forged document. So, how do you stop the process of creating what are clearly very good forgeries?

Mr. BERTONI. I will take a shot at that. We have criss-crossed the country looking at the processes for driver's license as well as SSNs, and I reiterate what Barbara says. We really need a system where we can have some independent third-party verification. So, if I am coming to the table with documents that look really good, even with training, and other tools that a driver's license clerk is given, or an SSA person is given, the documents are often just too good to catch. You really need to corroborate this information with third-party sources. In the case of the SSN, if I were to bring a birth certificate, SSA staff should bump that against State Bureau of Vital Statistics information from the issuing State. There are a number of other data sources that SSA could use to corroborate the name, date of birth, Social Security, and other elements. If the data comes back matching and you have other documents that corroborate the rest of the story, then you have a comfort level and you can issue the document. The same is true for driver's licenses. If you are a State using SSA's online process, you are going to get the full, I guess, the plate of services from SSA, including the death match. States that use a batch process, are not getting that match and if persons come to the table with a name, date of birth and SSN of a dead person and it is on the documents, SSA could do that check. I am sorry. The Department of Motor Vehicles could check with SSA, and it would still come back verified.

So, again, it goes back to what third-party verification are States doing, and what is the quality of that third-party verification. Another aspect is that if not SSA, or another government agency, some States use private vendors to perform data mining, and data cross-matching across the public and private sector sources to give the person that is verifying your identity documents greater comfort level that you are who you say you are. This brings me to the issue of how extensive identity theft is, and I will use the driver's license example. We took 1 month of transactions from 1 State and matched that data against SSA's master death file and got initially 160 instances where it looked like someone had used the identity documents of a deceased individual. We immediately forwarded 44 good ones to the State of issuance, because these folks were dead

10, 15, or 20 years, and it looked like identity theft was likely. We got a quick response back from the State that they had issued a license or identification card to 41 of 44 of these people. So, one State, 1 month of data show that this is a problem. There are a lot of States out there, and identity information is being used over and over and over again. I think there are driver's licenses out there that are issued to folks who shouldn't have them, and I think the problem is bigger than we all think it is, at least in the driver's license area.

Mr. HUSE. That is why, to sum this up, I think there are so many benefits to the cross-verification of data. Some privacy, of course, will be abridged, but anomalies will be reduced that everybody, whatever sector they are from, government, commercial, financial, will have to deal with these anomalies. These people were dead people that basically were used to produce this, we need to get a control over, it is not just government's problem. It is a universal problem. It will never, ever be perfect. That is a fact. There is nothing that can't be counterfeited. One day, though, all of this will lead us to a place where we will go to biometrics. We have to. That is not my role to suggest that. I just know that that is the ultimate answer.

Mr. BECERRA. It sounds like what you are saying is, if it is going to gain better protection of our privacy, we may have to give up a little bit of privacy——

Mr. HUSE. We may have to give up a little. It is this willingness to have our records cross-checked against——

Mr. BECERRA. This cross-checking isn't cheap. It is——

Mr. HUSE. No. It is expensive.

Mr. BECERRA. Mr. Chairman, thanks for the time.

Chairman SHAW. I think also by limiting the use of SSNs, we are actually going the other way. We are pulling back and we are increasing the right of privacy, which is something that we seem to be losing a little bit, as Ms. Tubbs Jones was pointing out, because of 9/11. I cannot remember a single time that I have been asked, somebody has asked to see my Social Security card. I am constantly asked for a SSN, and I have gotten to be, whether it is an application or something like that, I will just leave that blank, and usually nobody ever follows up to ask for it. This is something we have certainly got to do something about. When you think about the number one identifier in this country today is a card with a name and a number on it, period, no description, no date of birth, nothing else involved in it and this is being used as a prime identifier, there is something wrong with that picture and something we need to work on. We are just so vulnerable with regard to the use of those, and those numbers really have to be protected. Someone was—I think Mr. Johnson brought up the question that and you can see on that board to the right where the military identification uses the same numbers as Social Security.

Mr. HUSE. Exactly.

Chairman SHAW. Rank, name, and serial number. I used to kid Mr. Johnson. I would say, when you were in prison in Vietnam, the Vietnamese have your SSN, because that is the serial number, and when you go to many of the PXs on Army bases or any military base, you try to give them a check and not put your serial number

on it, they won't take it, and that means that they are getting the SSN, and we had testimony a few years ago, I think it was a colonel whose credit was absolutely destroyed because of, because somebody somewhere in the chain from the PX to the bank had picked up his SSN and just used that as the jumping off spot in order to assume his identity. We have, at this point, a vote on the floor. I think it is a point of order, and I assume that——

Ms. TUBBS JONES. Mr. Chairman, since we have a vote, can I ask just one other question, real short?

Chairman SHAW. Your questions go on for a long time.

Ms. TUBBS JONES. I know.

Chairman SHAW. I have got the gavel. You are——

Ms. TUBBS JONES. Okay. I won't have any problem. Just gavel me. By the time someone realizes that there is an identity theft problem and they go to law enforcement, the track is pretty cold, isn't it?

Mr. HUSE. Very often, yes.

Ms. TUBBS JONES. See. I am done, Mr. Chairman, and you didn't even know it.

Chairman SHAW. Very good. That is a record. I am a little confused about exactly how long we are going to be gone, but we will be coming back and go into the second panel immediately upon our return. So, I appreciate your patience in dealing with the schedule that we have. We will be in recess until approximately 10 minutes after the next vote.

[Recess.]

Chairman SHAW. We are going to go ahead and start. One of our witnesses has not returned as yet, but the vote has been over for a few moments and Mr. Collins is coming in now. So, we are going to go ahead and start with the next panel. We have Theodore Wern who is the Chicago, Illinois Regional Coordinator, the Identity Theft Resource Center in Chicago. Chris Hoofnagle, who is the Deputy Counsel, Electronic Privacy Information Center. We have an additional witness from Georgia, whom Mr. Collins will introduce when he returns. Mr. Wern.

**STATEMENT OF THEODORE WERN, CHICAGO AND ILLINOIS REGIONAL COORDINATOR, IDENTITY THEFT RESOURCE CENTER, SAN DIEGO, CALIFORNIA**

Mr. WERN. Thank you. Good afternoon. My name is Ted Wern, and I am the Midwest Regional Coordinator for the Identity Theft Resource Center. I am also an attorney in private practice in Chicago, Illinois. I began my work with the Resource Center after I recovered from my own personal identity theft problems. My battle lasted about 3 years, and from that process, I learned what millions of Americans have learned—that identity theft can truly wreak havoc on a person's life. What I have also learned as an attorney and as an educator to corporations in this area is that identity theft can result in some very significant liabilities for corporations. Therefore, my role both as an attorney, and as a volunteer for the Resource Center is to ensure responsible information handling, both for the benefit of potential individual victims as well as for the benefit of institutions which face potential liability in this area. Next I would like to provide a real-life perspective on the

problem of identity theft by talking about a small sample of cases that the Identity Theft Resource Center has handled in the past, keeping in mind that they handle thousands of cases each year, and these are just a few that seem particularly relevant to this hearing.

The first case involves a widow of the September 11th attacks. Approximately a year after her husband died in those attacks, she found out that her deceased husband's SSN was being used by an illegal immigrant for both fraudulent credit purposes and employment purposes. We don't know exactly how that person got the SSN, but public death records, which often display SSNs, are probably a very good guess. We also handle numerous cases involving the theft of children's identities. Mr. Johnson had a concern about this, and in response to that, children are becoming a new target of identity thieves. Here is why. Basically, a child's SSN and personal information can be stolen when the child is young, 6, 7, or 8 years old, by either a family member or stranger. By the time the child finds out, i.e., when the child is 18 or 19, or after adult age, to apply for credit or sign a landlord lease, by that time the thief has had 15 or 12 years to use that information to his or her advantage. So, the reason the children are such a hot target is because there is this lengthy discovery period for the crime.

The other group of cases to talk about, and one stands out in particular, involves military personnel. I would like to highlight a case that was the centerpiece of the Parade Magazine issue that comes in your Sunday newspapers. It was issued just this past Sunday. It involved a man named John Harrison who was a retired Army captain. His name and SSN and other personal information were stolen and used by a man who was able to buy, for example, a Harley Davidson, who was able to rent an apartment, was able to buy a timeshare, and the list goes on and on, all with Mr. Harrison's name. The importance of this article, and the story is that within hours of this article hitting the news stands, the Resource Center was flooded with calls and e-mails from citizens who were concerned about their identities, and the vast majority of those citizens were elderly persons, military personnel, and people who were concerned about their SSN appearing or being displayed on their military identification cards, which is a common practice, Medicare identification cards and of course, health identification cards as Mr. Cardin showed us a few moments ago.

The common thread from all of these cases is the fact that the SSN is at use in all of them. Without the SSN being available to criminals, none of these cases would have been possible. I would love to give you hard data about how many thieves extract their SSN from particular sources, whether they be death records or government records, but the data just isn't available, because, one, thieves rarely get caught; and two, when they are caught, their stories about where they got the information are hardly credible. What I can tell you, however, is that the SSN is the golden piece of data for identity thieves. A thief can only go so far with a date of birth or with an address. The SSN rounds out the crime, and with it, along with other information, getting fraudulent credit is as easy as picking up the phone or signing up on the Internet. So, even though we don't know exactly how the thieves are getting the

information, what we do know is that the number itself is worthy of any protections, any confidentiality restrictions that the government or the private industry can impose on it.

Let me point out that our goal here is not to create an undo burden on industry. We have looked at this bill, and we believe that, as Chairman Shaw indicated earlier, that it is a balancing act. You have to look at the potential benefits of the bill weighed against the burdens. In this case, we believe after careful study that the benefits of this bill far outweigh the potential burdens. With regard to that balancing, first of all, the SSN has no intrinsic value to governments or private industry. What I mean by that is that you don't use a SSN to dial up a person at home. You don't send marketing materials to a SSN. It is a random number, the only significance of which is to identify the particular person. There is no intrinsic value in the number itself. So, as Mr. Cardin raised before, why is his number and my number on our health identification cards? So that our doctor can have an emergency response number to call us or so that our medical records can be sent to that number? No. It is a random number, and there are plenty of other random numbers that could replace that number. So, especially in the area of publicly displaying these numbers on identification cards, unless it is for a legitimate IRS purposes or some of the exceptions that you have laid out in your bill, but for general commercial purposes like this, it just makes no sense. It is a random number. Why not get it out of circulation?

Also, with regard to balancing, it is important to point out that this is not a bill that imposes huge financial or administrative burdens on the industries or the government agencies that are subjected to it. We are not talking about huge capital expenditures here. We are not talking about complete overhauls to data systems. There are simple practical solutions of taking this number off the market, basically removing it from circulation. Furthermore, with regard to costs and benefits, there is an economic benefit for corporations and government agencies to not having that number out there for two reasons. One, there is a serious source of liability for corporations and government agencies who are responsible for information getting out into the public and identity thieves grabbing it. For example, when you have a large identity theft situation and outbreak, there is enormous class action potential in that situation, and these sorts of cases are growing exponentially in the marketplace today. So, this bill, in fact, is doing what exactly some of my clients, when we give our corporate workshops, are asking us to help them do, and that is help them to remove sensitive information from public display within their organizations, because they are very concerned about this source of liability. Finally, very obviously, as you reduce identity theft, you reduce direct losses to merchants, to banks, to credit card companies, and the losses in the last year we estimated at $17 billion. We took the average direct loss of an identity theft victim, losses that are borne by credit card companies and other creditors, multiplied it by the number of estimated victims which are between 700,000 and a million last year. Those are real numbers. So, not only do you have—if you can prevent identity theft, a prevention of liability. You also have a pre-

vention of direct losses. So, with these points in mind, I think the balancing act strongly favors this bill.

[The prepared statement of Mr. Wern follows:]

**Statement of Theodore Wern, Chicago and Illinois Regional Coordinator, Identity Theft Resource Center, San Diego, California**

**"Identity Theft and the Social Security Number"**

Members of the committee: Thank you for the opportunity to provide both written and oral testimony for your committee today and for your interest in the topic of identity theft.

The Identity Theft Resource Center (ITRC) is passionate about combating identity theft, empowering consumers and victims, assisting law enforcement, reducing business loss due to this crime and helping victims. Our organization is honored by your invitation and will continue to make its opinions available upon request to your representatives over the next few months as you grapple with this complex crime. The following testimony was written along with ITRC's executive directors, Linda and Jay Foley, and I have their permission to represent ITRC today at this hearing.

**About ITRC and the experts testifying:**

ITRC's mission is to research, analyze and distribute information about the growing crime of identity theft. It serves as a resource and advisory center for consumers, victims, law enforcement, legislators, businesses, media and governmental agencies.

In late 1999, ITRC Executive Director Linda Foley founded this San Diego-based nonprofit program after becoming a victim of identity theft. In her case, the perpetrator was her employer. Co-Executive Director Jay Foley has spent hundreds of hours speaking and corresponding with thousands victims while assisting in their recovery, listening as they discuss their revictimization by "a system that doesn't care, understand or listen."

ITRC also works with credit grantors, representatives from the credit reporting agencies (CRAs), law enforcement officers, governmental agencies and private businesses to prevent and resolve identity theft problems.

As one of the few groups that deal with a victim at all stages of the recovery process, we have a unique perspective on the crime. ITRC's information does not arise only from moment of discovery statistics. Its information comes at the cost of minutes, hours, days, weeks, months and years of a victim's life.

I (Theodore Wern) was an identity theft victim and serve as the ITRC Chicago and Illinois Regional Coordinator and victim advocate. My own case was complicated and required me to go to the extreme measure of changing my Social Security Number (SSN) in order to stop the crime from continuing. Because of my experiences, I am one of ITRC's designated specialists in severe cases. Since I work with others who must also change their SSN (only recommended in extreme situations), I serve as one of ITRC's representatives on a taskforce with the Social Security Administration (SSA) on defining and smoothing the procedures for changing one's SSN in extreme cases of id theft. My expertise as a corporate attorney also gives me added insight into the business implications of using the SSN as an identifier, as well as liability issues surrounding this subject.

The ITRC has worked for a number of years to make changes in laws, policies, business practices and trends to combat this crime. As a result ITRC has composed a list of recommendations that we feel will make a difference both in crime prevention (keeping the information from the hands of criminals and preventing the issuance of fraudulent credit) and in victim recovery.

ITRC's Testimony: ITRC has been asked to address the following points:

- The problem of identity theft including its impact on victims
- Issues surrounding the use and abuse of the SSN
- Recommendations for new laws regarding the SSN, including those listed in the Social Security Number Privacy and Identity Theft Prevention Act of 2001 (H.R. 2036).

**Part One: Summary of the Problem**

H.R. 2036 succinctly summarizes the history of the creation of the SSN and how this Pandora's box was opened. Unfortunately, in 1943, President Roosevelt could not have predicted the impact of the information age and the role computer technology would play in our lives. He could not have foreseen how it would change business practices or expose United States citizens to a harsh crime—that of financial identity theft.

Identity theft is not a new crime. The crimes of criminal identity theft and identity cloning (the use of another person's name instead of your own) can be traced back to biblical times. Credit card fraud and checking account fraud began soon after the advent of those financial transactions.

As stated in Mr. Shaw's summary, the Federal Government requires virtually every individual in the United States to obtain and maintain a Social Security account number in order to pay taxes, to qualify for Social Security benefits, or to seek employment. The use of this number as an identifier has grown tremendously and it is now common practice to use the SSN for purposes that have nothing to do with the extension of credit or governmental purposes. This extensive use of the SSN provides criminals with easy access to fresh credit and a new identity. To an identity thief, a victim's name, date of birth and address can be valuable, but such data alone is often not sufficient to commit identity theft. A thief generally needs a SSN as well. Because the SSN is "golden data" to the identity thief, it should be given the greatest privacy protections.

As pointed out in Mr. Shaw's summary:

- *An individual's Social Security account number may be sold or transferred without the individual's knowledge or permission.*
- *Today, the Social Security account number is generally regarded as the single-most widely used record identifier by both government and private sectors within the United States.*
- *No one should seek to profit from the sale of Social Security account numbers in circumstances that create a substantial risk of physical, emotional, or financial harm to the individuals to whom those numbers are assigned.*
- *The prevalence of the use of the Social Security account number and the ease by which individuals can obtain another person's Social Security account number have raised serious concerns over privacy and opportunities for fraud.*
- *Social Security cards may be counterfeited for illegal aliens and individuals use false Social Security account number information to improperly apply for and receive benefits under Federal and State programs.*
- *Misuse of the Social Security account number is a central component of identity theft, considered the fastest growing financial crime in the country as well as welfare and Social Security fraud.*
- *Growing concern over fraud and privacy and the absence of a comprehensive Federal law regulating the use of Social Security account numbers prompt the need for the Congress to act.*

ITRC does not believe it will be possible to completely eliminate this crime but we certainly hope to do the following:

- Make it extremely difficult for criminals to obtain SSN and other information that can be used to commit financial identity theft by severely cutting back on the exchange of such information.
- Tighten the procedures used by the issuers of credit so that criminals have a more difficult time in using ill-gotten information.
- Assist in victim recovery and shorten the time and duress suffered by its victims.

Because the federal government, through the SSA, created and maintains SSNs, it is appropriate for the federal government to take steps to stem the abuse of SSNs both in private industry and by governmental agencies. It will be far more efficient for the federal government to pass regulations about the use and misuse of the SSN than to rely on state regulations. California has come a long way in addressing the abuse of the SSN but to do this in 49 more states would be a daunting task.

**Part Two: Victim Impact**

Identity theft is a dual crime and no one is immune, from birth to beyond death. Who are these victims? It could be you, unknown to you at this very moment. I'd like to introduce you to some of ITRC's clients/victims who have turned to us for assistance. Many of these cases are taken directly from emails ITRC has received from victims. We present them to you so that you can see what we work with on a daily basis. Personal identifiers have been changed to protect each victim's privacy and some grammar/spelling corrections have been made.

