AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ENHANCING SOCIAL SECUIRTY NUMBER PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

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

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 15, 2004

Serial No. 108–59

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
99–677 WASHINGTON : 2005

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

ENHANCING SOCIAL SECURITY NUMBER PRIVACY

Tuesday June, 15, 2004

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

The Subcommittee met, pursuant to notice, at 11:00 a.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
June 08, 2004

CONTACT: (202) 225–9263

Shaw Announces Hearing on Enhancing Social Security Number Privacy

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 enhancing Social Security number (SSN) privacy. **The hearing will take place on Tuesday, June 15, 2004, 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 Subcommittee and for inclusion in the printed record of the hearing.

BACKGROUND:

Identity theft is one of the fastest growing white-collar crimes, and it wreaks havoc with individuals' lives. Identity theft occurs when someone uses a victim's personal information—SSN, credit card number, or other identifying information—to commit fraud or other crimes.

According to a Federal Trade Commission-sponsored survey, almost 10 million people discovered they were victims of identity theft in 2002. On average, victims spent $500 and took 30 hours clearing their names and restoring their credit. In the interim, many may have lost job opportunities, had loans refused, or even gotten arrested for crimes they didn't commit.

One reason identity thieves prize SSNs is because they are central to many business transactions. While SSNs were originally created in 1936 to track earnings for Social Security eligibility and benefit purposes, today SSNs are widely used in the public and private sectors as account numbers, to verify identity, and to compile information across databases for use in everything from tracking down criminals to issuing credit. Despite SSNs' integral role in all sorts of transactions, their confidentiality is not well protected. SSNs are often on display to the general public on employee badges, licenses, in court documents, or on the Internet.

In order to protect the privacy of SSNs, Subcommittee on Social Security Chairman E. Clay Shaw, Jr. introduced bipartisan legislation, the *Social Security Number Privacy and Identity Theft Prevention Act of 2003* (H.R. 2971). The bill would prohibit the sale, purchase, and display to the general public of SSNs in the public and private sectors, with certain exceptions for law enforcement, national security, public health, and other specified circumstances. The legislation also prevents consumer reporting agencies from releasing SSN information other than in a full consumer report, and prevents businesses from denying products or services if an individual refuses to divulge his or her SSN.

In addition, the bill would require improvements in the process of issuing SSNs, and would create new criminal and civil penalties for those who misuse SSNs—for example, those who sell another individual's SSN or counterfeit SSNs; or those who violate the bill's prohibitions on sale, purchase, and display to the general public.

In announcing the hearing, Chairman Shaw stated: "We can no longer ignore the role SSNs play in facilitating identity theft. My bill is designed to protect SSN pri-

vacy while preserving its vital use in our society and economy, by ensuring SSNs are assigned accurately, exchanged only when necessary, and protected from indiscriminant disclosure."

FOCUS OF THE HEARING:

The Subcommittee will examine how criminals use SSNs to commit identity theft, the impact on victims, and will receive feedback from consumer advocates and representatives from the public and private sector regarding the *Social Security Number Privacy and Identity Theft Prevention Act of 2003*.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, *http://waysandmeans.house.gov,* select *"108th Congress"* from the menu entitled, *"Hearing Archives"* (*http://waysandmeans.house.gov/Hearings.asp?congress=16*). Select the hearing for which you would like to submit, and click on the link entitled, *"Click here to provide a submission for the record."* Once you have followed the online instructions, completing all informational forms and clicking "submit" on the final page, an email will be sent to the address which you supply confirming your interest in providing a submission for the record. You ***MUST REPLY*** to the email and ***ATTACH*** your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, by close of business Tuesday, June 22, 2004. **Finally,** please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225–1721.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item 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. All submissions and supplementary materials must be provided in Word or WordPerfect format and MUST NOT exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies 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. All submissions must include a list of all clients, persons, and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission 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.

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
June 14, 2004
SS–9—Revised

CONTACT: (202) 225–9263

Change in Time for Hearing on Enhancing Social Security Number Privacy

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 enhancing Social Security number privacy, previously scheduled for Tuesday, June 15, 2004, at 10:00 a.m., in room B–318 Rayburn House Office Building, ***will now be held at 11:00 a.m.***

All other details for the hearing remain the same. (See Subcommittee Advisory ***No. SS–9,*** dated June 8, 2004

Chairman SHAW. Good morning. Welcome to all our guests. We were up until midnight cranking out a tax bill last night. I appreciate, Ben, you and Sam being here. Today the Subcommittee will hear testimony about the growing threat of identity theft, the need to prevent identity theft and terrorists from stealing innocent Americans' Social Security numbers (SSNs), and my bipartisan, and I underscore bipartisan, "Social Security Number Privacy and Identity Theft Prevention Act of 2003," H.R. 2971. I think you are a cosponsor of that.

The SSN is woven into the fabric of many of our dealings with governments and businesses. They are widely used as personal identifiers even though the original purpose was simply to track earnings for determining eligibility and benefit amounts under Social Security. Some of the uses of the SSNs help us achieve important goals like reducing waste, fraud and abuse in government programs; enforcing child support; and aiding law enforcement. Unfortunately there is also wide use of SSNs for everyday business transactions. Concerns about identity theft are rapidly growing. According to the Federal Trade Commission (FTC), identity theft is the number one consumer complaint, amounting to 42 percent of complaints received in 2003. Americans are becoming more aware of the role of SSNs in identity theft thanks to the efforts of the SSA (SSA), the FTC, the U.S. Postal Inspection Service, and other agencies. Due to the increasing public pressure to act, businesses are starting to move away from using SSNs, and several States have passed legislation that does protect SSNs.

While everybody recognizes the need to protect the SSNs, Federal laws do not do enough to prevent the unnecessary disclosure. As a result, SSNs are sought-after tools for identity theft; worse yet, terrorists use of SSN fraud and identity theft to assimilate themselves into our society. Identity theft continues to threaten our

individual and national security. Clearly we need a comprehensive law to better protect the privacy of SSNs, and protect the American public from being victimized. That is why I, along with several Members of the Subcommittee, including the Ranking Member Mr. Matsui, introduced H.R. 2971, the "Social Security Number Privacy and Identity Theft Prevention Act of 2003." This bill would restrict the sale and public display of SSNs, limit dissemination of SSNs by consumers reporting agencies, make it more difficult for businesses to deny services if a customer refuses to provide his or her SSN, and establish civil and criminal penalties for the violation.

Providing for uses of SSNs that benefit the public while protecting their privacy is a very complex balancing act. This bill achieves that balance by ensuring SSNs are assigned accurately, exchanged only when necessary, and protected from the indiscriminate disclosure. This 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 2002. In the 107th Congress, I, along with Ranking Member Matsui and 80 other Members of Congress, sponsored a similar bill. Consideration of this legislation was rightly preempted by necessary congressional response to the September 11 attacks.

My hope is that this hearing will serve as a catalyst toward action, first through markup in this Subcommittee and the full Committee, followed by similar action by other Committees of jurisdiction, so that we may bring this important legislation to the House. Again, I underscore that in going through my statement, you may wonder, well, if you have had all this time why haven't you done anything? The problem really lies in that there is so much jurisdiction throughout Capitol Hill, that has stalled us at many, many areas where we shouldn't have been stalled down. I look forward to hearing from each of our witnesses, and I thank each of you in advance for sharing with us your experience and your recommendations. I would now yield to the gentleman from Maryland, my friend Mr. Cardin.

Mr. CARDIN. Thank you, Chairman Shaw. First let me thank you for conducting this hearing, and thank you for your leadership on this issue. It is a difficult matter, the proper use of SSNs and the misuse of SSNs and the role that people illegally obtaining SSNs have used in identity theft. So, these are issues that are of great concern to all of us in Congress.

Mr. Chairman, if I am correct, I think this is the 11th hearing that our Subcommittee has held in the last 4 years on this general subject because of our concern, and I do applaud you for the introduction of H.R. 2971, the "Social Security Number Privacy and Identity Theft Prevention Act of 2003". You are correct. This enjoys strong bipartisan support. I am proud to be a cosponsor of that bill. I think it is absolutely essential that Congress act in this area to give the clear message about the seriousness of the misuse of SSNs.

A SSN should be your identifying number for Social Security. It should not be used for every other purpose imaginable that is currently being used by society and by commerce, but it is being used

for other purposes, and it presents a real dilemma for us as to how we reverse this use and how we can protect a person's privacy.

It is a very serious issue, because what identity theft has meant to our Nation, the FTC has received more than a half million calls on the identity fraud line, and they have projected that about 5 percent, 5 percent of our adult population of the United States, some 10 million people, were victims of some kind of identity theft in just the last 12 months. So, this is a huge issue that we need to deal with. We can't just be quiet on the subject by saying it is difficult in that so many people have our SSNs, and how are we ever going to be able to retrieve the privacy that was intended when the Social Security system was created.

I look forward to hearing the testimony of our witnesses today as we try to develop a strategy to balance the needs of our society and the protection of our constituents. Mr. Chairman, I look forward to working with you and the other Members of the Committee as we attempt to get through the maze of the different jurisdictional problems in Congress and pass the necessary protective laws here in this body. Thank you.

Chairman SHAW. Thank you, Mr. Cardin. I would like to yield at this time to Mr. Ryan, who is here and wants to introduce a member of the second panel, but he is concerned that his schedule might not allow him to be here, so I would yield to him for that introduction.

Mr. RYAN. I thank the Chair. I have a bill coming to the floor momentarily, so I won't I be able to stay until that time, but I wanted to just take a couple of moments to introduce someone who is on the next panel who is a perfect person to have testifying with us today. That is Mark Ladd, who is the Register of Deeds for Racine County. Mark is very experienced, has been the Register of Deeds in Racine since 1994. He is the past President of the Wisconsin Register of Deeds Association. He is also a member of the Board of Directors of the National Association of County Recorders and Election Clerks, and he is the Co-Chair of the Property Records Industry Association Technology Board, which is, I think, in that capacity where he is going to offer a lot of expertise. He is also a good friend of mine, and I am excited that Mark is here to testify in the next panel.

I hope that I can make it. It is only when you have a bill coming to the floor, which I have on the Suspension Calendar, that it presents a very unpredictable schedule. So, I thank the Chair for indulging me to be able to introduce my friend and a good expert from Racine, Wisconsin, who will be testifying on the next panel. Thank you, and I yield.

Chairman SHAW. Okay. The first panel, which is already assembled at the table, are also four perfect witnesses: Howard Beales, who is the Director of the Bureau of Consumer Protection in the FTC; Patrick O'Carroll, Acting Inspector General, SSA; Barbara Bovbjerg, who is Director of Education, Work force and Income Security; Lawrence Maxwell, Assistant Chief Inspector of the Investigations and Security. Welcome, all of you. We have each of your full statements that will be made a part of the record. You may proceed as you see fit, and if you could capsule your statement into 5 minutes, we would be most appreciative.

STATEMENT OF J. HOWARD BEALES, III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. BEALES. Thank you, Mr. Chairman. I am Howard Beales. I am Director of the FTC's Bureau of Consumer Protection, and I am pleased to present the views of the Commission this morning. In a survey we conducted last year, the Commission learned some startling results about the incidence of identity theft and the impact of this crime on its victims. The data showed that within the 12 months preceding the survey, almost 3 and one-fourth million persons discovered that an identity thief opened new accounts in their names. An additional 6.6 million people learned of the misuse of an existing account. Overall nearly 10 million people, or 4.6 percent of the adult population, discovered that they were victims of some form of identity theft.

These numbers translate to nearly $48 billion in losses to businesses, nearly $5 billion in losses to victims, and almost 300 hours spent by victims to resolve their problems. Moreover, identity theft is a growing crime. The survey indicated a significant increase in the previous 2 to 3 years, nearly a doubling from one year to the next, although the research also showed that this increase has slowed recently. Notably the recent increase involved the misuse of existing accounts, which tends to cause less economic injury to victims and is generally easier for them to identify and to fix.

Overall, the survey analysis puts the incident rates of identity theft into sharper focus and demonstrates the need for concerted action between the public and private sectors to act aggressively to reduce identity theft, SSNs play a pivotal role in identity theft. Thieves use the SSN as a key to access the financial benefits available to their victim. Preventing identity thieves from obtaining SSNs will help to protect consumers from this pernicious crime. The potential for misuse arises because SSNs are crucial to the proper functioning of our financial system. Socials are used to match consumers to their credit and other financial information. Without them, information may be attributed to the wrong consumers, and the accuracy of credit reports may be degraded. Enabling SSNs to be used appropriately will help to ensure that consumers continue to enjoy the benefits of our current credit system.

The Commission is studying the efficacy of increasing the number of points of identifying information that a credit reporting agency is required to match to ensure that a consumer is the correct individual to whom a consumer report relates before releasing that report to a user. The study to be completed by this December should greatly increase our knowledge of the importance of SSNs in the matching process, and we look forward to reporting our findings.

Socials are collected by public and private entities for various purposes, and several Federal and State laws restrict the use or disclosure of SSNs depending on the source. The nationwide credit bureaus are primary private sources of SSNs, collecting information from financial institutions for credit reporting purposes. This information typically includes the consumer's identifying information, such as name, address and SSN, as well as information relating to the consumer's credit accounts. The identifying information collected by the credit bureau is one of the most reliable and com-

prehensive sources of this information, because individuals tend to provide their financial institutions with accurate and up-to-date information. Moreover, credit bureau databases contain information for over 200 million consumers.

The Gramm-Leach-Bliley Act (P.L. 106–102) imposes certain restrictions on the reuse and re-disclosure of the identifying information that is collected by credit bureaus as a general matter. The act prohibits financial institutions from disclosing nonpublic personal information to nonaffiliated third parties without first providing consumers with notice and the opportunity to opt out of such disclosure. This general restriction, however, is subject to certain exceptions. The information may flow from financial institutions to others for certain purposes specified in the statute and in the rule, including, for example, to process transactions or to report consumer information to credit bureaus. When information is disclosed under these exceptions, the recipient may not use or disclose that information except in the ordinary course of business to carry out the activity covered by the exception under which the information was received.

The Fair and Accurate Credit Transactions (FACT) Act of 2003 (P.L. 108–159) provides several new and important measures to prevent identity theft and facilitate victim recovery. One prominent benefit will be greater access to free consumer reports. Several other measures also act to prevent identity theft. The National Fraud Alert System will put potential creditors on notice that they must proceed with caution. The red flag rulemaking will require financial institutions and creditors to analyze patterns and take appropriate steps to prevent the crime. When fully implemented, these provisions should help to reduce the incidence of identity theft and to help victims recover when problems do occur.

Identity theft places substantial costs on individuals and businesses. We look forward to working with businesses on better ways for them to protect the valuable information of the consumers with whom they do business as well as other means of preventing identity theft. We anticipate that Nation will help and reduce the impact on victims as well. Thank you, and as you know, Mr. Chairman, I have a prior obligation at noon, and I will stay as long as I can to answer questions. I would be happy to answer questions for the record, but I may have to leave early.

[The prepared statement of Mr. Beales follows:]

Statement of J. Howard Beales, III, Director, Bureau of Consumer Protection, Federal Trade Commission

I. **INTRODUCTION**

Mr. Chairman, and members of the Subcommittee, I am J. Howard Beales, III, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on identity theft and Social Security numbers. The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. Through this testimony, the Commission will describe the results of a recent survey on the prevalence and impact of identity theft, the ways in which Social Security numbers are collected and used, new protections

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

for consumers and identity theft victims, and the Commission's identity theft program.

II. UNDERSTANDING THE IMPACT OF IDENTITY THEFT

On November 1, 1999, the Commission began collecting identity theft complaints from consumers in its national database, the Identity Theft Data Clearinghouse (the "Clearinghouse").[2] Every year since has seen an increase in complaints.[3] The Clearinghouse now contains over 600,000 identity theft complaints taken from victims across the country. By itself, though, these self-reported data do not currently allow the FTC to draw any firm conclusions about the incidence of identity theft in the general population. To address this important issue, the FTC commissioned a survey last year to gain a better picture of the incidence of identity theft and the impact of the crime on its victims.[4] The results were startling. The data showed that within the 12 months preceding the survey, 3.23 million persons discovered that an identity thief opened new accounts in their names. An additional 6.6 million consumers learned of the misuse of an existing account. Overall, nearly 10 million people—or 4.6 percent of the adult population—discovered that they were victims of some form of identity theft. These numbers translate to nearly $48 billion in losses to businesses, nearly $5 billion in losses to individual victims, and almost 300 million hours spent by victims trying to resolve their problems.

Moreover, identity theft is a growing crime. The survey indicated a significant increase in the previous 2–3 years—nearly a doubling from one year to the next, although the research showed that this increase has recently slowed. Notably, this recent increase primarily involved the misuse of an existing account, which tends to cause less economic injury to victims and is generally easier for them to identify and fix. Overall, the 2003 survey analysis puts the incidence rates of identity theft into sharper focus, and demonstrates the need for a concerted effort between the public and private sectors to act aggressively to reduce identity theft.

III. SOCIAL SECURITY NUMBER USES AND IDENTITY THEFT

Social Security numbers play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims. Preventing identity thieves from obtaining Social Security numbers will help to protect consumers from this pernicious crime. The potential for misuse arises because Social Security numbers are crucial to the proper functioning of our financial system. Social Security numbers are used to match consumers to their credit and other financial information. Without them, information may be attributed to the wrong consumer, and the accuracy of credit reports may be degraded. Enabling Social Security numbers to be used appropriately will help to ensure that consumers continue to enjoy the benefits of our current credit system. The Commission is studying "the efficacy of increasing the number of points of identifying information that a credit reporting agency is required to match to ensure that a consumer is the correct individual to whom a consumer report relates before releasing a consumer report to a user" as required by the Fair and Accurate Credit Transactions Act of 2003.[5] This study, to be completed by December, 2004, should greatly increase our knowledge of the importance of Social Security numbers in the matching process. The Commission looks forward to reporting its findings to Congress.

Social Security numbers are collected by public and private entities for various purposes, and several federal and state laws restrict the use or disclosure of Social Security numbers, depending on the source.[6] The nationwide credit bureaus are pri-

---

[2] *See infra* Section V for a discussion of the Commission's mandate to maintain an identity theft complaint database pursuant to the 1998 Identity Theft Assumption and Deterrence Act.

[3] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

[4] The research took place during March and April 2003. It was conducted by Synovate, a private research firm, and involved a random sample telephone survey of over 4,000 U.S. adults. The full report of the survey can be found at http://www.consumer.gov/idtheft/stats.html.

[5] Pub. L. No. 108–396, § 318 (2003).

[6] As GAO has reported, government and commercial entities use social security numbers for a number of different purposes, including to verify the eligibility of applicants, manage records, and conduct research. 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) and *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO–02–352 (Washington, D.C.: May 31, 2002). As examined in detail in GAO's January 2004 report, private sector entities (information resellers, consumer reporting agencies, health care organizations) obtain social security numbers both directly from consumers and other businesses, and the entities use them for a variety of purposes, including identification and to match the consumer to information stored in the consumer's credit report. *See* U.S.

Continued

mary private sources of Social Security numbers, collecting information from financial institutions for credit reporting purposes. This information typically includes a consumer's identifying information—such as name, address, and Social Security number—as well as information related to the consumer's credit accounts. The identifying information collected by the credit bureaus is one of the most reliable and comprehensive sources of this information, because individuals tend to provide their financial institutions with accurate and up-to-date identifying information and the credit bureau databases contain information for over 200 million consumers.[7]

The Gramm-Leach-Bliley Act ("GLBA")[8] imposes certain restrictions on the reuse and redisclosure of the identifying information—including Social Security numbers—that is collected by credit bureaus from financial institutions.[9] As a general matter, the GLBA prohibits financial institutions from disclosing nonpublic personal information ("NPI") to nonaffiliated third parties without first providing consumers with notice and the opportunity to opt out of such disclosure. This general restriction, however, is subject to certain exceptions. The information may flow from financial institutions to others for certain purposes specified in the statute and rule, including, for example, to process transactions or to report consumer information to credit bureaus.[10] When information is disclosed under these GLBA exceptions, the recipient may not use or disclose that NPI except "in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received]."[11]

IV. **NEW PROTECTIONS FOR IDENTITY THEFT VICTIMS**

On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was enacted.[12] Many of the provisions amend the Fair Credit Reporting Act ("FCRA"),[13] and provide new and important measures to prevent identity theft and facilitate identity theft victims' recovery. Some of these measures will take effect this year.[14] They will codify many of the voluntary measures initiated by the private sector and improve other recovery procedures already in place.

One prominent benefit of these amendments to the FCRA is the greater access to free consumer reports.[15] Previously under the FCRA, consumers were entitled to a free consumer report only under limited circumstances.[16] Beginning in December of this year with a regional rollout, nationwide and nationwide specialty consumer

---

General Accounting Office, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs and Laws Limit the Disclosure of This Information*, GAO–04–11 (Washington, D.C.: Jan. 22, 2004).

[7] *See* Consumer Data Industry Association's Web site, *available at http://www.cdiaonline.org/about.cfm*.

[8] Subtitle A of Title 5 of the GLBA, 15 U.S.C. §§ 6801–6809.

[9] The GLBA applies to any "nonpublic personal information" ("NPI") that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, Social Security number, address, telephone number, mother's maiden name, and prior addresses. *See, e.g.*, 65 Fed. Reg. 33,646, 33680 (May 24, 2000) (the FTC's Privacy Rule). This identifying information generally is not covered by the Fair Credit Reporting Act. *See FTC v. Trans Union*, Dkt. 9255, Op. of the Commission at pp. 30–31 (Mar. 1, 2000) (holding that consumer name, Social Security number, address, telephone number, and mother's maiden name do not constitute a consumer report under the FCRA).

[10] These exceptions are found in § 502(e) of the GLBA, and in §§ 313.14 and 313.15 of the FTC's privacy rule. The other GLBA privacy rules contain substantially similar provisions. The § 313.14 exceptions relate to the processing and servicing of transactions at the consumer's request, and the § 313.15 exceptions contain a broad range of unrelated exceptions, such as preventing fraud, assisting law enforcement, complying with subpoenas, and reporting to credit bureaus. Section 313.13 also contains an exception to the notice and opt out requirement, but that section is not relevant here because it relates to contractual arrangements with service providers and joint marketers.

[11] 16 C.F.R. 313.11(a)(1)(iii), (c)(3) (2000).

[12] Pub. L. No. 108–396 (2003) (codified at 15 U.S.C. § 1681 *et seq.*).

[13] 15 U.S.C. § 1681 *et seq.*

[14] The statute set effective dates for certain sections and required the Commission and the Federal Reserve Board jointly to set effective dates for the remaining sections. *See* Effective Dates for the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 602.1 (2004).

[15] Pub. L. No. 108–396, § 211 (2003).

[16] Previously, free reports were available only pursuant to the FCRA when the consumer suffered adverse action, believed that fraudulent information may be in his or her credit file, was unemployed, or was on welfare. Absent one of these exceptions, consumers had to pay a statutory "reasonable charge" for a file disclosure; this fee is set each year by the Commission and is currently $9. *See* 15 U.S.C. § 1681j. In addition, a small number of states required the CRAs to provide free annual reports to consumers at their request.

reporting agencies[17] must provide free credit reports to consumers once annually, upon request.[18] Free reports will enhance consumers' ability to discover and correct errors, thereby improving the accuracy of the system, and also enable consumers to detect identity theft early.

Other measures that act to prevent identity theft include:

- *National fraud alert system:*[19] Consumers who reasonably suspect they have been or may be victimized by identity theft, or who are military personnel on active duty away from home,[20] can place an alert on their credit files. The alert will put potential creditors on notice that they must proceed with caution when granting credit in the consumer's name. The provision also codified and standardized the "joint fraud alert" initiative administered by the three major credit reporting agencies. After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each credit reporting agency now shares that request with the other two nationwide credit reporting agencies, thereby eliminating the need for the victim to contact each of the three agencies separately.
- *Truncation of credit and debit card receipts:*[21] In some instances, identity theft results from thieves obtaining access to account numbers on credit card receipts. FACTA seeks to reduce this source of fraud by requiring merchants to truncate the full card number on electronic receipts. The use of truncation technology is becoming widespread, and some card issuers already require merchants to truncate.[22]
- *"Red flag" indicators of identity theft:*[23] The banking regulators and the FTC will jointly develop a rule to identify and maintain a list of "red flag" indicators of identity theft. The goal of this provision is for financial institutions and creditors to analyze identity theft patterns and practices so that they can take appropriate action to prevent this crime.
- *Disposal of Consumer Report Information and Records:*[24] The banking regulators and the FTC are coordinating a rulemaking to require proper disposal of consumer information derived from consumer reports.[25] This requirement will help to ensure that sensitive consumer information, including Social Security numbers, is not simply left in a trash dumpster, for instance, once a business no longer needs the information.[26]

FACTA also includes measures that will assist victims with their recovery. These provisions include:

- *Identity theft account blocking:*[27] This provision requires credit reporting agencies immediately to cease reporting, or block, allegedly fraudulent account information on consumer reports when the consumer submits an identity theft report,[28] unless there is reason to believe the report is false. Blocking would mitigate the harm to consumers' credit records that can result from identity theft. Credit reporting agencies must also notify information furnishers who must then cease furnishing the fraudulent information and may not sell, transfer, or place for collection the debt resulting from the identity theft.

---

[17] Section 603(w) of the FCRA defines a "nationwide specialty consumer reporting agency" as a consumer reporting agency that compiles and maintains files on consumers relating to medical records or payments, residential or tenant history, check writing history, employment history, or insurance claims, on a nationwide basis. 15 U.S.C. § 1681a(w).

[18] *See* Free Annual File Disclosures, 16 C.F.R. §§ 610.1 and 698.1 (2004).

[19] Pub. L. No. 108–396, § 112 (2003).

[20] The Commission is developing a rule on the duration of this active duty alert. *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23372 (April 28, 2004) (to be codified at 16 C.F.R. pt. 613).

[21] Pub. L. No. 108–396, § 113 (2003).

[22] FACTA creates a phase-in period to allow for the replacement of existing equipment.

[23] *Id.* § 114.

[24] *Id.* § 216.

[25] Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21388 (April 20, 2004) (to be codified at 16 C.F.R. pt. 682).

[26] In its outreach materials, the FTC also advises consumers to shred any sensitive information before disposing of it.

[27] Pub. L. No. 108–396, § 152 (2003).

[28] The Commission is developing a rule to define the term "identity theft report." *See* Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, 69 Fed. Reg. 23370, 23371 (April 28, 2004) (to be codified at 16 C.F.R. pt. 603).

- *Information available to victims:*[29] A creditor or other business must give victims copies of applications and business records relating to the theft of their identity at the victim's request. This information can assist victims in proving that they are, in fact, victims. For example, they may be better able to prove that the signature on the application is not their signature.
- *Prevention of re-reporting fraudulent information:*[30] Consumers can provide identity theft reports directly to creditors or other information furnishers to prevent them from continuing to furnish fraudulent information resulting from identity theft to the credit reporting agencies.

When fully implemented, these provisions should help to reduce the incidence of identity theft, and help victims recover when the problem does occur.

V. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[31] The Identity Theft Act strengthened the criminal laws governing identity theft[32] and focused on consumers as victims.[33] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints, to make available and to refer these complaints to law enforcement for their investigations, and to provide victim assistance and consumer education. Thus, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[34]

To fulfill the Act's mandate, the Commission implemented a program that focuses on three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website, (2) maintaining and promoting the Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

A. Assisting Identity Theft Victims

The Commission takes complaints from victims through a toll-free hotline, 1–877–ID THEFT (438–4338),[35] and a secure online complaint form on its website, www.consumer.gov/idtheft. In addition, the FTC provides advice on recovery from identity theft. Callers to the hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the

---

[29] Pub. L. No. 108–396, § 151 (2003).

[30] *Id.* § 154.

[31] Pub. L. No. 105–318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

[32] 18 U.S.C. § 1028(a)(7) made identity theft a crime by focusing on the unlawful use of an individual's "means of identification," which broadly includes "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.,* credit cards), electronic identification number or routing code, and telecommunication identifying information.

[33] Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105–274, at 4 (1998).

[34] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Corporate Marketing Solutions, Inc.*, CIV—02 1256 PHX RCB (D. Ariz Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards) and *FTC v. C.J.*, CIV—03 5275 GHK (RZx) (C. D. Cal. July 24, 2003) (final order); *FTC v. Hill*, CV–H–03–5537 (S.D. Tex. Dec. 3, 2003) (final order); and FTC v. M.M., CV–04–2086 (E.D. NY May 18, 2004) (final order) (defendants sent "phishing" spam purporting to come from AOL or Paypal and created look-alike websites to obtain credit card numbers and other financial data from consumers that defendants used for unauthorized online purchases.). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam (Jan. 16, 2003) (*at http://www.ftc.gov/opa/2003/01/idpfinal.htm*).