Case 1: Child ID theft

The victim, Jose, owes about $65,000, $4,700 in child arrears and has 3 DUI warrants in his name. One problem: Jose is only 6 years old now and those arrears are to himself. The perpetrator is his father, now divorced from Jose's mother, an illegal immigrant who is subject to deportation when found.

Case 2: Identity theft of the deceased

Perhaps one of the most poignant stories we have heard (NJ Star Ledger reported it) is the theft of a man's identity who died in the World Trade Center attack on Sept. 11th. His widow was notified about 10 months after the event to discuss her husband's recent auto accident. She went through hours of turmoil only to discover that an illegal immigrant had created a false driver's license and was living and working as her deceased husband.

Unfortunately this is only one of more than several dozen cases that we have worked on involving the deceased. In some cases the imposter has purchased the information, in others the imposter is a family member or even a caregiver. Some may ask what is the harm in using the SSN of the deceased. Not only can identity theft involving a deceased person affect the estate but also the survivors still dealing with the grief of losing a loved one. In one other case, a mother has had to fight collectors trying to collect money from accounts opened in her daughter's name, a daughter who died several years ago. Each new call opens up the wound again.

Case 3: Workplace identity theft

T's identity was stolen by her doctor's receptionist. She found out when applying for her first home loan, her dream home. Months later, after clearing her records, spending her own time to research how her thief got her information and used it, and seeing another family move into her home, she was able to convince authorities to prosecute her offender. The result—the thief is now living in a halfway house, driving the car she bought with T's identity and working for another doctor as a staff member. T was finally able to buy a house almost 2 years later, at a higher purchase cost, with a higher interest rate due to the multiple accounts that had been opened in her name after the placement of a fraud alert.

Case 4: Victim recovery issue

Victim owns her own business. For the past 3 years, she has been in a fight with her bank. They repeatedly open new fraudulent accounts in her name and grant fraudulent access to her existing accounts, even generating dual credit cards and sending them to the imposters as well as herself. At one point she went to the local branch of her bank regarding the transfer of her account information. With multiple pieces of identification in her possession she was devastated by the bank officers who would not acknowledge her right to discuss the accounts in question or accept her identifying documents including passport, driver's license, utility bills, business license and SS card. To date she still has problems with her bank and her accounts. She is currently talking to an attorney and plans to sue the multiple companies who continue to torment her and refuse to correct their errors. She believes that lawsuits are her only option left.

Case 5: Financial id theft turns into criminal case

Two nights ago, I was arrested as part of a 4-year ongoing theft of my identity. The arrest was over bad checks written in Lincoln, NE near where I reside.

The issue, other than the arrest and all that goes with it, is the fact that J.P.M. was able to open fraudulent accounts because the Nebraska DMV issued her a license with her picture and my information. I don't know what documentation she provided them, but we clearly do not have the same physical features. This should have sent up a red flag to the DMV. As a result, J.P.M. illegally used my identity to spend almost $40,000, with new credit cards and with fraudulent checks.

I am doing the best I can to be compensated for the money spent on bail, loss of work time, personal stress, which all occurred while I was finishing my undergraduate degree and throughout my master's degree. Needless to say, this has interfered with my performance in school because of the time it takes to free myself as a citizen and as a consumer. The arrest was the last straw, and I've been told that the statute of limitations to sue the woman who stole my identity has expired. I am looking for help.

Case 6: SSN used as driver's license number

Victim had car broken just prior to a move from HI to DE. A file with all of her personal information was stolen in HI including her driver's license that used her SSN as the identity number. Since then a fraudulent cell phone account was setup with Voicestream generating a bill for $10,000.00. The victim has made some payments during the course of the account dispute due to the bullying action of collectors threatening to attach to possessions. Because of that payment, Voicestream refuses to acknowledge the account is fraudulent.

Case 7: Security breach

Victim was referred to ITRC by the FBI Victim/Witness Coordinator. The victim is a 72 year old retired Air Force Major. His dentist told him his identifying information might have been stolen. The dentist had befriended a man who saw the victim's dental records. This man then copied and used all of victim's info. The dentist found out when he saw files out of place. This befriended man/handyman was the only person who had access. The imposter purchased a condo, a BMW, and used the victim's HMO for medical services. The victim's HMO paid for this. Upon arrest, it was discovered that the imposter had a prior record of fraud. The imposter is now in jail on non-related charges.

Case 8: Identity Cloning

Victim lives in San Diego and is receiving disability benefits. The imposter is living and working in IL. Fraud is impacting her disability benefits. The IRS and SSA have been contacted. Victim is fearful of losing housing and being unable to cover living expenses due to the lengthy time of recovering her good name and clearing the records.

Case 9: Co-Worker ID theft

The victim recently found out of the identity theft. In 1999, a co-worker stole her credit card. The victim went through all the necessary procedures with her credit card company to remove the charges including filing a police report. In January 2002, the victim applied for a loan with a small finance company. The victim was told her social security number had already been used to apply for a loan with this company. The victim retrieved the application and found it was used back in 1999 by the same woman who stole her credit card. The victim had never been contacted by this company. The company's reply was that they denied the application. Unfortunately, in doing so, they did not indicate that it was denial due to fraud but due to not enough income.

Victim did speak to the finance company about this and even spoke with the Vice President in South Carolina who was not helpful. Victim still has not received a copy of her credit report so she is not sure if the imposter has done any real damage or not. Victim is certain that she used her social security number and she is not sure how else she can file a report if the police are not helpful.

Case 10: Extreme identity theft case

Victim's identity was stolen by a co-worker 10 years ago. She knows who the imposter is and he has been questioned but released by police (refusal to take action due to "extenuating family circumstances"). In the meantime, the victim has been unable to stop the imposter from opening credit and checking accounts, fraudulently applying for welfare, etc. She has had to change her SSN, driver's license number and name, essentially recreating herself in order to separate and protect her from the actions of the imposter.

Case 11: Reoccurring identity theft

My wife was a victim of identity theft in 1999. After many letters, a police report and an affidavit of forgery, we thought everything was settling. We were reassured that the loan and credit that was taken out in our name was removed from our reports and that our credit was restored. We asked several times for correspondence that this was taken care of but no one returned a letter. As time passed and we received no bills and we forgot about it. That is until we received an Equifax report on 6–2–02 showing that the fraud was still on the report. I tried to contact the office that I communicated with before but no one would return my call.

The date reported was after we had notified Equifax of the dispute. Are they in violation of the (FCRA)? Please advise or direct.

Case 12: Family ID theft

Victim's relative used victim's identity to clear out victim's bank accounts. This relative has victim's SSN and stolen checks. Victim has filed a police report and is in contact with the managers at her bank. Law enforcement is not investing a great deal of time on case, usually claiming that this is a family dispute.

Family identity theft is one of the most difficult crimes we work on, in part due to lack of police action and in part due to the emotional impact of this crime. How does one turn one's own mother in to the police? Unfortunately, we receive about 3–5 of these types of cases each week.

Case 13: Domestic abuse and harassment

The victim was divorced in 1987. She now lives in Florida. The ex-husband is operating in San Diego. Due to the actions of her ex, the victim is having IRS and SSA problems and is dealing with 3 accounts opened in her name. Unfortunately ID theft is the perfect tool to harass another person and to perpetuate domestic abuse after a divorce or separation.

Case 14: Stolen wallet

I live in TX. On June 2, 2002 my wallet was stolen in New York City. On June 6, 2002 a woman began using my identity from the wallet including drivers license, social security number from a medical insurance card, place of employment and stolen cards to establish instant credit at 9 different stores in 3 different states. I have placed a fraud alert on my credit report with the three credit reporting agencies but there has already been theft totaling in excess of $16,000 dollars. I am now having difficulty getting anyone to follow through with a police report and also changing my drivers license number. Because the theft occurred out of my home state, I have to follow up on the phone and not getting much response or help.

Case 15: Military spouse

I have had the frustrating and humiliating experience of somebody taking my maiden name and social security number in order to open numerous fraudulent utility accounts leaving my credit reports a mess. I am also a military wife who is required to show my social security number on my ID card, which is used for everything.

Case 16: Enable credit granting behavior

I was a victim of credit fraud/ID theft beginning in November of 2001, and continuing until approximately April of 2002. All of the many fraudulent credit applications using my name and identifying information were done in the Los Angeles area. Somehow, my personal identifying information (SSN, name, birth date, etc.) were obtained and used to apply for instant store credit at Radio Shack, Gateway Computers, and approximately a dozen other merchants. Additionally, my personal credit card was "taken over" by these criminals. By calling Visa and posing as me, they changed my billing address, and claimed that they had lost the credit card. They then received my new Visa card in the mail at the fraudulent address. They applied for many credit cards under my name and were even successful at getting a few, then charging the cards up to the maximum very quickly.

Case 17: Mail theft by an acquaintance

I just found out on June 14, 2002 that I am the victim of identity theft by my housekeeper/babysitter. Since she had access to my mail it was easy. She opened the first account in April 2001. She has charged over 10,000.00 that I am aware of and I have jewelry etc. missing from my home.

This is so recent that I don't even know what I'm up against yet—what I do know is that this has hurt my eleven year old daughter very badly. My daughter sang in the housekeeper's wedding last May, I wonder now if the wedding was all charged to me!

I would be happy to talk to anyone about this. I live in a small town of 12,000 people right now I know 4 people personally that this has happened to including the president of one of the banks here in town. Something must be done!! She is having trouble getting creditors off her back.

Case 18: Domestic abuse, insurance fraud

My ex-husband and his employer used my Social Security number to file medical claims on my health insurance. My ex has not been covered on my insurance since 1999, and I have changed employers and insurance carriers since that time. However, claims for February 2002 through May 2002 have been filed on my current insurance. He has obtained the information without my knowledge. I found out about the claims after receiving Explanation of Benefit forms from my insurance provider. The claims have been denied, so the insurance provider states that they are doing their job. The insurer will not file a report with the police.

Case 19: IRS complications

Someone has stolen my social security number and from that caused me to have false credit bureau claims and a warning from the IRS that I had underreported my income. Creditors have harassed me and required me to go to extraordinary

lengths to prove that I could not have incurred the debt in question. The IRS has required extensive documentation as well. Right now the activity has settled down, but anytime the next shoe could fall.

Even though there is a certain person I suspect of engaging in this identity theft, law enforcement authorities turn a deaf ear. I really don't blame them; it's not a high priority crime to them. To me, it is a major theft and close akin to rape.

This whole situation has been aided by the use of computers and the overuse of the social security number. I understand that the original law establishing the issuance of social security numbers stated that that number should only be used for social security, but indeed that has not been the case.

Case 20: Victim frustration—complex case

I became a victim of identity theft in March 2001. I found out when the person who had my social security number tried to open a credit card with a bank that I already had a card with. The woman was not able to give my correct birthday. They contacted me but they gave me a hard time saying that it was my daughter. They suggested that I contact the credit agencies about a fraud alert. That is when I found out that the person had many credit cards and a cell phone and they even bought a computer from Dell. Since I found out early I was able to stop almost everything before it was way out of hand. I filed a report with the Dallas police department and talked to a detective on a regular basis; only to find out they would do nothing. They had the address to which the credit cards and computer were sent but they would not go there. They even had another address where the person used a credit card in my name to buy a pizza. It took many months to clear everything up and I still have the fraud alert on my report for seven years. This is a crime that is to easy for someone to do and they get away with it because our laws are too easy and the officers are not trained on this type of crime. I feel I am luckier then most because I found out early and was able to clear up the damage within a year.

While you know my story, that only tells part of the picture. What I discovered disturbed me greatly:

1. Fraud alerts only help a little. Most places do not even honor them. So I'm not sure they help very much.
2. After I put the fraud alert on, they still opened a few more credit cards. All of the accounts they opened were done on the Internet.
3. I found that the credit card companies did not care much, they just closed the accounts. But before they will close the accounts you have to prove to them it was not you who opened the account.
4. They also made you wait on the phone a long time and you are transferred to many people before you found one that could help you. Most of the people I talked with acted like they were not educated enough on the subject.
5. They treat you like it was your fault and most of them need more training on this issue.
6. The police are no help at all.
7. The credit agencies take forever to remove the fraud accounts from your file.
8. The victim spends hundreds of hours writing letters and phone calls trying to remove the damage the thief caused while they are free to go to the next victim.
9. The Laws should help the victims, but you are alone when it comes to identify theft.

Case 21: Child ID theft

(Address, email and phone of victim will be provided to the members of the committee upon request. Copy and paste with permission of victim)

I am a mother of a thirteen-year-old son. I share joint legal custody with his father, who lives in a different county. Although my two boys primarily live with their father in ###, California, they visit frequently and spend all of their summers and vacations with my new husband and me.

About two years ago, my mother and I were in the process of setting up college fund accounts for my two sons. We were informed by our investor that my oldest son's social security number had several active accounts and recommended that we research this matter further before proceeding to open any financial accounts under his name and social security number. Unfortunately for my son, the thief is his own father. They both share the same base name and physical address. Therefore, the theft of my son's social security number was an easy accomplishment by his father.

In going through this case of Identity Theft, I have encountered various problems along the way. First being that the local law enforcement agency in the county in

which my son resides with his father, refused to take an identity theft report because their county does not have a department that handles such matters. Because of this and the fact that my son is a minor, it took several months, almost the remainder of the year to obtain a copy of my sons credit report. The three credit reporting agencies refused to issue any information because he was a minor. Instead of investigating the matter further, they sent a standard "refusal to issue information letter" based on the fact that he was under the age of 18 and that they do not issue reports for minors. Without this report, it has been nearly impossible to get any response from creditors as well as getting a credit issuer to take me seriously. The report was subsequently acquired, through diligence and perseverance.

I have also attempted to write letters to each lender and attach a copy of his credit report as proof of an existing account, I have had to send follow up letter as well, and have yet to hear a reply as they are not required to respond or assist with fraudulent accounts.

As a mother of a victim of Identity Theft, I would highly recommend that **all** state and local law enforcement agencies be required to generate a report on identity theft complaints in the jurisdiction where the victim lives and to provide a copy of the report to the victim, regardless of their subsequent decision on whether or not the agency will investigate the case. If by chance, there had already been laws in effect, it would clearly have been easier to obtain credit reports for a minor with parental documentation. It would also have directly influenced the ability to stop further debit from occurring.

As you might imagine the recourse for this action can lead in several directions. Although I do not wish to amend this crime out of vengeance towards my son's father. I am deeply worried that as my son approaches adulthood and tries to obtain college grants, scholarships, etcetera, he will be denied due to his already existing debt. To this day, his father has acquired over $250,000.00 in debt under our son's social security number. I cannot begin to imagine the long-term affect that this amount of debt will have on my son's future.

Knowing my son as I do, it has been a difficult decision to keep this information from him. As he has already suffered emotionally from the divorce, I deeply fear that this will emotionally tear him apart and sever all bonds he has created with his father. I also fear that the impact of knowing that his father was the criminal will have a psychological scaring on him for the remainder of his life.

Finally, in trying to rectify this matter with the social security administration, and in conjunction with my family law attorney, this entire matter must be handled with diligence and on an efficient manner. Because of the fact that I share joint custody with my ex husband, I have an incredible fear, based on past actions, that if and when his father is confronted with the truth of his crimes, he will then take matters to extreme action and kidnap my son, making it impossible for me to have any further contact with him. This also presents the problem of obtaining a new social security number. Because our son is still a minor, the new number will have to be disclosed to his father for medical and scholastic purposes. An even greater fear is that his father will continue to abuse his son in this manner. Based on passed history of his fathers actions of first destroying his own credit, and now destroying his son's credit, what will prevent him from committing the crime once again. Unfortunately, I do not see this cycle ending without laws to protect victims of fraud as well as minors.

**Part Three: Issues to be discussed**

It is clear that a list of commonalities can be derived from ITRC's victim accounts set forth above. Categories where the SSN has been an instrument to create havoc include:

- Use of the SSN for as a driver's license number
- ID theft of the Deceased
- Child identity theft
- Failure of governmental agencies to find alternate ways to protect identifying numbers used by the government: military ID number, Medicare/state health insurance number (could be done by random number matching to SSN in a closed, secure database)
- Employer use of the SSN as an individual employee (private or governmental) ID number, including public display of the SSN, e.g., timecards, badges
- The use of the SSN as an identifier by a business group, printed on a card carried by the person on a regular basis
- Mail theft—where the SSN is printed (unnecessarily) on the document being mailed and is intercepted by another person

- Theft of SSN given in good faith to or displayed or sold by a business which required the information to complete a transaction or activity—e.g., to obtain health care benefits.
- Collection of information not needed for the necessary task or program
- Failure to protect collected information—e.g., disposed of inadequately
- Database or information breach—failure to provide proper security
- Database or information breach—due to the actions of an individual who had access to the information that never should have been collected in the first place
- Domestic abuse, harassment of an ex—due to extensive use of the SSN as an identifier
- Restrictions on sale of SSN and credit info to third parties by governmental agencies or private entities
- Unrestricted ability to print SSN of individuals on web sites, e.g. Ancestry.com
- Failure to truncate parts of SSN on documents available to the public—electronic court records, birth and death certificates, etc., unless the requesting party has a legitimate reason for such information

**Part Four: Recommendations for Laws**

ITRC likes to use a Finding/Recommendation format to advise on new legislation. In this testimony, ITRC will limit its findings with the belief that this esteemed committee has studied this subject at length and does not need substantial background information.

This list is a preliminary discussion and ITRC's directors would be honored to continue to work with the committee as they explore this topic and prepare legislation that will protect all of us from SSN abuse.

**1. Use of the SSN as the driver's license number**

**Finding:** At this time, individuals have a choice in those remaining states that continue to use the SSN as the driver's license number. This practice means that each check written includes one's SSN and that individuals with social security numbers on their license suffer greater loss due to lost/stolen wallets.

**Recommendation:** Due to lack of consumer education, ITRC believes that states MUST be required to adopt a random number system and replace the SSN on all drivers' licenses within 1 year of the passage of this legislation.

**2. Identity theft and the Deceased**

**Finding:** Despite a person's death, a SSN continues to be active and may be used for the extension of credit. The Master Death Registry controlled by the SSA does not include the names of all deceased. Information is added to this list in a variety of methods, some of which are only consumer generated. Too many stories have been printed and too many cases have occurred where a deceased individual's SSN has been used to get credit.

*Example: Florida Department of Law Enforcement agents arrested William Troy Herman and Ronnie J. Skipper for fraud. Agents say the duo used the personal information of seven deceased individuals to obtain credit cards in the victims' names.*

This causes problems for the estate and additional stress on the bereaved. The letters we receive from them are painful and their distress is evident.

**Recommendation:** ITRC's executive directors are currently working with Senator Corzine and U.S. House Representative Gutierrez on legislation to correct this issue. It would make sure that all deaths are recorded on the death register, forwarded to the repositories that will then mark all of those SSNs as "Deceased, do not issue credit." This list must be designated as not to be sold, distributed or used for any purpose other than the one itemized above.

**3. Identity Theft of Children**

**Finding:** There are several types of child identity theft scenarios that ITRC typically sees:

- It's a split family. One of the parents finds out that the other parent (or the "friend" of the parent) has begun to use the child's identity to gain credit or a driver's license. This is usually because they have already ruined their own credit or driving record. They plan on "fixing" everything before that child reaches 18. They even swear they were planning on paying all the bills accrued under the child's SSN. The reality is that they eventually will ruin the child's credit just as they ruined their own.
- Upon reaching 16, the child applies for a driver's license. They are denied because someone already has a driver's license using that SSN.

- Upon reaching 17 and applying for a college loan, the teen finds out he or she cannot qualify due to a poor credit rating. This has sometimes resulted in a one-year delay in starting college.
- Upon reaching 18, the now adult child is denied credit, unable to gain employment or rent an apartment due to a poor credit rating. They find out that someone has used their info for the past 10 years and they are $15,000 in debt. Before their true adult life has begun, it is tainted and may take years to clear up.
- Now an adult and in the workplace, the victim finds it difficult but not impossible to get credit. Perhaps they think it is because of their youth and that the first card they did get they mishandled and perhaps had to pay off over time. They have never checked their credit reports until one day a collection notice reaches them—perhaps at the age of 25 or even 30. Once checking their credit reports, they find out that for the last 15 years someone else has been opening up accounts in their name.

Their imposters often are family members, parents or guardians, or may be illegal aliens who purchased the information from traffickers who purposely sell information that belongs to children due to the lengthy time prior to crime discovery.

**Recommendation:** Elderly and children are deserving of additional protection under the law. No one disagrees with that. We must assume the role of caregivers and make sure that those individuals are not abused—physically or financially. ITRC's recommendation is that the SSA creates a list using birth records of all SSN and birthdates. This list would be given to the repositories that may not sell, distribute or use it for other than the intended purpose. Should a credit application be submitted with the SSN of an individual (child) on the list, then that application must be further investigated and such investigation well documented. When a child reaches the age of majority, their information would be deleted from the list. ITRC would also like to see any person who commits child identity theft receive an enhanced penalty for this crime.

**4. The need to find alternate ways to protect identifying numbers used by the government: military ID number, Medicare/MediCal number, etc.**

**Finding:** On July 6, 2003, Parade Magazine's (in the Sunday paper) centerpiece discussed identity theft. More than 70% of the emails ITRC received were from people either concerned about lost and stolen wallet issues or from people who are angry at either governmental agencies (SSA, military) or health providers that place the SSN on a card they must carry on a daily basis. Those many concerns must not go unheard.

Lost and stolen wallets are a prime way for thieves to gather information. Unfortunately, the federal government as well as state governments (and health providers) also use SSN as employee or member numbers: military, elders and Medicare, etc. These numbers are seen by dozens of people through the course of daily activities. Colleges and universities must also be included in this list since NY is the only state that prohibits the use of the SSN as the student identifier and almost all college students we have spoken with have told us that it is being used as their student ID number—often written down on rosters, papers passed around classrooms, posted on bulletin boards, placed on college transcripts, etc.

**Recommendation:** If the SSN must be in the database, then we must find a way to assign a random number that will be on the card that is carried and put on the multiple forms that are filled out by the individual. Right now, college students, seniors and military are our most vulnerable population groups due to the fact that their SSN is so widely known and used. That number can be linked in a database if necessary, at a high level of security. If the federal government expects the business community to change systems, it must lead by example.

**5. Overuse of the SSN**

**Findings: The following categories demonstrate the problem of the overuse of the SSN.**

- Employer use of SSN as individual employee (private or governmental) ID number, including public display of such, e.g., timecards, timesheets, cash register use number, badges, etc.
- The use of the SSN as an identifier by a business group, printed on a card carried by the person on a regular basis.
- Mail theft—where the SSN is printed unnecessarily on the document being mailed and is intercepted by another person.
- Theft of SSN given in good faith to a business who required the information to complete a transaction or activity—e.g., get health care benefits.

- Domestic abuse, harassment of an ex—due to extensive use of the SSN as an identifier. Most of us know the SSN of our spouses, ex-lovers, etc. This crime is a perfect tool to harm another.

**Recommendations:** Private entities may not use the SSN other than for tax purposes or other purposes so designated by either state or federal governmental agencies. They may not publicly display, use, sell or share the information. Language for a bill may be found in California's SSN Confidentiality bills, many written by CA Senator Debra Bowen.

**6. SSN Protection**

**Findings:** It is critical that any entity, whether private or governmental, safeguard identifying information properly. The following categories are just some of the areas that must be included in any legislation considered.

- Need to render all sensitive information unreadable prior to disposal, electronic or in paper format
- Restrict collection of information not needed for the necessary task or program
- Need to require adequate database and paper information storage
- Need to require notification of any database or information breach

**Recommendations:** It is critical that minimum standards be set for acquiring, access, disposal, storage and breach of information fields that include the SSN as well as other sensitive information. This includes what information may be requested by a company and when. For example, no one is hired on the basis of a job application. That is a screening device and hundreds may be collected for a single job. Yet each one asks for your SSN. Why? All they need to do at that stage is ask if you have a SSN and would be willing to provide it upon request. That information can be exchanged when an employer is narrowed the field and is serious about a new hire. This protects consumers from overextension and viewing of the SSN (think of the many applications a job seeker fills out) and limits the company's liability in terms of acquiring and storage of sensitive information. Language for some of these bills can be found in some new California laws as well as in some of the bills now under consideration at the federal level.

**7. Restrictions on sale of SSN and credit info**

**Finding:** The less people with access to SSNs, the less opportunity there is for leakage to identity thieves.

**Recommendation:** Federal restrictions on the sale, exchange or transfer of SSN and credit info to third parties by governmental agencies or private entities.

**8. Restriction on public posting of SSN**

**Finding:** This problem falls into two categories: websites and public records. Both allow unlimited viewing by both criminals and people with legitimate purposes.

**Recommendations:**

- Federal restrictions regarding the publication of SSNs of individuals, alive or dead, on web sites, e.g., Ancestry.com.
- Federal requirements to truncate parts of SSN and other sensitive information (to be decided by committee) on documents available to the public, e.g., electronic court records, birth and death certificates, etc., unless the requesting party has a legitimate reason for such information.

**IN CONCLUSION:**

The crime of identity theft, like any other thing in our society grows, evolves and constantly changes along with the changes in our society. In 1970, the writers of the FCRA could not have predicted the credit trends and practices of the year 2003. They created the FCRA when all business was conducted in person, in communities where people were known and applications could be verified.

When FDR expanded the use of the SSN as an identifier, he could not have anticipated the Pandora's box that he would open. It was impossible to predict the impact of the information age and how computer technology would allow a crime like identity theft to flourish.

In 2000, the FTC held a hearing on ID theft in which ITRC participated. The FTC has continued to monitor this crime through its databases and through victim panels. The information has not changed, nor have the laws. In fact, members of ITRC's staff has attended hearings and provided information for years now to federal legislators and governmental agencies about changes that need to be made, but few if any bills have been passed. The most recent was passed because of its link to Home-

land Security. It imposes higher penalties for all those criminals who are not caught in the first place.

Now it has come down to the final question. Can you meet the challenge to create and pass the much-needed bills in a timely manner, prior to the end of this year? If you cannot, then all this action and activity is nothing more than talk. If you are serious about identity theft and feel you can address it sufficiently on a national basis, this is your opportunity to prove it. But keep in mind—we (consumer, victims, advocates and the business community who care about combating this crime) have high standards for the laws that you pass. We will not accept weak laws that either do little to help the situation or weaken existing laws that have a proven track history. State legislators will take action where the Federal government fails to.

ITRC's sole purpose is to combat this crime and to help victims. Its fear is that the public will be promised strong laws that allow for expansion and redirection as this crime evolves, but such laws will never materialize.

ITRC believes it is the time for some action. We need the subjects covered by this testimony to be addressed and signed into law. The greatest leaders throughout history have led by example. They never asked of others what they were not willing to do themselves. The federal government must also change their practices by protecting SSNs for military personnel, our seniors and governmental employees. Otherwise, they do not have the right to ask the business community to comply. This administration and this Congress must take the lead and set the standard for the rest of the country. It is up to you to show us that this crime is being taken seriously by one and all.

Thank you for your time and consideration.

---

Chairman SHAW. Mr. Hoofnagle.

**STATEMENT OF CHRIS JAY HOOFNAGLE, DEPUTY COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER**

Mr. HOOFNAGLE. Thank you, Chairman Shaw, and Members of the Subcommittee. My name is Chris Hoofnagle, and I am Deputy Counsel with the Electronic Privacy Information Center. We appreciate the opportunity to testify on this very important matter today. In our written testimony, we detailed the development of the SSN and historical attempts to regulate the identifier. As you are well aware, today the SSN plays an unparalleled role in the identification, authentication and tracking of Americans, but I would like to focus my comments today on several recent developments—developments that include large-scale theft of identity cases, the continued use of a SSN by private sector actors, including colleges and universities and the role of States in passing Social Security legislation. I believe these developments continue to institute more evidence that a national framework for privacy protection for the SSN is necessary. Accordingly, I am here to make only one recommendation today, and that is to ask the Committee to reintroduce H.R. 2036 from the 107th Congress. That is an excellent measure. Many of its provisions will allow us to put the SSN genie back into the bottle. Often in the privacy debate, people say it is too late, that your privacy is already gone, but as we have seen with telemarketing, it is possible to assign rights and responsibilities and personal data and help put our private information back into the bottle and safeguard individual rights.

Again, I think there are three recent trends that are worth highlighting. The first, of course, is that the SSN continues to be the key to identity theft, as Mr. Wern testified. In our written testimony, we identify several cases where identity thieves or computer crackers have targeted databases that contain the SSN. In a New

York case SSNs were stolen from a State insurance fund, a college and several private businesses. Another involved a computer help desk employee who using access codes for Ford Motor Credit was able to obtain tens of thousands of credit card reports with SSNs from Experian. Yet another involved employees who took advantage of a patient identification system that used the SSN to commit identity theft. Researchers at Michigan State University recently studied over 1,000 identity theft cases and found that victims in 50 percent of the cases specifically reported that the theft was committed by an employee of the company that maintained their personal information. There is very little an individual can do about these identity theft cases that are insider jobs or cases where personal information is stolen from a database, and this is one of the reasons why we think we need to get the SSN out of circulation, to stop reliance on the identifier, because in most cases, you can't prevent its theft.

Another trend illustrated in our written testimony is that many public and private sector entities continue to use the SSN for identification. As we have testified before, in most cases, it is wholly unnecessary for a business to collect your SSN. The Blue Cross/Blue Shield insurance cards that Representative Cardin and Mr. Wern held up contain their SSN, and there is absolutely no reason for them to do that. They could assign a random identifier, and the only case where they actually need to collect the SSN is when your health costs actually have a tax consequence. Nevertheless, recent news reports indicate that major companies, including Blockbuster Video, Sam's Club, and Costco continue to demand a SSN for membership. A related problem is that many colleges and universities in the country continue to use a SSN as the primary student identifier. In a recent study done by the American Association of Collegiate Registrars of 1,300 institutions, half of those polled claim that they still use a SSN as a primary identifier. It is actually on the card, the student identity card, or in the record database.

These trends involving use and misuse of the SSN and identity theft have actuated State leaders to create new protections for personal information. In the college and university context, about six States have passed laws saying that schools can't use the SSN as the identifier. In Florida, there was a special grand jury report that recommended that SSNs be scrubbed from public records and from private institutions. They noted specifically that one of the major problems about the SSN was that local governments were asking for it, and then the local government would place it in the public record. In California, Senate bill S. 1386 went into effect just a couple weeks ago, and that legislation requires people who maintain databases that have SSNs in it, to give notice to individuals if their SSN is stolen out of the database. So, assigning a responsibility to people who actually collect the SSN or maintain it can often create new protections. I see that my red light is on, so let me just come to our recommendation, and that is that we do hope that Chairman and other Members will reintroduce H.R. 2036, and we have ideas for substantive improvements to it that we are happy to share with you, many of which are included in our written testimony. Thank you for the opportunity to testify today.

[The prepared statement of Mr. Hoofnagle follows:]

**Statement of Chris Jay Hoofnagle, Deputy Counsel, Electronic Privacy Information Center**

Chairman Shaw, Ranking Member Matsui, and Members of the Subcommittee, thank you for extending the opportunity to testify on use and misuse of Social Security Numbers.

My name is Chris Hoofnagle and I am deputy counsel with the Electronic Privacy Information Center (EPIC), a not-for-profit research organization based in Washington, D.C. Founded in 1994, EPIC has participated in cases involving the privacy of the Social Security Number (SSN) before federal courts and, most recently, before the Supreme Court of New Hampshire.[1] EPIC has also taken a leading role in campaigns against the use of globally unique identifiers (GUIDs) involving the Intel Processor Serial Number and the Microsoft Corporation's Passport identification and authentication system. EPIC maintains an archive of information about the SSN online at http://www.epic.org/privacy/ssn/.

I appreciate the opportunity to testify today. In the testimony below, we will first review historical and recent attempts to regulate the use of the SSN. This section demonstrates that there is ample legislative and judicial support for limitations on the collection and use of the SSN.

The second section describes trends involving the SSN. These include:

- A statistical rise in identity theft complaints to federal authorities.
- The occurrence of several large-scale identity theft cases, many of which involved "insiders" or other trusted persons who had access to SSNs.
- Colleges, universities, and other schools continue to identify students by the SSN.
- Health providers and insurance companies continue to identify individuals by the SSN.
- Companies continue to condition access to products and services on disclosure of the SSN.
- Litigation has provided more privacy for SSNs in some cases.
- Privacy advocates and other activists have posted public officials' SSNs to protest government activity.
- A number of states are innovating solutions to the SSN problem.

Finally, in the last section we recommend that the Committee revisit 107 H.R. 2036, The Social Security Number Privacy and Identity Theft Protection Act of 2001. That bill, which enjoyed wide bipartisan support in the last Congress, should be reintroduced and passed by this Congress. Alternatively, we recommend that the Committee consider 108 H.R. 1931, the Personal Information Privacy Act of 2003. That bill would establish important protections for the SSN, including moving the SSN "below the line" on the credit report.

**I. Historical Regulation of the Collection and Use of the SSN**

The Social Security Number (SSN) was created in 1936 as a nine-digit account number assigned by the Secretary of Health and Human Services for the purpose of administering the Social Security laws. SSNs were first intended for use exclusively by the federal government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Over time, however, SSNs were permitted to be used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.

A major government report on privacy in 1973 outlined many of the risks with the use and misuse of the Social Security Number. Although the term "identify theft" was not yet in use, Records Computers and the Rights of Citizens described the risks of a "Standard Universal Identifier," how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted "prohibiting

[1] *Estate of Helen Remsburg v. Docusearch, Inc., et al*, C–00–211–B (N.H. 2002). In *Remsburg*, the "Amy Boyer" case, Liam Youens was able to locate and eventually murder Amy Boyer through hiring private investigators who tracked her by her date of birth, Social Security Number, and by pretexting. EPIC maintains information about the Amy Boyer case online at http://www.epic.org/privacy/boyer/.

use of an SSN, or any number represented as an SSN for promotional or commercial purposes."[2]

In response to growing risks over the accumulation of massive amounts of personal information and the recommendations contained in the 1973 report, Congress passed the Privacy Act of 1974.[3] Among other things, this Act makes it unlawful for a governmental agency to deny a right, benefit, or privilege merely because the individual refuses to disclose his SSN. This is a critical principle to keep in mind today because consumers in the commercial sphere often face the choice of giving up their privacy, their SSN, to obtain a service or product. The drafters of the 1974 law tried to prevent citizens from facing such unfair choices, particularly in the context of government services. But there is no reason that this principle could not apply equally to the private sector, and that was clearly the intent of the authors of the 1973 report.

Section 7 of the Privacy Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." At the time of its enactment, Congress recognized the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of this provision, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." Short of prohibiting the use of the SSN outright, the provision in the Privacy Act attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed where the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

It is certainly true that the use of the SSN has expanded significantly since the provision was adopted in 1974. This is particularly clear in the financial services sector. In an effort to learn and share financial information about Americans, companies trading in financial information are the largest private-sector users of SSNs, and it is these companies that are among the strongest opponents of SSN restrictions.

Outside the financial services sector, many companies require the SSN instead of assigning an alternative identifier. These requirements appear in a myriad of commercial interchanges, many of which absolutely do not require the SSN. For instance, Golden Tee, a popular golf video game, requires players to enter their SSN in order to engage in "tournament play."[4] The company could assign its own identifier for players, but instead relies upon the SSN, which puts players at risk by requiring them to further circulate personal information.