[35] The Commission has a separate toll-free line (877–FTC–HELP) to serve those with general consumer protection complaints.

misuse of their identities.[36] Victims are currently advised to:[37] (1) obtain copies of their credit reports from the three national consumer reporting agencies and have a fraud alert placed on their credit reports;[38] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the FCRA,[39] the Fair Credit Billing Act,[40] the Truth in Lending Act,[41] and the Fair Debt Collection Practices Act.[42] If another federal agency can assist victims because the nature of the victims' identity theft falls within such agency's jurisdiction, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form, which allows victims to enter their identity theft information into the Clearinghouse. Victims also immediately can read and download all of the resources necessary for reclaiming their credit record and good name, including the FTC's tremendously successful consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name.*[43] The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims and how to correct more intensive credit-related problems that may result from identity theft. It also describes other federal and state resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.3 million copies of the booklet since its release in February 2000, and recorded over 1.4 million visits to the Web version.[44]

B. **The Identity Theft Data Clearinghouse**

One of the primary purposes of the Identity Theft Act was to enable criminal law enforcement agencies to use a single database of victim complaints to support their investigations. To ensure that the database operates as a national clearinghouse for complaints, the FTC accepts complaints from external sources such as other state or federal agencies as well as directly from consumers through its call center and online complaint form. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA–OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. The Commission publishes annual charts showing the prevalence of identity theft complaints by states and by cities.[45] Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse in July of 2000, more than 970 law enforcement agencies, from the federal to the local level, have signed up for secure online access to the database. Individual investigators within those agencies have the ability to access the system from their desktop computers 24 hours a day, seven days a week.

The Commission actively encourages even greater use of the Clearinghouse. Beginning in 2002, in an effort to further expand the use of the Clearinghouse among

---

[36] Spanish speaking counselors are available for callers who select the Spanish-language option on the toll-free line.

[37] As the relevant provisions of FACTA become effective, the Commission will update its advice to victims on their new rights and procedures for recovery.

[38] These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name.

[39] 15 U.S.C. § 1681 *et seq.*

[40] *Id.* § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[41] *Id.* § 1601 *et seq.*

[42] *Id.* § 1692 *et seq.*

[43] *Identity Theft: When Bad Things Happen to Your Good Name* and the secure complaint form are available in Spanish.

[44] Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name.*

[45] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

law enforcement, the FTC, in cooperation with the Department of Justice, the United States Postal Inspection Service, and the United States Secret Service, initiated full day identity theft training seminars for state and local law enforcement officers. To date, seminars have been held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, Phoenix, New York City, Seattle, San Antonio, Orlando, and Raleigh. The FTC also helped the Kansas and Missouri offices of the U.S. Attorney and State Attorney General conduct a training seminar in Kansas City. More than 1500 officers have attended these seminars, representing more than 600 different agencies. Future seminars are being planned for additional cities.

The FTC staff also developed an identity theft case referral program.[46] The staff creates preliminary investigative reports by examining significant patterns of identity theft activity in the Clearinghouse and refining the data through the use of additional investigative resources. Then the staff refers the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers throughout the country for further investigation and potential prosecution. The FTC is aided in this work by its federal law enforcement partners including the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service who provide staff and other resources. Recently, an FBI analyst has worked intensively with the Clearinghouse complaints, using sophisticated analytical software to find related complaints and combine the information with other data sources available to the FBI.

C. **Outreach and Education**

The Identity Theft Act also directed the FTC to educate consumers about identity theft. Recognizing that law enforcement and private industry each play an important role in helping consumers both to minimize their risk and to recover from identity theft, the FTC expanded its outreach and education mission to include these sectors.

(1) *Consumers:* The FTC has taken the lead in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print and online materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

To increase awareness for the average consumer and provide tips for minimizing the risk of identity theft, the FTC developed a new primer on identity theft, *ID Theft: What's It All About?*.[47] Taken together with the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name*, the two publications help to educate consumers.

(2) *Law Enforcement:* Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described previously (*see infra* Section V.B), the staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. Other outreach initiatives include: (i) Participation in a "Roll Call" video produced by the Secret Service, which has been sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (ii) the redesign of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations.

(3) *Industry:* The private sector can help with the problem of identity theft in several ways. From prevention through better security and authentication, to helping victims recover, businesses play a key role in reducing the impact of identity theft.

(a) *Information Security Breaches:* The FTC works with institutions that maintain personal information to identify ways to help keep that information safe from identity theft.[48] In 2002, the FTC invited representatives from fi-

[46] The referral program complements the regular use of the database by all law enforcers from their desktop computers.

[47] Since its release in May 2003, the FTC has distributed almost 554,000 paper copies and over 75,000 web versions, and developed a Spanish version.

[48] The Commission also has law enforcement authority relating to information security. In addition to developing the Disposal Rule pursuant to FACTA, *see supra* Section IV, the Commis-

nancial institutions, credit issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance.[49] To provide standardized assistance in these types of cases, the FTC developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, that is available on the identity theft website.The kit provides advice on contacting consumers, law enforcement agencies, business contact information for the three major credit reporting agencies, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know to protect themselves from identity theft.

(b) *Victim Assistance:* Identity theft victims may spend substantial time and effort restoring their good names and financial records. As a result, the FTC devotes substantial resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.[50] To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001 through April 2004, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been nearly 557,000 hits to the Web version. The affidavit is available in both English and Spanish.

VI. **CONCLUSION**

Identity theft places substantial costs on individuals and businesses. The Commission looks forward to working with businesses on better ways for them to protect the valuable information of consumers with which they are entrusted as well as other means of preventing identity theft. The Commission anticipates that as the new provisions of FACTA take effect, they will further help to reduce identity theft as well as its impact on victims.

Chairman SHAW. Thank you, Mr. Beales, and we appreciate your time that you are able to spend with us. Mr. O'Carroll.

STATEMENT OF PATRICK P. O'CARROLL, ACTING INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. O'CARROLL. Good morning, Mr. Chairman, Mr. Cardin, and Members of this Committee. Thank you for inviting me here today to discuss SSN misuse and H.R. 2971. As we were all paying our respects to President Ronald Reagan last week, I couldn't help re-

---

sion also is responsible for enforcing its GLBA Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. FTC Safeguards Rule, 16 C.F.R. § 314.1 (2002). In brief, the Safeguards Rule requires financial institutions to develop a written information security plan that includes certain elements that are basic to security.

In the past few years, the FTC has also brought enforcement actions against four companies that the Commission alleged made false promises about securing sensitive consumer information, in violation of Section 5 of the FTC Act. 15 U.S.C. § 45(a) These actions resulted in settlements with those companies that collected sensitive information from consumers while making such promises. Those actions arise out of the Commission's finding that these companies' security measures were inadequate and their information security claims therefore were deceptive. *See, e.g., In re Microsoft Corp.*, FTC Dkt. C–4069, Final Decision and Order available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf (Dec. 20, 2002).

[49] *See, e.g.* the incidents involving TriWest (Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. Times, Jan. 12, 2003, § 1 (Late Edition), at 12) and Ford/Experian (Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA Times, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1).

[50] *See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

calling that his signing of the Inspector General Act made our work possible.

It is because the SSN is so heavily relied upon as an identifier, it is a valuable commodity for lawbreakers. I will focus today on SSN misuse, homeland security and identity theft, and what more needs to be done to insure the integrity of the SSN. While financial crimes involving SSN misuse are more numerous than terrorism-related crimes, the potential threat to homeland security nevertheless justifies intense concern. Our primary mission is to protect the integrity of SSA programs and operations, and because of that we focus investigative efforts on cases affecting SSN integrity. We investigate and arrest suspects for fraud against Social Security programs and crimes involving SSN misuse.

In our homeland security and identity theft responsibility, we work closely with other Federal agencies participating in 63 joint terrorism task forces and 29 antiterrorism advisory councils. We recently met with the U.S. Department of Homeland Security to discuss methods in which we could work together to address the SSN's critical role at critical infrastructure sites. We have begun staffing an SSN Integrity Protection Team that combines the talents of auditors, investigators and attorneys.

My office is working closely with this Subcommittee and the SSA to strengthen controls over enumeration, to ensure the integrity of identification documents and to make SSN fraud as difficult as possible. Together with you and with SSA, we have made important strides in reducing enumeration vulnerabilities. Still, we believe the SSA should implement the following changes: establish a reasonable threshold for the number of replacement SSN cards an individual may obtain during a year and over a lifetime to continue to address identified weaknesses within the information security environment; verify birth records before issuing SSNs to citizens under the age of 1; and to incorporate additional controls in the SSA's Enumeration-at-Birth process.

We have conducted numerous audits and made extensive recommendations to the SSA to improve the SSN misuse problem in the earnings reporting area, and, most importantly, to improve controls over SSN misuse as it pertains to homeland security. We believe SSA and lawmakers should examine the feasibility of the following initiatives: to limit public SSN availability to the greatest extent practicable without unduly limiting commerce; to enact strong enforcement mechanisms and stiffer penalties for SSN misuse; cross-verify legitimate databases that use the SSA as a key data element; and review the implications of releasing information on deceased individuals.

We believe new legislation should prohibit the sale of SSNs, including one's own, on the open markets; to limit the use of the SSN to appropriate and legitimate transactions; and to prohibit using SSNs as student or patient identification numbers or as part of car rental contracts or video rentals; and to enhance penalties for those few SSA employees who assist criminals in obtaining SSNs. We support legislation such as H.R. 2971, which severely limits the sale, purchase, and display of SSNs to the general public. We also believe legislation such as H.R. 1731, the Identity Theft Penalty Enhancement Act, is a significant step toward holding accountable

individuals who misuse SSNs to commit egregious crimes. Over the past years we have made progress protecting SSN integrity. We stand ready to do more. I would now be happy to answer any questions you may have. Thank you.

[The prepared statement of Mr. O'Carroll follows:]

Statement of Patrick P. O'Carroll, Acting Inspector General, Social Security Administration

Good Morning, Mr. Chairman, Mr. Matsui, and members of the Subcommittee. Let me first thank you for the invitation to be here today for this important hearing to discuss the pervasive problem of Social Security number (SSN) misuse and the Committee's proposed legislation to protect the privacy of SSNs, the *Social Security Number Privacy and Identity Theft Prevention Act of 2003* (H.R. 2971).

The SSN as a National Identifier

I would like to begin my testimony today with a simple declaration: The SSN is a national identifier. In past years, many would challenge that statement. Today, we live in a changed world, and the SSN's role as a national identifier is a recognized fact. Unfortunately, with that knowledge, we must also accept that because the SSN is so heavily relied upon as an identifier, it is a valuable commodity for lawbreakers. Given the importance of this unique, nine-digit number and the tremendous risk associated with its misuse, one of the most important responsibilities my office undertakes each day is oversight of SSN integrity. Today I would like to focus my testimony on how the SSN is misused to commit crimes, my office's role in addressing homeland security and identity theft and what more needs to be done to ensure the integrity of the SSN.

Misuse of the SSN to Commit Crimes

While financial crimes involving SSN misuse are more numerous than terrorism-related crimes, the potential threat to homeland security nevertheless justifies intense concern. An SSN allows an individual to assimilate themselves into U.S. society. SSNs, therefore, become valuable tools for terrorists or others who wish to live in the United States and operate under the "radar screen." Such individuals may obtain SSNs by purchasing them, creating them, stealing them, utilizing the SSN of a deceased individual or obtaining them from SSA directly through the use of falsified documents. Once an individual has an SSN, he has the ability to work, buy a home, and engage in a wide range of financial transactions including the raising and transferring of funds.

I am also concerned about the escalating occurrences of identity theft, which is the fastest-growing form of white-collar crime in the United States. In September 2003, the Federal Trade Commission (FTC) released a survey showing that 27.3 million Americans were victims of identity theft between 1998 and 2003—including 9.9 million people in the study's final year. FTC also reported that during the study's final year, losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses. Clearly, this is an epidemic that must be brought under control.

Identity theft is an "enabling" crime, one that facilitates other types of crime, ranging from passing bad checks and defrauding credit card companies to committing acts of terrorism. Additionally, criminals use identity theft to defraud Federal agencies and programs of millions of dollars.

For example, based on an investigation conducted by our Atlanta Field Division, a St. Petersburg, Florida resident was recently sentenced to 27 months of incarceration and ordered to make restitution to SSA for over $79,000 in survivors benefits she received for herself and three nonexistent children. To perpetrate this scheme, the individual assumed the identity of a former acquaintance by obtaining a North Carolina identification card in her friend's name. With this new identity, she used fraudulent birth certificates to apply for SSNs on behalf of two fictitious children. She also altered court marriage and divorce documents, falsely claiming that a known deceased man was her ex-husband and the fictitious children's father. She perpetrated this elaborate scheme so that she could apply for and receive Social Security survivors benefits for the fictitious children—and, until caught, was successful in doing so. Further investigation revealed that she had previously committed a similar crime resulting in additional survivors benefits for herself and another fictitious child.

Other Federal agencies such as the Department of Housing and Urban Development (HUD) have also experienced a significant increase in the number of identity

theft occurrences in their programs. Within programs administered by HUD, identity thieves are using someone else's SSN to obtain and then default on home mortgages—leaving taxpayers to pay their bills.

For those with an illicit motive, an SSN can be obtained in many ways:

- Presenting false documentation to SSA.
- Stealing another person's SSN.
- Purchasing an SSN on the black market.
- Using the SSN of a deceased individual.
- Creating a nine-digit number out of thin air.

Although SSA may never be able to completely prevent individuals from purchasing an SSN on the black market or stealing the SSN of another, we are proud that our efforts are making it more difficult to do so.

Our Role in Addressing Homeland Security and Identity Theft

Recognizing the importance of SSNs to terrorists and identity thieves, SSA and the OIG take very seriously our responsibility to ensure that these numbers are only issued to those with a legal reason for having one. As such, we continuously seek innovative ways to prevent SSN misuse and create collaborative partnerships with other Federal, State, and local entities to address both homeland security and identity theft concerns.

OIG Homeland Security Activities:

Our active involvement in addressing homeland security began on September 11, 2001, with our agents assisting in rescue efforts and site security at the World Trade Center. We immediately assigned supervisors and agents to the FBI Command Centers in New York City and New Jersey to process information and investigate leads. The Inspector General ordered all Field Divisions to assist in Joint Terrorism Task Forces (JTTF) and Anti-Terrorism Task Forces (ATTF) around the country—in fact, we are now active participants in 63 Joint Terrorism Task Forces and 29 Anti-Terrorism Task Forces, as well as the Foreign Terrorist Tracking Task Force.

While participating in these task forces, our agents have assisted in better securing many of our Nation's airports and nuclear facilities by ensuring that employees and individuals having access to secure areas within these locations are working under their true names and SSNs. Further, as part of its anti-terrorism activities in the Buffalo area, our New York Field Division investigated six men from neighboring Lackawanna suspected of terrorist-related activities. Our investigators determined the identities of the "Lackawanna Six" and their attendance and participation in an al Qaeda terrorist training camp in Afghanistan. One suspect had two Social Security cards in his possession at the time of his arrest. All six suspects pleaded guilty to providing material support or resources to designated foreign terrorist organizations and received sentences of 7 to 10 years in prison.

In carrying out our homeland security responsibility, we coordinate closely with other Federal agencies. For example, we recently met with representatives of the Department of Homeland Security (DHS) to discuss methods in which we could work together to address the SSN's role in homeland security. We welcome this opportunity and believe cooperative ventures such as these are imperative to ensure that all of the links in the homeland security chain stay connected. Based on our initial discussions, we plan to work with DHS to explore possible data matching and cross-verification opportunities—those that are currently provided for under law and those for which additional legislation may be required.

OIG Identity Theft Activities:

By law and by mission, our office has a narrow but important role in the overall effort to address identity theft. Much of the Federal government's response to identity theft issues rightly belongs to the FTC. State and local law enforcement agencies and financial institutions also have critical roles to play.

Because *our* primary mission is to protect the integrity of SSA's programs and operations, in the majority of our identity theft investigations, we continue to focus investigative efforts on cases that affect SSN integrity. For example, our Chicago Field Division took part in a 3-day inter-agency undercover operation that resulted in the arrest of 12 suspects dealing in fraudulently obtained Social Security cards, State driver's licenses, and U.S. passports. Our investigators determined that the group's leader and 11 others took part in an elaborate document-counterfeiting scheme to obtain valid SSNs for non-existent children. The names belonged to undocumented noncitizens who paid up to $5,000 each for valid documents. Members of the group were sentenced to up to 2 years in prison or given immunity from prosecution for their cooperation in the undercover sting.

To maximize our investigative resources, we dedicate agents that work on task forces with other law enforcement agencies nationwide to investigate identity crimes. We also work closely with prosecutors to bundle SSN misuse cases that, when presented separately, may not have been accepted for prosecution.

We are also continuing our efforts to identify opportunities for SSA to further strengthen the integrity of the SSN. One of my major concerns has been the use of fraudulent documents to obtain SSNs. In an August 2002 audit, we estimated that during FY 2000, SSA assigned at least 63,000 SSNs to noncitizens based on invalid immigration documents that SSA processes did not detect. Based on our recommendation, SSA improved its controls in this area and now verifies all immigration documents presented by noncitizens with the issuing agency before assigning an SSN. We believe SSA's decision to adopt our recommendation was laudable and significantly reduced the circumstances under which an unauthorized noncitizen may obtain a legitimate SSN from the Agency. We are currently examining the Agency's compliance with this and other enumeration controls. Additionally, we continue to explore and recommend further controls the Agency can implement to strengthen SSA's important responsibility of assigning SSNs.

SSN Integrity Protection Team:

Protecting the integrity of the SSN has become a major part of the work we do. The President's Fiscal Year 2004 Budget enabled us to begin staffing our SSN Integrity Protection Team to combat SSN misuse and identity theft. The Team is an integrated model that combines the talents of auditors, investigators and attorneys in a comprehensive approach, allowing SSA and OIG to:

- Support Homeland Security.
- Identify patterns and trends of SSN misuse.
- Locate systemic weaknesses that contribute to SSN misuse such as in the enumeration and earnings related processes.
- Recommend legislative or other corrective actions to enhance the SSN's integrity.
- Pursue criminal and civil enforcement provisions for individuals misusing SSNs.

Our SSN Integrity Protection Team will enable us to better target audit and investigative work. The Team will participate with other Federal, State and local entities to collaborate on potential SSN misuse activities. It is critical that we continue to receive funding in future budgets for this important initiative.

SSA Initiatives to Address SSN Integrity:

SSA has made significant progress in strengthening the defenses of the SSN, implementing important suggestions our office has made, and working with us to find solutions. In November 2001, the Commissioner of Social Security established an Enumeration Response Team (ERT) comprised of executives across the Agency, including representatives from the OIG. The Commissioner charged this group with identifying steps the Agency could take to improve the enumeration process and to enhance the integrity of the SSN. Since that time, the Commissioner and the ERT have implemented numerous policies and procedures designed to better ensure that only individuals authorized to do so, receive an SSN. For example, the ERT recommended, and SSA adopted, more stringent circumstances under which an individual may obtain a nonwork SSN. We are proud to serve on workgroups such as these and applaud the Commissioner and SSA for its strong commitment to improving SSN integrity.

Prior to the ERT, the Agency implemented other initiatives such as the Comprehensive Integrity Review Process (CIRP) and Enumeration at Entry process. The CIRP system identifies vulnerabilities in the enumeration process and issues alerts to SSA's field offices (FO) to develop and certify. The FO reviewer, usually a manager or supervisor, performs an enumeration integrity review of each alert. If the reviewer determines that there is a possibility of fraud, the alert is forwarded to the OIG for development and disposition.

The Enumeration at Entry initiative is a collaboration with the Department of Homeland Security (DHS) and the Department of State (DOS) to not only facilitate issuance of SSNs to legally admitted aliens whose immigration status permits such issuance, but it ensures through DHS and DOS certifications that the identity and immigration status of the alien is what is purported.

What Actions Still Need to Be Taken to Address SSN Misuse

Despite the significant progress SSA and Congress have made in recent years to address SSN misuse, we believe SSN integrity and protection still need improvement at three stages: at issuance, during the life of the number-holder, and following the number-holder's death.

At Stage One (issuance of the SSN), 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 fraudulently obtain an SSN from the Federal government. Together with you and with SSA, we have made important strides in reducing enumeration vulnerabilities, and that effort continues. Still, to strengthen our defenses even further, we believe SSA should implement the following changes.

- Establish a reasonable threshold for the number of replacement SSN cards an individual may obtain during a year and over a lifetime.
- Continue to address identified weaknesses within the enumeration process to better safeguard SSNs.
- Verify the validity of birth records with the issuing State before issuing an SSN to U.S. citizens under age 1.
- Work with State Bureaus of Vital Statistics to incorporate additional controls in SSA's Enumeration-at-Birth program, such as periodically reconciling the number of SSNs assigned through the program to the number of births reported by participating hospitals.

It is at Stages Two (during the life of the number holder) and Three (after the number holder's death) 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 extensive 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. Nevertheless, to more completely address SSN integrity during the life of the number holder and following that number holder's death, we believe SSA and lawmakers should examine the feasibility of the following initiatives.

- Limiting the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.
- Prohibiting the sale of SSNs, prohibiting their display on public records, and limiting their use to legitimate transactions.
- Enacting strong enforcement mechanisms and stiffer penalties to further discourage SSN misuse.
- Cross-verifying all legitimate databases that use the SSN as a key data element.
- Review the implications of releasing information on deceased individuals.

Limiting the SSN's Public Availability and Sale of the SSN

Perhaps the most important step we can take in preventing SSN misuse is to limit the SSN's easy availability. We believe 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, it will be extremely difficult to reverse the trend. We believe effective legislation should 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 through an Internet auction, we will continue to be plagued by the consequences.

To be fully effective, we also believe legislation 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.

Congress enacted the Identity Theft and Assumption Deterrence Act in 1998, responding to the growing epidemic of identity thefts by imposing criminal sanctions for those who create a false identity or misappropriate someone else's. The Internet False Identification Prevention Act, adopted in 2000, closed a loophole left by the earlier legislation, enabling our office and other law enforcement organizations to pursue vendors who previously could sell counterfeit Social Security cards legally by maintaining the fiction that such cards were "novelties" rather than counterfeit documents. More legislative tools are needed, and we have worked with Congress to identify legislation necessary to protect the integrity of the SSN. For example, the House is now considering H.R. 2971, the *Social Security Number Privacy and Identity Theft Prevention Act of 2003*, which would seriously restrict the use of SSNs in the private and public sector, and criminalize the sale of SSNs.

Penalties

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. We believe legislation should not only provide criminal penalties in the Social Security Act, but also enhance penalties for those few SSA employees who betray the public trust and assist criminals in obtaining SSNs.

For example, a former SSA Service Representative was sentenced to 3 years probation and community service after pleading guilty to a bribery charge in connection with issuing 100 to 200 Social Security cards to illegal aliens. She received between $50 and $150 for each card. We believe it is critically important to send a strong message to SSA employees tempted to facilitate crimes against Agency programs by pursuing the maximum sentence possible.

The House Committee on the Judiciary recently approved H.R. 1731, the *Identity Theft Penalty Enhancement Act*, which established enhanced penalties for aggravated identity theft. While increased criminal penalties are a welcomed addition to the arsenal available for use in combating identity theft, we also believe legislation should 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.

Cross-verification

Additionally, we strongly support cross-verification of SSNs through both governmental and private sector systems of records to identify and address inaccuracies. Our experience has shown that cross-verification can combat and limit the spread of false identification and SSN misuse. Further, we believe all law enforcement agencies should be provided the same SSN cross-verification capabilities currently granted to employers. In doing so, the law enforcement community would use data already available to the Federal, State and local governments and the financial sector.

Potentially, the rewards of cross-verification can be great, yet it would not require major expenditures of money or the creation of new offices or agencies. We believe legislation is needed to require mandatory cross-verification of identification data between governmental, financial and commercial holders of records and the SSA on a recurring basis. To offset SSA's cost for providing such services, the Agency could charge a modest fee to commercial and financial entities. The technology to accomplish these data matches and verifications exists now. Coupled with steps already underway by SSA to strengthen the integrity of its enumeration business process, cross-verification, once initiated, would be a critical step in combating the spread of identity fraud.

Let me give you an example of an identity theft case in which cross-verification may have prevented a crime against a Federal government program, saving taxpayers $62,000. A Salt Lake City grandmother learned last year from one of my Denver Field Division agents that her SSN was used to purchase a $146,000 HUD home. This identity theft went undiscovered until the home went into foreclosure because the criminals used this grandmother's SSN, but another name to purchase the home. Had HUD been allowed to verify the accuracy of the borrower's name and SSN with SSA, HUD would have recognized the discrepancy and denied the loan. In this one case alone, the Government would have saved the thousands of program dollars HUD had to pay to foreclose and resell the property. Additionally, this elderly Salt Lake City grandmother would have been spared the time and expense of repairing her credit record.

We believe cross-verification is one of the most important tools the Government and private sector can employ to reduce the instances of identity theft. We understand the important issue of consumer privacy that must be considered by Congress and others before allowing such data integrity matches. However, our ability to prevent these egregious crimes would be enhanced by additional legislation balancing the need for consumer privacy with the need for accurate identifying information.

Conclusion

We always appreciate the invitation to speak with this committee and the very important work you do to help ensure the integrity of SSA programs and the SSN. We are very pleased with the progress Congress and SSA have made in addressing the issue of SSN integrity over the last several years. However, we reiterate our concern that more must be done to ensure that only those individuals authorized to have an SSN receive one and that anyone who fraudulently obtains and misuses an SSN is adequately penalized. As such, we support legislation such as H.R. 2971, the *Social Security Number Privacy and Identity Theft Prevention Act of 2003,* which severely limits the sale, purchase and display of SSNs to the general public. We also believe legislation such as H.R. 1731, the *Identity Theft Penalty Enhancement Act,* is a significant step toward holding accountable individuals who misuse SSNs to

commit egregious crimes. We encourage this Committee and others in Congress to stay firm in your resolve to enact these two bills.

We also ask that Congress consider other measures such as increased cross-verification among Government and private sector entities, Civil Monetary Penalties for SSN misuse and other Social Security-related crimes when criminal prosecution is not available, and stronger penalties for those few SSA employees that betray the public trust by selling SSNs. We will certainly continue our vigilance in addressing these issues and stand ready to do more to enhance the safety and well-being of all Americans. I would now be happy to answer any questions you may have.

Chairman SHAW. Thank you. Ms. Bovbjerg.

STATEMENT OF BARBARA D. BOVBJERG, DIRECTOR OF EDUCATION, WORKFORCE, AND INCOME SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Ms. BOVBJERG. Thank you. Mr. Chairman, Members of the Subcommittee, good morning. I am pleased to be here today once again to discuss issues associated with the use and misuse of the SSN. The wide use of SSNs for non-Social Security purposes causes concern because these numbers, as these gentlemen have noted, 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 the private sector use of the SSN and the protections that companies apply, and then second on public sector uses and protections. My testimony is based on reports we have prepared for you over the last several years, and on ongoing work that focuses more specifically on SSNs in public records.

Let me speak first about the SSN in the private sector. We reported to you in January that companies use the SSN for a variety of purposes, only some of which are restricted by law. Consumer reporting agencies and health care organizations have come to rely on the SSN as an identifier in the course of doing their business, like assessing credit risk or tracking patient care. These businesses often obtain SSNs from the individuals seeking their services, and the re-disclosure of these SSNs to others is restricted by Federal law.

Some businesses that function as information resellers aggregate information, including SSNs, from various sources for resale. They obtain data from public records like bankruptcy proceedings, tax liens and voter registration rolls, and from private compilations like phone books. These businesses then resell this information to a variety of customers. The resellers we contacted told us that 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 re-disclosed. Many also say they truncate the SSN if they provide it at all. Indeed, Federal and State laws have apparently helped to control business display and distribution of personal information.

At the Federal level, the Fair Credit Reporting Act (P.L. 91–508), Gramm-Leach-Bliley, Health Insurance Portability and Accountability Act 1996 (HIPAA) (P.L. 104–191), among others, have controlled use, distribution and display of the SSN in specific indus-

tries. Several States, most notably California, have enacted laws restricting display and use of SSNs, and although limited to a particular State, these restrictions have caused private companies to alter their policies, in some cases nationwide. No law, however, restricts use and display of the SSN in all industries, in all locations, leaving the potential for misuse where protections are inadequate.

Let me now turn to the public sector. As we have reported previously, Federal, States and county government agencies rely extensively on the SSN to maintain records with unique identifiers and to maintain program integrity. 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, and that individual SSNs are still displayed on key public documents such as the Medicare card. We also found that some Federal agencies and many State and county agencies maintain public records that contain SSNs. Public records are documents routinely made available to the public for inspection, such as marriage licenses and property transactions.

When we examined this issue 2 years ago, some public officials told us they were considering making such records available on their Web sites to enhance customer service. We expressed our concern then that such actions would create new opportunities for identity thieves to gather SSNs on a broad scale. We are currently conducting work for the Subcommittee to determine where and how SSNs most regularly appear in public records. Preliminary data suggest that SSNs most frequently appear in court records, land records, uniform commercial code filings, and professional licensing records. We are still analyzing the extent to which these records are available electronically. Interestingly, some of the government agencies we surveyed reported that although SSNs appeared in the public records they retain, they had no specific use for them.

In conclusion, although SSNs are used for many beneficial purposes, the widespread use and retention of them in both the public and private sectors creates opportunities for identity theft. Although both government and private companies have strengthened their protections of personal data and have indeed reduced display of this information in the last several years, these actions are far from uniform and still leave troubling gaps.

Reducing Americans' vulnerability to SSN misuse will require finding the balance between the benefits of SSN use and the costs of improved and more consistent protection. We look forward to continuing to work with this Subcommittee to identify vulnerabilities and to devise adequate and cost-effective protections, and hope that these will serve the millions of Americans with SSNs. Thank you.

[The prepared statement of Ms. Bovbjerg follows:]

Statement of Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues, U.S. General Accounting Office

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss private and public sector entities' use of Social Security numbers (SSNs). Although the Social Security Administration (SSA) originally created SSNs as a means to track workers' earnings and eligibility for Social Security benefits, over time the SSN has come to be used for a myriad of purposes; individuals are frequently asked to supply personal information, including their SSNs, to both public and private sector entities. In addition, individuals'

SSNs can be found in a number of public sources such as records displayed to the public. Given the uniqueness and broad applicability of the SSN, many private and public sector entities rely extensively on the SSN sometimes as a way to accumulate and identify information for their databases, sometimes to comply with federal regulations, and other times for various business purposes. The potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs.

Although Congress has passed a number of laws to protect the security of personal information, the continued use of and reliance on SSNs by both private and public sector entities underscores the importance of determining if appropriate safeguards are in place to protect individuals' private information or if enhanced protection of individuals' personal information is needed. Accordingly, you asked us to talk about how certain types of private and public sector entities obtain SSNs and what protections, if any, exist to govern their use. My remarks today will focus on describing (1) how private sector entities obtain, use, and protect SSNs and (2) public sector uses and protections.

To determine how private sector entities obtain, use, and protect SSNs, we relied on our previous work that looked at how private sector entities obtain and use SSNs and the laws that limit disclosure of this use.[1] To determine how the public sector uses and protects SSNs, we also relied on our previous work that looked at the government's use and protection of SSNs.[2] We are currently conducting a survey of state and local agencies to determine the extent to which SSNs are displayed in public records, the types of records they are displayed in, and how those records are maintained. In addition, we are conducting structured interviews of federal agencies concerning the display of SSNs.

In summary, entities such as information resellers, consumer reporting agencies (CRAs), and health care organizations routinely obtain SSNs from their business clients and from public sources, such as marriage licenses, paternity determinations, and professional licenses. Businesses use SSNs for various purposes, such as to build databases, verify individuals' identities, or match existing records.[3] Given the various types of services these companies offer, we found that all of these entities have come to rely on the SSN as an identifier, which they say helps them determine a person's identity for the purpose of providing the services they offer. However, certain federal laws have helped to limit the disclosures of personal information these private sector entities are allowed to make to their customers. Private sector entities are either subject to the laws directly, given the nature of their business, or indirectly, through their business clients who are subject to these laws. Some states have also enacted laws to restrict the private sector's use of SSNs. However, such restrictions vary by state.

Public sector entities also rely extensively on SSNs. These agencies often obtain SSNs for compliance with federal laws and regulations and for their own agencies' purposes. We found that federal, state, and county government agencies rely extensively on the SSN to manage records, verify benefit eligibility, collect outstanding debt, conduct research and program evaluations, and verify information provided to state drivers' licensing agencies.[4] Given that SSNs are often the identifier of choice among individuals seeking to create false identities, these agencies are taking steps to safeguard SSNs. Yet despite these actions, SSNs appear in records displayed to the public such as documents that record financial transactions or court documents. In our current work for this Subcommittee, we are looking at the storage, display, and protection of SSNs in public records. Our preliminary survey data show that the types of records mostly likely to contain SSNs and be made available to the general public by state government entities are court records, death records, Uniform Commercial Code (UCC) filings, and professional licensing records. In addition, our preliminary results show responding state offices reported over 35 instances where they had no specific use for collecting SSNs. In a previous report, we proposed that Congress consider developing a unified approach to safeguarding SSNs used in all levels of government and particularly those displayed in public records, and we continue to believe that this approach has merit.[5]

---

[1] U.S. General Accounting Office, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information,* GAO–04–11 (Washington D.C.: January 22, 2004).

[2] See 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).

[3] GAO–04–11 (Washington D.C.: January 2004).

[4] GAO–02–352 (Washington D.C.: May 2002).

[5] GAO–02–352 (Washington D.C.: May 2002).

Background

The Social Security Act of 1935 authorized SSA to establish a record-keeping system to help manage the Social Security program, and this 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. SSA generally issues SSNs to most U.S. citizens, and SSNs are also available to noncitizens lawfully admitted to the United States with permission to work. SSA estimates that approximately 277 million individuals currently have SSNs. The SSN has become the identifier of choice for government agencies and private businesses, and thus it is used for a myriad of non-Social Security purposes.

The growth in the use of SSNs is important to individual SSN holders because these numbers, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves.[6] In addition, SSNs are used as breeder information to create additional false identification documents, such as drivers' licenses. Recent statistics collected by federal agencies and CRAs indicate that the incidence of identity theft appears to be growing.[7] The Federal Trade Commission (FTC), the agency responsible for tracking identity theft, reported that consumer fraud and identity theft complaints grew from 404,000 in 2002 to 516,740 in 2003. In 2003, consumers also reported losses from fraud of more than $437 million, up from $343 million in 2002. In addition, identity crime account for over 80 percent of SSN misuse allegations according to the SSA. Also, officials from two of the three national CRAs report an increase in the number of 7-year fraud alerts placed on consumer credit files, which they consider to be reliable indicators of the incidence of identity theft.[8] Law enforcement entities report that identity theft is almost always a component of other crimes, such as bank fraud or credit card fraud, and may be prosecuted under the statutes covering those crimes.

Private Sector entities Routinely Obtain and Use SSNs, and Certain Laws Affect The Disclosure of This Information

Private sector entities such as information resellers, CRAs, and health care organizations routinely obtain and use SSNs.[9] Such entities obtain the SSNs from various public sources and their business clients wishing to use their services. We found that these entities usually use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. Certain federal laws have limited the disclosures private sector entities are allowed to make to their customers, and some states have also enacted laws to restrict the private sector's use of SSNs.

Private Sector Entities Obtain SSNs from Public and Private Sources and Use SSNs for Various Purposes

Private sector entities such as information resellers, CRAs, and health care organizations generally obtain SSNs from various public and private sources and use SSNs to help identify individuals. Of the various public sources available, large information resellers told us they obtain SSNs from various records displayed to the public such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registrations, and professional licenses. Large information resellers said that they try to obtain SSNs from public sources where possible, and to the extent public record information is provided on the Internet, they are likely to obtain it from such sources. Some of these officials also told us that they have people that go to courthouses or other repositories to obtain hard copies of public records. Additionally, they obtain batch files of electronic copies of all public records from some jurisdictions.

Given the varied nature of SSN data found in public records, some reseller officials said they are more likely to rely on receiving SSNs from their business clients

---

[6] United States Sentencing Commission, *Identity Theft Final Alert* (Washington, D.C.: Dec. 15, 1999).

[7] U.S. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing,* GAO–02–363 (Washington, D.C.: Mar. 1, 2002).

[8] A fraud alert is a warning that someone may be using the consumer's personal information to fraudulently obtain credit. When a fraud alert is placed on a consumer's credit card file, it advises credit grantors to conduct additional identity verification before granting credit. The three consumer reporting agencies offers fraud alerts that can vary from 2 to 7 years at the discretion of the individual.

[9] Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information that includes SSNs for informational services. CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Health care organizations generally deliver their services through a coordinated system that includes health care providers and health plans, also referred to as health care insurers.

than they are from obtaining SSNs from public records. These entities obtain SSNs from their business clients, who provide SSNs in order to obtain a reseller's services or products, such as background checks, employee screening, determining criminal histories, or searching for individuals. Large information resellers also obtain SSN information from private sources. In many cases such information was obtained through review of data where a customer has voluntarily supplied information resellers with information about himself or herself. In addition, large reseller officials said they also use their clients' records in instances where the client has provided them with information.

We also found that Internet-based resellers rely extensively on public sources and records displayed to the public. These resellers listed on their Web sites public information sources, such as newspapers, and various kinds of public record sources at the county, state, and national levels. During our investigation, we determined that once Internet-based resellers obtained an individual's SSN they relied on information in public records to help verify the individual's identity and amass information around the individual's SSN.

Like information resellers, CRAs also obtain SSNs from public and private sources as well as from their customers or the businesses that furnish data to them. CRA officials said that they obtain SSNs from public sources, such as bankruptcy records, a fact that is especially important in terms of determining that the correct individual has declared bankruptcy. CRA officials also told us that they obtain SSNs from other information resellers, especially those that specialize in obtaining information from public records. However, SSNs are more likely to be obtained from businesses that subscribe to their services, such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies. Individuals provide these businesses with their SSNs for reasons such as applying for credit, and these businesses voluntarily report consumers' charge and payment transactions, accompanied by SSNs, to CRAs.

We found that health care organizations were less likely to rely on public sources for SSN data. Health care organizations obtain SSNs from individuals themselves and from companies that offer health care plans. For example, subscribers or policyholders provide health care plans with their SSNs through their company or employer group when they enroll in health care plans. In addition to health care plans, health care organizations include health care providers, such as hospitals. Such entities often collect SSNs as part of the process of obtaining information on insured people. However, health care officials said that, particularly with hospitals, the medical record number rather than the SSN is the primary identifier.

Information resellers, CRAs, and health care organization officials all said that they use SSNs to verify an individual's identity. Most of the officials we spoke to said that the SSN is the single most important identifier available, mainly because it is truly unique to an individual, unlike an individual's name and address, which can often change over an individual's lifetime. Large information resellers said that they generally use the SSN as an identity verification tool. Some of these entities have incorporated SSNs into their information technology, while others have incorporated SSNs into their clients' databases used for identity verification. For example, one large information reseller that specializes in information technology solutions has developed a customer verification data model that aids financial institutions in their compliance with some federal laws regarding "knowing your customer." We also found that Internet-based information resellers use the SSN as a factor in determining an individual's identity. We found these types of resellers to be more dependent on SSNs than the large information resellers, primarily because their focus is more related to providing investigative or background-type services to anyone willing to pay a fee. Most of the large information resellers officials we spoke to said that although they obtain the SSN from their business clients, the information they provide back to their customers rarely contains the SSN. Almost all of the officials we spoke to said that they provide their clients with a truncated SSN, an example of which would be xxx–xx–6789.

CRAs use SSNs as the primary identifier of individuals, which enables them to match the information they receive from their business clients with the information stored in their databases on individuals.[10] Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN

[10] We found that CRAs and information resellers can sometimes be the same entity, a fact that blurs the distinction between the two types of businesses but does not affect the use of SSNs by these entities. Five of the six large information resellers we spoke to said they were also CRAs. Some CRA officials said that information reselling constituted as much as 40 percent of CRAs' business.

is the primary factor that ensures that incoming data is matched correctly with an individual's information on file. For example, CRA officials said they use several factors to match incoming data with existing data, such as name, address, and financial account information. If all of the incoming data, except the SSN, match with existing data, then the SSN will determine the correct person's credit file. Given that people move, get married, and open new financial accounts, these officials said that it is hard to distinguish among individuals. Because the SSN is the one piece of information that remains constant, they said that it is the primary identifier that they use to match data.

Health care organizations also use the SSN to help verify the identity of individuals. These organizations use SSNs, along with other information, such as name, address, and date of birth, as a factor in determining a member's identity. Health care officials said that health care plans, in particular, use the SSN as the primary identifier of an individual, and it often becomes the customer's insurance number. Health care officials said that they use SSNs for identification purposes, such as linking an individual's name to an SSN to determine if premium payments have been made. They also use the SSN as an online services identifier, as an alternative policy identifier, and for phone-in identity verification. Health care organizations also use SSNs to tie family members together where family coverage is used,[11] to coordinate member benefits, and as a cross-check for pharmacy transactions. Health care industry association officials also said that SSNs are used for claims processing, especially with regard to Medicare. According to these officials, under some Medicare programs, SSNs are how Medicare identifies benefits provided to an individual.

Certain Laws Limit the Private Sectors' Disclosure of Personal Information That Includes SSNs

Certain federal and state laws have placed restrictions on certain private sector entities use and disclosure of consumers' personal information that includes SSNs. Such laws include the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Drivers Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA). As shown in table 1, the laws either restrict the disclosures that entities such as information resellers, CRAs, and health care organizations are allowed to make to specific purposes or restrict whom they are allowed to give the information to. Moreover, as shown in table 1, these laws focus on limiting or restricting access to certain personal information and are not specifically focused on information resellers. See appendix I for more information on these laws.

Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information

Federal Laws	Restrictions
Fair Credit Reporting Act	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to non-affiliated third parties.
Drivers Privacy Protection Act	Prohibits obtaining and disclosing SSNs and other personal information from a motor vehicle record except as expressly permitted under the law.
Health Insurance Portability and Accountability Act	Protects the privacy of health information that identifies an individual (including by SSNs) and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis.

We reviewed selected legislative documents of 18 states and found that at least 6 states have enacted their own legislation to restrict either the display or use of SSNs by the private sector.[12] Notably, in 2001, California enacted Senate Bill (SB)

[11] During the enrollment process, subscribers have a number of options, one of which is decided whether they would like single or family coverage. In cases where family coverage is chosen, the SSN is the key piece of information generally allowing the family members to be linked.

[12] On the basis of our interviews with private sector businesses and organizations, contacts with some state offices of attorney general, and identified state laws and legislative initiatives

Continued

168, restricting private sector use of SSNs. Specifically, this law generally prohibits companies and persons from certain uses such as, posting or publicly displaying SSNs and printing SSNs on cards required to access the company's products or services. Furthermore, in 2002, shortly after the enactment of SB 168, California's Office of Privacy Protection published recommended practices for protecting the confidentiality of SSNs. These practices were to serve as guidelines to assist private and public sector organizations in handling SSNs.

Similar to California's law, Missouri's law (2003 Mo. SB 61), which is not effective until July 1, 2006, bars companies from requiring individuals to transmit SSNs over the Internet without certain safety measures, such as encryption and passwords. However, while SB 61 prohibits a person or private entity from publicly posting or displaying an individual's SSN "in any manner," unlike California's law, it does not specifically prohibit printing the SSN on cards required to gain access to products or services. In addition, Arizona's law (2003 Ariz. Sess. Laws 137), effective January 1, 2005, restricts the use of SSNs in ways very similar to California's law. However, in addition to the private sector restrictions, it adds certain restrictions for state agencies and political subdivisions.[13] For example, state agencies and political subdivisions are prohibited from printing an individual's SSN on cards and certain mailings to the individual. Last, Texas prohibits the display of SSNs on all cards, while Georgia and Utah's laws are directed at health insurers and, therefore, pertain primarily to insurance identification cards.[14] None of these three laws contain the provisions mentioned above relating to Internet safety measures and mailing restrictions. Table 2 lists states that have enacted legislation and related provisions.

Table 2: Provisions Included in Enacted Legislation Reviewed

Provision	States Where Provision or Restriction Enacted
Specifically prohibits display on cards	AZ, CA, GA, TX, UT
Requires Internet safety measures	AZ, CA, MO
Restricts mailing of SSNs	AZ, CA

Source: GAO analysis.

Public Sector Entities Also Use SSNs and Some Agencies Limit Their Use and Display Even Though SSNs are Displayed in Some Public Records

Agencies at all levels of government frequently obtain and use SSNs. A number of federal laws require government agencies to obtain SSNs, and these agencies use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and do research and evaluation. Given the potential for misuse, some government agencies are taking steps to limit their use and display of SSNs and prevent the proliferation of false identities. However, given the open nature of certain government records, SSNs appear in some records displayed to the public. Our ongoing work is looking at the storage, display, and protection of SSNs in records displayed to the public.

Public Sector Entities Are Required by Laws and Regulations to Obtain SSNs for Various Purposes

Government agencies obtain SSNs because a number of federal laws and regulations require certain programs and federally funded activities to use the SSN for administrative purposes.[15] Such laws and regulations require the use of the SSN as an individual's identifier to facilitate automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both. For example, the Internal Revenue Code and regulations, which govern the administration of the federal personal income tax program, require that individuals' SSNs serve as taxpayer identification numbers.[16] A number of other federal laws require

---

related to the use of SSNs, we did a legislative review of 18 states that were identified as having laws or proposed laws governing SSN use. In the 18 states we researched, we reviewed more than 40 legislative documents, including relevant laws, proposed laws, legislative summaries, and other related documents, such as state regulations, executive orders, and referendums.

[13] Political subdivisions would include counties, cities, and towns.

[14] Georgia's law (O.C.G.A. § 33–24–57.1(f)) and Utah's law (Utah Code Ann. § 31–22–634) are both effective July 1, 2004. However, Utah's law provides certain extensions until March 1, 2005. Texas' law (2003 Tex. Gen. Laws 341) is effective March 1, 2005.

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

[16] This means that employers and others making payments to individuals must include the individuals' SSNs in reporting to IRS many of these payments. In addition, the Code and regula-

program administrators to use SSNs in determining applicants' eligibility for federally funded benefits. The Social Security Act requires individuals to provide their SSNs in order to receive benefits under the SSI, Food Stamp, Temporary Assistance for Needy Families, and Medicaid programs.[17] In addition, the Commercial Motor Vehicle Safety Act of 1986 requires the use of SSNs to identify individuals and established the Commercial Driver's License Information System, a nationwide database where states may use individuals' SSNs to search the database for other state-issued licenses commercial drivers may hold.[18] Federal law also requires the use of SSNs in state child support programs to help states locate noncustodial parents, establish and enforce support orders, and recoup state welfare payments from parents.[19] The law also allows states to record SSNs on many other state documents, such as professional, occupational, and marriage licenses; divorce decrees; paternity determinations; and death certificates, and to make SSNs associated with these documents available for state child support agencies to use in locating and obtaining child support payments from noncustodial parents.

Government agencies use SSNs for a variety of reasons. We found that most of these agencies use SSNs to administer their programs, such as to identify, retrieve, and update their records. In addition, many agencies also use SSNs to share information with other entities to bolster the integrity of the programs they administer. As unique identifiers, SSNs help ensure that the agency is obtaining or matching information on the correct person.

Government agencies also share information containing SSNs for the purpose of verifying an applicant's eligibility for services or benefits, such as matching records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments. SSNs are also used to ensure program integrity. Agencies use SSNs to collect delinquent debts and even share information for this purpose. In addition, SSNs are used for statistics, research, and evaluation. Agencies responsible for collecting and maintaining data for statistical programs that are required by statute, make use of SSNs. In some cases, these data are compiled using information provided for another purpose. For example, the Bureau of the Census prepares annual population estimates for states and counties using individual income tax return data linked over time by SSN to determine immigration rates between localities.[20] SSNs also provide government agencies and others with an effective mechanism for linking data on program participation with data from other sources to help evaluate the outcomes or effectiveness of government programs. In some cases, records containing SSNs are sometimes matched across multiple agency or program databases.[21]

Finally, government agencies use employees' SSNs to fulfill some of their responsibilities as employers. For example, personnel departments of these agencies use SSNs to help them maintain internal records and provide employee benefits. In addition, employers are required by law to use employees' SSNs when reporting wages. Wages are reported to SSA, and the agency uses this information to update earnings records it maintains for each individual. The Internal Revenue Service (IRS) also uses SSNs to match the employer wage reports with amounts individuals report on personal income tax returns. Federal law also requires that states maintain employers' reports of newly hired employees, identified by SSNs. States must forward this information to a national database that is used by state child support agencies to locate parents who are delinquent in child support payments.

---

tions require individuals filing personal income tax returns to include their SSNs as their taxpayer identification number, the SSNs of people whom they claim as dependents, and the SSNs of spouses to whom they paid alimony.

[17] Applicants give program administrators information on their income and resources, and program administrators use applicants' SSNs to match records with those of other organizations.

[18] States may also use SSNs to search another database, the National Driver's Registry, to determine whether an applicant's license has been cancelled, suspended, or revoked by another state. In these situations, the states use SSNs to limit the possibility of inappropriately licensing applicants.

[19] The law requires states to maintain records that include (1) SSNs for individuals who owe or are owed support for cases in which the state has ordered child support payments to be made, the state is providing support, or both, and (2) employers' records of new hires identified by SSN.

[20] The Bureau of the Census is authorized by statute to collect a variety of information, and the Bureau is also prohibited from making it available, except in certain circumstances.

[21] The statistical and research communities refer to the process of matching records containing SSNs for statistical or research purposes as "record linkage." See U.S. General Accounting Office, *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information*, GAO–01–126SP (Washington, D.C.: Apr. 2001).

Government Agencies Are Taking Steps to Limit the Use and Display of SSNs

Despite the widespread use of SSNs at all levels of government, not all agencies use SSNs. We found that some agencies do not obtain, receive, or use SSNs of program participants, service recipients, or individual embers of the public.[22] Moreover, not all agencies use the SSN as their primary identification number for record-keeping purposes. These agencies maintain an alternative number that is used in addition to or in lieu of SSNs for certain activities.

Some agencies are also taking steps to limit SSNs displayed on documents that may be viewed by others who may not have a need to view this personal information. For example, the Social Security Administration has truncated individuals' SSNs that appear on the approximately 120 million benefits statements it mails each year. Some states have also passed laws prohibiting the use of SSNs as a student identification number. Almost all states have modified their policies on placing SSNs on state drivers' licenses.

At the federal level, SSA has taken steps in its enumeration process and verification service to help prevent SSNs from being used to proliferate false identities. SSA has formed a task force to address weaknesses in its enumeration process and has (1) increased document verifications and developed new initiatives to prevent the inappropriate assignment of SSNs to noncitizens, and (2) undertaken initiatives to shift the burden of processing noncitizen applications from its field offices. [23] SSA also helps prevent the proliferation of false identities through its verification service, which allows state driver licensing agencies to verify the SSN, name, and date of birth of customers with SSA's master file of Social Security records.[24] Finally, SSA has also acted to correct deficiencies in its information systems' internal controls. These changes were made in response to the findings of an independent audit that found that SSA's systems were exposed to both internal and external intrusion, increasing the possibility that sensitive information such as SSNs could be subject to unauthorized access, modification, and disclosure, as well as the risk of fraud.

Public Records Can Also Be a Source of SSNs

Given the open nature of certain government records, SSNs appear in these records for a number of reasons. For example, SSNs may already be a part of a document that is submitted to a recorder for official preservation, such as veterans' discharge papers. Documents that record financial transactions, such as tax liens and property settlements, also contain SSNs to help identify the correct individual. As previously stated, government officials are required by law to collect SSNs in numerous instances. Moreover, some state laws allow government entities to collect SSNs on voter registries to help avoid duplicate registrations.

Courts at all three levels of government also collect and maintain records that are routinely made available to the public. Court records overall are presumed to be public. However, each court may have its own rules or practices governing the release of information. SSNs appear in court documents for a variety of reasons. In many cases, SSNs are already a part of documents that are submitted by attorneys or individuals. These documents could be submitted as part of the evidence for a proceeding or could be included as part of a petition for an action, such as a judgment or a divorce. In other cases, courts include SSNs on documents they and other government officials create, such as criminal summonses, arrest warrants, and judgments, to increase the likelihood that the correct individual is affected (i.e., to avoid arresting the wrong John Smith). Again, in some cases, federal law requires that SSNs be placed in certain records that courts maintain, such as child support orders.

In our prior report, we looked at the extent and nature of federal, state, and county governments' use of SSNs when they are contained in public records, and the options available to better safeguard SSNs that are found in these public records.[25] Our findings led us to suggest that Congress consider addressing SSN security and display issues in state and local government and in public records, including those maintained by the judicial branch of government at all levels. We proposed that

---

[22] GAO–02–352 (Washington D.C.: May 2002).

[23] See U.S. General Accounting Office, *Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens but Some Weakness Remain,* GAO–04–12 (Washington D.C.: October 15, 2003). See U.S. General Accounting Office, *Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification*, GAO–03–920 (Washington D.C.: September 15, 2003).

[24] GAO–03–920 (Washington D.C.: September 2003).

[25] GAO–02–352 (Washington D.C.: May 2002)

Congress convene a representative group of officials from all levels of government to develop a unified approach to safeguard SSNs used in all levels of government and particularly those displayed in public records.

At the request of this subcommittee, GAO was asked what types of public records SSNs are stored in, how are those records maintained, and to what extent SSNs are displayed inside those records. To do this work, we are surveying over 2,500 officials in state and local government agencies, including officials in all 50 states and the District of Columbia, and are conducting structured interviews of federal agencies. Our preliminary survey data show that the types of records most likely to contain SSNs and be made available to the general public by state government entities are court records, death records, UCC filings, and professional licensing records. At the local level, court records and land records are those most often cited as containing SSNs and being available to the general public. Preliminary data analysis indicates that identity verification is the most frequently given reason by both state and local respondents for collecting or using SSNs that are in records available to the public. Data matching and complying with state laws or regulations are also frequently cited as reasons for the collection or use of the SSN. However, responding state offices reported over 35 instances where they had no specific use for collecting SSNs.

Conclusions

Public and private entities use SSNs for many legitimate and publicly beneficial purposes. However, the more frequently SSNs are obtained and used, the more likely they are to be misused. As we continue to learn more about the entities that obtain SSNs and the purposes for which they obtain them, Congress and state legislatures will be able to determine if there are ways to limit access to this valuable piece of information and prevent it from being misused. However, restrictions on access or use may make it more difficult for businesses and government agencies to verify an individual's identity. Accordingly, policy makers will have to balance restrictions on the use of SSNs on the one hand with legitimate needs for the use of SSNs on the other.

Although individuals may choose to provide their SSNs to public and private sector entities to obtain their services, individuals are often required to have their SSNs in records that may ultimately be displayed to the public. Such public display of personal information can create opportunities for identity crimes. Safeguarding SSNs in records displayed to the public offers an additional challenge because of the inherent tension between the nature of public records, that is, the need for transparency in government activities, and the need to protect individuals' privacy. For this reason, in prior work, we recommended that Congress convene a representative group of officials to develop a unified approach to safeguard SSNs used in all levels of government and particularly those displayed in public records. We continue to believe that this would be a useful step toward preventing SSN misuse while acknowledging the needs of various levels of government.

At this subcommittee's request, we are continuing work on SSNs and their presence in public records and look forward to supporting continuing congressional consideration of these important policy issues. That concludes my testimony, and I would be pleased to respond to any questions the subcommittee has.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director; Tamara Cross, Assistant Director; or Alicia Cackley, Assistant Director of Education, Workforce, and Income Security Issues at (202) 512–7215. Individuals making key contributions to this testimony include Melinda Bowman, Raun Lazier, Joel Marus, and Caroline Sallee.

Appendix I: Federal Laws Affecting Information Resellers, CRAs, and Health Care Organizations:

Gramm-Leach-Bliley Act (GLBA):

GLBA requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some, but not all, sharing of their nonpublic personal information. Financial institutions are permitted to disclose consumers' nonpublic personal information without offering them an opt-out right in the following circumstances:

- to effect a transaction requested by the consumer in connection with a financial product or service requested by the consumer; maintaining or servicing the consumer's account with the financial institution or another entity as part of a pri-

vate label credit card program or other extension of credit; or a proposed or actual securitization, secondary market sale, or similar transaction;
- with the consent or at the direction of the consumer;
- to protect the confidentiality or security of the consumer's records; to prevent actual or potential fraud, for required institutional risk control or for resolving customer disputes or inquiries, to persons holding a legal or beneficial interest relating to the consumer, or to the consumer's fiduciary;
- to provide information to insurance rate advisory organizations, guaranty funds or agencies, rating agencies, industry standards agencies, and the institution's attorneys, accountants, and auditors;
- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;
- to a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency;
- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business if the disclosure concerns solely consumers of such business;
- to comply with federal, state, or local laws; an investigation or subpoena; or to respond to judicial process or government regulatory authorities.