It is critical to understand that the legal protection to limit the collection and use of the SSN is still present in the Privacy Act and can be found also in recent court decisions that recognize that there is a constitutional basis to limit the collection and use of the SSN. When a Federal Appeals court was asked to consider whether the state of Virginia could compel a voter to disclose an SSN that would subsequently be published in the public voting rolls, the Court noted the growing concern about the use and misuse of the SSN, particularly with regard to financial services.[5] The Fourth Circuit said:

> Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck. . . . Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous.[6]

The Court said that:

> The statutes at issue compel a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the funda-

---

[2] Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens* 108–35 (MIT 1973) (Social Security Number as a Standard Universal Identifier and Recommendations Regarding Use of Social Security Number).

[3] 5 U.S.C. § 552a.

[4] Official ITS Rules, at http://www.itsgames.com/ITS/its__rules.htm.

[5] *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993).

[6] *Id.*

> mental right to vote. As illustrated by the examples of the potential harm that the dissemination of an individual's SSN can inflict, Greidinger's decision not to provide his SSN is eminently reasonable. In other words, Greidinger's fundamental right to vote is substantially burdened to the extent the statutes at issue permit the public disclosure of his SSN.[7]

The Court concluded that to the extent the Virginia voting laws, "permit the public disclosure of Greidinger's SSN as a condition of his right to vote, it creates an intolerable burden on that right as protected by the First and Fourteenth Amendments."[8]

In a second case, testing whether a state could be required to disclose the SSNs of state employees under a state open record law where there was a strong presumption in favor of disclosure, the Ohio Supreme Court held that there were privacy limitations in the federal Constitution that weighed against disclosure of the SSN.[9] The court concluded that:

We find today that the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs. Our holding is not intended to interfere with meritorious investigations conducted by the press, but instead is intended to preserve one of the fundamental principles of American constitutional law—ours is a government of limited power. We conclude that the United States Constitution forbids disclosure under the circumstances of this case. Therefore, reconciling federal constitutional law with Ohio's Public Records Act, we conclude that [the provision] does not mandate that the city of Akron discloses the SSNs of all of its employees upon demand.[10]

In an important recent case from the U.S. Court of Appeals for the D.C. Circuit, a Court upheld the Federal Trade Commission's determination that SSNs are nonpublic personal information under the Gramm-Leach-Bliley Act.[11] The Court rejected First and Fifth Amendment challenges to regulations that restricted the use of the SSN without giving the individual notice and opportunity to opt-out. Additionally, the Court upheld regulations that prohibited the reuse of SSNs that are furnished to credit reporting agencies.[12]

While it is true that many companies and government agencies today use the Social Security Number indiscriminately as a form of identification and authentication, it is also clear from the 1936 Act, the 1974 Privacy Act, and these three cases—*Greidinger v. Davis*, *Beacon Journal v. City of Akron*, and *Trans Union v. FTC*—that there is plenty of legislative and judicial support for limitations on the collection and use of the SSN. The question is therefore squarely presented whether the Congress will at this point in time follow in this tradition, respond to growing public concern, and establish the safeguards that are necessary to ensure that the problems associated with the use of the SSN do not increase.

**II. Recent SSN Trends**

Just in the last eighteen months, there have been a number of important SSN developments. These developments, which range from large-scale incidents of identity theft to continued reliance on the SSN in the private sector, underscore the continued need for a national framework of protections for the SSN.

*Identity Theft Complaints Increase*

The FTC reported on January 22, 2003 a large increase in the number of fraud complaints and a doubling of the dollar loss attributable to fraudulent activities directed at US Consumers.[13] The agency noted that the number of fraud complaints rose from 220,000 in 2001 to 380,000 in 2002 and the loss to consumers grew from $160 million in 2001 to $343 million in 2002. The report revealed that identity theft topped the list, accounting for 43% of the complaints lodged in the Consumer Sentinel database.

---

[7] *Id.*
[8] *Id.*
[9] *Beacon Journal v. City of Akron*, 70 Ohio St. 3d 605 (Ohio 1994).
[10] *Id.*
[11] *Trans Union L.L.C. v. Fed. Trade Comm'n*, No. 01–5202, 295 F.3d 42 (D.C. Cir. 2002), at http://pacer.cadc.uscourts.gov/common/opinions/200207/01–5202a.txt.
[12] *Id.* In another recent case, the D.C. Circuit rejected a First Amendment challenge to the use of credit reports for marketing purposes. *Trans Union v. FTC*, 245 F.3d 809 (D.C. Cir. 2001), *cert. denied*, 536 U.S. 915 (2002).
[13] *Fraud Charges Jump in 2002 on Consumer Complaints, ID Thefts*, Electronic Commerce & Law Report, Vol 8(4), Jan. 29, 2003, 88.

*The SSN Continues to be the Key to Identity Theft*

On January 10, 2002, a special Florida grand jury commissioned to investigate identity theft recommended stronger legal protections for personal data, including SSNs, held by business and State agencies.[14] It called for laws that would prohibit the credit industry from selling personal data without consumer consent, and would stop State agencies from disseminating personal information under the open records law without individual consent, court order, or the articulation of a compelling need. The panel charged 33 individuals with criminal use of personal identifying information, fraud, grand theft, and money laundering. The grand jury estimated that the current $2.5 billion nationwide cost of identity theft is expected to grow to $8 billion by 2005. It cited health clubs and video rental stores requiring SSNs on applications and local governments asking for SSNs on routine transactions.

In August 2002, New York Attorney General Eliot Spitzer reported that law enforcement authorities had broken "a massive identity theft ring."[15] The information involved included SSNs, credit card numbers, and bank account information stolen from the NY State Insurance Fund, Social Security Administration, Empire State College, WNYC radio, Hollywood video, Worldcom Wireless, and American Express. The indictment alleges that this personal information was stolen between 1998 and 2002, and used to purchase computer equipment, cell phones, and other merchandise.

In November 2002, it was discovered that a former computer help desk employee had obtained 30,000 credit reports directly from a credit reporting agency. The former employee sold the reports to others for between $30–60 each.[16] The information was used for credit fraud.

In December 2002, personal health care information, including SSNs, of more than 500,000 military personnel, retirees and family members in 16 Midwestern and western States were stolen from a military contractor. Also stolen were some active-duty service members' claims processing information, which include their names, SSN, and list of medical procedures and diagnosis codes for medical care already performed.[17] TriWest stated that it attempted to notify beneficiaries by sending them letters and by posting notices on its web site. The database was not encrypted and TriWest relied on the SSN as an identifier.

In February 2003, two former employees of health facilities and six others were charged with stealing patient SSNs that were used to open fraudulent credit card and phone accounts.[18] The suspects stole $78,000 in goods and services. One of the facilities involved has now implemented a new patient information system that doesn't label patients by the SSN.

Because of these and other developments, the Wall Street Journal, in its 2003 "to not do list," advised individuals not to give out their SSN: "Don't give out your Social Security number unless you have to: With identity theft a growing problem, you should be extremely cautious about giving out that information. Many organizations ask for it, from volunteer groups to retail stores to Web sites, but not all of them require you to provide it."[19]

But as the cases listed above illustrate, many identity theft cases are "insider jobs," committed by employees who obtain access and misuse individuals' personal information stored in their employers' databanks. Researchers at Michigan State University recently studied over 1000 identity theft cases and found that victims in 50% of the cases specifically reported that the theft was committed by an employee of a company compiling personal information on individuals.[20] There is very little that an individual can do to prevent insider jobs, or cases where the SSN is stolen from a database.

---

[14] *Identity Theft in Florida*, Sixteenth Statewide Grand Jury Report, SC 01–1095, Supreme Court of Florida, Jan. 10, 2002, at http://www.idtheftcenter.org/attach/FL_idtheft_gj.pdf;see also *Florida ID Theft Panel Backs More Safeguards for Government and Corporate Data*, Privacy Times, Vol 22(3), Jan. 30, 2002, 3–4.

[15] *New York Authorities Say They've Cracked 'Massive' Identity Theft Ring, Four Indicted*, Electronic Commerce & Law Report, Vol 7(31), Aug. 7, 2002, p. 794.

[16] *Huge ID-theft ring broken; 30,000 consumers at risk*, Seattle Times, Nov. 26, 2002.

[17] *Patient Data, 500,000 SSNs Stolen From DOD System*, Privacy Times, Vol 23(1), Jan. 2, 2003, 2.

[18] Margaret Zack, *Eight charged with stealing patient IDs for credit cards*, Star Tribune, Feb. 21, 2003, p. 1B.

[19] *A To-Don't List For the New Year, Hot to Fix Your Life in 2003*, Wall Street Journal, Dec. 31, 2002.

[20] Study forthcoming; results provided in email from Judith M. Collins, Ph.D., Associate Professor, Leadership and Management Program in Security School of Criminal Justice, Michigan State University to EPIC (Apr. 22, 2003, 18:13:35 EST) (on file with EPIC).

*The SSN is Still Being Used as a Student Identifier*

Although privacy protections are important to students, student development, and to principles of academic freedom, schools have not always been sensitive to student informational privacy issues. A handful of states, including Arizona,[21] New York,[22] Rhode Island,[23] and Wisconsin[24] have enacted laws to regulate college and university use of the SSN. Nevertheless, in a survey of 1,300 institutions polled by the American Association of Collegiate Registrars and Admissions Offers, half reported that they use the SSN as the primary student identifier.[25]

In August 2002, it was revealed that a Princeton admissions officer used the SSNs of applicants to his school to view the Yale University's web site for admissions. The unauthorized entry allowed Princeton to learn whether Yale had accepted students who had applied to both schools. Cracking the system was easy: Anyone who knew an applicant's birth date and SSN could log on.[26]

In March 2003, federal prosecutors charged a University of Texas student with breaking into a school database and stealing more than 55,000 student, faculty, and staff names and SSNs. The student was charged with violating the Computer Fraud and Abuse Act of 1986 and the Identity Theft and Assumption Deterrence Act of 1998. This occurrence led to a new Texas law protecting against identity theft.[27]

Also in March 2003, it was reported that the California State University's $662 million computer system contains a security flaw that gives users access to student and employee SSNs and other confidential data. The problem was known for years, and university officials had told state auditors they were not going to fix the vulnerability, citing cost and time concerns.[28]

In May 2003, a 17-year-old student of a Chino, CA high school allegedly cracked the school's computer system, changing his and a classmate's grades and also tapping into confidential student information, including the SSN.[29] Apparently, 1,744 students had their SSNs in the database.

For model approaches to the transition to an alternative student identifier, I would look to the leadership of Virginia Rezmierski, Professor at the Gerald R. Ford School of Public Policy at the University of Michigan.[30] Additionally, officials at the University of Illinois have established a procedure to reduce reliance on the SSN.[31] The University of Pennsylvania is addressing the issue as well. That institution appointed Lauren Steinfeld, a former privacy expert at the Office of Management and Budget, to address SSN issues.

*The SSN Has Become a Default Health Identifier*

Many medical providers are using the SSN as a patient identifier. As David Miller noted in testimony before the National Committee on Vital Health Statistics:

"It should be noted that the 1993 WEDI [Workgroup for Electronic Data Interchange] Report, Appendix 4, Unique Identifiers for the Health Care Industry, Addendum 4 indicated 71% of the payers responding to the survey based the individual identifier on the Member's Social Security Number. However 89% requested the insured's Social Security Number for application of insurance. Clearly the Social Security Number is the current de facto identifier. . . ."[32]

But individuals and companies are resisting such use of the SSN. Acting on employees' suggestions, I.B.M. has requested that health companies stop using the

---

[21] Ariz. Rev. Stat. § 15–1823.
[22] N.Y. Educ. Code § 52–b.
[23] § 42–72.5–2(6); § 16–38–5.1.
[24] Wisc. Stat. Ann. § 118.169.
[25] Kristen Gerencher, *Social Security numbers up for grabs. Companies, government lax in preventing identity theft*, CBS MarketWatch, May 7, 2002, at http://cbs.marketwatch.com/news/story.asp?guid=%7B9A569387%2DE7FD%2D44AB%2D8F5F%2D112D25915DA5%7D&siteid=mktw
[26] John Schwartz, *Privacy vs. Security on Campus*, The New York Times, Aug. 4, 2002, p. 3.
[27] *Univ. of Texas SSN*, Privacy Times, Vol 23(6), Mar. 17, 2003, 11.
[28] Terri Hardy, *CSU computer flaw allows access to confidential data*, The San Diego Union Tribune, Mar. 22, 2003, p. A–13.
[29] Kristina Sauerweine, *Youth Hacked Into Database*, Los Angeles Times, May 21, 2003, p. 5.
[30] *See also Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities*, EDUCAUSE White Paper, Apr. 1997, at http://www.educause.edu/ir/library/pdf/pub3102.pdf.
[31] Carol Livingstone, Mike Corn & Lisa Huson, *University of Illinois Social Security Number Policy Implementation*, Jan. 10, 2001, at http://www.ssn.uillinois.edu/assets/applets/UIUC_SSN_Presentation_1_10_2002.pdf; Andrea L. Foster, *U. of Illinois May Be a Model in Protecting Privacy*, Chronicle of Higher Education, Aug. 2, 2002.
[32] Testimony of David S. Miller, Director, Health System Services, UHC, on the Unique Patient Identification Number at the National Committee on Vital Health Statistics hearing in Chicago, Jul. 21, 1998, at http://www.cchconline.org/privacy/uhc.php3.

SSN on insurance cards. According to IBM, fifteen insurers, which cover about 30,000 of the company's 500,000 employees worldwide have either not responded or indicated that they will not comply with the request.[33]

*SSN Required for Access to Products, Services*

Major companies, including Blockbuster, Sam's Club and Costco continue to demand the SSN and other unnecessary information on their applications for access to products and services.[34]

*SSN Litigation Has Yielded Mixed Results for Privacy Protection*

In February 2002, the New Hampshire Supreme Court ruled for the first time that New Hampshire State residents can sue companies that sell their personal data or SSN, or obtain their work address through the use of pretextual phone calls.[35] The Court found that the sale of such data was actionable if it subjected a person to foreseeable harm. It also ruled that people have a reasonable expectation of privacy in their SSNs, even though SSNs must be disclosed in certain circumstances. The ruling clears the way for a trial against Docusearch, the information broker who sold the SSN, home and work address of Amy Boyer to the man who stalked and murdered her.

In September 2002, the Fourth Circuit held that individuals cannot recover damages under the Privacy Act without a showing of actual harm.[36] This ruling is in conflict with the law in several other circuits, and the Supreme Court has granted certiorari in the case. In *Doe v. Chao*, the Department of Labor used individuals' SSNs to identify their compensation claims. As a result, the SSNs were cited in public records and are now widely available. Although the plaintiff was embarrassed and placed at risk as a result of the disclosure, the Fourth Circuit held that one needs other manifestations of emotional distress in order to prove that harm occurred. We believe that the Fourth Circuit improperly interpreted the damages section of the Privacy Act, and we plan to file an amicus brief with the Supreme Court in support of the plaintiff.

In June 2003, a federal judge in Detroit ruled that the Privacy Act creates a private right of action for violating procedural rules relating to SSNs, but only as they apply to federal agencies, not states or municipalities.[37] Judge Anna Taylor dismissed a suit seeking Privacy Act damages from the City of Detroit after its contractor mailed tax forms to residents with their SSNs printed on the mailing label. The Judge stated that plaintiff Daniel Schmitt failed to show that he was adversely affected or that Detroit acted willfully or intentionally because like the IRS, most local and State tax authorities request SSN for taxpayer identification purposes. The City vowed to keep SSNs off labels and attach a disclosure statement to the tax forms about SSNs, as required by the Privacy Act.[38]

*SSNs Are Being Used for Political Protest*

California-based Foundation for Taxpayer and Consumer Rights posted partial SSNs of state legislators who voted in opposition of privacy legislation.[39] The group purchased the SSNs online for $26, demonstrating that access to sensitive information is convenient and inexpensive.

In June 2003, the Attorney General of Washington State decided not to defend a law designed to prohibit a web site that posts the names, addresses and home-phone numbers of police in Western Washington. As a result, Bill Sheehan III of Mill Creek is free to continue publishing his web site, www.justicefiles.org, which includes names and salaries of many Western Washington police officers and in some cases their SSNs, birth dates, home addresses and phone numbers. Sheehan claims that publishing such information is the best way to hold law-enforcement officers accountable to the public.[40]

---

[33] Marc Ferris, *IBM asks providers to drop SSNs*, New York Times, Feb. 23, 2003, p. 3.

[34] *A dubious privilege*, Chicago Tribune, Feb. 23, 2003, p. 2.

[35] *Helen Remsburg, Admin of the Estate of Amy Boyer v. DocuSearch, Inc*., et al 2002 U.S. Dist. LEXIS 7952, NH Supreme Court No. 2002–255, Feb. 18, 2002; *N.H. Supreme Court Backs Privacy for SSNs, Personal Data*, Privacy Times, Vol 23(4), Feb. 18, 2003, 3–4.

[36] *Doe v. Chao*, 306 F.3d 170 (4th Cir. 2002).

[37] *Schmitt v. City of Detroit, et al*. 2003 U.S. Dist. LEXIS 10246, (E.D. Mich. 2003).

[38] *Privacy Act Permits Suits Over SSNs, but Not Against Cities*, Privacy Times, Vol 23(13), Jul. 1, 2003, 6.

[39] Christian Berthelsen, *Extreme lobbying upsets Assembly, Lawmakers mad at response to killing privacy bill*, San Francisco Chronicle, Jun. 19, 2003, at http://www.sfgate.com/cgi-bin/ article.cgi?file=/c/a/2003/06/19/ MN127207.DTL.

[40] *State won't defend law to shut down Web site that publishes police data*, Seattle Times, Jun. 24, 2003, p. B3.

*States Innovating Solutions*

California's Senate Bill 1386 went into effect on July 1, 2003.[41] That legislation requires companies that maintain SSNs and other personal information to notify individuals when they experience a security breach. The bill came in response to an April 2002 incident in which the records of over 200,000 state employees were accessed by a computer cracker. The California legislation exceeds federal protections, as there is no national requirement for notice to individuals when personal information is accessed without authorization.

More specifically, the legislation creates a notice requirement where there has been an unauthorized acquisition of an individual's name along with a Social Security Number, a driver's license number, or an account number and corresponding access code. The notice requirement is also triggered when there is a reasonable belief that a security breach occurred. Notice must be given "in the most expedient time," but may be delayed where it would impede a criminal investigation.

Although this state law does not directly regulate collection or use of the SSN, it is likely to provide more privacy for Californians. The legislation places new responsibilities on those who collect the SSN, as a result, businesses are more likely to avoid collecting the SSN.

**III. Recommendations**

*107 H.R. 2036, The Social Security Number Privacy and Identity Theft Protection Act of 2001, was a good proposal. This Congress should revisit and pass this important bill.*

We recommend that the Committee visit the Social Security Number Privacy and Identity Theft Protection Act of 2001, 107 H.R. 2036, as a guide to limiting the use of the SSN. The measure was sponsored by Representative Clay Shaw (R–FL). In the 107th Congress, the bill enjoyed bi-partisan sponsorship of over 70 Members. The measure contained a comprehensive set of rights to protect individuals from identity theft.

Title I of the bill would have established important protections against public-sector sale or display of SSNs. These provisions will prohibit the display of the SSN on checks and government-issued employment cards. The bill would have prohibited disclosure of the SSN to inmates, and appearance of the SSN in public records. Increasingly, public records are a source for the collection of personal identifiers that then can be reused for any purpose.

The bill would have also prohibited "coercive disclosure" of the SSN—the practice of denying a product or service when an individual refuses to give a SSN. Additionally, Section 203 of that bill would have placed the SSN "below the line" on credit reports. This is an important and much needed protection that would stem trafficking in SSNs.

Alternatively, we recommend that the Committee consider 108 H.R. 1931, the Personal Information Privacy Act of 2003. That bill was introduced by Representative Kleczka (D–WI) in May and referred to the Committee on Ways and Means. H.R. 1931 would establish important protections for the SSN, including moving the SSN "below the line" on the credit report. The bill would also limit the use of "transaction and experience" information, and require opt-in consent before credit or insurance prescreening letters are sent. Such letters are a major source of the identity theft problem. Under the bill, aggrieved individuals have a private right of action against violators.

**IV. Conclusion**

Without a framework of restrictions on the collection and use of the SSN and other personal identifiers, identity theft will continue to increase, endangering individuals' privacy and perhaps the security of the nation. The best legislative strategy is one that discourages the collection and dissemination of the SSN and that encourages organizations to develop alternative systems of record identification and verification. It is particularly important that such legislation not force consumers to make unfair or unreasonable choices that essentially require trading the privacy interest in the SSN for some benefit or opportunity.

It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal privacy. Given the unique status of the SSN, its entirely inappropriate use as a national identifier for which it is also inherently unsuitable, and the

[41] http://www.leginfo.ca.gov/cgi-bin/postquery?bill__number=sb__1386&sess=PREV&house=B&author=peace

clear history in federal statute and case law supporting restrictions, it is fully appropriate for Congress to pass legislation.

I am grateful for the opportunity to testify this afternoon and would be pleased to answer your questions.

---

Chairman SHAW. We have your written testimony. It will be made part of the record, and it will be examined closely. Mr. Collins, will you introduce Mr. Edwards, please.

Mr. COLLINS. It is my pleasure, Mr. Chairman, to introduce to you a fellow Georgian, Mr. Steve Edwards. Mr. Edwards joined the Georgia Bureau of Investigation in 1973. For the last 15 years, his work has focused specifically on financial investigations, health care fraud, and computer crime investigations. He has been on the National White Collar Crime Center Board since 1997, and now he is Vice Chairman, which represents southeast region States—West Virginia, Virginia, Kentucky, Tennessee, North and South Carolina, Georgia, and Florida, as well as Puerto Rico and the Virgin Islands. For his next trip to the Virgin Islands, he plans to take one of the Congressman from Georgia. He also served as a negotiator for Georgia Special Weapons and Tactics (SWAT) team. He is a coordinator of the U.S. Department of the Treasury's Financial Crimes Enforcement Network, and he has just done a super job for Georgia, working in the Georgia Bureau of Investigation. Welcome, Mr. Edwards.

**STATEMENT OF STEVE EDWARDS, STATE COORDINATOR, FINANCIAL CRIMES ENFORCEMENT NETWORK, VICE CHAIRMAN, BOARD OF DIRECTORS, NATIONAL WHITE COLLAR CRIME CENTER, RICHMOND, VIRGINIA, MEMBER, GEORGIA'S STOP IDENTITY THEFT NETWORK, CHAIR, INFRAGARD ATLANTA CHAPTER WATCH AND WARN COMMITTEE, AND SPECIAL AGENT IN CHARGE, FINANCIAL INVESTIGATIONS UNIT, GEORGIA BUREAU OF INVESTIGATIONS, DECATUR, GEORGIA**

Mr. EDWARDS. Thank you, Mr. Collins. It is a pleasure to be here, and I am a little overwhelmed by that introduction. I don't deserve that, but thank you very much. Thank you, too, Chairman Shaw, for the opportunity to address the Subcommittee concerning identity theft. What I would like to talk about or take the opportunity to discuss is the Georgia Stop Identity Theft Network, and some of the reasons that we formed that network. A primary complaint of victims of identity theft is that they are unable to get satisfaction. They are often unable to find an agency or an organization that is willing to assume responsibility for helping them to deal with the crime they have experienced. Victims of identity theft also have difficulties with legal jurisdiction. For example, if a victim who resides in Georgia is confronted with identity theft that occurred in California, local law enforcement in Georgia may tell them that they do not have jurisdiction or they are not a victim. To address this problem, Georgia and some other States, a few other States, require that a police report be generated for all reported cases of identity theft. This police report is a useful tool for the victim when reporting a violation to other organizations. In essence, a primary need for victims of identity theft is a one-stop

shop, whether physical or online. The Stop Identity Theft Network in October 2002 actually developed and created and put online a complaint program. Since that program has been in existence, we have had 233 complaints processed through it.

The way it works is after the victim files a complaint, the network submits the complaint to the cities, counties, and State law enforcement having jurisdiction or venue. Not only in the State of Georgia, but across the country. Along with the complaint is a letter explaining to the agency what it means and the other agencies that have received the same complaints so they can coordinate their efforts. In the past 30 years, I have been a Georgia Bureau of Investigation agent. I have seen no other crime directly affect more friends, associates, and family members than identity theft. Since 2000, when I became actively involved in the development of the Stop Identity Theft Network, I have received an average of two or three telephone calls per month from someone I know who has been a victim of identity theft. The illegal use of SSNs is key to laying the groundwork to take over someone's identity. Containment of widespread use of SSNs could have a substantial impact in the prevention of identity theft. This containment is important not only in areas of government, but the use of SSNs as individual identifiers within the private sector as well. Examples of current broad use of SSNs—and this has already been discussed, but I will say it again—driver's license, student records, bank accounts, utility services, insurance policies, credit bureau records, cash checking services, medical services, apartment rental, employment, membership, and even in some areas library access.

While it may not be feasible to restrict the use of SSNs to administer Social Security taxation, it is recommended that SSNs be restricted for other uses. The development of these restrictions is appropriately the responsibility of Congress and consistent with other privacy measures, particularly in the absence of uniform aggressive action among State and local governments, as well as the private industry, to reduce opportunities for identity theft. In those instances where SSNs are deemed suitable for recording their existent need to create statutory incentives for organizations to safeguard this information. While few States have some form of accountability already on the books, there is no uniformity. In addition, creating a statutory category of liability would serve both to increase the victim's chances in civil court and to put the organizations on notice to change their behavior. It has been recognized that no Federal law currently limits use or disclosure of SSNs among private entities. The SSA cannot control how private entities keep use or distribute SSNs. Thus leaving the burden on the consumers who have no real power. Many bills responding to the problem of identity theft have been introduced in recent Congresses, and several are again pending. These bills, such as H.R. 2036 which you sponsored in the 107th Congress, Mr. Chairman, would enhance privacy protection and otherwise help prevent fraudulent misuse of SSNs. As you know, other measures are pending in the Congress to protect personal identifiers. While we are not necessarily endorsing every aspect of these various measures, we certainly commend them to your careful consideration as Congress acts along with the States to better enable effective responses

and efforts to prevent identity theft. Thank you, and thank you Mr. Collins, for the opportunity to testify before you today; I am eager to answer any questions you or other Members of the Subcommittee have. Thank you all.

[The prepared statement of Mr. Edwards follows:]

**Statement of Steve Edwards, State Coordinator, Financial Crimes Enforcement Network, Vice Chairman, Board of Directors, National White Collar Crime Center, Richmond, Virginia, Member, Georgia's Stop Identity Theft Network, Chair, Infragard Atlanta Chapter Watch and Warn Committee, and Special Agent in Charge, Financial Investigations Unit, Georgia Bureau of Investigations, Decatur, Georgia**

Chairman Shaw and members of the subcommittee, thank you for this opportunity to address this subcommittee concerning the subject of identity theft.

Introduction

My name is Steve Edwards, and I am Special Agent in Charge of the Financial Investigations Unit of the Georgia Bureau of Investigations (GBI), State Coordinator to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), and Vice Chairman on the Board of Directors of the National White Collar Crime Center (NW3C). In addition, I am a committee member on the State of Georgia's STOP IDENTITY THEFT Network and serve as chair on the FBI's InfraGard Atlanta Chapter Watch and Warn Committee.

GBI is an independent, state-wide agency that provides assistance to Georgia's criminal justice system in the areas of criminal investigations, forensic laboratory services and computerized criminal justice information.

NW3C is a non-profit corporation that provides a national support network for law enforcement agencies, state regulatory bodies, state and local prosecution offices, and other organizations involved in the prevention, investigation, and prosecution of high-tech and economic crime.

Overview of the Problem: On-the-ground Perspective

I would like to take this opportunity to briefly discuss Georgia's STOP IDENTITY THEFT (STOP I.T.) Network and some of the reasons for its formation. A primary complaint of victims of identity theft is, in my experience, that they are unable to "get satisfaction." By this I mean that they are often unable to find an agency or organization that is willing to assume responsibility for helping them to deal with the crime they have experienced. As a result, victims needlessly contact one organization after another in an effort to handle the violation, and may, in the end, receive no assistance at all. In many cases, for example, local law enforcement tell victims of identity theft, "you are not a victim"—particularly if the victim has suffered no direct financial loss. Their advice is often that the victim should contact the organization that was used for the perpetration. The organization involved, in turn, refers the victim to local law enforcement.

Victims of identity theft also have difficulties with the matter of legal jurisdiction. For example, if a victim who resides in Georgia is confronted with identity theft that has resulted in a violation in California, local law enforcement in Georgia may state that they do not have jurisdiction. To address this problem, Georgia, and other states, require that a police report be generated for all reported cases of identity theft. This police report is a useful tool for the victim when reporting the violation to other organizations, such as a credit bureau. Unfortunately, other factors—including lack of resources—often prevent local law enforcement from taking action beyond the generation of a report.

In essence, a primary need for victims of identity theft is a "one-stop-shop," or a single "location"—whether physical or online—where victims can receive information about identity fraud prevention, file a complaint, and receive guidance concerning recovery from identity theft violations. In 2000, Georgia's STOP I.T. Network was conceived as such a location. In October 2002, STOP I.T. went online for the first time, and since then 233 complaints have been received and processed.

After receiving a complaint from a victim, STOP I.T. serves as an intermediary between the victim and a number of agencies. For example, a complaint from a victim in Georgia is forwarded by STOP I.T. to city, county and state law enforcement appropriate to the complaint; to local and state law enforcement in any state where the victim identifies activity associated with the identity theft; to the FTC; and to the Internet Fraud Complaint Center. In addition, STOP I.T. sends to each organi-

zation a letter of explanation that includes a list of every other organization that has received the complaint. Finally, victims receive information to assist them in protecting against the continued fraudulent use of their personal information and in recovering financial and other losses that have resulted from the violation.

In the 30 years that I have been involved in financial crime, I have seen no other crime directly affect more friends, associates, and family members than identity theft. Since 2000, when I became actively involved in the development of STOP I.T., I have received an average of 2 or 3 telephone calls per month from someone I know who has been a victim of identity theft. Data collected across the nation—to the extent that data on identity theft exist—also indicate that identity theft is a crime that is pervasive and expanding rapidly.

Overview of the Problem: Broad Perspective

Identity theft—or the use of "another person's personal information in some way that involves fraud or deception" [1]—is currently one of the fastest growing crimes in the United States.[2] Two of the most common forms of identity theft include "true name fraud" and "account takeover fraud." [3] True name fraud occurs when someone uses an individual's personal information to open a new account, and account takeover involves illegal access to an individual's existing account for the purpose of making fraudulent charges against the account. Identity theft is also used to facilitate other crimes—including money laundering, bankruptcy fraud, computer crimes, and acts of terrorism—by providing a means of concealing the identity of the criminal and accessing funds or privileges available to the victim. It is important to note, however, that financial loss is not a necessary component of identity theft. "Criminal identity theft," for example, occurs when a victim's personal information is used by a criminal and subsequently associated with records of criminal violations, outstanding arrest warrants, or other public information without the knowledge of the victim.

The Federal Bureau of Investigation (FBI) and other law enforcement agencies have estimated that between 700,000 and 1.8 million Americans are victimized by identity theft each year—a figure that has increased substantially in recent years. In addition, recent surveys (conducted by Star Systems, a national electronic payments network) indicate that about 1 in 20 adults in the United States, or about 12 million Americans, have been victimized by identity theft at least once.[4]

In 2002, the number of identity theft cases reported to the Federal Trade Commission (FTC) rose to 161,819—almost twice the number reported in 2001.[5] Other cases were reported directly to local law enforcement; reported to other federal agencies, including the FBI, Secret Service, Internal Revenue Service, and Postal Inspection Service; or never reported at all.

The cost of identity theft to businesses has been estimated to be more than $11.9 billion each year.[6] The costs to victims of this crime include loss of credit, harm to reputation, and loss of wages, in addition to the direct loss of money, attorney fees and other recovery expenses. Despite these losses, and the considerable attention that has been paid to the problem in recent years, the average arrest rate for all identity theft cases reported by victims remains around 5 percent.[7]

Identity Theft and the Use of Social Security Numbers

Since the illegal use of social security numbers (SSNs) "is key to laying the groundwork to take over someone's identity," [7] containment of the wide-spread use of SSNs could have a substantial impact on the prevalence of identity theft in the future. This containment is important not only in areas of government that use SSNs as individual identifiers, but also in private organizations, which are increasingly including SSNs on personal records and distributing this information for a variety of purposes. Examples of the current broad use of SSNs include

- *Driver's Licenses*: As many as eleven states and the District of Columbia currently display the SSN on the face of their drivers' licenses. Several other states require a SSN for the issuance of a driver's license but do not display the number on its face.
- *Student Records*: Half of colleges and universities use SSNs to identify students, and 79% include them in official transcripts, according to a March 2002 survey by the American Association of Collegiate Registrars and Admissions Officers.
- *Other Records*: A SSN is often required or requested for services such as bank accounts, utility services, insurance policies, check cashing services, medical services, apartment rental, extension of credit, employment, memberships, and library access. SSNs are also used as reference numbers for credit bureau reports, which are widely distributed, often without the knowledge of the credit holder.

While it may not be feasible to restrict the use of SSNs to the administration of Social Security taxation, for which it was originally designed, it may be feasible to restrict the use of SSNs to a set of identified purposes for which there is a legitimate legal reason to collect a SSN. In addition, government agencies and businesses that collect SSNs can be required to restrict access to SSNs—by employees and other organizations—and to dispose of records that include SSNs using specified procedures, e.g., encrypting personal information on databases and shredding paper documents containing personal information.

The development of these restrictions is appropriately the responsibility of Congress, and consistent with other privacy measures recently passed, particularly in the absence of uniform, aggressive action among state governments, local governments, and private industry to reduce opportunities for identity theft. In addition, the increasing number of cases being pursued by law enforcement throughout the country evidence the immediate importance of developing these restrictions. For example,

- July 1 and 2, 2003, Consuelo Onate-Banzon and Rony Razon, and four other individuals, were arrested on charges of identification and social security fraud. According to the FBI, Onate-Banzon and Razon worked for the Virginia Department of Motor Vehicles (DMV) and allegedly produced and sold as many as 1,000 fraudulent Virginia driver's licenses, with the help of co-conspirators.[8]
- On May 8, 2003, Dorian Thomas, age 27, was indicted on charges of conspiracy, bank fraud, and identity theft. Thomas, an employee of a financial institution in California, had "obtained the confidential member profile information of account holders through financial institution computers and provided it to others,"[9] who then completed more than $100,000 in fraudulent bank transactions.[10]
- Charmaine Northern, age 23, "pled guilty on March 10, 2003, to obtaining confidential customer account information from the computer at the financial institution where she was working and using it to open credit card accounts and incur unauthorized charges estimated to be approximately $50,000."[13]
- Kimberly Smart, age 27, was sentenced on December 5, 2002, "in connection with using her financial institution position to obtain customer account information from the financial institution computer and provide it to others."[11] The losses incurred in this case were approximately $121,146.63.
- Philip Cummings, a 33-year-old former "help desk" employee of Teledata Communications, Inc., faced charges on November 26, 2002, of accessing credit bureau databases, selling confidential information, and participating in a fraud scheme that resulted in a loss of more than $2.7 million to 30,000 victims.[12]
- Ivy Johnson, a former employee of H & R Block in White Plains, New York, was charged in January 2003, for obtaining customers' personal information, and using the information to divert tax checks, open new credit card accounts, and making ATM withdrawals in victims' names.[13]

All of these cases involved access to and use of SSNs. Future cases of similar violations may be reduced if requirements for specific safeguards are mandated and enforced by federal statute. In addition to legislative restrictions, education and training is also important for the reduction of identity fraud in the future. This education and training should include

- Educating individuals to take active steps to protect their personal information;
- Training state and local law enforcement to identify and effectively handle identity theft cases, since these cases are often first reported to state and local rather than federal law enforcement agencies; and
- Educating businesses, including banks and credit bureaus, to guard against and detect identity theft.