Financial institutions are required by GLBA to disclose to consumers at the initiation of a customer relationship, and annually thereafter, their privacy policies, including their policies with respect to sharing information with affiliates and nonaffiliated third parties.

Provisions under GLBA place limitations on financial institutions disclosure of customer data, thus affecting some CRAs and information resellers. We found that some CRAs consider themselves to be financial institutions under GLBA.[26] These entities are therefore directly governed by GLBA's restrictions on disclosing nonpublic personal information to non-affiliated third parties. We also found that some of the information resellers we spoke to did not consider their companies to be financial institutions under GLBA. However, because they have financial institutions as their business clients, they complied with GLBA's provisions in order to better serve their clients and ensure that their clients are in accordance with GLBA. For example, if information resellers received information from financial institutions, they could resell the information only to the extent that they were consistent with the privacy policy of the originating financial institution.

Information resellers and CRAs also said that they protect the use of non-public personal information and do not provide such information to individuals or unauthorized third parties. In addition to imposing obligations with respect to the disclosures of personal information, GLBA also requires federal agencies responsible for financial institutions to adopt appropriate standards for financial institutions relating to safeguarding customer records and information. Information resellers and CRA officials said that they adhere to GLBA's standards in order to secure financial institutions' information.

Drivers Privacy Protection Act (DPPA):

The DPPA specifies a list of exceptions when personal information contained in a state motor vehicle record may be obtained and used (18 U.S.C. § 2721(b)). These permissible uses include:
for use by any government agency in carrying out its functions;
for use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; motor vehicle market research activities, including survey research;
for use in the normal course of business by a legitimate business, but only to verify the accuracy of personal information submitted by the individual to the business and, if such information is not correct, to obtain the correct information but only for purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual;

- for use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency;
- for use in research activities;

[26] Under GLBA, the term financial institution is defined as "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956," which goes into more detail about what are "activities that are financial in nature." These generally include banking, insurance, and investment industries.

- for use by any insurer or insurance support organization in connection with claims investigation activities;
- for use in providing notice to the owners of towed or impounded vehicles;
- for use by a private investigative agency for any purpose permitted under the DPPA;
- for use by an employer or its agent or insurer to obtain information relating to the holder of a commercial driver's license;
- for use in connection with the operation of private toll transportation facilities;
- for any other use, if the state has obtained the express consent of the person to whom a request for personal information pertains;
- for bulk distribution of surveys, marketing, or solicitations, if the state has obtained the express consent of the person to whom such personal information pertains;
- for use by any requester, if the requester demonstrates that it has obtained the written consent of the individual to whom the information pertains;
- for any other use specifically authorized under a state law, if such use is related to the operation of a motor vehicle or public safety.

As a result of DPPA, information resellers said they were restricted in their ability to obtain SSNs and other driver license information from state motor vehicle offices unless they were doing so for a permissible purpose under the law. These officials also said that information obtained from a consumer's motor vehicle record has to be in compliance with DPPA's permissible purposes, thereby restricting their ability to resell motor vehicle information to individuals or entities not allowed to receive such information under the law. Furthermore, because DPPA restricts state motor vehicle offices' ability to disclose driver license information, which includes SSN data, information resellers said they no longer try to obtain SSNs from state motor vehicle offices, except for permissible purposes.

Health Insurance Portability and Accountability Act (HIPAA):

The HIPAA privacy rule also defines some rights and obligations for both covered entities and individual patients and health plan members. Some of the highlights are:

- Individuals must give specific authorization before health care providers can use or disclose protected information in most nonroutine circumstances, such as releasing information to an employer or for use in marketing activities.
- Covered entities will need to provide individuals with written notice of their privacy practices and patients' privacy rights. The notice will contain information that could be useful to individuals choosing a health plan, doctor, or other service provided. Patients will be generally asked to sign or otherwise acknowledge receipt of the privacy notice.

Covered entities must obtain an individual's specific authorization before sending them marketing materials.

Health care organizations, including health care providers and health plan insurers, are subject to HIPAA's requirements. In addition to providing individuals with privacy practices and notices, health care organizations are also restricted from disclosing a patient's health information without the patient's consent, except for purposes of treatment, payment, or other health care operations. Information resellers and CRAs did not consider themselves to be "covered entities" under HIPAA, although some information resellers said that their customers are considered to be business associates under HIPAA. As a result, they said they are obligated to operate under HIPAA's standards for privacy protection, and therefore could not resell medical information without having made sure HIPAA's privacy standards were met.

Fair Credit Reporting Act (FCRA);

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report (15 USC 1681b). These permissible purposes are:

- as ordered by a court or a federal grand jury subpoena;
- as instructed by the consumer in writing;
- for the extension of credit as a result of an application from a consumer or the review or collection of a consumer's account;
- for employment purposes, including hiring and promotion decisions, where the consumer has given written permission;
- for the underwriting of insurance as a result of an application from a consumer;

- when there is a legitimate business need, in connection with a business transaction that is initiated by the consumer;
- to review a consumer's account to determine whether the consumer continues to meet the terms of the account;
- to determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status;
- for use by a potential investor or servicer or current insurer in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation; and
- for use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof.

Under FCRA, Congress has limited the use of consumer reports[27] to protect consumers' privacy and limits access to credit data to those who have a legally permissible purpose for using the data, such as the extension of credit, employment purposes, or underwriting insurance. However, these limits are not specific to SSNs. All of the CRAs that we spoke to said that they are considered consumer reporting agencies under FCRA. In addition, some of the information resellers we spoke to who handle or maintain consumer reports are classified as CRAs under FCRA. Both CRAs and information resellers said that as a result of FCRAs restrictions they are limited to providing credit data to their customers that have a permissible purpose under FCRA. Consequently, they are restricted by law from providing such information to the general public.

Chairman SHAW. Thank you very much. Mr. Maxwell.

STATEMENT OF LAWRENCE E. MAXWELL, ASSISTANT CHIEF INSPECTOR, INVESTIGATIONS AND SECURITY, UNITED STATES POSTAL INSPECTION SERVICE

Mr. MAXWELL. Thank you, Mr. Chairman and Members of the Committee. I really appreciate your having us here today and your focus on this very important issue. As a way of background, myself and others in the Postal Inspection Service have reviewed the provisions in the new legislation, and we are very enthusiastic. I have had 27 years in law enforcement, most of which has been in mail fraud investigations, and I truly welcome a lot of the provisions here, particularly the preventive and the enhanced penalty methods.

One of the things, for those who aren't familiar with the Postal Inspection Service, we date ourselves as the oldest Federal law enforcement agency, going back to Ben Franklin and the statute, mail fraud, was enacted in 1870s, and it makes it the oldest and the first consumer protection law on the books, arguably the best. I still think it is the best. One may ask, well, how did somebody who is in the hand delivery business get propelled into identity theft in the electronic communications age? Well, I will bring you up to that in a second how the tie-in is.

The Postal Inspection Service covers Maine to Guam. There is roughly 2,000 of us, making us a very small agency. Approximately 300 inspectors are devoted to mail fraud, and we pride ourselves primarily on consumer fraud. As stated earlier, identity theft remains a vexing problem, insidious in nature, and clearly a predator on those unsuspecting. It totally devastates your life. It takes months, years to put it back together again afterward. So, clearly

[27] The FTC has determined that certain types of information, including SSNs, do not constitute as consumer report under FCRA because they are not factors in determining credit eligibility.

it is something that we have been living with for some time, and we are aggressively pursuing and should.

From our experience, mail itself, based on an FTC study recently, only represents about 4 percent of identity crimes; 4 percent, that is, in stolen mail, information obtained from mail that has been stolen. We used to think it was worse. In fact, a lot of our prevention messages cued in on that, to protect your mail from theft. However, we have since learned that really it comes more from the after fact, the use of mails to file applications, credit information and so forth. However, that doesn't stop us from taking assertive actions on mail theft programs.

In the mail fraud area, primarily what we have seen in both arrest statistics, a combination of arrests from mail theft and fraud, totals 3,000 of our 10,000 arrests each year. As you can conclude, that is a very substantial number of our activities in the criminal area. What we have found as a strategy, and that is really what we are here to address today, outreaching is extremely important. Ourselves and the FTC have been partners for some time. We have had a formal memorandum of understanding. We share data, fraud data, and we do a number of prevention and educational campaigns together.

Clearly the events of 2 years ago propelled all of us in the law enforcement community to work better together, and although the Postal Inspection Service only has 200 statutes which it has to worry about, still we find a lot of the overlaps in areas where we can fill in the gaps and help out. For example, we are on a number of financial crimes investigative task forces around the country. We are also part of the National Joint Terrorism Task Force and the Joint Terrorism Task Force primarily focusing on mail information and financial information, again relating back to what we are talking about today.

Finally, one of the major initiatives is with the credit card industry itself with a group called the Financial Crimes Task Force. We have been together since the middle of the nineties, and that is the industry involved in credit cards and the Postal Service inspectors dealing on ways to share best practices and enforcement. That has worked out very well. In fact, we have come out with a publication which I have made available to all of you called Fighting Identity Theft, and in there it actually highlights the use of the importance of SSNs by minimizing the use of SSNs on page nine, if you care to look at that at some time.

Another portion of our focus would be on deterrence. Of course, as a law enforcement officer I would be remiss not saying how important it is to arrest those responsible for committing crimes. Deterrence serves a big purpose particularly when it is a high-profile case. Last year, for example, there was a case involving Carlos Lomax in Pittsburgh. He stole the identity of none other than Will Smith, the actor, obviously a prominent name, and he was doing quite well. In his guilty plea, and his cooperation, he agreed to film a video which we have available which he discusses some of the techniques he uses in identity theft.

Finally, the strategy I most favor is prevention. We have a number of prevention campaigns, and to just spin the old adage, crime does not pay, we have used it to pay. We have had a couple of U.S.

attorneys in the U.S. Department of Justice support us in putting asset forfeiture money and fine money into a fund called the Consumer Protection Fund. We have used that fund to conduct massive educational campaigns, joint campaigns.

To my left, your right, is a poster where we had a partnership with Showtime where they made two feature films on postal inspector cases. For years we were known as "the silent service," and we are finding now in prevention and getting the word out we can't be silent. They made a movie in the second of a series on identity theft specifically to dramatize the issue. On the right is a poster from the identity theft campaign which we conducted last September. In that campaign we had a massive outreach of mailings. We produced a mini-drama which is on digital video disk, which I have also made available highlights how identity theft occurs and how it is reported and how it is enforced. Then, at the very end, and, I think, in dramatic fashion, it gives you tips on what to do to prevent identity theft. We also did a saturation mailing and produced this brochure, which I think is very valuable. In closing, I would just reiterate the importance of that strategy using deterrence and prevention and primarily education, because fraud is a crime where people can prevent it. They don't have to participate if they know what to do. Thank you for your time.

[The prepared statement of Mr. Maxwell follows:]

Statement of Lawrence E. Maxwell, Assistant Chief Inspector, Investigations and Security, United States Postal Inspection Service

Good morning, Mr. Chairman, members of the subcommittee. On behalf of the United States Postal Inspection Service, thank you for holding this hearing and giving me the opportunity to discuss the subject of identity crimes and the significant role Postal Inspectors play in combating it.

I'm Lawrence E. Maxwell, Assistant Chief Inspector, Investigations and Security, for the U.S. Postal Inspection Service.

Role of the Postal Inspection Service

The U.S. Postal Service delivers more than 200 billion pieces of mail a year, containing money, messages, and merchandise, to 138 million addresses at some of the most affordable postage rates in the world. U. S. Postal Inspectors are mandated to safeguard all of it—including the people who move it and the customers who use it.

Congress empowered the Postal Service "to investigate postal offenses and civil matters relating to the Postal Service." Through its security and enforcement functions, the Postal Inspection Service provides assurance to American businesses for the safe exchange of funds and securities through the U.S. Mail; to postal customers of the "sanctity of the seal" in transmitting correspondence and messages; and to postal employees of a safe work environment.

As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public.

Postal Inspectors work closely with U.S. Attorneys, other law enforcement agencies, and local prosecutors to investigate postal cases and prepare them for court. There are approximately 1,900 Postal Inspectors stationed throughout the United States who enforce roughly 200 federal laws covering investigations of crimes that adversely affect or fraudulently use the U.S. mail and postal system.

Last year, U.S. Postal Inspectors made more than 11,000 arrests. Of those, over 6,000 were related to mail theft. One-third of those involved identity theft. In the first eight months of our 2004 fiscal year, we exceeded the number of identity theft arrests made throughout all of last year.

What is Identity Theft?

Identity theft occurs when a thief steals key pieces of someone's identifying information, such as name, date of birth, and Social Security number, and uses the infor-

mation to fraudulently apply for credit or to take over a victim's credit or bank accounts. Identity theft occurs in a variety of ways. Those that involve the use of the mail receive swift and aggressive action by Postal Inspectors. We ensure that consumers are being protected. In addition, we work with the mailing industry to develop best practices on how best to design mailing pieces to prevent identity theft. Our collaboration with the mailing industry is another example of how the industry as a whole is serious about the issue and working to stay ontop of it for the benefit of consumers. Mail is important to consumers who receive itand to the businesses that send it.

Tactics Used by Identity Thieves

In the past, pre-screened credit offers were more vulnerable to identity theft because they simply required the customer to sign the solicitation and return it. But now credit card companies have begun automatically discarding applications when they are returned with a change of address. Actions by the industry have made these mailings less attractive to would-be identity thieves.

Identity theft is continuing to evolve with the expansion of the Internet and other electronic means. The mail is no more vulnerable than other sources of personal information, such as corporate and government records and computer databases. Financial institutions have implemented many safeguards to reduce the likelihood that personal financial information found within the mail can be stolen. The Postal Service is continually working to improve the security of the mail, and Postal Inspectors are making great strides in apprehending those who would use the mail to further their crimes.

Identity fraud is digging deep into consumer's pockets—millions of dollars were lost in the past year by financial institutions and victims across the country. Thieves use a variety of tactics to drain a victim's finances, including stealing mail; posing as a loan officer and ordering a victim's credit report (which lists account numbers); "shoulder surfing" at the ATM or phone booth to get a victim's PIN code; and "dumpster diving" in trash bins looking for credit applications, canceled checks or other bank records.

Until a few years ago, a thief could submit an address change to divert customers' mail without their knowledge. Usually, redirected mail is sent to a commercial mail receiving agency in an attempt to insure the perpetrator's anonymity. In response to recommendations by the Chief Postal Inspector, a prevention measure that addresses fraudulent change-of-address orders was adopted by the U.S. Postal Service. Post Offices now send a "Move Validation Letter" to both the old and new address when a change is filed. The letter instructs an individual to call an "800" number if a change was not filed. This simple measure has virtually eliminated false changes-of-address submitted to the Postal Service as an avenue for committing identity theft.

Impact on Victims

One of the most insidious aspects of identity theft is the length of time the scheme is carried out before it comes to anyone's attention. It may be months before a victim realizes they've been targeted. It's not until a consumer gets turned down for credit, a car loan, or a mortgage on a dream house because of a bad credit rating—knowing they've paid their bills—do they begin to realize what has taken place. Most victims do not learn about the theft of their identity until 14 months after it has occurred. More than half of the victims we interviewed report their cases have been open, on average, 44 months. They also reported that, as victims, they spent, on average, 175 hours actively trying to restore their credit and "to clear their good name."

Identity theft can do more than ruin a person's credit; it can cause more serious damage. Identity theft hurts a victim in two ways. First a victim must deal with the obvious financial issues. Second, a victim must contend with privacy and practical issues such as overcoming a credit history that isn't theirs. The problem doesn't go away with a few phone calls—it can stick with a victim for a long time. That's why it's such a serious issue. Victims run the gamut of society, they're wealthy, they're poor, they're old, and they're young. Anyone can become a victim.

In a recent Postal Inspection Service investigation based in Chicago, Illinois, the destructive activities of an identity thief resulted in the loss of thousands of dollars and the death of a primary victim. The scheme began in July 1999 when the identity thief began dating the estranged wife of a Chicago resident. Without the victim's knowledge, the wife assisted the thief in stealing her former spouse's identity by providing the thief with the spouse's personal information.

In January 2000, the spouse filed a complaint with the Chicago Police Department after realizing that he was a victim of identity theft with losses over $200,000.

In February, the spouse received a package from the thief wrapped as a FedEx delivery. After holding the package for several days, the spouse received a voice mail message from the thief indicating the package was a gift. As he sat in his living room, he opened the package, which exploded, killing him instantly.

Last year a colleague of mine learned about identity theft the hard way. His bank called and asked if he had authorized a $4,500 cash advance on his credit card in Miami, Florida that day.

He was stunned. The bank had called only hours after the withdrawal was made, following an alert initiated because certain account parameters indicated something might be wrong. Luckily for him, the bank simply asked that he sign an affidavit that he had not been in Miami and hadn't made the withdrawal. He wasn't held liable for the money. And he never found out what ID the thief had used to get access to his account.

Unfortunately, my colleague's ordeal wasn't over. He received a call a few months later from a cellular phone company, asking if he'd opened an account with them in Miami. Someone had racked up $1,800 in calling charges under his name and then disappeared. Once again, he signed an affidavit disclaiming knowledge of the charges, and the account was cleared. This time, he called the three main credit bureaus and reported the fraud.

My colleague is just one of hundreds of thousands of individuals who are victimized each year. The culprits may be found among employees (or patrons) of mailrooms, airlines, hotels or personnel offices—anyone who has access to a person's financial information. They can use your credit card or instead use encoding equipment, sold by business supply companies, and blank cards with magnetic strips on the back, to encode your account number onto a counterfeit card with a different name. Thieves sometimes seek jobs specifically to get access to financial information; alternately, they may bribe employees in such positions to supply them with the data they want.

The problem is compounded by the ease with which a phony ID can be obtained. On the Web are scores of sites with complete instructions on creating a "new you." Personal computers, "scanners" and color printers (or copiers), all facilitate creating false identification documents.

Commitment of Resources Jurisdiction

Because identity theft crimes can involve the use of the mail, the U.S. Postal Inspection Service has become a lead agency in investigating these crimes. Even in cases where the original theft does not involve the mail, the mails may used to send the credit cards to a commercial mail receiving agency or alternate address. That's why Postal Inspectors are involved in investigating this crime and take it so seriously.

Each of the Inspection Service's 18 field divisions investigates identity theft within their respective boundaries. Identity theft investigations are reported, categorized, and tracked in an Inspection Service national database used by management to coordinate the appropriate investigative response. During the past few years, Inspection Service resources devoted to identity theft investigations have increased significantly—by 38 per cent.

Identity Theft Investigations

In a typical case last year, Postal Inspectors arrested eight West African nationals who were operating a multimillion-dollar counterfeit and stolen credit card enterprise nationwide. And Postal Inspectors in New York arrested 16 members of a gang that ran a passport photo business, supplying false identifications for cashing checks stolen from the mail.

Last year Postal Inspectors announced the results of a round-up of 103 mail thieves throughout the western United States. A multi-agency task force comprising U.S. Postal Inspectors, members of the U.S. Marshals Fugitive Apprehension Strike Task Force, U.S. Secret Service, state and local police, and the Northern California Identity Theft Task Force targeted mail thieves in California and Nevada. Similar operations took place in Arizona, Hawaii, Utah and New Mexico. Federal and state prosecutors supported the work of the task force by aggressively prosecuting individuals involved in mail and identity theft.

Here are a few more examples of identity theft cases investigated by Postal Inspectors in the past year. In Detroit, Postal Inspectors investigated a gang of mail theft recidivists who were recruiting street people, called "runners," to obtain cash advances from banks and casinos via credit cards. Inspectors executed a search warrant at the residence of a suspect and recovered more than 180 documents listing victims' personal IDs. Inspectors and agents from the Detroit Metro Identity Theft Task Force identified and arrested the ringleader of the group who, at the time of

his arrest, had more than 700 car rental applications with names, dates of birth, Social Security numbers, and credit card accounts of potential victims. The ringleader and a cohort reportedly called credit card issuers, purporting to be the true account holders, and requested that replacement credit cards be mailed to them. The car rental manager who supplied the rental applications and an employee who worked at a health plan office were later indicted for providing documents to the gang. Total fraud losses exceeded $700,000.

An Illinois man was sentenced to 25 months in prison and ordered to forfeit $590,000 in assets to banks after pleading guilty to the unlawful possession of an access device, mail fraud, and bank fraud. A joint investigation by Postal Inspectors and special agents of the Social Security Administration determined he had fraudulently applied for more than 200 credit cards using numerous victim IDs.

Postal Inspectors in Jacksonville, Florida, arrested six people believed to be running a major identity theft ring. The arrests were the result of a joint investigation by the Northeast Florida High Tech Task Force, which includes Postal Inspectors, members of the Jacksonville Sheriff's Office, and several other federal, state, and local law enforcement agencies. Victims of the ring included employees of the Winn-Dixie Corporation and Hollywood, Florida, police and fire departments. The six suspects were charged with 44 counts of violations related to the Racketeering Influenced Corrupt Organization (RICO) Act, including criminal use of personal information, grand theft, organized fraud, and manufacturing fraudulent IDs. One of the suspects has already pled guilty to RICO violations and related charges.

Las Vegas police arrested a man for "driving under the influence" and later discovered he had an outstanding arrest warrant for identity theft in Arizona. Phoenix Postal Inspectors reported he stole a person's Social Security number, applied for numerous credit cards in the victim's name, and had the cards mailed to a box he rented at a commercial mail receiving agency. Postal Inspectors and Secret Service agents searched the man's business and discovered numerous fraudulent documents.

Statutes Used in Identity Theft Cases

A number of statutes enable us to take action against identity theft involving the use of the mail. Under Title 18, U.S. Code, Section 1708, Postal Inspectors may arrest individuals for the possession of stolen mail or filing a false change-of-address order; the penalty is a $2,000 fine or up to five years' imprisonment, or both. In 1998, the Identity Theft and Assumption Deterrence Act of 1998, was signed into law. This law expanded the scope of the identity fraud statute (18 U.S.C. § 1028), and made it a federal crime for the unauthorized use of personal identification in the commission of any federal law (felony or misdemeanor), or a state or local felony.

But one of our top weapons in the fight against identity theft is a statute originally enacted over 125 years ago: the criminal mail fraud statute. If someone applies for a credit card in your name, perpetrators may be prosecuted under Title 18, USC 1341. The penalty is a $1,000 fine or up to five years' imprisonment, or both—unless a financial institution is affected, in which case the fine may be raised to $1 million and imprisonment for up to 30 years. The public policy that underlies this statute remains valid today: *The postal system created by Congress to serve the American public should not be used to conduct schemes that seek to cheat the public.*

Our experience demonstrates that enforcement laws and mechanisms, coupled with an aggressive education campaign and enforcement efforts described below, are invaluable tools in the arsenal of law enforcement.

Interagency and Industry Cooperation

To address the fundamentals of identity theft, the Postal Inspection Service works diligently with the credit card industry, financial institutions and other law enforcement and regulatory agencies. In 1992, the Postal Inspection Service sponsored its first Credit Card Mail Security Initiative meeting in Washington, DC. We continue to promote and host these semi-annual meetings.

Many of the preventive strategies discussed at our meetings have been implemented by our financial industry partners, and have resulted in reduced losses attributed to mail theft and the subsequent identity theft that occurs from it. The now-common concept of credit card activation was first proposed by a Postal Inspector and was promoted through the Credit Card Mail Security Initiative meetings. The industry embraced and implemented this prevention strategy, which resulted in the reduction of significant industry fraud losses over the past decade.

In addition, working in conjunction with industry partners, Postal Inspectors analyze information from credit card thefts to identify "Hot Spots" for investigative attention. The Postal Inspection Service notifies the financial industry of zip code

areas suffering abnormal losses, so they can take extra precautions when mailing to those areas.

Thanks to the collaborative efforts between the Postal Inspection Service and its working-group partners, we are beginning to see the results of this and many other fraud prevention initiatives. In addition to modifying industry practices, our collaboration has produced a number of fraud prevention guides, including the Fraud Detection and Reference Guide; Account Takeover Prevention Guide; and Detecting and Preventing Credit Application Fraud.

The working group was also responsible for the Identity Theft Consumer Awareness video and the Identity Theft brochure. At the conclusion of my testimony, I have included prevention tips prepared by the Postal Inspection Service in collaboration with its working partners.

In 2003, the Postal Inspection Service decided to broaden the scope of the Credit Card Mail Security meetings to include presentations on money laundering, Internet fraud, and bank fraud schemes. As the focus has expanded, the name of our working group has changed to the Financial Industry Mail Security Initiative (FIMSI). The initiative has decided to capture many of the best practices developed over the years and share them with industry and law enforcement in the form of a 50-page document, reporting upon identity theft problems and issuing recommendations directed towards credit card companies and credit lenders for reducing or preventing it. One of those recommendations dealt specifically with limiting the use or display of social security numbers in sensitive records and mailings.

To manage the vast data associated with these crimes, the Postal Inspection Service has developed a new financial crimes database. This computer application compiles a myriad of intelligence data relating to financial crimes, and provides Postal Inspectors with information that assists in identifying trends, criminal hotspots, and the scope of identity theft activity. Information for this database is provided by credit card issuers, other financial institutions, mail order companies, Postal Inspection Service investigations, and the victims themselves.

According to a report released by the FTC this past September, mail theft as a source for identity theft happened in only 4% of the cases surveyed. As we have made it more difficult for mail theft to be a component of identity theft, criminals have turned to other means, oftentimes recruiting the assistance of insiders, in other words "employees," who have access to the personal information, especially the social security numbers, of clients or other employees. Personal information like social security numbers contained in corporate and government records and computer databases is a fertile area for dishonest employees working in conjunction with identity thieves.

This is why we support H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act, and welcome the additional consumer protection provisions it will provide. It is important to do whatever we can to keep identity theft from happening in the first place

Task Force Efforts

In addition to partnering with members of the financial and mailing industry, task force efforts by law enforcement have been a successful approach to the identity theft issue. Postal Inspectors are active participants on financial crimes task forces throughout the nation. In Pittsburgh, Pennsylvania, the Postal Inspection Service leads the Financial Crimes Task Force of Southwestern Pennsylvania. This task force began operation on January 17, 1995, and is housed at the Pittsburgh office of the Postal Inspection Service. Originally, this task force was formed to target major credit card fraud in the Pittsburgh area. However, with the increased number of instances of identity theft spreading rapidly throughout America, this taskforce has directed most of its resources toward identity theft investigations.

One of the recent cases involved actor Will Smith as a victim of identity theft. When Smith played Agent J in the movie Men in Black that was showbiz. But when convicted felon Carlos Lomax impersonated actor Will Smith, that was identity theft. Will Smith never knew his identity had been stolen until he attempted to purchase a new home and found his credit had been compromised. Postal Inspectors and the Financial Crimes Task Force of Southwestern Pennsylvania arrested Lomax for identity theft, and Lomax was sentenced to serve 37 months in jail and pay $64,000 in restitution.

The Minnesota Financial Crimes Task Force, which includes Postal Inspectors, Secret Service agents, and local law enforcement officers, last year arrested a Nigerian national for a $1 million account-takeover scheme. Postal Inspectors executed a federal search warrant at the suspect's residence and recovered approximately $16,000 in cash, three vehicles, artwork, electronics equipment, and merchandise derived from the scheme. An investigation revealed the man used bank employees

to identify high-dollar, dormant accounts with balances of $100,000 or greater for his scheme, and shipped the fraudulently obtained merchandise to his home in Nigeria.

Public Awareness and Education Efforts

Over 2,000 of our 6,000 mail theft arrests last year involved identity theft—and it's getting worse. But arrests are not the only solution. That is why the Postal Inspection Service addresses the identity theft issue on two levels—aggressive investigative efforts and creating prevention and awareness programs.

While the Postal Inspection Service works hard to identify and prosecute identity crimes, we also recognize our ability to lessen the impact of this crime upon the public through various prevention campaigns. Postal Inspection Service efforts to prevent identity theft target the public and business communities to educate them about these schemes, and the problems associated with them. These efforts have included the publication of a brochure titled, *Identity Theft, Safeguard Your Personal Information,* and the March 2000 release of the Showtime movie, *The Inspectors 2,* based on Postal Inspection Service files relating to identity theft investigations.

In an effort to educate consumers about this fast-growing crime, the Postal Inspection Service created an informational video titled *Identity Theft: The Game of the Name.* Also, the Postal Inspection Service and thePostal Service's Consumer Advocate Office partnered during last year's National Consumer Protection Week, from February 3 through 8. The week's theme was "Identity theft, the No.1 consumer fraud in the nation."