"Best Practices" to Combat Identity Theft

The following is an analysis of best practices either currently in place in the states or needed to fulfill assistance functions for victims of identity theft. These conclusions were generated through a synthesis of published commentaries and critiques of existing legislation, peer-reviewed academic articles, and analysis of pending legislation.

First, it is important to use a broad definition that explains the substance of the sort of information that should be considered "identifying information." This definition should be broad enough to include account numbers, scanned or re-encoded credit or account access cards, and SSNs. Following the establishment of a working definition of the problem, the research of NW3C has indicated that there are numerous opportunities to help victims of identity theft.

Practice 1: Explicit recognition of identity theft as a crime committed against the individual.

States have taken a variety of approaches to dealing with identity theft victims. Chief among the issues that create inconsistencies among states is the nature of victimization in identity theft cases. For example, victims in states that do not recognize identity theft as a crime must often seek assistance through civil suits or ancillary charges. While the place of the civil suit is to rectify injustices that escape the criminal justice system, it is an arduous task least likely to be pursued by most people. Such circumstances exemplify a need for legislation that explicitly criminalizes the dissemination and misuse of identifying information such as SSNs rather than just the theft facilitated by information misuse. Specifically, statutory frameworks should explicitly criminalize identity theft in a manner that clearly underscores the method of information obtainment, as well as monetary damages.

Practice 2: Eligibility of identity theft victims for victims' rights assistance.

The foremost need expressed by victims in recent NW3C research is for notification of victimization. Indeed, the most comprehensive framework for protecting the rights of victims and restoring them to their pre-victimized state is of little use if victims do not know that a crime has been committed. This is especially true in the instance of a SSN that is stolen from medical or business documents without the knowledge of the victim.

In states that do recognize the individual whose identity has been stolen as an injured party, the degree of victimization is often deemed to be trivial in comparison to other offences, especially violent ones. In some states, victims' assistance and, in some cases basic notification and participation rights, are denied to victims of property crime and only afforded to those who can demonstrate some form of physical injury. In other states, victims of non-violent crimes are only given full protection if the predation is judged to be a felony offence. It is therefore of great importance that those statutes that exist to aid crime victims recognize the victims of identity theft as targets of a serious crime who may require assistance in pulling their lives back together.

Practice 3: Phasing out use of private identifying information on non-secure documents.

While many states no longer use SSNs as identifiers on drivers' licenses, these numbers are still widely used on non-secure public documents. For example, many schools that use SSNs as student identification numbers include these numbers on a variety of forms and correspondence, and order forms and applications often solicit personal information. Consequently, a Nexis public records search can reveal SSNs and dates of birth in seconds. Additionally, organizations that accumulate personal information apply varying levels of security. Ultimately, it is unhelpful for a dozen organizations to strictly protect personal information if only one organization makes that information publicly available. This issue is associated with the idea of liability for breaching a duty of confidentiality, but it is also a change in focus that requires unique legislative attention. In other words, it is important not only to protect personal information but also to establish safeguards for handling those forms that document personal information. What is required is legislation that mandates strict controls on the circumstances under which the recording of personal information is justified.

Practice 4: Eligibility for compensation and financial assistance.

Financial assistance is typically reserved for victims of violent crimes where the perpetrator has not been ordered to provide restitution or does not have the means to provide effective restitution. Such practices can also be helpful in identity theft cases that result from privacy breaches. Financial assistance, unlike restitution, is able to provide for and compensate immediate financial outlays without concern for the offender's ability to pay. As the Privacy Rights Clearinghouse has demonstrated, a victim of identity theft typically spends as much as $1,200 out-of-pocket to correct the damage caused by the crime. Thus, just as victims of violent crimes have a need for funds to cover immediate emergency expenses, so do victims of identity theft. Therefore, legislation may be needed to assure that victims of identity theft can qualify for federal victim assistance funds.

Practice 5: Aid to identity theft victims in clearing their names.

Regardless of the efficiency of the legal system in prosecuting identity theft cases, victims often face many difficulties in removing fraudulent information that is asso-

ciated with their names. Consequently, victims of identity theft remain vulnerable to future victimization through the continued use of their SSN on government documents, most of which require the use of the SSN as a personal identifier. A great need exists for aid in purging erroneous records maintained by credit bureaus, police departments, and other organizations that result from the crime of identity theft. Often, the mechanism for such corrections is complex, creating barriers for citizens of limited means or comprehension. Therefore, legislative guidance for aid to victims of identity theft would be helpful. Examples of policies that have been enacted by statute (nearly all from California) to address this problem are

- Providing public agency aides to assist victims by making phone calls, preparing forms, or taking other steps on behalf of the victims;
- Requiring that court records reflect that the person whose identity was falsely used to commit a crime did not commit that crime (Cal. Penal Code 530.5(c)); and
- Allowing the victim to petition the court for an expedited determination of factual innocence (Cal. Penal Code 530.6).

Legislative Treatment of Social Security Information

In those instances when SSNs are deemed suitable for recording, there exists a need to create statutory incentives for companies (especially, but not limited to, credit card companies) to safeguard this information. While a few states have some form of accountability already on the books (California's Information Practices Act and Delaware's concept of reckless disclosure of information stand out), none have gone so far as to explicitly create an actionable duty of care for all entities that collect private identifying information to protect said information to at least the level to which a reasonable person would have protected it. Delaware is the only state to even mention the reckless or negligent disclosure of personal information in their identity theft legislation.

While civil actions are always available to punish such disclosures, they do not possess the desired deterrent effect unless they are easily factored into a rational analysis of policy options. As it stands, one can only assume that the current rate of identity theft and credit card fraud are an acceptable cost of business for the corporations that currently treat with social security numbers and other private identifying information in an unsafe way. Creating a statutory category of liability would serve both to increase the victim's chances in court and to alter the equation for those corporations, putting them on notice to change their behavior lest it eat into their profit margin.

California is one state that has imposed liability on entities that handle personal data. Cal Civ Code § 1798.29 (2003), for example, requires any agency that "owns or licenses computerized data that includes personal information" to report security breaches to the people whose personal information may have been compromised. Cal Civ Code § 1798.82 (2003) extends similar requirements to people and businesses doing business in California. This approach is proposed for Federal law in S. 1350, the Notification of Risk to Personal Data Act, recently filed by Senator Feinstein.

Of course, regardless of how rigorously SSNs are protected, there will be instances in which they are abused. On this matter, the following recommendations are proposed:

- Make possession of fraudulent social documents either illegal in and of itself or allow it to create a permissible inference of forgery. There is already a provision in many forgery and credit card fraud statutes that states that the ownership of some small number of forged or unauthorized instruments is enough to create an inference of a guilty motive without the necessity of proving a definite intent. Additional measures can be taken to address unauthorized possession of identifying documents or information. Some states have already adopted various measures of this type. Alabama and Kentucky lead the way in this regard, and set the required number of identity documents (a term that would include social security cards) in one's possession that are not one's own to create an inference of identity trafficking at five.
- When SSNs are abused, they are often abused for long periods of time. While a victim of a burglary may change their locks, a victim who was targeted through their SSN has little ability to prevent this means of victimization in the future. Unless SSNs are easily changed, the victims of these crimes have little protection against repeat predation, especially as the SSN is passed to other unscrupulous types. To address this problem, some sort of repository for compromised SSNs, which could flag SSNs that have been the target criminal abuse, could be established.

Current Legislative Issues

It has been recognized that no federal law currently limits use or disclosure of SSNs among private entities, leaving them free to deny credit or services without SSNs; and that the Social Security Administration (SSA) cannot control how private entities keep, use or distribute SSNs, thus leaving the burden on consumers who have no real power.[14]

Many bills, taking a variety of approaches to preventing or enhancing responses to identity theft, have been introduced in recent Congresses, and several are again pending in this, the 108th Congress. Some of these legislative measures propose enhancements in the penalties under the federal ID Theft statute in the interest of increasing the deterrent effects, or would make modifications aimed at facilitating investigations or prosecutions. Others go more directly to the topic at hand today: augmenting the protections against disclosure and misuse of certain information, including SSNs.

These bills, such as H.R. 2036 which you sponsored in the 107th Congress, Mr. Chairman, would enhance privacy protections and otherwise help prevent "fraudulent misuse" of SSNs by restricting display or use of SSNs, restricting dissemination of SSNs or any derivative or their use as PINs without an individual's consent, and providing for regulation and criminal punishment of sales and purchases of SSNs. As you know, measures are also pending to protect other personal identifying information by, for example, prohibiting sale and disclosure of personally identifiable information by commercial entities to non-affiliated third parties absent prescribed procedures for notice and opportunity to restrict such disclosures.

Specifically,

- H.R. 70, the Social Security On-line Privacy Protection Act, would prohibit an interactive computer service from disclosing to a third party an individual's SSN or related personally identifiable information without the individual's prior informed written consent.
- H.R. 220, the Identity Theft Prevention Act of 2003 pending before this subcommittee, would, among other things, amend the Social Security Act and Internal Revenue Code to protect the integrity and confidentiality of SSNs, prohibiting their use or disclosure except for specified social security and tax purposes.
- H.R. 637, the Social Security Number Misuse Prevention Act, and the companion bill, S. 228, would, among other things, prohibit display, sale, or purchase of SSNs without affirmative, express consent of the persons to whom they belong; prohibit use of SSNs on government-issued checks, the appearance of SSNs on driver's licenses or motor vehicle registrations, and inmate access to SSNs; prohibit commercial entities from requiring individuals to provide SSNs when making purchases or from denying such purchases if the persons refuse to provide such numbers; and establish civil and criminal penalties for misuse of SSNs. (Similar provisions are included within other, broader bills, including but not limited to S. 745, the Privacy Act of 2003.)
- H.R. 1931, the Personal Information Privacy Act of 2003, would, in part, prohibit commercial acquisition or distribution of SSNs, or derivatives, as well as their use as personal identification numbers, without written consent.

Two other bills very recently filed in the House of Representatives and pending before the Ways and Means Committee, H.R. 2617, the Consumer Identity and Information Security Act of 2003, and H.R. 2633, the Identity Theft Protection and Information Blackout Act of 2003, include (but are not limited to) provisions that would similarly place prohibitions or restrictions on certain uses of SSNs.

While we are not necessarily endorsing every aspect of these various measures, we certainly commend them to your careful consideration as Congress acts, along with the states, to better enable effective responses and efforts to prevent identity theft.

Conclusion

Thank you for the opportunity to testify before you today. Mr. Chairman, I am eager to answer any questions you or other members of the subcommittee may wish to direct to me.

References

1. U.S. Department of Justice. (2003, July 27). *Fraud*. Retrieved July 7, 2003, from http://www.usdoj.gov/fraud.htm

2. U.S. Department of Justice. (n.d.). *Identity theft: Prosecution and protection*. Retrieved July 2, 2003, from http://www.usdoj.gov/usao/txs/releases/May%202002/020502-identitysheet.htm

3. Benner, J., Givens, B. & Mierzwinski, E. (2000). Nowhere to Turn: Victims speak out on identity theft: A CALPIRG/Privacy Rights Clearinghouse report. *Privacy Rights Clearinghouse*. Retrieved June 13, 2002, from http://www.privacyrights.org/ar/idtheft2000.htm

4. Star Systems (STARsm). (2003, April 16). *Americans want action on identity theft*. [Press Release]. Retrieved July 7, 2003, from http://www.star-systems.com/cfm/news-press.cfm?id=81

5. Federal Trade Commission. (2003, January 22). *National and state trends in fraud and identity theft: January–December 2002*. Retrieved July 1, 2003, from http://www.consumer.gov/sentinel/pubs/Top10Fraud__2002.pdf

6. Identity Theft Resource Center. (2003, February). *Facts and statistics*. Retrieved July 2, 2002, from http://www.idtheftcenter.org/facts.shtml

7. Identity Theft Resource Center. (2003, February). *Facts and statistics*. Retrieved July 2, 2002, from http://www.idtheftcenter.org/facts.shtml

8. Federal Bureau of Investigation. (2003, July 7). *Operation easy rider: FBI puts stop to driver's license fraud*. Retrieved July 7, 2003, from http://www.fbi.gov/homepage.htm

9. U.S. Department of Justice. (2003, May 12). *Three indicted on conspiracy to commit bank fraud and identity theft*. [Press Release]. Retrieved July 3, 2003, from http://www.cybercrime.gov/thomasIndict.htm

10. Sanchez, E. (2003, May 13). Scam alert: Insider help giving a new look to bank robberies. *The Sacramento Bee*. Retrieved July 3, 2003, from http://www.sacbee.com/content/news/scam__alert/v-print/story/6657347p–7609218c.html

11. U.S. Department of Justice. (2003, May 12). *Three indicted on conspiracy to commit bank fraud and identity theft*. [Press Release]. Retrieved July 3, 2003, from http://www.cybercrime.gov/thomasIndict.htm

12. Masters, B.A. (2002, November 26). Huge ID-theft ring broken; 30,000 customers at risk. *The Washington Post*. Retrieved July 3, 2003, from http://seattletimes.nwsource.com/html/consumeraffairs/134584039__idtheft26.html

13. O'Connor, T. (2003, January 2). Four charged in ID-theft scam. *The Journal News*. Retrieved July 3, 2003, from http://www.nyjournalnews.com/newsroom/010203/A102idtheft.html

14. Harry A. Valetk, *Identity Theft: What It Is and How to Protect Against It*, originally published on GigaLaw.com and found November 22, 2002, at http://www.wiredpatrol.org/idtheft/whatisit.html

Chairman SHAW. Mr. Collins.

Mr. COLLINS. Thank you. Mr. Edwards, there has been talk about the Inspector General, the SSA having statutory authority to share information with law enforcement. How often have you requested information from SSA to pursue a criminal?

Mr. EDWARDS. On several occasions, Mr. Collins, but in each case it was denied to me.

Mr. COLLINS. What was the reason given?

Mr. EDWARDS. At the time, and this is not in the most recent past, but at the time I was told that they could not provide that information. Basically, the information I have been able to obtain from Social Security over the years is, I can give them a number and they will tell me if it is a valid number or not. They will not tell me who the number belongs to or whether it is being used by the correct person.

Mr. COLLINS. How long ago has it been since your last request? Do you know?

Mr. EDWARDS. Within the last couple of years? Yes, sir. It has not been in the recent past; quite frankly, because of the frustration, unless I just need a verification of a SSN, I rarely call them.

Mr. COLLINS. The Inspector General stated in its testimony that we need criminal penalties for Social Security misuse itself, as well as civil monetaries. You mentioned that possession of fraudulent documents should be illegal in and of itself. Describe some cases where such law would have been helpful in investigating or prosecuting an identity theft.

Mr. EDWARDS. Identity theft covers a lot of different crimes, and there is a lot of crimes that are predicate acts to identity theft. So, we have used all kinds of charges, including false writings to the State for driver's license. We have used it in cases where an individual has actually falsified a signature to obtain a credit card or some kind of bank loan or something along that line. So, all of these different tools that exist out there are very useful to us. We have an identity theft statute in the State of Georgia, and where it has helped our victims, and that is who it really helps, is giving them a vehicle for when. Particularly, like the scenario I gave where the identity was compromised in California, under Georgia law we can indict that individual and extradite them back, and there doesn't have to be a financial loss, just the virtue that an individual went around portraying that they were someone else using that individual's identifiers in the State of Georgia is a crime now and it is a felony. It carries 5 years, and we are just starting to test that. It went into law a year ago, July, and we are just now starting to test that law in the courts. We have had a couple of cases that have been successful.

Mr. COLLINS. How many other States have that?

Mr. EDWARDS. I am not familiar, Mr. Collins. Quite frankly, maybe two or three. If that many.

Mr. COLLINS. Thank you, Mr. Edwards.

Mr. EDWARDS. Thank you, sir.

Chairman SHAW. If I could direct a question to Mr. Wern and Mr. Hoofnagle with regard to, we have been hearing today a lot, people have been referring to the identifier as putting the genie back into the bottle. Obviously, the numbers are out there now, and they will remain out there no matter what we do. We can certainly stop the distribution, or certainly retard the distribution through criminal statutes, but a lot of that information is already in the public domain. I know in Florida, with the total access that everybody has to public records, it is going to be very difficult to go back and take those numbers off of the public records. Whether you are talking about death certificates or probate files or it goes on and on, probably divorce files, I would assume they are probably in there somewhere, it is going to be very, very difficult. It occurs to me that if you simply prohibit the use of SSN as an identification for nongovernmental purposes, that it would make that number somewhat useless for other purposes. Now, quite obviously if we were looking at this as an identifier, we would require very stringent requirements as to photographs or counterfeit proofing. You would have an address and date of birth and other pertinent information on the card itself, you would be sure to keep absolutely current with all of that, all of that information, and you would have had tremendous safeguards around it and everything else, which obviously the crooks have picked this up as something that was never anticipated by those who wrote the statutes.

I understand, Mr. Edwards, that we are looking into the area that you and Mr. Collins were just discussing with regard to the access law enforcement has, at least to the name, they are governed under the Internal Revenue Code, there are restrictions on giving any information, but I think it is more based toward wages and things of this nature. We are going to look into it and see if it prohibits their giving the name of whomever, whatever number you have; or at least you should be able to say, I have got John Doe and he has got X–Y–Z number, is this his number? They should be able to say yes or no to that. So, we need to work on that. We use that number for so many number purposes. Tracking deadbeat dads. That was something I had a lot to do with in welfare reform when we reformed the welfare system in this country. We don't want to make it more difficult to track deadbeat dads so they can fulfill their parental responsibilities. We do need, we desperately need to stop the distribution of these numbers as an identifier and as the golden, I think you, Mr. Hoofnagle, referred to it as the golden key or something of that nature, to stealing identification. Mr. Wern, you mentioned that you were victimized and you went through this for about 3 years. I understand from people who have been in your place, that they are being warned that it may not be over, that this nightmare may recur. You have recurring nightmares in this area. How did they get your number, and was it the SSN that was the key to the identity theft that you suffered?

Mr. WERN. We don't know for absolute sure how the perpetrator got the number. He was caught and interrogated, but his story just didn't make a whole lot of sense. My best guess, probably 80 percent sure, is that it was on a dental record that was stolen from my mail. I had some mail stolen, and one of the things that I know for a fact was stolen was a dental report or a bill that I know also had that SSN on it. My SSN was the key to that crime simply because it was sort of the final piece of information he needed. It was easy enough to get my address. He knew where I lived, he took my mail. It was easy enough to get my name and date of birth as well from other public records. Once he had the SSN, he used it and damaged to the point, to the point where I actually had to change the SSN, which is an extreme measure that we don't recommend people doing. It carries a lot of problems with it, but when you get to a situation where another person is essentially cloning you, you don't have a choice.

Chairman SHAW. Several things in the law that I want this Committee—that we will be looking at, is use of a counterfeit SSN. You have an illegal alien who is in this country, working. He gets a counterfeit Social Security card and number, the identification, and he can go to work. Then it is under a false number. Later he is legally admitted into the United States and gets a green card and gets a work permit. He can actually go back and claim the money that was paid into Social Security under that false number on his behalf, which to me is somewhat bizarre that somebody can go back and claim the fruits of their crime after they are entitled to work under the laws that we have. These are there are so many things that just don't make a whole lot of sense, and the more you look into this whole use of SSNs and how they are used and

abused, it becomes more and more apparent that we definitely need to at least neuter the use of this number as an identifier so that if somebody does get hold of it, it will be sort of a, "so what." One of the ways to do it is to just stop the nongovernment use of this number, period. Mr. Cardin, do you have any questions for these witnesses?

Mr. CARDIN. First, let me thank you all for being here. I apologize I was not here during your entire testimony. As more and more we talk about this, I am wondering, Mr. Chairman, how difficult would it be to restrict the use of SSNs to governmental purposes and not in the private sector. It would require a lot of changes, the habits of the private sector. So, your comment was that the missing ingredient, that was the one bit of information that allowed the identity theft to be effective obtaining your SSN probably from a medical record that there was no need for it to be on. So, there is clearly an abuse in the private sector on the use of SSNs. It is convenient for them, it is a reliable number, it is set up by their government. I understand all those arguments as to why it is convenient to use the SSN for identification by the private sector, but that is not its intent. The other question about trying to verify who you are. The fact that you know someone's SSN is no guarantee at all that that is who you are. So, I am just wondering, Mr. Chairman, what is the trade-off here, how difficult it would be for the private sector if we in fact restricted those numbers? I don't have any specific questions for any of the witnesses. Again, I thank them for being here.

Chairman SHAW. Well, I thank all of you for being here today. The first panel as well, which I neglected to thank as we ran out the door to make the last vote. I think it has been a very interesting discussion here, and the three of you certainly have added considerably to the store of knowledge that we are trying to build up. I am very hopeful that we will not only be able to get a bill out of this Committee, which I don't think is going to be a great deal of trouble, I think we can do it, we have done it before but that we can work with the other committees to see that they move it. I think it is the Committee on the Judiciary and the Committee on Financial Services that have a piece of this legislation. There may be another jurisdiction involved, but everybody guards their turf up here on Capitol Hill, particularly this Committee. We really guard ours. We want to be sure that the other committees either waive jurisdiction or that they pass on the provisions of the bill within their jurisdiction. It is the fastest growing type of white collar crime that we have, and it may be the fastest growing crime, period. We know the conditions are getting worse and worse. Mr. Wern, we don't want to see more people go through the agony that you went through. Credit is so important in this country. We certainly appreciate the three of you coming forward. We are about ready to adjourn. Did you have anything?

Ms. TUBBS JONES. Thank you gentlemen for coming. I am sorry I couldn't be here, but you know what life is like on the Hill. Thank you, Mr. Chairman.

Chairman SHAW. I was a judge too, Ms. Tubbs Jones. One time I came in late, in fact I came late a lot of times, and the bailiff looked over and he said, judge, you are late. I said, oh, did you

start without me? So, I think once you have been a judge, you kind of get used to your own time clock, and you do what you have to do. Well, thank you all very much. It has been a very beneficial hearing. We are now adjourned.

[Whereupon, at 3:43 p.m., the hearing was adjourned.]

[Submissions for the record follow:]

*July 24, 2003*

The Honorable E. Clay Shaw, Jr.
Chairman
Subcommittee on Social Security
B–316 Rayburn House Office Bldg.
Washington, DC 20515

The Honorable Robert Matsui
Ranking Democratic Member
Subcommittee on Social Security
1106 Longworth House Office Bldg.
Washington, DC 20515

Dear Chairman Shaw and Ranking Member Matsui:

The undersigned organizations applaud your efforts over the past several years to craft legislation that will ensure the integrity of the social security number (SSN) in the years ahead. We are extremely concerned about the proliferation of identity theft and other financial crimes that exploit individual SSNs, and believe strong legislation should be enacted to combat such nefarious acts. We eagerly await your introduction of legislation to address these issues during this session of the 108th Congress.

As public and private employee benefit plan sponsors, however, we are concerned that such legislation could unintentionally hinder the delivery of benefits from, and the efficient administration of, public and private employee benefit plans.

In your bipartisan legislation introduced during the 107th Congress, the "Social Security Number Privacy and Identity Theft Prevention Act of 2001," (H.R. 2036), the definitions and provisions relating to the "sale," "purchase" or "display" of a person's SSN could make it more difficult to deliver comprehensive health and retirement benefits to public and private employees alike. Indeed, the language could place plan administrators in jeopardy of, on the one hand, violating the strict fiduciary requirements applicable to retirement plans and, on the other hand, exposing themselves to criminal penalties under the bill. It is unreasonable to put plan administrators of a voluntary employee benefit system in this position.

In general, public and private employee benefit plans use SSNs because they enable the accurate and timely administration of benefits for a highly mobile workforce, and because use of the number is mandated for tax reporting requirements. Plan administrators take seriously the responsibility that the use of SSNs requires, and they use the utmost caution and security when SSNs are used in plan administration and communications.

Public and private sector defined benefit and defined contribution pension and savings plans, like 401(k), 403(b), and 457 plans, use SSNs to identify plan participants, account for employee contributions, implement the employee's investment directions, track "rollovers" from other plans, and allow employees to view their account activity or benefit accrual online (typically in conjunction with a secure "PIN"). The broad prohibitions of H.R. 2036 could impede, for example, an individual's ability to stay current on the accumulation of benefits for his or her retirement.

SSNs are also used as the primary identifier in many medical and health benefit and prescription drug plans to coordinate communications between the doctor, the medical service provider, and the plan. H.R. 2036's broad prohibitions could, for example, hinder the delivery of medications to the individual.

H.R. 2036 allowed the nonabusive legitimate uses of social security numbers for national security, law enforcement, public health and advancing public knowledge purposes in proposed new section 208A(c) (section 201(a) of H.R. 2036). An "Employment Exception" could be included as well. It would be substantially similar to that in S. 228, which exempts any interaction between businesses, governments, or business and government. The exemption appears in Section 3(a) of S. 228, creating Sec-

tion 1028A in Chapter 47, Title 18, United States Code. Senators Feinstein, Gregg, and Leahy introduced S. 228 on January 28, 2003.

We firmly believe your legislation should permit the use of an individual's SSN for any employment or employment-related purpose (such as the administration of an employee benefit plan) and for any recordkeeping purpose related to an investment made by the individual. In H.R. 2036, you recognized the importance of this issue by specifically excluding application for government benefits or programs from the definition of "sale" or "purchase." We believe our proposed "Employment Exception" would follow your intent to not hinder the administration of employee programs and delivery of benefits in the public and private sector employment arena as well.

An "Employment Exception" could be included in the new section 208A(c) of the bill. Alternatively, the definitions of "sale," "purchase" and "display" as drafted in new section 208A(a) (section 201(a) of H.R. 2036) could be modified and text in Section 202(b) of the bill could be slightly revised. We have attached proposed legislative language that is designed to enable the bill to achieve your objective of limiting the misuse of social security numbers without interfering with the efficient and effective administration of public and private employee compensation and benefit plans.

We look forward to continuing to work with staff and with the Committee to effectively address the problem of identity theft without creating unintentional barriers to the provision of public and private pension, health and other benefits to employees. Please do not hesitate to contact us should you require additional information or wish to discuss this issue in more detail.

Sincerely,

American Benefits Council
American Society of Pension Actuaries
College and University Professional Association for Human Resources
ERISA Industry Committee
Financial Executives International's Committee on Benefits Finance
National Association of State Retirement Administrators
National Council on Teacher Retirement
National Rural Electric Cooperative Association
Profit Sharing/401(k) Council of America

---

**Proposed Amendments**

The undersigned organizations propose the following be included in the upcoming legislation to be introduced by House Ways and Means Social Security Subcommittee Chairman E. Clay Shaw, Jr., and Ranking Member Robert T. Matsui, which is designed to ensure the integrity of the social security number (SSN) in the years ahead. Our proposed amendments, which are based on the "Social Security Number Privacy and Identity Theft Prevention Act of 2001," (H.R. 2036) introduced in the 107th Congress, are designed to enable the bill to achieve its sponsors' objective of limiting the misuse of SSNs without interfering with the efficient and effective administration of public and private employee compensation and benefit plans. In each instance, new text is underscored, and deletions are [bracketed].

**Option 1—Employment Exception**

Strike "and" after ";" on Page 18, line 25.
Replace "." with "; and," on page 19, line 8.
Insert at page 19, line 9:

'(8) if the display, sale, or purchase of such a number is for a use occurring as a result of an employment-related interaction between employers and employees of businesses or government (regardless of which party initiates the interaction), for any purpose mandated or permissible under Title 26 or Title 29 on the United States Code;'

**Option 2—Clarify Language to Prevent Unfair Treatment of Employee Benefit Plans**

PROPOSED AMENDMENTS TO SECTION 201: These amendments clarify that the prohibitions contained in Section 201 of the bill will not apply to public and private employer-sponsored plan uses of SSNs. These amendments also clarify that "government benefit or program" includes benefits related to employment with such governments.

1. AMENDMENT DEFINING "SALE": This amendment clarifies that an SSN is not sold when it is provided in connection with an employment-related transaction that has a bona fide purpose unrelated to the use of the SSN, such as the administration of an employee benefit or compensation plan.

**Amend Section 208A(a)(2) (section 201(a) of H.R. 2036 defining "sale") to read as follows:**

"(2) SALE—The term 'sell' in connection with a social security account number means to obtain, directly or indirectly, anything of value in exchange for such number. Such term does not include the submission of such number as part of the process for applying for any type of Government benefits or programs (such as grants or loans or welfare or other public assistance programs) or any activity necessary to effect an employment-related transaction that has a bona fide purpose unrelated to the use of the social security number."

2. AMENDMENT DEFINING "PURCHASE": This amendment clarifies that an SSN is not purchased when it is obtained in connection with an employment-related transaction that has a bona fide purpose unrelated to the use of the SSN, such as the administration of an employee benefit or compensation plan.

**Amend section 208A(a)(3) (section 201(a) of H.R. 2036 defining "purchase") to read as follows:**

"(3) PURCHASE—The term 'purchase' in connection with a social security account number means to provide, directly or indirectly, anything of value in exchange for such number. Such term does not include the submission of such number as part of the process for applying for any type of Government benefit or programs (such as grant or loan applications or welfare or other public assistance programs), or any activity necessary to effect an employment-related transaction that has a bona fide purpose unrelated to the use of the social security number."

3. AMENDMENT DEFINING "DISPLAY": This amendment clarifies that an SSN is not displayed to the general public when it is placed in a viewable manner in connection with an employment-related transaction that has a bona fide purpose unrelated to the use of the SSN, such as the administration of an employee benefit or compensation plan.

**Amend section 208A(a)(4) (section 201(a) of H.R. 2036 defining "display") to read as follows:**

"(4) DISPLAY—The term 'display' means, in connection with a social security account number, the intentional placing of such number, or a derivative thereof, in a viewable manner on an Internet site that is available to the general public or in any other manner intended to provide access to such number or derivative by the general public. As used in this section, the term 'general public' does not mean any person connected with any activity that is necessary to effect employment-related transactions that has a bona fide purpose unrelated to the use of the social security number.

PROPOSED AMENDMENTS TO SECTION 202: This amendment clarifies that an employee is not considered a consumer for purposes of this section and that section 202 of H.R. 2036 would not apply in the context of the employer-employee relationship, such as the administration of an employee compensation or benefit plan.

**Amend section 202(b) as follows:**

"(b) EXCEPTION—Subsection (a) shall not apply to any person in any case in which such person is required under Federal law, in connection with doing business with an individual, to submit to the Federal Government such individual's Social Security account number; *or, in connection with employment of the individual, including the provision of compensation or benefits thereof."*

**Rationale for Specific Changes in Option 2**

Section 201(c) unwisely subjects public and private employee benefit plans to regulations promulgated by a federal agency with no expertise in employee benefit plans. Section 201(c) grants the Attorney General authority to promulgate regulations to carry out the prohibitions against sale, purchase, and display of SSNs, and provides the Attorney General complete discretion over whether or not to consult with an agency that has expertise over employee benefit plans. Regulations that require the amendment of hundreds of thousands of public and private employee benefit plans should not be promulgated by an agency with no expertise or jurisdiction over the laws governing those plans.

Section 202 could unintentionally restrict access to employee benefit plans. Section 202 prevents any "individual, partnership, corporation, trust, estate, cooperative, association, or any other entity" from refusing to "do business" with an individual who does not provide them with an SSN. Without clarifying that section 202(a) does not apply to public and private employee benefit plans, plan sponsors might be prevented from obtaining an individual's SSN for plan enrollment, benefit payments, and other legally mandated and routine plan administrative functions. The exemption in section 202(b) to this prohibition, while helpful, does not go far enough.

**Statement of Stuart K. Pratt, Consumer Data Industry Association**

The Consumer Data Industry Association (CDIA) is pleased to submit written testimony in connection with a hearing on the misuse of Social Security numbers and we thank Chairman Shaw for holding this hearing. CDIA has appeared in person before this subcommittee before and we hope our testimony will be helpful to you.[1]

Founded in 1906, the Consumer Data Industry Association (CDIA), formerly known as Associated Credit Bureaus, is the international trade association that represents more than 500 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

Consumer reporting agencies are careful stewards of personal information and they adhere to strict procedures outlined in federal and state laws.[2] The information infrastructure of the consumer reporting system is the backbone of the consumer credit economy.[3]

Our members have a strong interest in the legitimate and lawful use of all information, including Social Security numbers. Used properly, SSNs play a substantial role in reducing fraud, enhancing workplace security, promoting public safety, sup-

[1] *Preventing Identity Theft by Terrorists: Hearing before the House Comm. on Financial Services Subcomm. on Oversight and Investigations and the House Comm. on Ways and Means Subcomm. on Social Security*, 107th Cong. (Nov. 8, 2001) (testimony of Stuart K. Pratt, Vice President, Vice President, Associated Credit Bureaus); *Use and Misuse of Social Security Numbers: Hearing before the House Comm. on Ways and Means Subcomm. on Social Security*, 106th Cong. (May 11, 2000) (testimony of Stuart K. Pratt, Vice President, Vice President, Associated Credit Bureaus).

[2] All consumer reporting agencies are bound by the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq*. and numerous state credit reporting laws. Among other things, the FCRA requires consumer reporting agencies to maintain reasonable procedures to assure maximum possible accuracy, 15 U.S.C. § 1681e(b) and prohibits data furnishers from furnishing data to consumer reporting agencies if they know the information has an error, § 1681s–2(a). In addition, a consumer reporting agency is prohibited from furnishing a consumer report to anyone without a "permissible purpose"—a narrow and statutorily limited list of permitted uses. § 1681b.

[3] For example, it was recently noted that

> Maintaining a reliable and robust national credit reporting system is essential to ensure the continued availability of consumer credit at reasonable costs * * * The ready availability of accurate, up-to-date credit information from consumer reporting agencies benefits both creditors and consumers. Information from consumer reports gives creditors the ability to make credit decisions quickly and in a fair, safe and sound, and cost-effective manner. Consumers benefit from access to credit information from different sources, vigorous competition among creditors, quick decisions on credit applications, and reasonable costs for credit.

*Fair Credit Reporting Act: How it Functions for Consumers and the Economy: Hearing before the House Comm. on Financial Services Subcomm. on Financial Institutions and Consumer Credit*, 108th Cong. (June 4, 2003) (statement of Dolores S. Smith, Director, Division of Consumer and Community Affairs, Board of Governors of the Federal Reserve System).

porting homeland defense, reducing state and federal entitlement fraud, enhancing child support enforcement, and facilitating commerce to a diverse, mobile electronic society.

Before I specifically address how the SSN is used by our industry and the importance of this number, I have found it helpful to provide a short review of what a consumer reporting agency is, what is contained in a consumer report, and the law that governs our industry.

**CONSUMER REPORTING AGENCIES AND CONSUMER REPORTS**

Consumer reporting agencies maintain information on individual consumer payment patterns associated with various types of credit obligations on approximately 190 million Americans. The data compiled by these agencies is used by creditors and others permitted under the strict prescriptions of the FCRA.