In 1999, Postal Inspectors along with partner organizations undertook Project kNOw Fraud, which was the largest consumer awareness campaign undertaken in this country. Through a mailing to 123 million addresses we warned the public of the dangers of telemarketing fraud. The successful campaign was followed up with the National Fraud Against Seniors Awareness Week in August of 2002. In September of last year Postal Inspectors unveiled another national awareness campaign. Last year's topic was identity theft.

Actor Jerry Orbach, who also was a victim of identity theft, was the campaign's spokesman. This awareness campaign featured a two-pronged approach, providing prevention and awareness information to consumers and addressing businesses on the need to safeguard their files and databases of customers' personal information. The campaign included:

- A house-to-house mailing to residences in ten states identified by the FTC as reporting the most identity theft complaints. The ten states were California, New York, Texas, Florida, Illinois, Pennsylvania, Georgia, Michigan, New Jersey, and Arkansas. The mailing was made in September, 2003, in conjunction with a press conference.
- Distribution of an updated brochure on identity theft. The brochure was distributed in connection with identity theft presentations made by Postal Inspectors to consumer groups.
- Production and release of a Public Service Announcement (PSA) featuring actor Jerry Orbach. This thirty-second PSA was released in September in conjunction with the press conference.
- An identity theft insert outlining prevention tips that was included with monthly financial industry statements and with all Stamps by Mail orders placed during the months of September, October, and November 2003.
- Production of an identity theft poster that includes prevention tips that was displayed in all Postal Service retail lobbies, numerous credit unions, financial institutions, and police departments in September.
- Production of an identity theft informational video and articles on identity theft prevention that was published in internal and external publications as well as newspaper ads in the same ten states that were identified as reporting the most complaints.

The Mullen agency of Pittsburgh provided support for our Identity Theft campaign on a pro bono basis. But what really made this campaign unique is the funding source. We've all heard the saying, "crime doesn't pay." In the case of this awareness campaign, it does pay. This campaign was funded through fines and forfeitures paid by criminals in a past fraud case.

Prevention Tips

In numerous formats, including our website at www.usps.com/postalinspectors, we provide the following recommendations to the public:

- Deposit your outgoing mail in a blue Postal Service collection box and promptly remove mail from your mailbox after delivery.

- Shred unneeded documents that contain personal information before discarding them.
- Order credit reports every year from each of the three major credit reporting agencies and thoroughly review them for accuracy.
- *Never* give personal or financial information over the telephone or the Internet unless you initiated the contact and trust them.
- Report lost or stolen credit cards immediately.
- If you applied for a credit card and didn't receive it when expected, call the financial institution.
- Sign new credit cards immediately—before someone else does.
- Memorize your Social Security number and passwords. Don't use your date of birth as your password and don't record passwords on papers you carry with you.
- Never leave transaction receipts at ATM machines, on counters at financial institutions, or at gasoline pumps.
- Don't carry your Social Security card or birth certificate; leave them in a secure location.
- Don't disclose credit card or other financial account numbers on a Web site unless the site offers a secure transaction.
- Closely monitor the expiration dates on your credit cards and contact the issuer if you don't receive a replacement prior to the expiration date.
- Beware of mail or telephone solicitations that offer prizes or awards—especially if the offer asks you for personal information or financial account numbers.
- Match your credit card receipts against your monthly bills and check your monthly financial statements for accuracy.
- Watch for your monthly financial statements and bills. If you don't get them when expected, contact the sender.

For victims of identity theft, we recommend the following initial steps to begin the long and arduous task of responding to the crime:

1. If the crime involved the U.S. Mail, contact your nearest U.S. Postal Inspection Service office and report it.
2. Call the fraud units of the three major credit bureaus and request a "fraud alert" be placed on your credit file. Check your monthly financial statements for accuracy.
3. Order copies of your credit report from the credit bureaus to check whether any fraudulent accounts were opened without your knowledge or consent.
4. Contact your banks and creditors, by phone and in writing, and report the crime. You may be advised to close some or all of your accounts. At the least, change your PIN codes and passwords immediately.
5. Record the names and phone numbers of people with whom you discussed your case and retain all original reports and supporting documents. Keeping accurate and complete records are a big step toward helping you resolve your problem.
6. Contact your financial institutions and request they flag your accounts. Instruct them to contact you immediately if there is unusual activity on your accounts.
7. File your complaint online with the Federal Trade Commission, or call their Identity Theft Hotline at 1–877–IDTHEFT. The FTC has counselors to assist identity theft victims with resolving financial and other problems that can result from this crime.

Educating the public and working to reduce the opportunities where the U.S. Postal Service can be used for illegal purposes are crucial elements in our fight against identity theft crimes. As always, we will do our part to remove criminals from society. We appreciate your recognition of the importance of this issue.

Chairman SHAW. Thank you, Mr. Maxwell. I thank all the witnesses. Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman. Mr. O'Carroll, in your testimony you mentioned cross-verification with numerous agencies. Is the U.S. Department of Veteran Affairs one of those?

Mr. O'CARROLL. Yes, it is, Mr. Johnson.

Mr. JOHNSON. How do you deal with them directly? A lot of my buddies got listed as being dead, and they couldn't get their status reinstated because of a lack of identification, as you might imagine. How do you address that issue?

Mr. O'CARROLL. Yes, Mr. Johnson. We have a matching agreement with the Veterans Administration where the SSA matches the SSNs of veterans against our databases for validity. There have been instances in the past, we have done an audit on it. Inadvertently the SSA listed people as deceased when they aren't deceased. We have brought that to the SSAs attention.

Mr. JOHNSON. How does that happen in the system?

Mr. O'CARROLL. Well, many of the death reportings are voluntary from a lot of different sources. Occasionally when a source indicates that a person is deceased, and it is entered into the records, before it is verified by another party on it, that information is recorded. What we are recommending is a second verification on it so that that doesn't happen anymore.

Mr. JOHNSON. Are those numbers reissued?

Mr. O'CARROLL. No, they are not reissued then. Once you get an SSN, sir, that is yours for life and forever. They don't reissue SSNs.

Mr. JOHNSON. If the guy is dead, and you resurrect him, do you give him his SSN back again?

Mr. O'CARROLL. Yes. He does. He or she will get it back.

Mr. JOHNSON. Okay. Second, do you issue Social Security cards to students who are here on student visas who do not work?

Mr. O'CARROLL. In actuality, they are not supposed to be issued to non-work students. The SSN is issued to students if they can show documentation from Immigration showing that they are authorized to work, at which time they will be given an SSN.

Mr. JOHNSON. This is if they are authorized; but what if they are not working at all and never intend to? A lot of them do come here and are under their—they are supported by their home county. They don't pay any income tax. They don't pay a thing us to, not a nickel, but they go to school, and they have a student visa. Now, how do you differentiate?

Mr. O'CARROLL. Well, the student visa is not reason to be issued an SSN. It has to be issued for work purposes. We have done audits where some schools have issued—or have issued letters saying that a student is working, when, in fact, they haven't been working, and that way was a way that they bypassed the rules and regulations in order to get an SSN. It is something that is recognized, and it is something that we have been working very closely with SSA doing studies of universities and making sure that they are, in fact, following the laws and using the actual document to show that a person is working. It is a loophole that has been out there, and it is being closed as we speak.

Mr. JOHNSON. Do you have employers, when they hire somebody, theoretically they are supposed to check their status, and theoretically you are supposed to have the computer capability to have somebody call you and say, hey, is this a valid number and name, and you are supposed to be able to say yes or no immediately. Is that in operation right now?

Mr. O'CARROLL. Correct. The SSA does have that.

Mr. JOHNSON. You do have that. I understand that a lot of businesses are not taking advantage of that; is that true?

Mr. O'CARROLL. That is correct, sir.

Mr. JOHNSON. How do we rectify that?

Mr. O'CARROLL. Well, one of the portions of the support of Congress is to make it mandatory that employers do check that each time. As it stands in the past, SSA now has ways of doing it where it can be done electronically, it can be done on the telephone, it can be done in person. What we are hoping for in the future is to have electronic means for verifying all employees. We have got different public outreaches to encourage employers to do it, and we are hoping for Congress to encourage employers also to make it mandatory that they do it in the future.

Mr. JOHNSON. One further question for anybody that wants to answer it: Are we still failing to go after people who sell or tell you that they have lost their identification and come back for another one, because last time our testimony indicated that there was upward of 80 or more before you even looked at it.

Mr. O'CARROLL. Those are two of the provisions in this law is one to take a look at the people asking for numerous replacement Social Security cards.

Mr. JOHNSON. Well, how about one? If you have got the computer system to do it, why can't do you it after one?

Mr. O'CARROLL. Well, there are legitimate reasons why people lose their Social Security card. Quite frankly, what we have been saying within the Office of the Inspector General is it is the number, not the card that is the problem to society.

Mr. JOHNSON. Well, I understand that, but they still sell them, don't they?

Mr. O'CARROLL. That is a major concern of ours is that when they get replacement cards, that they could be sold again, and that is why we are asking to tighten up on it.

Mr. JOHNSON. Just one follow-up. Are you still waiting to 80 before you check them out?

Mr. O'CARROLL. Yes. The number has dropped considerably on the number of replacements. It is not up to 80. What we are looking for is 20 in the lifetime. We still think that is a large number to be asking for, and we are asking to have that number reduced.

Mr. JOHNSON. I will bet the Postal Service doesn't wait that long. You guys do a good job, by the way. They briefed us well in Texas. Thank you. Thank you, Mr. Chairman.

Chairman SHAW. Thank you. I still have my original Social Security card.

Mr. JOHNSON. So do I.

Chairman SHAW. Let me do a follow-up of what Sam was asking you with regard to students. If a student wants to open a bank account, and he doesn't work, and it is an interest-bearing account, he would need an SSN, wouldn't he?

Mr. O'CARROLL. If you remember, Mr. Chairman, there was the hearing that we had with the use of the tax identification number, so that is a way in order to report.

Chairman SHAW. Oh, I see.

Mr. O'CARROLL. Taxable information without using an SSN.

Chairman SHAW. That is right. Thank you for refreshing me on that. Mr. Cardin.

Mr. CARDIN. Thank you, Mr. Chairman. I want to follow up on the private sector and the cooperation we are receiving from the private sector as it relates to theft, identity theft, SSNs and related issues, including the issue that Mr. Johnson raised. It seems to me that we are having a difficult time passing new laws here because of the wide use of SSNs by commerce, which we all understand. It seems to me that the private sector, private employers and private companies have a great deal at stake here, and I am curious as to whether you think they are doing enough to assist us in identity theft, at least initially. Second, after a person has found their identity has been stolen, and they have gone through this difficult issue, it has been reported to us that the theft continues, and there is still a difficult time in getting the private sector to work with us to make sure that the person who has been victimized is no longer victimized. So, I would be interested in your response as to whether you think the private sector, private employers, private financial companies, private companies generally are doing enough to help us and assist us to develop a strategy to minimize identity theft in this Nation.

Mr. BEALES. Congressman, I think by and large the private sector has been very cooperative and very responsive. What has tended to happen in this area is identity thieves exploit a particular source of information or a particular channel to get credit. It takes some period of time to recognize that channel and recognize that problem. Once it is recognized, there are some fairly strong incentives to put measures in place to shut down that particular channel. Unfortunately it is an ongoing process because identity thieves work very hard to find a new way to do that.

Mr. CARDIN. Can I just challenge you on that for one moment? If I make a small mistake on the use of my credit card, it seems to me it gets bounced the next time I try to use it pretty quickly. It seems like the credit industry knows how to get things into the computer pretty quickly to respond to what they believe is important. I don't see the same zeal, the same commitment as it relates to identity theft. Am I wrong?

Mr. BEALES. Well, I think it has varied. I think the most common form of identity theft is credit card misuse, and I think the things you are pointing to are in place and address that form of identity theft and have really improved tremendously over time as people have used pattern recognition kinds of software and kinds of technologies to identify problems before there is too much charged on existing credit card accounts. So, I think there is a lot of that. There is no doubt that there is more that can be done in many areas, and that there is an ongoing need to recognize new threats as they emerge and to put measures in place to address them.

Mr. CARDIN. The victim finds that his or her credit is affected. There are so many different avenues in which this information travels. It would seem to me that the private sector could develop the type of software response that could try to help the victim, and I haven't seen that.

Mr. BEALES. Well, I think the key to helping the victim, once there has been an identity theft victim, is now in place by statute under Nation that was passed last year, and that is the system for placing fraud alerts has been codified in that statute. You can do it with one call to any one of the three credit bureaus and place the fraud alert for all three. With an identity theft report, like a police report, you can block fraudulent information that would appear on the credit report and keep it from being re-reported, and those measures we are in the process of rulemaking now and will be in place shortly.

Mr. CARDIN. Yes. I think the frustrating part is that you can find a person's credit destroyed very quickly because the system is in place to identify individuals who are believed to have had a credit problem, even if it is a theft situation, but to rehabilitate it seems like to takes a lot longer to be able to work through the system. I just question whether we have the same commitment in the private sector to deal with the victims as it is to in some cases over respond and take away a person's good credit who doesn't deserve to have that credit taken away. Just my own observation.

Mr. MAXWELL. May I add to that?

Mr. CARDIN. Sure.

Mr. MAXWELL. The initial part of your question, if I understood it correctly, was about the cooperation with industry. In our experience I have been encouraged, but the dichotomy you have, you have the business interest wanting to serve the customer to keep them as customers, but then they also have their competition with their other associated industries for the credit card group. I mentioned earlier for example, they are competing factions. We have a mail order task force. They are competing factions. So, sometimes it is hard to get them to cobble together like a shared database or best practices. They seem reluctant, which I understand why.

Where I have seen and been encouraged is we tried—when we started this campaign, we reached out to the credit card companies to partner with us and actually put an identity theft warning on their statements. We never took that full measure because we couldn't get every company to agree to it. Their counsels, independent counsels, had some problems with it; however, some unilaterally did it on their own. So, I was encouraged by that, but I think the problem we will still have to overcome is that issue of competition and in the fact that we will give a little, but it is a constant balance. I think that more and more there is a benefit seen at the end by having the customers happy, satisfied and protected. Ultimately that is the case, and that is what we found in the Postal Service, I know. You can cut a lot of measures. We tried changing the commercial mail-receiving agency rules, and that was a very tough row to hoe. Again, you have a lot of industry you have to consider, but I am encouraged. We have come a long way.

Chairman SHAW. Mr. Hulshof.

Mr. HULSHOF. Thank you, Mr. Chairman. Let me start, Mr. Maxwell, by echoing what Mr. Johnson said. The Saint Louis Postal Inspector's Office had the opportunity to brief me in the Saint Louis office. This was right in the aftermath of the mailbox pipe bombs in the Midwest, and so I really got a good glimpse of what it is that you all do. I will have to admit that the day was capped

off by allowing me to participate in the computer-simulated firearms training, which was a lot of fun, and I didn't maim too many innocent people.

So, Ms. Bovbjerg, let me get to really the subject of today's hearing. I am sorry about the microphone here, Mr. Chairman. It seems to be in and out. We have talked about the private sector, Ms. Bovbjerg. What I want to talk about, because I know coming up in a later panel is what is happening in the public sector, and as you point out, and we are going to hear from a witness in the second panel, Federal law requires the use or the collection of SSNs for various reasons related to tracking deadbeat parents. The SSNs must appear on the pleadings in court orders related to child support. In fact, the Code of Federal Regulations requires that the SSN appear on garnishment orders involving postal employees as well as, and not to resurrect, Mr. Becerra, our discussion and debate last night in the full Committee, but SSNs are used to collect fines, crime victim restitution and beyond.

So, I know you recognize in your statement that there is a survey of State and local agencies to determine the extent to which SSNs are displayed in public records. When might that survey be completed, and what can you tell us about it?

Ms. BOVBJERG. Well, mine is not working either. We are due to report out to Chairman Shaw in September on this work, and it is a really complex survey, and so we have some things. Like we know that some States have the SSN in public records, but they don't need it, and they are not really sure why it is there. We can't tell you what the incidence of that is yet because we don't have all of our surveys back.

What we are looking at is really what kind of records does the SSN appear in. We are trying to be able to say how many people this might affect by the way that we structured our survey. It is a little different than some things we have done for you in the past. We are also looking at what format is it in, because 2 years ago when we did this work, we were all, I think, pretty alarmed when we heard that these things were all going to be electronic, and this was going to be a boon to customer service. We are looking at, well, just how electronic is it going to be?

I think that what we are hearing anecdotally and the people that we talk with about these things is there is just a greater sensitivity to this issue in no small thanks to this Subcommittee work. We have seen a dramatic shift in the public record world in the kinds of things that people are concerned about now. They are a lot less concerned about the speed of customer service and a lot more concerned about how do we make sure that we have only the data we need, how do we make sure that it is not going to the wrong place. There is a lot more of that.

So, we will be reporting both survey results and results of our interviews. I think you know largely the early returns is there are some good news. There are some things that are being done. The good news at the Federal level, just by the way, is that the Privacy Act works, but when you get into State and local governments, it is not uniform, there isn't a single law that affects them. We continue to believe that the government, the Federal government, should consider working with State and local governments to de-

velop something that is more uniform, more uniform protections, but at the same time consider that there are some very important uses to which the governments put the SSN, one of them being child support enforcement, tax enforcement, and program integrity at SSA. Just a few.

Mr. HULSHOF. Well, and certainly as a supporter of the Chairman's bill, I wasn't aware until really preparing for this hearing that the Code of Federal Regulations in some instances insists that the SSN be recorded, and so I see that we are at a conflict here obviously. The other concern that I would expect would be that any new legislation that would be introduced and hopefully pass, Mr. Chairman, your bill, would certainly be prospective. Again, I will just relate that in the State of Missouri, our State Court Administrator who is set to testify, a lot of our courts in rural areas are finally now getting online as far as providing those court documents. So, in other words, going back retroactively to somehow close these records would just really be an extraordinarily difficult task, but look forward to the survey and any recommendations that maybe come along with that study. So, thank you.

Ms. BOVBJERG. Well, one thing I do want to encourage you to think about is there is use and there is protection, and that you can require use, but you don't have to display it while you are using it. I think that is one of the things you are seeing that the Federal courts are starting to try to deal with.

Mr. HULSHOF. Thank you.

Chairman SHAW. Mr. Hulshof, the bill that you are cosponsor of that you refer to as my bill, but it is our bill, is prospective, and there is a 2-year period for implementation, so I think we have covered that base. I hope so.

Mr. HULSHOF. Good.

Chairman SHAW. Mr. Becerra.

Mr. BECERRA. Thank you Mr. Chairman, and let me also say, as my colleagues have said, thank you very much for pursuing this so diligently. I hope that we are able to move forward your bipartisan legislation soon because it is better to get what is good out of the bill now versus wait until we perfect it later. Thank you all for your testimony. Let me ask a couple of quick questions, see how much I can get through in 5 minutes.

What can we do, and I open this to any of you who wish to comment. What can we do to help victims of identity theft to restore their good name and credit and to retain and restore again also their privacy? We are dealing with trying to prevent it. We know that in millions of cases we are too late. The talk of prevention is not going to help them because they have already had their identity stolen. Now they are facing the consequences of months, maybe years, of reclaiming their good name and credit. What can we do? Can you think of anything we can do legislatively to try to help victims who are currently in the process of trying to restore their good name and credit?

Mr. MAXWELL. There may be a possibility to enact some form of, for lack of a better word, Committee, but group, working group, task force group that is tasked primarily with expediting consumers' restoration, if you will. To me it seems like most consumers, particularly the elderly, become frustrated with the sys-

tem, whether it be complaining about fraud or the health care problem or just going to get help. When they are faced with a myriad of phone calls and letters to write, it kills them.

Mr. BECERRA. Other than having a group that can advise, let me give you a quick example. Should we, for example, pass a law that says that a private entity that has used a SSN for whatever purpose, a bank, a credit agency, if, indeed that agency uses SSNs, it must treat as priority status an individual's claim that his or her identity was misused, and therefore has to clear that record so that when you as a private entity get that type of request by an individual, you must give it priority status? You can't just put it at the end of the list of complaints and work that you would have to deal with in the course of your business dealings.

Mr. MAXWELL. That would be an excellent first step. Definitely an excellent first step, and I think, as a follow-up, if there could be some body created to help expedite that, too. That first step would be putting the onus on the firm, the most responsible.

Mr. BECERRA. Anyone who wants to use a SSN understands they have got an obligation to help a victim of identity theft clear it up quickly. If you are going to use the card, or the number, understand that some people will be victims; not perhaps of your own doing, but because you are a user of the card, you then are obligated to help victims who had their number used inappropriately resolve that issue as quickly as possible.

Mr. MAXWELL. That sounds promising to me.

Mr. O'CARROLL. Mr. Becerra, two things that are of interest to us. One is our major concern is the integrity of the SSN in relation to Social Security programs. However, what we have been big on encouraging is cross-verification, so that any Social Security that is numbered that is out there either in the Federal government or in commerce is being verified to know whether it is a valid number or not, and that kind of leads into what you were saying, is that way we can through verification, we can identify the misuse that is out there, and hopefully someday by government matching agreements, there will only be one person with one SSN of record in the Federal government. So, that is an issue with us on trying to prevent it.

Mr. BECERRA. That is still more on the preventative side, which I think that is really where we have to go, because we don't want to have victims. To some degree I think there is still some help we can provide. If you have a good verification system, that makes it easier for those who didn't abuse their use of the card help that victim restore his or her good name and credit. So, if I am a bank and I wasn't at fault, and some other entity allowed the number to be misused, at least I can help verify quickly the claim of that individual that indeed he or she is that person and not the other individual.

One quick question for Mr. O'Carroll. My understanding is that your current policy is to allow 52 replacement cards per year—is for Social Security to allow 52 replacement cards per year. Why the heck are we at such a high number? It used to be 80-something, as I think Mr. Johnson said. Why the heck are we still at—why would anyone need more than one? I never pull out my Social Security card itself as an identifier; it is just a number. So, why

would anyone need to request a card, even if you have lost the card itself? You know what your number is, or someone else does. Why would you need to request replacement cards?

Mr. O'CARROLL. I think the logic that you are getting at and everyone else is, and as Mr. Johnson brought up, is probably for resale of that number or giving that card to somebody else, which is a concern on a fraudulent basis. One of the issues that the Agency looked at and we were a part of was taking a look, instead of having that card, is maybe making it a certificate or something larger than a card that would be put away and wouldn't be out in the common commerce on it. As with anyone, when you start thinking about if we came up with a new format for a Social Security card, everybody in the United States would want a new one and you can imagine the implications that would be. So, from looking at it from, I guess, the mechanical side of it, yes, the card is really the number and not the card.

Mr. BECERRA. Unlike a diploma you hang up on your wall, you are not going to put a SSN up on your wall. Once you have it, you want to store it away and hide it as best you can. So, let me ask you a real quick question. Do we ask for some form of certification or verification as to why you are requesting another card? Do we say to you, prove to me that you need it or why you need it?

Mr. O'CARROLL. No. At this point, no, sir.

Mr. BECERRA. So, Mr. Chairman, this to me seems like an area where we could immediately address this. Once you have got your card obviously we hope the people can be diligent in safekeeping their number. To have the SSA continue to allow people to get replacement cards, which could really only be used for purposes of resale or for fraudulent purposes, this is something that——

Mrs. TUBBS JONES. Will the gentleman yield?

[The opening statement of Ms. Tubbs Jones follows:]

Opening Statement of The Honorable Stephanie Tubbs Jones, a Representative in Congress from the State of Ohio

Mr. Chairman,

Allow me to commend you on both your timing and your topic for this morning's hearing. As national legislators we must tackle what is becoming the fastest growing national crime trend in modern history: Identity theft! As so often happens with modern technology and high tech innovations, the use of technological advancement far out paces the public policy, protection measures and regulations governing the administration of technological advancement.

While identity theft is on the rise and the social security number (ssn) is but one avenue to affect the crime, the prolific and generally accepted practice of use of the social security number as an identifier makes it a prime target. It is fitting that we, as Members of the Social Security Subcommittee, address the issue in an open forum. As Americans get older and increase the number of retirement/entitlement programs for which they are eligible—the use of the social security number becomes the number one identifier for all types of service providers. As we launch this massive and still yet confusing voluntary national prescription drug program—we are once again offering to new and established entities the privilege to use the social security number as an identifier.

The public and private sector have recognized and dialogued about the balance between the privacy issues and the protection of open commerce. Entities from the mortgage bankers, to national credit bureaus, to municipal records keepers and credit card companies—up to and including the U.S. government—have all come together in one forum or another to address the issue. Before us today, we also have H.R. 2971—of which I am a co-sponsor—"The Social Security Number Privacy and Identity Theft Prevention Act of 2003. This is clearly a step in the right direction.

Mr. Chairman, according to Federal Trade Commission (FTC) data (2002 is the most recent data available) my home state of Ohio ranks 30th in the nation in identity theft cases and CLEVELAND, in my Congressional District, is number one in the state. I have provided copies of the FTC information as a part of my statement today and would like to have it included in the record of today's proceedings. Local jurisdictions have highlighted the issue: the Associated Press reported how Hamilton County in the State of Ohio will hear recommendations from their task force to limit/restrict the amount of information—including the SSN from the county clerks' Web site; NBC reported just last week on how blood donors at the UCLA Blood and Platelet Center may be unwitting victims of identity theft as a result of a misplaced laptop with all of their personal data—including the SSN! This follows the alleged theft of another UCLA laptop from their financial office that contained similar personal information that could put even more people at risk. The need for increased laptop security notwithstanding, perhaps we need to somehow limit both the demand for and the use of the SSN.

In 1935, with the passage of the Social Security Act, every employee covered by the social security program had to have an identifying number. Since then, the Civil Service Commission; the Internal Revenue Service; the Treasury Department; The Veteran's Administration; The Department of Defense—just to name a few government entities—have all made disclosure and use of the SSN an almost prerequisite identifier. We in Congress have made several attempts to monitor and regulate the use of this number. Mr. Chairman, I look forward to hearing from the witnesses this morning as they lend their expertise and personal experiences to our effort to lend some clarity and protection to the public.

Mr. BECERRA. Certainly.

Mr. JONES. I have a son who had to get a replacement card in order to get a passport or something. There was some other agency that would not accept that he did not have an SSN, and so it was a requirement that he needed to get a replacement.

Mr. BECERRA. I think there is a perfectly good explanation, and therefore you could have some certification under penalty of perjury or something that says, I need this card because this agency is requesting it, and there you have then something that gives you some sense of comfort that the person is requesting it for a purpose other than just because they want another card.

Mr. JOHNSON. Yes, but not 80 of them.

Mr. BECERRA. That is exactly it, and the way technology and automation works today, chances are that we should be able to have the U.S. Department of State or the agency that issues passports talk directly to the Social Security agency, Federal government to Federal government, on whether or not this person has this number and it belongs to him or her.

Mr. O'CARROLL. Social Security, the answer to that part of it, is working very closely with the U.S. Department of State, Immigration and Naturalization Servies, and U.S. Department of Homeland Security, on that type of a match for verifying that information.

The other part of it, though, is you were saying on these replacement cards, and not to steal the thunder of your Committee, your Subcommittee on this thing that is one of the provisions of this thing, is to look at the issuance of the replacement cards, and it is part of the study that is being recommended. Quite frankly, we feel that that is a fraudulent loophole, the number of replacement cards that are out there. It is a throwback to days when all the SSN was used for was tracking wages. Everyone was happy to give out numerous Social Security cards at the time because it was for

the purpose of tracking wages, not as it is today where it is becoming a——

Mr. BECERRA. You don't have to go to the SSA. I can tell you down at some streets in Los Angeles. where you can get the same card without having to ask the SSA to send you one. So, it is not as if there is some particular value in getting this replacement.

Mr. O'CARROLL. Hopefully we are buying cards from that person and arresting them.

Ms. BOVBJERG. Could I just jump in on this issue for just 5 seconds? Last year this Subcommittee had a hearing on some of these issues where the Commissioner was here where I testified, and we recommended that we not give out 52 replacement cards a year, that we at least reduce the number. There are some legitimate reasons to need replacement cards, but very few of them would require 52. At that time, SSA said that they had in front of Office of Management of Budget a proposal to reduce the number of cards per year and lifetime. That was a year ago. So, I don't know what has happened to that proposal, but that is a recommendation that we have made as well to SSA. So, we share your concern.

Chairman SHAW. I will inquire of the Commissioner and place that information in the record.

[The information follows:]

June 22, 2004

Hon. Jo Anne B. Barnhart
Commissioner of Social Security
500 E Street, SW
Washington, D.C. 20254

Dear Commissioner Barnhart:

We wanted to bring to your attention the issue of Social Security number (SSN) replacement cards, which was discussed extensively at our Subcommittee hearing on enhancing SSN privacy held on June 15, 2004.