Consumer credit histories are derived from, among other sources, the voluntary provision of information about consumer payments on various types of credit accounts or other debts from thousands of data furnishers such as credit grantors, student loan guarantee and child support enforcement agencies. A consumer's file may also include public record items such as a bankruptcy filing, judgment or lien. Note that these types of data sources often contain SSNs, as well.

For purposes of data accuracy and proper identification, generally our members maintain information such as a consumer's full name, current and previous addresses, Social Security Number (when voluntarily provided by consumers) and places of employment. This data is loaded into the system on a regular basis to ensure the completeness and accuracy of data.[4]

It is interesting to note that the vast majority of data in our members' systems simply confirms what most of you would expect; that consumers pay their bills on time and are responsible, good credit risks. This contrasts with the majority of systems maintained in other countries, such as Japan or Italy, which store only negative data and do not give consumers recognition for the responsible management of their finances.

As important as knowing what we have in our files is also knowing what types of information our members *do not* maintain in files used to produce consumer reports. Our members do not know *what* consumers have purchased using credit (e.g., a refrigerator, clothing, etc.) or *where* they used a particular bank card (e.g., which stores a consumer frequents). They also don't have a record of *when* consumers have been declined for credit or another benefit based on the use of a consumer report. Medical treatment data isn't a part of the databases and no bank account information is available in a consumer report.

**THE FAIR CREDIT REPORTING ACT (FCRA)**

In addition to our general discussion of the industry, we believe it is important for your Subcommittee to have a baseline understanding of the law which regulates our industry.

Enacted in 1970, the Fair Credit Reporting Act was significantly amended in the 104th Congress with the passage of the Credit Reporting Reform Act.

Congress, our Association's members, creditors and consumer groups spent over six years working through the modernization of what was the first privacy law enacted in this country (1970). This amendatory process resulted in a complete, current and forwarding-looking statute. The FCRA serves as an example of successfully balancing the rights of the individual with the economic benefits of maintaining a competitive consumer reporting system so necessary to a market-oriented economy.

The FCRA is an effective privacy statute, which protects the consumer by narrowly limiting the appropriate uses of a consumer report (often we call this a credit report) under Section 604 (15 U.S.C. 1681b), entitled "Permissible Purposes of Reports."

Some of the more common uses of a consumer's file are in the issuance of credit, subsequent account review and collection processes. Reports are also, for example, permitted to be used by child support enforcement agencies when establishing levels of support.

Beyond protecting the privacy of the information contained in consumer reports, the FCRA also provides consumers with certain rights such as the right of access; the right to dispute any inaccurate information and have it corrected or removed;

---

[4] Note that there are in fact a number of major credit reporting systems in this country. Within CDIA's membership the three most often recognized systems would be Equifax, Atlanta, Georgia; Experian, Costa Mesa, California; and TransUnion, Chicago, Illinois. These systems not only manage their own data, but provide data processing services for the hundreds of local independently-owned automated credit bureaus in the Association's membership.

and the right to prosecute any person who accesses their information for an impermissible purpose. The law also includes a shared liability for data accuracy between consumer reporting agencies and furnishers of information to the system.

**SOCIAL SECURITY NUMBER USES**

Let me now turn to the question of how our industry uses the SSN.

Under the Fair Credit Reporting Act, our industry has a duty to "... employ reasonable procedures to ensure the maximum possible accuracy ..." of the consumer report. Further, we must design systems that accurately allow our customers to extract *only* the data requested on a specific individual.

We must accomplish this dual mission of accuracy both in terms of building databases, but also properly identifying files in our systems in the context of a highly mobile society. Consider the following:

- Approximately 16% of the nation's population moves each year according to the U.S. Census Bureau, which means many addresses change each year. (This equates to approximately 42 million Americans)
- Based on National Center for Health Statistics, it is estimated that there are 2.4 million marriages and 1.2 million divorces annually. This event frequently triggers changes in addresses as well as last names.
- In 1998 there were 6 million homes in the U.S. that are considered vacation or second homes. Consumers often switch billing addresses if they stay at such residences for long periods of time and in some cases maintain billing addresses for both residences with various creditors. (Source: U.S. Census Bureau House Vacancy Survey as extrapolated by the National Association of Realtors)

These data clearly speak to the challenge our members face where identifying data often changes.

In light of the mobility of our society, the Social Security Number plays a very significant role in ensuring data quality. Our members process 2 billion data elements a month. These elements are a combination of credit history data and identifying information. Consider the following very real example.

Where a consumer has changed a last name due to marriage or divorce and has moved to a new address, which is common in either case, the SSN is the most stable identifying element in the file. First, it helps us to identify the consumer's file with precision during this life transition where he or she is likely applying for new credit, seeking approval for utilities, and seeking to rent or purchase a new residence. The consumer expects that the consumer report will be available for all of these necessary transactions and the SSN helps our members to meet this expectation. Second, the consumer expect his or her file to be accurate and the SSN helps us to maintain the file accurately even when the consumer is in the midst of updating creditors with changes in name and address.

The SSN is also a critical element in producing information products, which are commonly called locator services. These services are made available, for example, to child support enforcement agencies for purposes of locating non-custodial parents;[5] to pension funds which must locate beneficiaries; to law enforcement for locating criminals or witnesses;[6] to healthcare providers that must locate individuals who have chosen not to pay their bills, to state benefits agencies to reduce public assistance fraud,[7] and for other similar uses.

---

[5] The U.S. Department of Health and Human Services noted that "[r]outine transfer of child support payment information to credit bureaus ... is essential because these obligations may constitute a superior lean on a creditor's income." *A Guide About Child Support Enforcement for Credit Grantors, U.S. Department of Health and Human Services, Family Support Administration. November 1988.* In addition The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought. *Information Privacy Act, Hearings before the Comm. on Banking and Financial Services, House of Representatives, 105th Cong., 2d Sess. (July 28, 1998) (statement of Robert Glass).*

[6] Then-FBI Director Louis Freeh testified before Congress in 1999 and noted that in 1998, his agency made more than 53,000 inquiries to commercial on-line databases "to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations." This information, according to Director Freeh, "assisted in the arrests of 393 fugitives, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning." *Hearing before the Senate Comm. on Appropriations Subcomm. for the Departments of Commerce, Justice, and State, and the Judiciary and Related Agencies, March 24, 1999 (Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation).*

[7] Consider the following examples:

Continued

Further, the SSN plays a role in fraud prevention products. Where a consumer makes application for a product or service, information products that help the business to ensure that they are doing business with the right consumer use information products to authenticate or verify the application information. This is true in both for bricks-and-mortar business and in e-Commerce.

If applicant data does not match, then the business can take additional steps to verify the consumer's identity and thus prevent fraud.

**FRAUD PREVENTION AND IDENTITY THEFT**

In your press release announcing this hearing, you mention the potential for misuse of the SSN. Our industry has a history of bringing forward initiatives to address fraud. These efforts focus on the use of new technologies, and better procedures and education. CDIA and its members have a long history of being leading innovators of identity fraud solutions. The attachment provides a short thumbnail of our involvement in identity fraud remediation since 1993.[8]

**CONCLUSION**

In conclusion, you can see by our actions that in large part our uses of the SSN are governed under the Fair Credit Reporting Act, one of the most extensive privacy laws in the country. Beyond law, our members have a history of proactively limiting how SSNs are used outside of the FCRA. No one particular element of information is the key to identity theft. The underlying theme in all of this is balance.

Laws that overreach in attempting to limit use of the SSN are likely to merely take fraud prevention tools out of the hands of legitimate businesses at the expense of consumers. Ironically, to prevent fraud you must be able to crosscheck information. To maintain accurate databases, you must be able to maintain a range of identifying elements. Absent the availability of the SSN, we will be less able to build accurate data bases, to accurately identify records and to help prevent the very crime through the development of fraud prevention and authentication tools.

---

- "Individuals confined to a correction facility for at least 1 full month are ineligible to continue receiving federal Supplemental Security Insurance (SSI) program benefits. . . . Between January and August 1996, the sharing of prisoner data between SSA and state and local correction facilities helped SSA identify about $151 million overpayments already made and prevented about $173 million in additional overpayments to ineligible prisoners." *General Accounting Office, Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards, GAO–02–352 (May 2002), 15, citing General Accounting Office, Supplemental Security Income: Incentive Payments Have Reduced Benefit Overpayments to Prisoners, GAO/HEHS–00–02 (Nov. 22, 1999).*
- "Applicants for Temporary Assistance for Needy Families (TANF), a program designed to help low-income families, are required to provide their SSNs. Some agencies share SSN information to verify eligibility and identity. Between January and September 1999, New York State estimated that SSN verification saved about $72 million." *General Accounting Office, Social Security Numbers, Government Benefits from SSN Use but Could Provide Better Safeguards, GAO–02–352 (May 2002), 15, citing General Accounting Office, Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity, GAO–HEHS-00–119 (Sept. 13, 2000).*
- "The Department of Education uses SSNs to match data on defaulted education loans with the National Directory of New Hires (NDNH). . . . As a result of this matching . . . the department reported collecting $130 million from defaulted student loan borrowers in 2001." *General Accounting Office, Social Security Numbers, Government Benefits from SSN Use but Could Provide Better Safeguards, GAO–02–352 (May 2002), 16.*
- Federal agencies that are owned money share that information with the Treasury Department which matches the debtors' SSNs with those taxpayers that are owed tax refunds and reduces the refund by the amount owed. In 2001, the Treasury Department offset tax refunds by $1 billion. *Id*.

[8] While we agree that identity fraud is a significant problem, we also hope the committee will consider any legislation in the context of the most accurate and reliable data on the scope of the problem. One witness has suggested that the number of identity fraud victims could be between 700,000–1.8 million per year. *Misuse of Social Security Numbers: Hearing before the House Comm. on Ways and Means Subcomm. on Social Security*, 108th Cong. (July 10, 2003) (statement of Steve Edwards, Special Agent in Charge, Financial Investigations Unit, Georgia Bureau of Investigations; State Coordinator, U.S. Department of the Treasury, Financial Crimes Enforcement Network; and Vice Chairman of the Board of Directors, National White Collar Crime Center). CDIA feels that the best review of the level of identity fraud victimization is closer to 60,000 to 92,000 per year, *General Accounting Office, Identity Theft: Prevalence and Cost Appear to be Growing, GAO–02–363 (March 2002), 4*, or 162,000 per year. *FTC Reports: Figures and Trends on Identity Theft, January 2002–December 2002*. The GAO figures were developed based on interviews with three national consumer reporting agencies. Consumer reporting agencies are probably the best source understanding the scope of identity fraud victimization as victims are mostly likely to contact consumer reporting agencies as a first response.

Thank you for this opportunity to offer testimony. CDIA is available to assist your and your committee at any time.

---

***Consumer Reporting Agency Responses to Identity Fraud***

- 1993. Consumer Data Industry Association, then known as Associated Credit Bureaus, formed a Fraud and Security Task Force.
- 1998. Creation of True Name Fraud Task Force led by former Vermont Attorney General M. Jerome Diamond. The work of the task force included meetings with law enforcement, consumer organizations, privacy advocates, legislators and staff, victims, and others.
- The capstone of the True Name Fraud Task Force was a series of initiatives announced in March 2000. These initiatives meant the consumer reporting industry was the first industry to step forward and not only educate its members about the problems consumers experienced, but to seek specific changes in business practices. The initiatives are to:
  - Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.
  - Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
  - Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
  - Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.
  - Launch new software systems that will monitor the victim's corrected file for 3 months, notify the consumer of any activity, and provide fraud unit contact information.
  - Fund, through CDIA, the development of a series of consumer education initiatives through CDIA to help consumers understand how to prevent identity theft and also what steps to take if they are victims.
- 2001. CDIA announced a police report initiative so that when a police report is provided as part of the process of disputing fraudulent data, Equifax, Experian and TransUnion will block these disputed items from appearing on subsequent consumer reports regarding that individual.
  - "Another collaborative effort with tremendous promise is your new police report initiative. . . . I appreciate that certain consumer-based initiatives require you to balance accuracy issues—knowing that the consumer's report contains all relevant credit information, including derogatory reports—against customer service. From my perspective, your police report initiative strikes just the right balance." *J. Howard Beales, III, Director of the FTC's Bureau of Consumer Protection, before the Consumer Data Industry Association. Jan. 17, 2002*.
- 2002–03. ID Fraud Victim Data Exchange. CDIA and its members committed in 2002 to start a pilot test in early-2003 so that when an ID fraud victim calls any one of the participating credit reporting agencies, the victim will be notified that his or her identifying information will be shared by the receiving credit reporting agency with the other two participating credit reporting agencies and that the following steps will be taken by each recipient of the victim's information:
  - A temporary security alert will be added to the victim's file. This security alert will be transmitted to all subsequent users (e.g., creditors) which request a copy of the file for a permissible purpose under the Fair Credit Reporting Act.
  - The victim will be opted out of all non-initiated offers of credit or insurance.
  - The CRA will ensure that a copy of the victim's file is in the mail within three business days of the victim's request.
- Our efforts are paying off.
  - *Most calls are prevention related.* CDIA members report a majority of consumers who contact fraud units are taking preventative steps and are not reporting a crime.

- *Victims are learning of the fraud earlier.* According to an FTC report in June 2001, 42% of victims learn about the crime within 30 days or less, a full 10% less than in the prior report. CDIA estimates another 35% learn of the crime within one to six months and 7% learn of the crime in six months to a year.
- *Victimization of the elderly is dropping.* In 2001, the FTC estimated that 6.3% of identity fraud victims were over 65, a 5% decrease from 2000.

***About CDIA***

Founded in 1906, the Consumer Data Industry Association (CDIA), formerly known as Associated Credit Bureaus (ACB), is the international trade association that represents more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

For more information about CDIA, its members, or identity fraud or other issues, please visit us at www.cdiaonline.org or contact us at 202–371–0910.

**Statement of the Honorable Darlene Hooley, a Representative in Congress from the State of Oregon**

Just last week this very committee heard testimony on the many problems caused by the misuse of Social Security numbers and the ever increasing problem of identity theft.

I have become increasingly concerned about the vast quantities of sensitive, personal information that is now vulnerable to criminal interception and misuse. Currently, the ease of obtaining the Social Security number of an individual is shocking. Numbers are sold, exchanged and printed with an alarming carelessness. With a Social Security number and a few pieces of other easily obtainable personal information, fraudulent accounts can be opened and lives can be ruined. Many individuals work their entire life to build a spotless credit record, only to have it destroyed by a criminal armed merely with a Social Security number. The protection of Social Security numbers is a vital step to slowing the growth of identity theft and protecting people's lives.

I've been active in trying to prevent further horror stories of misused Social Security numbers. Two and a half years ago, a young boy in Salem named Tyler Bales lost his battle with a rare genetic disease called Hurler syndrome. As if it were not hard enough to lose your sixteen month old child, Tyler's parents later learned—courtesy of the IRS—that someone was claiming Tyler as a dependent on their 2000 income tax return.

Because of disclosure issues, the IRS could not give out the identity of this thief to local law enforcement, even though ID theft is a felony offense in the state of Oregon. To date, two and one half years later, the Bales still do not know the identity of this thief.

For this reason, I request that the House Committee on Ways and Means consider the "ID Theft Loophole Closure Bill" as the committee seeks legislation to prevent the misuse of Social Security numbers. This legislation simply changes the law to allow the IRS to furnish the name, Social Security number and address of a suspected identity thief to state and local law enforcement agencies for the exclusive purpose of locating the individual.

Identity theft is not a victimless crime. We must cut the red tape that is preventing thieves from being prosecuted for their crimes, and I believe this legislation is the right tool for the job.

**Statement of the Honorable Max Sandlin, a Representative in Congress from the State of Texas**

Thank you Mr. Chairman and Ranking Member Matsui, for the opportunity to testify today on the impact of the use and misuse of Social Security numbers.

I am pleased that my colleagues on the Ways and Means committee have convened a hearing on how the growing use of Social Security numbers as a national identifier has resulted in the mounting problem of identity theft. As you know, while our Social Security numbers were expressly created to catalogue workers' earnings for benefit purposes, nearly every branch of our society has co-opted Social Security numbers as an identification method. Our Social Security numbers can be found on

records kept by schools, banks, businesses, and many states even list them on people's drivers licenses.

While the use of Social Security numbers is very convenient and facilitates commerce through easy credit checks, we need to be cognizant of how the over exposure of Social Security numbers also easily enables criminals to commit identity theft. Simply by stealing an individual's purse, a thief may have immediate access to an individual's name and social security number and use that information to open new credit cards, establish new bank accounts, and even initiate new cell phone service, all to ring up charges that their victims will be left to contest. In the mean time, innocent, hard working, victims may find their credit destroyed, and may not even know about the theft until they are turned down for a mortgage or car loan. Once this occurs they are then forced to embark on an arduous process to restore their financial standing, while their dreams for a new home or needed vehicle remain on hold.

The Federal Trade Commission noted that identity theft has increased over 88% just in the last year, with nationwide complaints totaling 162,000. In my home state, over 14,000 Texans filed victim complaint statements last year with the Federal Trade Commission. Their tragic experiences provided the impetus for our state legislature's enactment of a law to combat identity theft last month. While we were only the second state in the nation to do so, seven other states are actively considering similar legislation.

We must continue to find ways to protect the citizens of this country from fraud and abuse caused by criminals committing identity theft. The Social Security Administration, credit bureaus, businesses, individuals and other federal, state and local government agencies must all coordinate resources to offer a comprehensive plan of action and protection. On the federal level, I am pleased to be a co-sponsor of H.R. 2035. This bill requires consumer reporting agencies to provide free credit reports annually upon the request of a consumer, as well as require the truncation of credit card numbers on printed receipts. By enacting common sense legislation like this, individuals will be able to detect identity theft at an early stage, before their credit reports are permanently damaged.

Congress has a responsibility to help the American people, and our National economy, prosper. Strengthening financial privacy laws and protecting Social Security numbers will help to achieve these goals. Thank you for your time.