As you know, the Subcommittee had been informed previously that some unscrupulous individuals may sell their legitimate SSN cards to others, thereby enabling them to work under an SSN that is not their own and to commit other forms of identity fraud. Both a witness from the General Accounting Office (GAO) and the SSA Acting Inspector General were asked whether the agency had changed its policies to restrict the number of SSN replacement cards. Each replied that under the SSA's current policies, individuals may obtain an unlimited number of replacement cards.

To ensure the public record on this issue is accurate, please provide your current policies with respect to the issuance of replacement cards and whether any change to those policies is anticipated.

Also, as you may know, a provision to limit the number of replacement cards has been included in the *Social Security Number Privacy and Identity Theft Prevention Act of 2003* (H.R. 2971). Your comments on this provision would be welcomed by the Subcommittee.

Your reply by July 9, 2004 is most appreciated. Should you have further questions, please contact the Subcommittee Staff Director, Kim Hildred, at (202) 225–9263.

Sincerely,

E. Clay Shaw, Jr.
Chairman

August 2, 2004

Hon. E. Clay Shaw, Jr.
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your letter dated June 22, 2004, regarding the SSA's (SSA) policies related to the issuance of replacement Social Security number (SSN) cards. You asked us to provide our policy on issuing replacement cards, and whether we anticipate changes in that policy. You also asked for our comments on a provision in H.R. 2971, the *Social Security Number Privacy and Identity Theft Prevention Act,* that would limit the issuance of replacement SSN cards.

SSA currently has no limitation on the number of replacement SSN cards an individual may be issued (either over the course of a year or a lifetime), other than a protocol in its electronic processes that prevents the issuance of a replacement card within 7 days of a previous card issuance. Section 204 of H.R. 2971 would restrict the issuance of multiple replacement cards, specifying both yearly and lifetime limits.

I, too, am concerned that issuing unlimited replacement cards may contribute to identity fraud. We are exploring ways to prevent individuals from obtaining replacement cards to facilitate someone else committing identity fraud. For example, I have instructed my staff to develop procedures that will identify instances where requests for replacement cards rise above a reasonable threshold. If fraud is suspected, SSA staff will follow established protocols and refer the matter to our Office of the Inspector General for appropriate action.

We will keep you apprised of our activities in this area and would welcome the opportunity to continue to work with you to find an appropriate balance between our responsibility to provide the American people with the service they expect and deserve, and our commitment to deter SSN fraud.

Thank you for bringing this issue to my attention. If I can be of further assistance, please do not hesitate to contact me or have your staff contact Mr. Robert M. Wilson, Deputy Commissioner for Legislation and Congressional Affairs, at (202) 358–6030.

Sincerely,

Jo Anne B. Barnhart
Commissioner

Chairman SHAW. I want all of you to know that you have witnessed a very historic moment where Mr. Johnson and Mr. Becerra are in full agreement.

Mr. JOHNSON. That is California and Texas.

Mr. BECERRA. Mr. Chairman, that is worth putting on our wall as some kind of diploma.

Chairman SHAW. I have made note of it. Ms. Tubbs Jones.

Mrs. TUBBS JONES. Thank you, Mr. Chairman. Good afternoon to the witnesses. I want to pick up on one of the questions that was asked. My staffer Melvena says: how do private sector entities gain access to our Federal verifying mechanisms in order to use Social Security as an identifier?

Ms. BOVBJERG. I can talk about the employer side. I can talk about the motor vehicle side. They can do it in several different ways. It depends on how many records they want to verify. They can do it by phone, they can do it online. As a practical matter, though, employers don't do this. They don't verify. We are doing work right now for this Subcommittee that is due out in the winter on the effect that this has. Specifically, on the records that Social Security doesn't know what to do with because the name, date of birth, and the number don't match, and these records are coming from employers.

Mrs. TUBBS JONES. For example, my automatic teller machine card, if I go on line or call a number, 1–800, whatever it is, I call and I say I want to access my checking account. Then they ask me for my SSN to be put into the system in order to access my checking account. Then they ask me for a 4-digit pin number, which is

also part of my SSN, to get to my checking account. What kind of regulation do we have on that?

Ms. BOVBJERG. The reason they have your number is because financial institutions are required to have that information for tax purposes.

Mrs. TUBBS JONES. Okay. So, that then allows them an option to go wherever else they want to go with it, because they have access to the number in that way.

Ms. BOVBJERG. Well, I would like to think that they are not only asking you for your number but for something like your mother's maiden name or something like that, because just having the number, if someone were to.

Mrs. TUBBS JONES. That might be private too, though. I'm kidding, go on.

Ms. BOVBJERG. You want something that if someone has your SSN, they couldn't go back to the bank.

Mrs. TUBBS JONES. I understand, but what I am saying the import of it is, is that they are using this number that supposedly was supposed to be sanctimonious or sanctified; it would never be able to be used for any other purpose very easily in the process. I think I would agree with my colleague here, that maybe what we need to do is to put some imposition or some requirement on those that use it to be able to provide some protection for the public when they choose to use it in a way that benefits their particular process.

Let me go to the gentleman from the Inspector General's Office. I come from Cleveland, Cuyahoga County, former District Attorney in Cuyahoga County. So, we did a lot of work with postal inspectors. One of the most difficult things about prosecuting much of the theft, or identity theft in many of the areas, is that very few people want to really do white-collar crime. It takes a lot of work, it takes a lot of money, it takes a lot of time to invest in that type of work. What has been your success with, once you get a document or have done your research, gotten it together—prosecution of identity theft?

Mr. MAXWELL. I mentioned earlier that of our 10,000 arrests for all crimes last year, 3,000 were identity theft, which is a very large proportion. That tells me—plus, of the cases I have read and been briefed about, we have a very good track record that way. There are cases that aren't as attractive enough to prosecute, but if you have generally more than one complaint or if one victim has a large loss and it is a complex matter, generally the U.S. Attorney will be more than happy to devote resources to it. If it is not a large loss, if there are very few victims, generally the climate—and that is true universally for fraud cases.

Mrs. TUBBS JONES. Coming from the State prosecutor's office, we always go back and forth as to whether the States and the Feds really pay attention to what cases. Just for the record, Mr. Chairman, I would like to submit something from the FTC that shows figures and trends in Ohio.

[The information follows:]

IDENTITY THEFT

Identity Theft Victim Complaint Data

Figures and Trends
In Ohio

January 1- December 31, 2002

Federal Trade Commission
Washington, DC

IDENTITY THEFT

Figure 1
How Victims' Information Is Misused[1]
January 1 – December 31, 2002

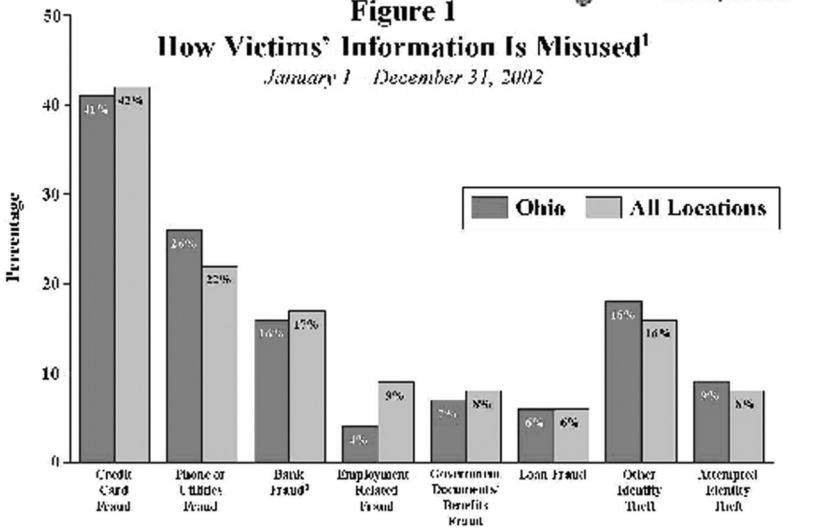


Figure 2

How Victims' Information Is Misused[1]

Total Number of Identity Theft Victims: Ohio = 4,065 * All Locations = 161,819**

January 1 – December 31, 2002

Credit Card Fraud

Ohio 41% *** All Locations 42%

Theft Subtype	Ohio	All Locations
New Accounts	[illegible]	[illegible]
Existing Accounts	[illegible]	12.1
Unspecified	1.8	[illegible]

Phone or Utilities Fraud

Ohio 26% *** All Locations 22%

Theft Subtype	Ohio	All Locations
Wireless - New	8.0%	10.3%
Telephone - New	7.0	5.2
Utilities - New	7.2	5.0
Unauthorized Charges to Existing Accounts	0.7	0.7
Unspecified	2.5	2.2

Bank Fraud[2]

Ohio 16% *** All Locations 17%

Theft Subtype	Ohio	All Locations
Existing Accounts	7.0%	8.1%
New Accounts	3.2	3.7
Electronic Fund Transfer	3.4	3.1
Unspecified	1.7	2.0

Employment-Related Fraud

Theft Subtype	Ohio	All Locations
Employment-Related Fraud	[illegible]	[illegible]

Government Documents or Benefits Fraud

Ohio 7% *** All Locations 8%

Theft Subtype	Ohio	All Locations
Driver's License Issued / Forged	[illegible]	[illegible]
Tax Fraud / Tax Return	1.2	1.9
Social Security Card Issued / Forged	1.1	[illegible]
Gov't Benefits Applied For / Received	0.5	[illegible]
Other Gov't Docs Issued / Forged	0.4	[illegible]
Unspecified	0.1	[illegible]

Loan Fraud

Ohio 6% *** All Locations 6%

Theft Subtype	Ohio	All Locations
Business / Personal / Student Loan	[illegible]	[illegible]
Auto Loan / Lease	[illegible]	[illegible]
Real Estate Loan	[illegible]	[illegible]
Unspecified	[illegible]	[illegible]

Other Identity Theft

Ohio 18% *** All Locations 16%

Theft Subtype	Ohio	All Locations
Other	8.5%	[illegible]
Illegal / Criminal	[illegible]	[illegible]
Medical	[illegible]	[illegible]
Internet / E-Mail	1.7	1.4
Apartment / House Rented	0.8	1.0
Bankruptcy	0.3	0.4
Securities / Other Investments	0.1	[illegible]

Attempted Identity Theft

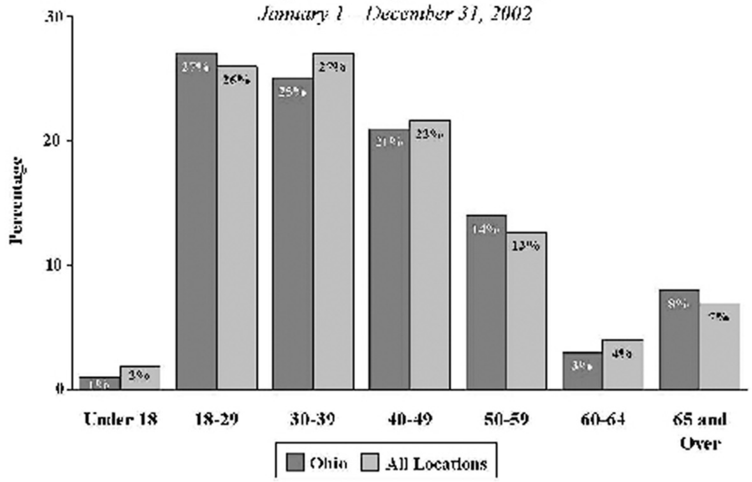
Theft Subtype	Ohio	All Locations
Attempted Identity Theft	[illegible]	[illegible]

[illegible]

Figure 3

Complaints by Victim Age[1]

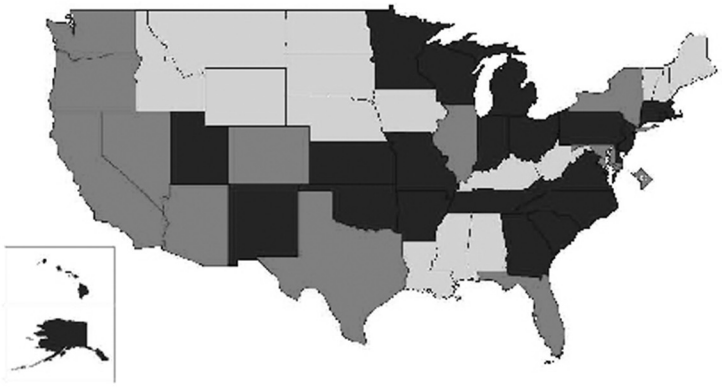
January 1 – December 31, 2002



[illegible]

IDENTITY THEFT

Figure 4a
Identity Theft Victims by State (Per 100,000 Population)[1]
January 1 – December 31, 2002



[1] Figure is using the Census 2002 state population estimates (source: U.S. Census Bureau) 99% of the 161,819 total victims reporting indicated their state of residence.

Federal Trade Commission
Consumer Sentinel, 2003

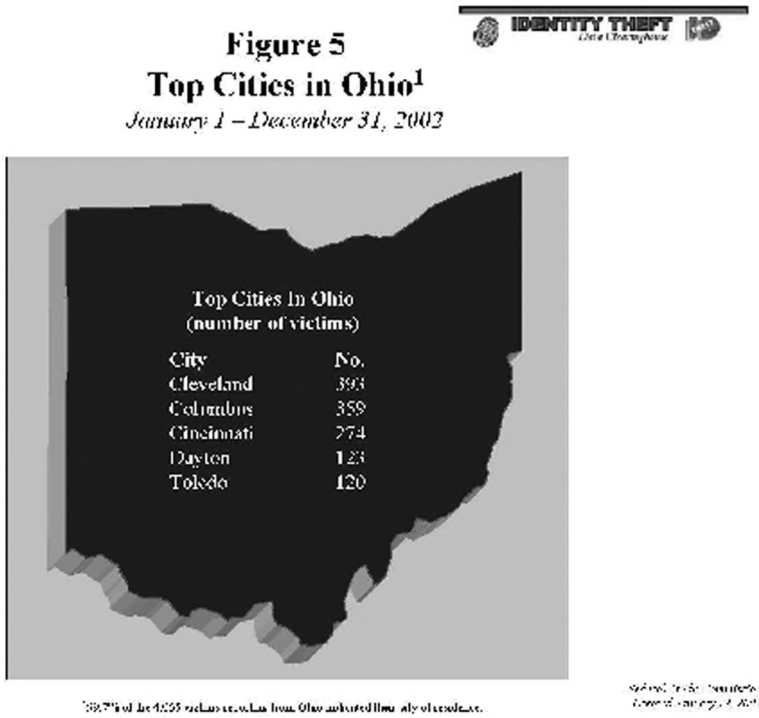
IDENTITY THEFT

Figure 4b
Identity Theft Victims by State (Per 100,000 Population)[1]
January 1 – December 31, 2002

Rank	Victim State	Victims Per 100,000 Population	Number of Victims	Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	District of Columbia	123.[illegible]	704	27	Rhode Island	39.2	41
2	California	99.7	33,738	28	Delaware	38.7	303
3	Arizona	88.0	4,517	29	Minnesota	38.1	1,872
4	Nevada	85.3	1,705	30	Ohio	35.8	4,065
5	Texas	68.9	14,257	31	Tennessee	34.5	1,962
6	Florida	68.2	10,898	32	Kansas	33.2	892
7	New York	66.9	12,698	33	Wisconsin	33.1	1,777
8	Washington	66.1	4,194	34	Oklahoma	32.4	1,118
9	Maryland	66.0	3,492	35	North Carolina	32.0	2,839
10	Oregon	64.3	2,230	36	Arkansas	30.1	806
11	Colorado	61.8	2,960	37	Louisiana	29.7	1,329
12	Illinois	60.5	7,476	38	Alabama	28.7	1,276
13	Georgia	57.5	4,709	39	Mississippi	28.6	814
14	New Jersey	57.1	4,832	40	New Hampshire	28.2	365
15	Hawaii	48.9	593	41	Idaho	27.9	351
16	Virginia	48.0	3,595	42	Nebraska	26.5	454
17	Michigan	47.2	4,640	43	Wyoming	24.9	123
18	Missouri	45.7	2,558	44	Montana	24.5	221
19	New Mexico	45.2	822	45	Maine	24.0	306
20	Indiana	43.8	2,612	46	Kentucky	23.8	977
21	North Carolina	43.8	3,734	47	West Virginia	19.9	360
22	Pennsylvania	41.[illegible]	5,030	48	Iowa	18.5	552
23	Massachusetts	40.9	2,597	49	Vermont	17.6	107
24	Connecticut	40.6	1,393	50	South Dakota	16.4	124
25	Utah	39.7	886	51	North Dakota	12.6	81
26	Alaska	39.6	248				

[1] Figure is using the Census 2002 state population estimates (source: U.S. Census Bureau) 99% of the 161,819 total victims reporting indicated their state of residence.

Federal Trade Commission
Consumer Sentinel, 2003



Mrs. TUBBS JONES. It shows that Ohio is 30th in the country in number of States with regard to identity theft. Unfortunately, it shows that the city of Cleveland, which is my congressional district, is number one in the city in the State of Ohio with identity theft issues. I am standing up for all those great people from the city of Cleveland and greater Cleveland.

I am encouraged that we are holding this hearing, Mr. Chairman, and I am looking forward to having the opportunity to work with you to deal with the issue of identity theft because it becomes very, very important, particularly when we begin to talk about those senior citizens who have to go through a long process in order to get through. They are having a hard enough time getting prescription drug discount cards right now, to have to go through this and do anything else. I thank you, Mr. Chairman, and I don't have any time to yield back.

Chairman SHAW. Thank you. Mr. Brady.

Mr. BRADY. Thank you, Mr. Chairman, for holding this hearing, this important issue. Although I will confess there are days as a Member of Congress when I would pay someone to steal my identity, so you would have to take all that goes with it, but you can have it. I want to talk to Ms. Bovbjerg, if I could, about the enforcement issue so we can get a little better picture. We talk about this at each of the hearings, but who is responsible for ensuring that businesses and those to whom they sell SSNs only disclose according to law? Who monitors the day-to-day release? Who prosecutes

them, and how many businesses, I don't need the number, but how often do we really go after those who are breaking the law in this matter and what kind of penalties do they get?

Ms. BOVBJERG. With regard to the private sector, I want to be careful with how I talk about this. The business that is collecting the number, the consumer reporting agency, there are rules about how they can disclose and what they can do with the other entity with whom they are doing business.

What happens after it goes to the other entity, who knows? It seems like something of an honor system where, if it happens to you or to me that our identity is stolen, we might ultimately track it back to that entity and we would file a complaint and there would be Federal law enforcement involved. I am a little bit concerned that it seems very indirect. Our sense is that the collecting entity is complying with the law. They seem concerned about that; they have made changes to their systems to do that, but once they have that contract with the other entity, that the other entity signs and says we know we are not supposed to disclose and we are not going to do it, who knows what happens after that? It is sort of a very trusting kind of a system.

Mr. BRADY. So, do we often catch bad actors violating the law?

Ms. BOVBJERG. With that, I would have to turn to the law enforcement folks at the table. It is too bad the FTC person isn't still here.

Mr. BRADY. Jump in.

Mr. MAXWELL. As I keep alluding to the numbers, it is one of our largest proportion of criminal prosecutions in our cases; of 10,000 arrests, we arrest 3,000 for identity theft alone, not to mention the number of investigations that we conduct just involving identity theft. The fact that it is so widespread, the fact that the Internet has generated vast numbers of opportunities for these people to conduct the fraud in combination with the mail really enhances our field for it. However, as your colleague alluded to before, depending on the district, the prosecutions may differ. There may be higher guidelines for prosecution than in others.

We do take our cases to the State offices as well if we can't get prosecution Federally and we think it is a very good case but resources do not permit, or other reasons. Sometimes we have had luck there. I don't have the numbers in my head from that, but I could provide those if that would be a benefit to anyone here.

Mr. BRADY. What kind of penalties do the businesses face if they release unauthorized numbers?

Mr. MAXWELL. That I would have to refer to probably be more of a——

Mr. O'CARROLL. That is really outside of our purview on the information that businesses release. The FTC probably would have been the best to speak on that, Mr. Brady.

Mr. BRADY. So, you do the prosecutions, you do the investigations, but you don't track what the ultimate outcome is?

Mr. MAXWELL. Oh, yes. No, we do in our cases. We take a case from opening to closing. If we have a complaint or if we identify a situation, we will investigate it, we will follow it through, we will present it to the U.S. Attorney, and we will sit at the table with

them if there is a trial. We don't close the case until there is a conviction and a termination.

Mr. BRADY. What kind of penalty? What would be an average? What happens?

Mr. MAXWELL. It depends on the statute that is used. Sometimes it is 1029, which is the access device. That is primarily a Secret Service jurisdiction. Our favorite and the one that we hold claim to is mail fraud. So, again, it could take penalties up through prison term over 5 years, depending on what is adjudicated based on the guidelines, the sentencing guidelines, and moneys can be up to 10,000 or more depending on the severity.

Mr. BRADY. What is the most common case? Someone who has a pattern and has done a number of these fraudulently, for a first offense, what are they going to get?

Mr. MAXWELL. The first offense. I would suspect again, I cited the Carl Lomax case in Pittsburgh last year, and he took the identity of several celebrities, notably Will Smith, the actor. I forget what he was sentenced to exactly, but it was several years in prison, probably under f5, with penalty, but he agreed to cooperate with us. There is often an incentive there for them to cooperate. He produced a video telling the different techniques he has, so we can use that for our training, but the average, it would be hard for me to say without averaging it, taking a look.

Mr. BRADY. Do we need stronger oversight and stronger penalties?

Mr. MAXWELL. I am more of a fan of the prevention ends. I think our criminal statutes, Congress has definitely equipped us well. It is a matter of getting access to information, it is a matter of people knowing who to report it to. It is a matter, as earlier discussed, of cooperation with the private sector, with the companies which we address through different task forces. Any encouragement coming from the Federal Government certainly helps. I think as far as the statutes that are now on the books, I think we are fine. We are happy with mail fraud and 1029.

Mr. BRADY. I guess my thought, and I will wrap it up with this, Mr. Chairman, is that I think there are a lot of things we can do on prevention. I worry that the horse is out of the barn on SSNs; that one of the things we can do is to try and discourage bad actors from using them in fraudulent ways. The way you do that is to make it pretty tough on those who do and introduce some element of you may well get caught in doing this even on a smaller scale. That always means more resource and different approaches, but prevention we have got to do much more there. We talk about it a lot, but, I think we also, whatever we can do on enforcement I think may help the numbers that are already floating out there, which is probably everyone in this room, by the way.

Mr. MAXWELL. One of the things that I often refer to in a strategy is, you can work a number of cases and that looks good, but if you work several with some notable names, that brings it to the forefront in the media, like this Will Smith case. We also used Jerry Orbeck in that campaign over there, where he was a victim of identity theft and he talked specifically of his individual case. The public often can recognize an affinity with that celebrity. So, that helps, too. So, yes, you are right. Deterrence, the arrests, but

also get it out in the media, get it out, announced, and talk about it.

Mr. BRADY. Thank you, panel. Thank you, Mr. Chairman.

Chairman SHAW. I thank all of you. Mr. Pomeroy tells me that his questions have been answered by the witnesses. So, this panel is dismissed with our appreciation. Thank you very much. The current status of the Committee is that the bells that you heard have been calling us to the floor. We have been told that there are going to be four votes. That takes a little while, but what I would like to do is to introduce the second panel, and then we will recess until approximately 1:00 pm. That will give everyone a chance to taste the wonderful food we have here in the Capitol. You have eaten here before, huh?

The next panel will be made up of Patricia Foss, from Elkton, Maryland. Mark Ladd, who has already been introduced as the Public Sector Co-Chairman of Privacy/Access Workgroup (PRIA) from Wisconsin. Chris Hoofnagle, Associate Director of the Electronic Privacy Information Center (EPIC). Brian McGuinness, who is the First Vice President of the National Council of Investigation and Security Services (NCISS). He is from my State in Miami, Florida. Mike Buenger, who is the President of the Conference of State Court Administrators (COSCA), Jefferson City, Missouri. Mr. Hulshof wants to introduce him, so I will yield to Mr. Hulshof at this time.

Mr. HULSHOF. As I referenced earlier and had a chance to chat with Mike, it is great to have him here. Not only is he our State Court Administrator, but he is the President of the national organization. We are honored to have him here today, Mr. Chairman.

Chairman SHAW. Thank you. We also have Fred Cate, who is Professor of Law at the University of Indiana, and Edmund Mierzwinski, who is the Consumer Program Director of the U.S. Public Interest Research group (PIRG). We welcome all of you, and we look forward to seeing you at 1:00 p.m.. We will stand in recess.

[Recess.]

Chairman SHAW. If the witnesses will take their seats, we will resume the hearing. Thank you for tolerating our schedule, which is always somewhat unpredictable. Ms. Foss, you are going to lead off, please.

STATEMENT OF PATRICIA FOSS, ELKTON, MARYLAND

Ms. FOSS. Thank you, Mr. Chairman, for the opportunity to talk about my experience as an identity theft victim and also know that I, as a victim, applaud you all for looking at this serious issue. Like millions of Americans, my experience began when I was notified by my bank that my credit had been suspended due to nonpayment. After contacting the bank, I learned to my surprise another woman had received thousands of dollars of credit using my name and my Social Security card. She had my birth date off by 1 day. I was stunned to learn that she had gotten a home improvement loan from one bank and an automobile loan from another bank. I am not sure about the car, but we know she did not have a home. My SSN virtually gave her everything she needed to steal my good name and my good credit.

That was the day I received an introduction to the crime of identity theft and how easy it was to be a victim, even when people like me are extremely careful of their personal information. I was fortunate enough when I was talking to the bank to receive good advice from them about what I had to do next and who to contact and what agencies I needed to talk to. That was when the real work began. I understand that an average identity theft victim spends over 30 hours trying to clear their name and prove their innocence. I can tell you I definitely exceeded that, especially if you count the nights when I laid awake and wondered what was going to happen next.

At the time that this happened to me, it was back in 1999 and it really wasn't a common thing at the time, so I and countless other people hadn't even heard of what it was. It took a lot of my time, my life away from me. This is the example of the file that I kept for a year of trying to get all the paperwork done that was required of me to prove that I was indeed who I am. It was, seriously, like having another job. I had to send to each credit bureau as well as countless banks that the other me had used notarized letters and documents like my birth certificate and my driver's license and including my SSN. It was kind of ironic, because I felt more vulnerable having all that information now out there for countless other strangers in trying to prove my innocence than I had ever done before the crime happened in the first place.

I spent hours on hold, and I spent hours in transfer hell. I had to take time off of work to visit my own bank and get things notarized pretty much on a daily basis at least for the first couple of months, and it really took me over a year of dealing with at least 20 different organizations to completely clear the credit reports and prove that I was the victim and not the criminal. I still check my credit reports at least biannually for fear that either this woman or somebody else is going to use my identity again.

In hindsight, I was really one of the lucky people. Unlike many cases, the police actually arrested the woman who was impersonating me. She was, ironically, an acting student. I thought that there was some humor in that. I was told that she walked in one of the banks that I had reported the crime to and was leisurely making another withdrawal out of an account that she had in my name. After she was caught, I was afraid that she also had my home address and there would be repercussions once she found out that I had turned her in, and so I spent a few nights in fear over that. I completed a form to be notified as to what had happened in her trial, and the next I heard was last week when I was asked if I could testify before this Committee. I know since my experience numerous State and Federal laws have been passed to criminalize identity theft, and I think it is better than it was when this happened to me, but I would say that much more still needs to be done, because the number of identity theft victims continue to increase every year.

Chairman Shaw, I applaud your efforts to restrict the dissemination of SSNs. To this day, I still don't know how this woman got mine. No one does, and she didn't admit anything when she was prosecuted, apparently. As you go through your deliberations I guess I would ask you to consider the following things: I believe

that credit grantors are a big part of the problem. I don't understand why they don't check more into people's credentials before they hand them money. If they don't follow those kind of procedures, shouldn't they be somehow accountable in some ways? I can't understand that kind of carelessness as what happened with me.

Also, I guess I would ask, where is the funding for enforcement? I know that there are punishment penalties in the bill. If there is not money for enforcement, I can't imagine that many of these people are going to be caught. Truly, the heroes in my story were the police, one bank's fraud officer, the postal inspectors and the special agents in the Social Security Office of the Inspector General, but I was one of the lucky ones. Last, I feel that I would like to see more funding for agencies like the SSA or some agency so that people like me could have a central point of contact and somebody to help them through the mass of paperwork that is required of them. Thank you again for letting me tell my story.

Chairman SHAW. Thank you. If I may, just out of curiosity, was she found guilty and what was her penalty?

Ms. FOSS. I just found that out yesterday, which was interesting. She was prosecuted. She was found guilty. The sentence was, I believe, 6 months; and she was required to pay back $69,000 in restitution to the organizations that had given her the money.

Chairman SHAW. So, the system worked in your case.

Ms. FOSS. The system worked in my case, but it sure took a long time.

[The prepared statement of Ms. Foss follows:]

Statement of Patricia Foss, Elkton, Maryland

Chairman Shaw and members of the committee, thank you for the opportunity to talk about my experiences as a victim of identity theft. I'm grateful to you for addressing this critical issue.

Like millions of other Americans, my experience began when I was notified by my bank that my credit had been suspended because of non-payment. After contacting the bank, I learned to my surprise that another woman had received thousands of dollars of credit using my name and my perfect credit history. I was stunned to learn that she had obtained a home improvement loan at one bank, and an automobile loan from another. My social security number had provided her with the access she needed to damage my good name and credit.

That was the day I received an introduction to the crime of identity theft, and how easy it was to become a victim, even when you're careful about your personal information.

I was fortunate enough to receive good advice from my bank, MBNA, and was provided information on how to respond. But that was where the real work to prove my innocence began. I understand that on average an identity theft victim spends over 30 hours proving their innocence. I'm sure I exceeded that number, especially if you count the nights I lay awake wondering where she would strike next. She not only stole my identity, she took weeks of my life away from me.

I had to send each credit bureau, as well as the countless banks the other "me" had used, notarized letters and copies of documents like driver's license and birth certificate. I spend hours on hold and in transfer hell. I had to take time off of work to visit my own bank, and had to deal daily with proving I was the real Patricia Foss. It was truly like having a second job.

It took me almost a full year of dealing with over 20 different organizations to completely clear my credit reports and prove that I was the victim, and not the criminal. I still check my credit reports biannually with the fear that sooner or later, this woman, or someone else, will use my identity again.

In hindsight, I was one of the lucky ones. Unlike many cases, the police actually arrested the woman who stole my identity. She was appropriately, an acting student. I was told that she walked into one of the banks to which I'd reported the

crime and was leisurely making another withdrawal. After she was caught, I was afraid that she also had access to my home address and would threaten my safety once she realized that I'd reported her crime. I had completed a form to request that I be notified of the outcome of her trial. That was the last I heard until last week when I was contacted about testifying before this subcommittee.

I know that since my experience, numerous state and federal laws have been passed to criminalize identity theft. More obviously needs to be done as the number of identity theft victims continues to increase every year.

Chairman Shaw and members of the subcommittee, as a victim, I applaud your efforts to restrict the dissemination of social security numbers. To this day, I still do not know how this woman impersonating me obtained mine. As you go through your deliberations, I would also ask you to consider the following;

- Credit grantors continue to be a part of the problem. Shouldn't banks and other credit grantors be required by law to conduct a more complete check of credentials before handing people money? If they don't follow such procedures, shouldn't they be held accountable in some way? I do not understand how they can afford to be so careless.
- Where is funding for enforcement? I was pleased with the provisions to add more criminal penalties to punish identity theft criminals. But if there isn't money for enforcement, they won't be caught in the first place. The heroes in my story were the police, one bank's fraud officer, and the postal inspectors. But then, I was lucky.
- More funding is needed for agencies like the Social Security Administration to help victims have a central point of contact and assistance negotiating the mass of paperwork required to clear their name.

Thank you for the opportunity to speak with you about my experience.

Chairman SHAW. Yes. Mr. Ladd.

STATEMENT OF MARK LADD, PUBLIC SECTOR CO-CHAIR, PRIVACY/ACCESS WORKGROUP, PROPERTY RECORDS INDUSTRY ASSOCIATION, RACINE, WISCONSIN

Mr. LADD. Good afternoon, Mr. Chairman. Again, I am Mark Ladd. I am the Register of Deeds for Racine County, Wisconsin; and I am the Public Sector Co-Chair for the PRIA's Privacy/Access Workgroup. I appreciate the opportunity to come and speak regarding H.R. 2971 and its impact on land records custodians. The collateralization of real property is a fundamental part of our economy. Leveraging real property is possible because of the publicly available information regarding a specific parcel of land. Our Nation's private ownership of land is based on a necessary access to publicly recorded land information.

On the other hand, citizens are concerned that personal information is sometimes contained in these real property records and can be used for identity theft. By example, SSNs are often included in mortgage documents, tax liens, divorce decrees and other documents that convey real property. However, for land records custodians, there is little legal purpose for having that number included in the record.

The PRIA hosted a roundtable forum on this topic back in February of 2003. We had 25 different roundtable participants with a broad range of industry expertise: State, local government, Federal government representatives, land records officials, trade associations from the real estate industry, as well as a couple of organizations dedicated to consumer privacy. At the conclusion of the roundtable, we actually spun up a Privacy/Access listserve, an e-mail discussion to continue to foster additional conversation on the

topic. That list serve discussion was followed up by 2 days of facilitated educational discussions during our winter conference earlier this year. In the discussions, we reviewed the historical foundations of American's land records system and our public records laws and then we debated several suggestions for model legislation.

It is with this background in mind that I would like to offer our comments regarding H.R. 2971. Section 101 of the bill prohibits the display to the general public of a SSN and then goes on to define "display" as posting on a website. Well, the Internet has become an important tool for many land records custodians to publish records. More and more counties are developing Internet-based sites designed so that citizens can conduct business with government when it is convenient for the citizens, and these sites often include data as well as images of documents.

Now, again, our discussions show that few occurrences of the SSN land records are required by government agencies or required by land record agencies, but, rather, they may be required by the Internal Revenue Service or State taxing authorities. A lot of times SSNs appear in a document, and they are placed there by the document preparer for the benefit of their business process or the business process of one of their partners. However, we have no statutory authority under current law to refuse to enter these documents into the public record. In its current form, this bill would prohibit us from using the Internet to post our records, and this removes an important tool from our use. Another thing to note is, even with this provision, SSNs can still become part of the public record and an individual's privacies are at risk in the courthouse because, again, these are public records that anyone can come and obtain. We would think that there are several elements that need to be addressed in any type of legislation to deal with this issue.

First, we applaud this provision of H.R. 2971 in that this needs to be on a day forward basis. Redaction and the expunging of the records is physically difficult, if not impossible. The prohibition should be on putting the SSN in any document that will become part of the public record, and this should also include the authority to public records officials to reject the recording. However, that authority needs to be permissive, rather than prescriptive. Prescriptive authority is impossible for us to manage. The sheer volume of documents to check for that SSN in a 27-page mortgage, in an office of my size only 300 documents a day, in larger offices thousands of documents a day, it is just impossible to manage.

If a document contains a SSN, after this law is adopted, we would suggest that land records officials be empowered to redact the number. That is an important provision for an administrative function that we provide. Providing certified copies of documents requires us to provide an exact copy of the document that was presented to us. Without that type of authority, we can't fulfill that role. Again, we recognize that it is an impossible task for land records officials to manage. We are poor gatekeepers, just due to the size of the task, but we believe that our recommendations can provide the goal of protecting SSNs without jeopardizing the flow of commerce or placing an unbearable burden on the shoulders of local government. I look forward to answering further questions as the hearing continues. Thank you.

[The prepared statement of Mr. Ladd follows:]

Statement of Mark Ladd, Public Sector Co-Chair, Privacy/Access Workgroup, Property Records Industry Association, Racine, Wisconsin

Good morning Mr. Chairman and members of the Committee:

My name is Mark Ladd. I am the Register of Deeds for Racine County, WI, and I am the Public Sector Co-Chair of the Property Records Industry Association (PRIA) Privacy/Access workgroup. I appreciate the opportunity to speak to you today regarding personal information and privacy issues as it relates to the land records industry.

The PRIA is a public/private partnership and its mission is to work together to identify issues, define problems and develop solutions to bring consistency to the property records industry. The PRIA membership includes over 260 land records officials and 105 private sector partners. The PRIA has completed projects such as developing a document-formatting white paper, notary essentials white paper and created the model statute for Military Discharge (DD214s) documents and developed the Military Discharge DD214 Tangible Interest form. The PRIA currently has several projects in development including, Electronic Recording Standards in alliance with the Mortgage Bankers Association; Archival Back-up and Disaster Recovery; Parcel Code Review; 1st Page Indexing Requirements and the Records Access Policy Advisory Committee.

The collateralization of real property, often taken for granted, is a fundamental part of our economy. Leveraging real property is possible because of the public availability of information regarding a specific parcel. Our nation's private land ownership is based on necessary access to publicly recorded real property information. For many reasons, the property record system requires that the general public have a right to know who owns or has certain interests in real property. Two of these reasons, for example, are:

(1) to protect the investors lien rights, and

(2) to assure fair assessment and taxation of like properties.

On the other hand, citizens are concerned that personal or sensitive information is sometimes contained in real property records and may be used for criminal intent, such as identity theft. An example of sensitive information with little legal purpose to protect investor lien rights, yet quite useful to identity thieves, is a Social Security number. Social Security numbers can appear in some mortgage documents, tax liens, or even a divorce decree that conveys real property.

Privacy interests and the interest for disclosure of land records information often appear at odds with each other. This poses a dilemma for land records officials attempting to balance these two points of view. This is perhaps one of the greatest public policy questions faced in recent years. The PRIA is convinced that a workable balance can, and in fact, must be reached on this issue. That balance should protect personal privacy without impeding commerce or overburdening land records offices.

Realizing there was little or no communication between various groups within the United States regarding Privacy and Access issues, the PRIA convened the nation's first roundtable forum in WashingtonD.C. on February 26, 2003 to discuss this issue.

The 25 roundtable participants covered a broad range of industry representatives including representatives of the federal government (IRS and GAO), state and federal court systems, Land Records Officials, national associations in the real estate industry including the National Association of County Recorders, Election Official and Clerks, the International Association of County Recorders Election Officials and Treasurers, the American Land Title Association, the American Escrow Association, the National Public Records Research Association, the Mortgage Bankers Association, the Appraisal Institute, American Bar Association, national credit bureaus, as well as two of the most influential organizations dedicated to consumer privacy issues. In addition, there were 150 registered observers, representing a broad spectrum of the industry.

Several topics were covered during the roundtable in a lively, thought provoking, daylong discussion. The PRIA has minutes and created a CD, both are available on the PRIA website located at www.pria.us

At the conclusion of this meeting the PRIA formed a committee to continue to advance this issue. A Privacy/Access listserve was established as a forum to foster additional discussion on the topic of personally identifiable information contained in public records. The listserve activity included a discussion of:

(1) what information is required for the conduct of commerce?

(2) could rules relating to document creation address the needs of all interested parties? and

(3) should we consider restricting access to certain types of records?

The list serve discussion was followed by two days of facilitated educational discussions during our 2004 Winter Conference in Washington D.C. During these discussions PRIA members reviewed the historical foundations of American public records and then addressed the policy issue by debating several suggestions for model legislation.

It is with this background in mind that we offer the following comments relating to HR 2971.

Section 101 of the proposal contains a prohibition of the "display to the general public" of a Social Security number (Page 3, Lines 18 &19). "Display" is later clarified as "to intentionally place such number in a viewable manner on an Internet site."

The Internet has become an important tool for many land records custodians to publish records. More and more counties are developing what is being called a "virtual courthouse." These Internet based sites are designed so that citizens can conduct business with government when it is convenient for the citizen and these sites can include data as well as images of documents.

The PRIA discussions reveal that few occurrences of the Social Security number in land records are required by any government agency with the exception of the IRS and state taxing authorities. For non-taxation documents, the Social Security number is normally included by the document preparer for the benefit of their business practices or that of a business partner. While the problems associated with this practice may seem obvious to us, this is a standard practice with a number of financial institutions. Land records officials have no statutory authority under current law to refuse to record such documents.

In the bill's current form, this provision would prevent land records custodians from posting currently recorded land records on the Internet, thus removing an important tool from our use.

Another provision of Section 101 further defines a Social Security number as "any derivative of such number" (Page 5, Lines 20 & 21).

Some land records officials have had conversations with the IRS regarding removing the Social Security number from Federal Tax Liens. One solution often repeated by the IRS is including only the last four digits of the Social Security number. This would appear to be a violation of this provision. Since Federal Tax Liens attach to an individual and not a specific parcel of real property, it will become very difficult for title searchers to determine the applicability of these liens.

Section 102 requires the Attorney General to consider the cost or burden to local governments of complying with the restrictions imposed by any rules to be adopted under this bill (Page 8, Lines 1–7).

This clause is helpful, as the task of assuring that documents, some of which may be quite voluminous, do not contain Social Security numbers, represents a Herculean undertaking on a daily basis, even in the smallest of jurisdictions.

Using Racine County as an example. Racine County has a population of 190,000—a medium sized county. In 2003 Racine County recorded just under 80,000 documents that contained approximately 400,000 total pages. That equates to 1600 pages that must be reviewed by a staff of 6, every business day. During most of 2003 the office was operating with a backlog of 2–3 weeks, without any requirement to search for Social Security numbers in the documents.

Most of the review that staff performs on real estate documents is done by checking the first and last pages of a document. If we were required to check for the inclusion of a Social Security number, which could be anywhere in the document, it would more than double the task of reviewing documents.

From a national perspective there were approximately 125 million real property documents recorded in 2003.

Section 201 moves to another area that local government offices administer, specifically, birth records. This section contains a requirement to independently verify any birth record provided in support of the application process (Page 20, Lines 21–23).

The PRIA would like clarification of this provision's intent and impact. Our concern is that vital record offices issue certified copies of birth records that contain a certification statement that includes the issuing officer's signature and the department seal. Most states have adopted (or will soon be adopting) standards for security paper to be used for these certificates. These standards include features that make the paper tamper evident. Independent verification from State and local offices would only be necessary when a certificate appears to have been altered or is not on security paper.

The financial burden to state and local governments in implementing any aspect of this provision should be addressed as well.

Section 201 goes on to require a feasibility study, which includes the costs of electronic third party verification of identity documents (Page 21, Lines 16–21).

Most state and local offices are only beginning to investigate the costs of developing such systems. We cannot overstate the fact that the current fiscal environment faced by most state and local governments makes this type of development a challenge even when policy makers support the goals and benefits of such an undertaking.

In Wisconsin, I serve on the committee that has been assembled by the Department of Health and Family Services Vital Records Bureau to develop the specifications for such a system. My optimistic estimates are that this project could be minimally operational in two to four years with a mature system being six or more years down the road.

As I stated in my introductory remarks, the Property Records Industry Association has had extensive discussions regarding this topic and I would now like to offer our suggestions as to elements that this type of legislation should encompass.

1. Legislation should be effective on a "day-forward" basis. It should not require redaction or expungment in records already filed or recorded.

2. Consider prohibiting the inclusion of Social Security numbers on documents that will become part of the public record. This could include providing land records officials the authority to reject a document for filing/recording that includes a Social Security number. Practically speaking however, rejection authority needs to be permissive rather than prescriptive. As I described earlier, the shear volume of documents and the number of pages involved will make prescriptive authority difficult to manage.

3. Next we suggest that if a document recorded after the effective date of the legislation contains a Social Security number, the land records official should have the authority to redact the Social Security number from the document.

This is an important provision for an important ministerial function—that of providing certified copies of records in our offices. Our certification statement requires that we provide an exact copy of a recorded document. We need to be explicitly empowered to redact the Social Security number without compromising the integrity of future certified copies we issue.

4. The PRIA acknowledges the nearly impossible task faced by land records officials in attempting to keep Social Security numbers out of the public record and it believes this responsibility is more properly placed on document preparers and individual consumers. Accordingly, PRIA believes that, for any law prohibiting a Social Security number in land records, land records officials should be immune from suit relating to documents filed/recorded that include Social Security numbers.

While land records officials will assist when and where they can, the scope of the task of checking every page of every document for Social Security numbers is simply beyond their ability to perform. The time to prevent Social Security numbers from becoming part of the public record is when the document is created—before the parties execute them, not when they are presented for recording.

There is simply too much dependence in today's marketplace on the social security number. The PRIA believes education is a major component in developing solutions to this problem. Already we are seeing insurance companies and others using an alternative ID number on insurance cards rather than the social security number.

Utilizing existing associations such as the PRIA, Mortgage Bankers Association, Fannie Mae, Freddie Mac, American Land Title Association, American Escrow Association, etc. and with the help of the federal government, this problem can be drastically reduced if not eliminated.

Thank you for giving the PRIA the opportunity to address this important public policy issue. Our discussions and policy debates instruct us that the time to address this problem is during the drafting of the documents. We believe that our recommendations can achieve the goal of protecting Social Security numbers in regards to the public record without jeopardizing the flow of commerce or placing an unbearable burden on the shoulders of local government.

Chairman SHAW. Thank you, Mr. Ladd. It sounds like you may need a State statute. Mr. Hoofnagle.

STATEMENT OF CHRIS JAY HOOFNAGLE, ASSOCIATE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. HOOFNAGLE. Thank you, Chairman Shaw, for holding this hearing today and for continuing to build a rich legislative history on why Congress needs to act to enhance the privacy and integrity of SSNs. My name is Chris Hoofnagle. I am Associate Director with the EPIC. We have been involved with SSN regulation for many years and also in litigation. We filed an amicus brief in a very important case known as the Amy Boyer case where a woman was located and essentially stalked through the help of a data broker and a private investigator. We have submitted detailed written testimony for the record today. I just want to highlight some of the points we make in this written testimony, and I look forward to your questions afterward.

As you are well aware, today the SSN plays an unparalleled role in identification, authentication and tracking of Americans. Its use in the public and private sector heightens the risk of identity theft and abuse because institutions use the SSN both to identify people but also to authenticate them. So, Representative Tubbs Jones was bringing up this issue earlier, the same number you use to identify a credit file is often used to authenticate or to verify the identity of someone; and from a security standpoint, that is a major risk. It is not unlike choosing an e-mail address and using your e-mail address as the password, the exact same series of letters.

The other issue I wanted to highlight from our testimony is the role that public records play in providing personal information to commercial data brokers and to others who are amassing personal information about individuals. Oftentimes we are compelled by law or compelled from wanting to enjoy the rights and benefits of our society into providing personal information that ends up in a public register; and once your SSN or other information ends up in a marriage license or a land record, anyone can come along and use that personal information for any purpose. So, we do think that it is important in your legislation to include strong language keeping the SSN, and keeping certain personal identifiers out of public records before they reach the general public.

There are several parts of H.R. 2971 that we think are very strong, and they belong in any SSN privacy bill. The first is the provision on coercive disclosure. We think it is very important that businesses not be able to withhold a product or service when they ask for a SSN without authority to do so, and I think that your legislation is well crafted in section 109 because businesses that actually have a legal right to the identifier will still be able to request the SSN. We think it is very important that Section 108 be included in any legislation that moves to the full House. section 108 would move the SSN below the credit header line and require individuals who are trying to buy SSNs to have a permissible purpose under the Fair Credit Reporting Act before getting access to the identifier. I think that is a very important protection, and we commend you for including it in the legislation.

Finally, we think it is very important that States be discouraged from placing the SSN on drivers' licenses and other identifiers provided to individuals. We would recommend one enhancement to the legislation in this regard. We have become aware that some States

do not put the SSN on the actual card. They don't publish it on the card, but they embed it into the bar code or into the magnetic strip, and then businesses or other individuals can swipe the driver's license and collect the SSN from individuals. I think it is important that prohibitions recognize the risk of automated data collection from drivers' licenses and how SSNs might be swept in that equation.

We also encourage you to look to the leadership of the States in developing SSN legislation. A number of States have passed very strong regulations that deal with use of SSN in the private sector, the use of the SSN in the context of colleges and universities and with regards to course of disclosure; and their leadership should be emulated at the Federal level.

As I am running out of time, let me highlight what Ms. Foss said earlier about the role of credit granting and identity theft. In our written testimony we have given numerous examples of cases where victims had their identities stolen and it would not have occurred but for the presence of the SSN. The identity thief filled out an application to get credit. Oftentimes, the date of birth was wrong, the name was wrong, address was wrong. The SSN was right, and so the SSN was a key to identity theft in all of those cases, and it sounds as though those cases are similar to yours, Ms. Foss. So, we encourage an examination of credit granting practices as well, it appears as though they are contributing to the identity theft problem. Thank you, Mr. Chairman. I look forward to your questions.

[The prepared statement of Mr. Hoofnagle follows:]

Statement of Chris Jay Hoofnagle, Associate Director, Electronic Privacy Information Center

Introduction

Chairman Shaw, Ranking Member Matsui, and Members of the Subcommittee, thank you for extending the opportunity to testify enhancing the privacy and integrity of Social Security Numbers.

My name is Chris Hoofnagle and I am associate director 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/.

In previous testimony to this Subcommittee, EPIC has recommended a strong framework of Fair Information Practices to create rights and responsibilities for individuals and collectors of the SSN. In 2001, EPIC Executive Director Marc Rotenberg traced the history of the SSN as an identifier, highlighted the use of the SSN in the financial services sector, and raised privacy issues associated with the Social Security Administration's Death Master File.[2] In 2002, EPIC testified that the problem of identity theft had grown worse, that the states were acting to limit collection and disclosure of the SSN, and that 107 H.R. 2036, the Social Security

[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/.

[2] *Social Security Numbers and Identity Theft, Joint Hearing Before the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security,* Nov. 8, 2001 (testimony of Marc Rotenberg, Executive Director, EPIC), available at http://www.epic.org/privacy/ssn/testimony_11_08_2001.html.

Number Privacy and Identity Theft Protection Act of 2001 could limit misuse of the SSN.[3] In 2003, EPIC appeared again to testify in favor of privacy protections, highlighting recent abuses, the continuing unnecessary use of the SSN as an identifier by both private and public sector entities, and the developing trends of state legislation crafted to limit collection and use of the identifier.[4]

Chairman Shaw, we commend you for developing a rich legislative record on the need to protect the SSN and to combat identity theft. In today's testimony, we wish to continue to contribute to the record and make a recommendation that you advance legislation to secure the SSN and protect Americans from identity theft. First, we provide an overview and recommendations for 108 H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003. Second, we highlight examples of state SSN regulation that could be adopted at the federal level to provide an umbrella of protections for the SSN. In the third section, we argue that identity theft is caused by excessive reliance on the SSN and by lax credit granting practices.

I. Recommendations for 108 H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003

Introduced in July 2003, H.R. 2971 is the latest of a series of bills designed to enhance protections for the SSN and to promote the integrity of the identifier. It enjoys bipartisan support in the House of Representatives.

Title I of the bill sets forth limitations on government disclosure of SSNs. Broadly put, this title would prohibit executive, legislative, or judicial entities from disclosing the SSN, subject to certain exceptions.

We think it important to limit the exceptions for governmental sale of the SSN. Specifically, we recommend that subsection (V), which allows unlimited sale of SSNs to thousands of credit reporting agencies (CRAs), be removed from the bill. This exception is too broad and allows unrestricted transfers of government records containing social security numbers to CRAs, possibly for purposes unrelated to credit reporting, including direct marketing.

It is not the role of government to collect SSNs from citizens, who are often under legal compulsion to provide the identifier, and then release the SSNs to the private sector for the purpose of compiling dossiers. Professor Daniel Solove has fully articulated how this model of information flow is unfair to individuals and privacy invasive:

> Imagine that the government had the power to compel individuals to reveal a vast amount of personal information about themselves—where they live, their phone numbers, their physical description, their photograph, their age, their medical problems, all of their legal transgressions throughout their lifetimes whether serious crimes or minor infractions, the names of their parents, children, and spouses, their political party affiliations, where they work and what they do, the property that they own and its value, and sometimes even their psychotherapists' notes, doctors' records, and financial information.
>
> Then imagine that the government routinely poured this information into the public domain—by posting it on the Internet where it could be accessed from all over the world, by giving it away to any individual or company that asked for it, or even by providing entire databases of personal information upon request. In an increasingly "wired" society, with technology such as sophisticated computers to store, transfer, search, and sort through all this information, imagine the way that the information could be combined or used to obtain even more personal information.[5]

If this exception remains in the legislation, we recommend that it be narrowed. Currently, the exception allows disclosure of the SSN to CRAs without any limitation on use of the identifier. A narrower exception would allow disclosure but limit use of the identifier for "credit reporting practices consistent with the Fair Credit Reporting Act, 15 U.S.C. 1681."

---

[3] *Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves, Joint Hearing Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims,* Sept. 19, 2002 (testimony of Chris Jay Hoofnagle, Legislative Counsel, EPIC), available at http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[4] *Hearing on Use and Misuse of the Social Security Number, Hearing Before the House Ways and Means Subcommittee on Social Security,* July 10, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, EPIC), available at http://www.epic.org/privacy/ssn/testimony7.10.03.html.

[5] Professor Daniel Solove describes this problem in *Access and Aggregation: Public Records, Privacy, and the Constitution,* 86 Minnesota Law Review 1137 (2002), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=283924.

In section 101, we recommend harmonizing the definition of "sale" with other references to the term that appear in the legislation. The definition appearing in section 107, which defines sell as "to obtain, directly or indirectly, anything of value in exchange for such number," is more appropriate.

Section 102 specifies the authority of the Attorney General to create exemptions to the general prohibition on government disclosure of the SSN. We agree with the standard set forth by the legislation—that SSNs should not be disclosed absent a compelling interest that cannot be served through the employment of alternative measures. We are concerned, however, that the Attorney General will still approve of privacy-invasive transfers of the SSN despite this high standard. In documents obtained under the Freedom of Information Act, EPIC has shown that private-sector commercial data brokers (CDBs) play a large role in collecting SSNs and other information for sale to law enforcement.[6] Simply put, there is a risk that the Attorney General will act in self-interest, and approve broad disclosures of SSNs to CDBs that then resell the identifier back to law enforcement or other entities.

We recommend several substantive safeguards against permissive regulations that would allow broad disclosure of the SSN. First, the rulemaking should be open to public comment. Public polling shows that individuals are concerned about increasing use of the SSN; allowing public comment will effectively express popular opposition to expanding use of the identifier.

Second, we think that the qualifier "undue" should be removed from the standard articulated in Section 101 (a)(I)(ii)(II), and that identity theft be added as one of the risks to be considered by the rulemakers. As currently drafted with "undue" as a qualifier and without the special recognition of identity theft as a risk of SSN disclosure, the language will tilt the balance in favor of expanding disclosure of the SSN. A more appropriate balance would be struck with language specifying, "it is reasonably certain that the social security numbers will not be used to commit or facilitate fraud, identity theft, or bodily, emotional, or financial harm."

Third, we think that exceptions to the general prohibition should be limited in duration. A time limit will encourage users of the SSN to transition to alternative identifiers. Exceptions that are not time limited will ensure that SSN users never transition to alternative measures.

Last, entities receiving SSNs should be held to technical safeguards to shield the identifier from employee misuse or theft. We recommend that the following factor be added to the rulemaking: "(III) the social security numbers sold, purchased or displayed will be protected by adequate safeguards, including but not limited to encryption measures and regular auditing of SSN access and disclosure."

Section 103 would codify an important safeguard—a prohibition of printing SSNs on checks issued by governments. This is a common sense protection against identity theft. It is necessary because a standard check with a SSN contains all the personal information necessary for commission of identity theft.

Section 104 would prohibit states from displaying the SSN on driver's licenses. Again, this is a common sense approach to preventing identity theft. Indeed, many states already incorporate a ban on printing the SSN on driver's licenses.[7] Such a prohibition makes it more likely that the SSN will not appear in the wallet of individuals, thus reducing the risk that a lost or stolen wallet will provide the personal information necessary to commit identity theft.

We recommend that section 104 also prohibit states from encoding the SSN on magnetic strips, barcodes, or smartcards on the driver's license, as we are aware that while some states do not print the SSN on the card, they may embed the identifier digitally on the card.[8] Anyone with a card reader can swipe the card and capture the identifier. Increasingly, businesses are capturing patrons' personal data

---

[6] *See e.g.* Electronic Privacy Information Center, ChoicePoint, available at http://epic.org/privacy/choicepoint/; Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement,* University of North Carolina Journal of International Law & Commercial Regulation (Spring 2004).

[7] *See* Ariz. Rev. Stat. § 28–3158; C.R.S. § 42–2–107; C.R.S. § 42–3–302; D.C. Code Ann. § 50–402; O.C.G.A. § 40–3–23; HRS § 286–109; HRS § 286–239; Idaho Code § 49–306; Idaho Code § 49–2444; Ky. Rev. Stat. Ann.§ 186.412; Mont. Code Ann. § 61–5–111(2)(b); Nev. Rev. Stat. Ann. § 483.345;.N.H. Rev. Stat. Ann. § 263:40–a; N.D. Cent. Code 39–06–14; Ohio Rev. Code Ann. § 4501.31; Okla. Stat. Ann. tit. 47, § 6–106 (2002); Pa. Cons. Stat. Ann. § 1510; Tenn Code Ann. § 55–50–331; Tex. Trans. § 521.044; Va. Code Ann. § 46.2–342; Wash. Rev. Code Ann. § 26.23.150.

[8] Beatriz da Costa, Jamie Schulte and Brooke Singer, *Who is Swiping?*, n.d., available at http://www.we-swipe.us/research.html.

from driver's licenses.[9] Removing the SSN from encoded portions of driver's licenses will cut down on unnecessary collection of the identifier.[10]

Section 106 would prohibit government entities from allowing prisoners to have access to the SSN. We think that this too is a common sense protection, in light of the Metromail case, where a company employed prisoners to enter personal information from surveys into computers. This resulted in a stalking case where a prisoner harassed a woman based on information she submitted on a survey. The woman received mail from a convicted rapist and burglar who knew everything about her—including her preferences for bath soap and magazines. The woman sued and as a result of a class-action suit, Metromail may no longer use prisoners to process personal information.[11] Nevertheless, a general prohibition on inmate access to SSNs is appropriate, and California and Kentucky already have passed legislation to keep SSNs out of the hands of prisoners.[12]

Section 107 generally prohibits disclosure of the SSN in the private sector, subject to exceptions. We think it important to limit exceptions to the general prohibition in order to curb private sector use of the SSN. First, the exception for public health purposes should be limited to "emergency public health purposes." In its current articulation, this exception could allow medical providers and insurance companies to continue to rely upon the SSN in normal operations. Limiting the exception will encourage the industry to shift away from the identifier. We note that Empire Blue Cross is transitioning its 4.8 million customers away from the SSN as an identifier, demonstrating that it is possible for large health care operations to use an alternative identifier.[13]

Section 107 contains an exception for SSNs of the deceased, meaning that they could be freely traded on the market. We think there are important public policy reasons to place some protections on SSNs of the deceased. SSNs of deceased individuals should receive protection for the same reasons that justify protections for living individuals; those reasons include preventing fraud and identity theft. Additionally, criminals are known to assume the identities of deceased individuals in order to engage in criminal acts and to avoid law enforcement. Some protection for these identifiers is justified.

Section 108 codifies a much-needed protection for the SSN. Prior to the implementation of the Gramm-Leach-Bliley Act, CRAs and other entities sold SSNs in credit headers to individuals outside Fair Credit Reporting Act regulation. We understand that some businesses are still selling SSNs from credit headers that were collected before implementation of Gramm-Leach-Bliley. Section 108 would eliminate this unregulated sale of SSNs by tying the identifier to the credit report, and thus to protections in the Fair Credit Reporting Act.

Section 109 contains important protections against the practice of "coercive disclosure," a practice where an entity conditions provision of a product or service based on disclosure of the SSN. Maine, New Mexico, and Rhode Island have established protections against coercive disclosure, and we think it a good idea to federalize this important right to enhance privacy of the SSN.[14]

Title II contains measures to help protect the integrity of the SSN. Section 202, which addresses enumeration at birth, provides an excellent opportunity to address objections to SSN issuance to children that many Americans posses based on political or religious beliefs. In *Bowen v. Roy,* 476 U.S. 693 (1986), better known as the "Little Bird of the Snow" case, a family that applied for child welfare benefits sued the Department of Health and Human Services for requiring that a SSN be issued to their indigent child. The family alleged that enumeration violated their religious beliefs and that the conditioning of benefits on issuance of the SSN violated the Free Exercise Clause. The Supreme Court disagreed, holding that the government could require the child to obtain a SSN in order to receive benefits.

---

[9] *See e.g.* Jennifer 8. Lee, *Finding Pay Dirt in Scannable Driver's Licenses,* New York Times, March 21, 2002.

[10] Louisiana has already prohibited embedding the SSN into a driver's license. La. R.S. § 32:410. West Virginia has attempted to address this problem of license swiping by allowing the use of license scanners for age verification purposes but prohibiting the recording of SSNs in the process. W. Va. Code Ann. § 60–2–22.

[11] During litigation, Metromail claimed that they had not violated the woman's privacy, that they had no duty to inform individuals that prisoners were processing their personal data, and that the data processed was not highly intimate or embarrassing. *Beverly Dennis, et al. v. Metromail, et al*., No. 96–04451, Travis County, Texas.

[12] Cal Pen Code § 4017.1, § 5071; Cal Wel & Inst Code § 219.5; Ky. Rev. Stat. Ann. § 131.191.

[13] *Empire Blue Cross Will End Use Of SSNs, Use Alternate Number System,* Privacy and Security Law Report (Jun. 7, 2004) at 666.

[14] 2003 Me. ALS 512; N.M. Stat. Ann. § 57–12B–3; R.I. Gen Laws § 6–13–17.

In that case, the trial court found that the government could, in fact, administer child welfare programs without enumeration. This bill allows Congress to revisit the issue and provide an alternative for those having a religious or ethical objection to permanent enumeration. Alternatives could include a tax-identification number that expires at the age of eighteen, when the child can more fully consider whether to obtain a SSN. Another could specify heightened security requirements or anti-fraud measures to administer benefits to those objecting to enumeration. The study to be performed by the Commissioner of Social Security should require consideration of these issues.

Title III of the legislation creates new criminal penalties for misuse of the SSN. Section 302 prohibits individuals from knowingly providing a false SSN to another person. We think that there should be an exception to this rule for cases where an individual provides a false SSN without any intent to commit fraud. For instance, in situations where an entity demands a SSN without justification, individuals should be able to fabricate one if they are not engaged in fraud and are simply attempting to protect their privacy. We think the following language should be added to Section 302 (in the provision amending Section 1129(a) of the Social Security Act to create a new provision at 1129(a)(3)(B)): "Notwithstanding the previous sentence, an individual is permitted to represent a number to be the social security number assigned by the Commissioner of Social Security to another so long as the individual does not do so with the intent to engage in fraud or other criminal activity."

II. States Have Innovated Clever Protections for the SSN; Congress Should Consider Incorporating Them in 108 H.R. 2971

In recent years, state legislatures have functioned in their traditional roles as "laboratories of democracy," creating new approaches to enhancing the privacy of SSNs. These privacy protections demonstrate that major government and private-sector entities can still operate in environments where disclosure and use of the SSN is limited. They also provide examples of protections that should be considered at the federal level.

Some States Have Placed Broad Prohibitions on Disclosure and Use by Government and Private Entities

Two weeks ago, Colorado Governor Bill Owens signed H.B. 1311, legislation that creates important new protections for the SSN that will take effect later this summer. The new law will limit the collection of the SSN and its incorporation in licenses, permits, passes, or certificates issued by the state. The law requires the establishment of policies for safe destruction of documents containing the SSN. Insurance companies operating in the state must remove the SSN from consumers' identification cards. Finally, the legislation creates new penalties for individuals who use others' personal information to injure or defraud another person.

A law taking effect in January 2005 in Arizona prohibits the disclosure of the SSN to the general public, the printing of the identifier on government and private-sector identification cards, and establishes technical protection requirements for online transmission of SSNs.[15] The new law also prohibits printing the SSN on materials mailed to residents of Arizona. Exceptions to the new protections are limited—companies that wish to continue to use the SSN must do so continuously, must disclose the use of the SSN annually to consumers, and must afford consumers a right to opt-out of continued employment of the SSN. Arizona's new law is based on California Civil Code § 1798.85.

Special Protections Have Been Crafted for Students

A number of states have passed legislation limiting colleges and universities from employing the SSN as a student identifier. Limiting use of the SSN in this context reduces the risk of identity theft, as databases of student information, student identity cards, and even posting of grades sometimes contain SSNs.

In Arizona, major universities can no longer use the SSN as the student identifier.[16] In Colorado, as of July 2003, public and private postsecondary institutions were required to establish protections for the SSN and discontinue its use as the primary student identifier.[17] New York and West Virginia prohibit all public and private schools from using the SSN as a primary identifier.[18] Kentucky law allows students to opt-out of use of the SSN as student identifier.[19]

---

[15] Ariz. Rev. Stat. § 44–1373.

[16] Ariz. Rev. Stat. § 15–1823. Rhode Island and Wisconsin have similar protections. R.I. Gen. Laws § 16–38–5.1; Wis. Stat. Ann. § 36.11(35).

[17] C.R.S. § 23–5–127.

[18] N.Y. Educ. Law § 2–b; W. Va. Code Ann. § 18–2–5f.

[19] Ky. Rev. Stat. Ann.156.160. *See also* Ky. Rev. Stat. Ann.197.120.

Protections Crafted for Public, Vital, and Death Records

Commercial data brokers obtain SSNs from a number of sources, including public records that individuals are required to file in order to enjoy important rights and privileges offered by society. For instance, marriage licenses have been a source for SSNs and a number of states, including Arizona, California, Indiana, Iowa, Kentucky, Louisiana, Maine, Montana, Ohio, and Michigan, have enacted legislative protections to prevent their disclosure.[20]

Birth and death records are rich in personal information, and states have acted to shield SSNs collected in these life events against disclosures. Arizona, California, Illinois, Kansas, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, New Hampshire, and other states limit the appearance of the parents' SSN on birth records.[21] Similarly, several states restrict disclosure of the SSN in records associated with death.[22]

Protections Against Pretexting Should Be Considered

We wish to raise one additional concern here—even legitimate collection of the SSN contributes to unauthorized access to the identifier. That is, we are increasingly aware of manuals for private investigators and other materials suggesting that SSNs can be obtained from motor vehicle departments, applications for professional licenses, and even tax returns.[23] In these cases, the investigator probably obtains the identifier through a friend or contact working at the institution with a SSN. Alternatively, the manuals suggest the use of "pretexting," a practice where an investigator requests personal information from an entity while pretending to be another person or while pretending to have a legitimate reason for access to the information. The Gramm-Leach-Bliley Act prohibits pretexting with respect to financial, securities, and insurance companies, but the law doesn't apply to pretexting targeted at employers, utility companies, or other entities that have SSNs. The Subcommittee should consider whether expanding protections against pretexting would enhance the privacy of the SSN.

III. Excessive Reliance on the Social Security Number and Lax Credit Granting Practices Are Exacerbating the Identity Theft Problem

News media stories abound on the plight of the victim of identity theft. No one is safe from the crime—impostors have been able to obtain credit in the names of young children and even babies.[24] While Congress has heightened penalties for identity theft, we recommend that further attempts to fight the crime be centered on the credit granting process, and in particular, the practice of granting credit only on a SSN match.

Identity thieves can rely on aspects of the instant credit granting system to commit fraud. The first weakness in the system flows from extreme competition to acquire new customers. This has resulted in grantors flooding the market with "prescreened" credit offers, pre-approved solicitations of credit made to individuals who meet certain criteria. These offers are sent in the mail, giving thieves the opportunity to intercept them and accept credit in the victim's name.[25] Once credit is granted, the thief changes the address on the account in order to obtain the physical card and to prevent the victim from learning of the fraud.[26] The industry sends out

---

[20] Ariz. Rev. Stat. § 25–121; Cal Fam Code § 2024.5; Burns Ind. Code Ann. § 31–11–4–4; Iowa Code § 595.4; Ky. Rev. Stat. Ann. 402.100; La. R.S. 9:224; 19–A M.R.S. § 651; MCL § 333.2813; Mont. Code Ann. § 40–1–107; Ohio Rev. Code Ann. § 3101.05.

[21] *See* Ariz. Rev. Stat. § 36–322; Cal Health & Saf Code § 102425; 410 ILCS 535/11; K.S.A. § 65–2409a; 22 M.R.S. § 2761; Md. Ann. Code § 4–208; ALM GL ch. 111, § 24B; Minn. Stat. § 144.215; Miss. Code Ann. § 41–57–14; Mo. Rev. Stat. § 193.075; Mo. Rev. Stat. § 454.440; N.H. Rev. Stat. Ann. § 5–C:10.

[22] *See* Ariz. Rev. Stat. § 16–165; Cal Health & Saf Code § 102231; Idaho Code § 67–3007; Burns Ind. Code Ann. § 16–37–3–9; La R.S. § 23:1671; N.D. Cent. Code § 23–02.1–28.

[23] *See e.g.* Lee Lapin, How to Get Anything on Anybody 533–543 (Intelligence Here, 3d ed. 2003) (section titled "How to Find Anyone's Social Security Number" suggests thirty sources for the SSN, including driver's license applications, bankruptcy filings, court records, bank files, utility records, professional and recreational licenses, and employment files).

[24] 24]Identity Theft Resource Center, Fact Sheet 120: Identity Theft and Children, available at http://www.idtheftcenter.org/vg120.shtml.

[25] *Identity crises—millions of Americans paying price,* Chi. Tribune, Sept. 11, 2003, p2.

[26] Id.

billions of these pre-screened offers a year. It 1998, it was reported that 3.4 billion were sent.[27] In 2003, the estimate increased to 5 billion sent.[28]

Competition also drives grantors to quickly extend credit. Once a consumer (or impostor) expresses acceptance of a credit offer, issuers approve the transaction with great speed. Experian, one of the "big three" credit reporting agencies, performs in this task in a "magic two seconds."[29] In a scenario published in an Experian white paper on "Customer Data Integration," an individual receives a line of credit in two seconds after only supplying his name and address.[30] Such a quick response heightens the damage to business and victims alike, because thieves will generally make many applications for new credit in hopes that a fraction of them will be granted.

The second factor that makes identity theft easy to commit is that credit grantors do not have adequate standards for verifying the true identity of credit applicants. Credit issuers sometimes open tradelines to individuals who leave obvious errors on the application, such as incorrect dates of birth or even the incorrect name. Identity theft expert Beth Givens has argued that many incidences of identity theft could be prevented by simply requiring grantors to more carefully review credit applications for obviously incorrect personal information.[31]

TRW Inc. v. Andrews illustrates the problems with poor standards for customer identification.[32] In that case, Adelaide Andrews visited a doctor's office in Santa Monica, California, and completed a new patient's information form that requested her name, birth date, and SSN.[33] The doctor's receptionist, an unrelated woman named Andrea Andrews, copied the information and used Adelaide's Social Security Number and her own name to apply for credit in Las Vegas, Nevada. On four occasions, Trans Union released Adelaide's credit report because the SSN, last name, and first initial matched. Once Trans Union released the credit reports, it made it possible for creditors to issue new tradelines. Three of the four creditors that obtained a credit report issued tradelines to the impostor based on Adelaide's file, despite the fact that the first name, birth date, and address did not match.[34]

A survey of other prominent identity theft litigation shows numerous cases where credit was granted as a result of a SSN match despite other obvious inaccuracies. For instance, in *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997), Fleet Bank of Albany, New York, issued two credit cards to "Ronald Aylward," allegedly of East Moriches, New York, who used both the victim's name and SSN in applying for the cards. The victim, however, lived in Missouri all of his life.

In *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003), impostors obtained American Express cards using the victims' correct names and SSNs but directed all the cards to be sent to the impostors' home. In *Vazquez-Garcia v. Trans Union De P.R., Inc.*, 222 F. Supp. 2d 150 (D. P.R. 2002), a resident of Puerto Rico who was born in 1962 learned that Sears had issued a credit card to a resident of Nevada who was born in 1960. The impostor had falsely used the victim's SSN to apply for credit cards in his own name and succeeded in getting credit despite the mismatch on age and location. In *Dimezza v. First USA Bank, Inc.*, 103 F. Supp. 2d 1296 (D. N.M. 2000), an impostor obtained credit using the victim's SSN but a different name and address.

And finally, those who attempt to assign liability for negligent credit granting have not been successful in the courts. In *Huggins v. Citibank*, 355 S.C. 329 (S.C. 2003), a plaintiff-victim alleged that banks should be liable when they negligently

---

[27] *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, Hearing Before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information,* Jul. 12, 2000 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse) (citing Edmund Sanders, *Charges are flying over credit card pitches,* L.A. Times, Jun. 15, 1999, p. D–1), available at http://www.privacyrights.org/ar/id_theft.htm.

[28] Rob Reuteman, *Statistics Sum Up Our Past, Augur Our Future*, Rocky Mountain News, Sept. 27, 2003, p 2C; Robert O'Harrow, *Identity Crisis; Meet Michael Berry: political activist, cancer survivor, creditor's dream. Meet Michael Berry: scam artist, killer, the real Michael Berry's worst nightmare*, Wash. Post Mag., Aug. 10, 2003, p W14.

[29] Experian, Inc., Customer Data Integration: The essential link for Customer Relationship Management White paper 15, 2000, available at http://www.experian.com/whitepapers/cdi_white_paper.pdf.

[30] Id.

[31] *Legislative Hearing on H.R. 2622, The Fair and Accurate Credit Transactions Act of 2003, Before the Committee on Financial Services,* Jul. 9, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, Electronic Privacy Information Center).

[32] 534 U.S. 19 (2001); Erin Shoudt, *Comment. Identity theft: victims "cry out" for reform*, 52 Am. U. L. Rev. 339, 346–7 (2002).

[33] Id. at 23–25.

[34] *Id.*

extend credit in a victim's name to an impostor.[35] The defendants argued that no duty existed because the victim was not actually a customer of the bank. In August 2003, the South Carolina Supreme Court rejected the proposed cause of action. Although it expressed concern about the rampant growth of identity theft, the court found that the relationship between credit card issuers and potential victims of identity theft was "far too attenuated to rise to the level of a duty between them."

These cases show that excessive reliance on the SSN can contribute to identity theft. California has attempted to address this problem by requiring certain credit grantors to comply with heightened authentication procedures. California Civil Code § 1785.14 requires credit grantors to actually match identifying information on the credit application to the report held at the credit reporting agency. Credit cannot be granted unless three identifiers from the application match those on file at the credit bureau. The categories to be matched include "first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number."[36] Simply requiring credit grantors to look beyond the SSN as a customer identifier and authenticator will begin to address a wide range of identity theft.

Conclusion

Thank you, Chairman Shaw, for continuing to develop a rich legislative record supporting greater privacy for the SSN. We think that the privacy and integrity of SSNs could be enhanced through the passage of federal legislation that limits the collection and approved uses of the identifier. We urge the Subcommittee to examine state laws that have created new, clever protections for the SSN. We also urge the Subcommittee to consider that excessive reliance on the SSN contributes to identity theft. We look forward to continuing to work with the Subcommittee on this and other privacy matters.

Chairman SHAW. Thank you. Mr. McGuinness.

STATEMENT OF BRIAN P. MCGUINNESS, FIRST VICE PRESIDENT, NATIONAL COUNCIL OF INVESTIGATION AND SECURITY SERVICES, MIAMI, FLORIDA

Mr. MCGUINNESS. Good afternoon, Mr. Chairman, Members of the Committee, wherever you may be. My name is Brian McGuinness. I am appearing today on behalf of the NCISS as its first Vice President. I am past President of the Florida Association of Licensed Investigators, and I have been a licensed investigator for over 20 years. Before that, I was a criminal investigator for 7 years with the Miami Dade County Public Defenders Office. I really appreciate the opportunity to comment on H.R. 2971 today. Our profession has been trying to help identity theft victims for years.

Much of H.R. 2971 seems to be on the right track. Publication of SSNs to the general public can only lead to improper use, including theft, fraud, even potential physical harm. We support legislation that will curtail such information being offered for sale over the Internet to the general public, but we are very concerned about sections 107 and 108, which will in fact hinder relief for victims and cause many unintended consequences.

A number of years ago, the FTC entered into a consent agreement whereby the identifying information that precedes a credit report was deemed not part of the report and therefore not covered by the Fair Credit Reporting Act. The "header" information does not contain any financial data and has been an invaluable resource

[35] *See also Garay v. U.S. Bancorp,* 2004 U.S. Dist. LEXIS 1331 (E.D.N.Y. 2004); *Smith v. Citibank,* 2001 U.S. Dist. LEXIS 25047, (W.D. Mo. 2001); *Polzer v. TRW, Inc.,* 256 A.D.2d 248 (N.Y. App. Div. 1998).

[36] *Id.*

to employ in all manner of investigations. Header information is only available through vetted contracts with major credit bureaus by legitimate businesses and law enforcement agencies. We are unaware that credit headers are being used by identity thieves. The crooks know where their victims are. They don't need to locate them.

Section 108 would deal a blow to both the civil and criminal justice systems by effectively eliminating the access to credit header information for the purpose of locating suspects and witnesses. Locating females after a marriage or a divorce is particularly difficult without using the SSN identifier. There are over 43,000 Robert Joneses in the United States. Many of them have the same or similar dates of birth. Investigators need to be able to positively differentiate between subjects when rendering reports that would be used for many purposes, including evidence in court proceedings.

Law enforcement agencies have many means at their disposal and are generally exempt from legislation restricting access to information, but even law enforcement Members admit that restricting access to credit headers will tip the scales of justice in favor of the prosecution and will decrease the defendant's ability to receive a fair trial. At a time when our justice system is being criticized for errors proven by DNA evidence, we find it hard to believe that Congress would attempt to take away the defendants primary means of locating witnesses.

Let me tell you all of an example from my own experience attempting to assist a domestic maid whose son had been kidnapped by her husband 5 years previously. In her 5-year search she had mounted a letter-writing campaign which yielded a 2-inch stack of letters similar to yours, Ms. Foss, from apathetic police officers and politicians expressing their regret but providing no real assistance. I entered her husband's SSN in a database and learned about a West Palm Beach address he had used when applying for credit. I checked directory assistance and confirmed there was a non-published telephone number in his name at that address. A 5-year journey of desperation, anguish and frustration was ended in 5 minutes by simply having access to header information.

A New York investigator was retained by the courts in a guardianship proceeding to recover over $300,000 in assets stolen from a 97-year-old retiree by a neighborhood care giver. Using credit headers he determined identities and locations of the wrongdoer's relatives and eventually their assets that had been taken away from the victim. The victim's assets had been used to purchase real property, expensive automobiles and to increase the thief's bank account balances. The suspect pled guilty and was sentenced to 3 to 9 years in State prison for second degree grand larceny and ordered to pay $360,000 in restitution to the victim's estate.

With few exceptions, law enforcement does not have the resources to assist identity theft victims. As pointed out in my prior written testimony, victims are often told their losses are below the threshold required before agencies will investigate. In fact, many victim turn to licensed private investigators for assistance. We, therefore, ask that all of Section 108 be deleted. We routinely provide our clients with documents and reports containing necessary identifying information. section 107 would effectively deny us the

ability to obtain or provide our clients with such information. There is an exemption for law enforcement and collection of child support, but the exemption should also include reports prepared in connection with litigation, service of process, due diligence investigation of insurance claims, civil and criminal fraud, criminal defense, identity fraud and stalking or any other violations of law.

Although H.R. 2971 provides the Attorney General with the ability, I am sorry, with the authority, rather, to provide additional exemptions, we believe it is critical for Congress to spell them out in advance. The bill as introduced would have a substantially deleterious impact on the court system and individual victims of crime. Such major issues should be resolved by elected officials and not delegated to the Department of Justice. Congress should proceed very carefully. Taking away the tools from investigators serving the justice system is not the way to go about resolving identity theft. I would be pleased to answer any questions that you may have.

[The prepared statement of Mr. McGuinness follows:]

Statement of Brian P. McGuinness, First Vice President, National Council of Investigation and Security Services, Miami, Florida

Good morning Mr. Chairman and members of the Committee. My name is Brian P. McGuinness and I am appearing today on behalf of the National Council of Investigation and Security Services. I am first vice president of NCISS and past president of the Florida Association of Licensed Investigators. I have been a licensed private investigator in Florida for twenty years and before that I was a criminal investigator for seven years with the Dade County Public Defenders Office.

I appreciate the opportunity to comment on H.R. 2971, the Social Security Number and Identity Theft Prevention Act of 2003. You have asked us to address the uses private investigators currently make of Social Security numbers and other personally identifiable information and for our views on specific provisions of this bill that would affect the private investigator community.

As a profession that has been trying to help victims through the identity theft maze for years, we applaud Congress' efforts to finally put laws on the books that will bring victims some relief. Although a percentage of identity thieves no doubt gather their victim's identities from the Internet, our experience is that most such thefts result from the purloining of documents, files, charge slips, credit cards, and wallets from restaurants, stores, trash bins, the mails and private property.

Much of HR 2971 seems to be on the right track, but we are very concerned about Sections 107 and 108, which will, in fact, hinder relief for victims and cause many unintended consequences.

A number of years ago, the Federal Trade Commission entered into a consent agreement whereby the identifying information that precedes a credit report, which is called "header" information, was deemed not part of the credit report and therefore not covered by the Fair Credit Reporting Act as a Consumer Report. The "header" report does *not* contain any financial information. This information has been an invaluable resource for investigators to locate witnesses, heirs, debtors, and to employ in all manner of fraud and theft investigations.

We are unaware of any evidence that credit headers are being used by identity thieves for any purpose. Licensed investigators and police use credit headers to locate witnesses and suspects. Identity thieves know where their victims are; they don't need to find them.

Header information is only available through vetted contracts with major credit bureaus by legitimate businesses and law enforcement agencies. These information providers audit the users of such data, including the use of "stings" to assure compliance with contract provisions.

Because the FTC has ruled that investigators rendering reports in connection with employment or credit are themselves consumer reporting agencies, the language in Section 108 of HR 2971 appears to eliminate the use of credit headers for most legitimate purposes. It will make it impossible for civilian investigators to obtain or report information necessary to identify suspects and exonerate the innocent without first obtaining the written permission of a suspect as required by the FCRA. Section 108 has an unintended consequence which would deal a blow to both the

civil and criminal justice systems by effectively eliminating access to credit header information for the purpose of locating suspects and witnesses.

Law enforcement agencies have NCIC and many other means at their disposal, and are always exempted from legislation restricting access to the same information sources that HR 2971 would deny private investigators. As a matter of fairness, even law enforcement members admit that restricting access to credit headers will tip the scales of justice in favor of the prosecution and augurs against the defendant's ability to receive a fair trial. At a time when our justice system is being criticized for errors proven by DNA evidence, we find it hard to believe that Congress would intend to take away a defendant's primary means of locating witnesses.

The header search is by far the most important search currently used by investigators when locating female witnesses. Since women often change surnames over the course of their lives due to marriage or divorce, it makes it even more critical to be able to identify them by their SSN. The SSN does not change and allows us to locate these otherwise difficult to find witnesses.

In past hearings, Lexis Nexis has testified that there are 46,000 men in America named Bill Jones. Many of them have the same or similar dates of birth. Licensed private investigators need to be able to positively differentiate between subjects when rendering reports which will be used for many purposes including evidence in court proceedings.

We hope you are also aware that with few exceptions, law enforcement does not have the resources to successfully assist identity theft victims. In fact, many victims turn to licensed private investigators for assistance. We therefore ask that all of Section 108 be deleted.

Most states have legal jurisdiction over private investigative and security firms. They undergo fingerprint-based criminal background checks, are regulated, are tested and for the most part receive training and often continuing education. We believe that regulated licensed private investigators and security firms should be allowed continued access to header information. Many of the reports that private investigators prepare containing the personally identifiable information that this committee seeks to protect are privileged attorney work product.

We abhor scam fraud artists and rogue information brokers who advertise on the Internet to the general public that they will provide information on anybody to anybody for a price no matter who the customer. Publication of personally identifiable information to the general public can only continue to lead to improper use, theft, fraud and even potential physical harm. We support efforts to limit access to such data to the general public. We also support any legislation that will curtail such information being offered for sale over the Internet to the general public.

Section 107

Private investigators, for a fee, as a regular part of their routine, ascertain, collect, assemble, evaluate and provide their clients documents and reports containing personally identifiable information. Such information often includes the Social Security numbers of individuals. Section 107 of HR 2971 would effectively deny us the ability to provide our clients with such information. The section provides an exemption for law enforcement and the collection of child support.

But, the exemption should also includeproviders of reports prepared in connection with litigation, in anticipation of litigation, due diligence, investigation of insurance claims, civil and criminal fraud, criminal defense, identity fraud, and stalking or any other violations of law.

There are appropriate uses for such information which is not only critical for private investigators but for attorneys, journalists, medical researchers, insurance companies, self regulatory bodies, as well as government and law enforcement agencies. Licensed private investigators use the information in fraud prevention, child support enforcement, uniting separated families, locating heirs to estates, locating pension fund beneficiaries, locating organ and bone marrow donors, to assist those engaged in significant journalistic endeavors, apprehending criminals, aiding citizens in obtaining access to public record information and in assisting the very individuals that this legislation seeks to protect.

Although HR 2971 provides the Attorney General with the authority to provide additional exemptions, we believe it is critical for Congress to spell them out in advance. The bill, as introduced, would have a substantial deleterious impact on the court system and individual victims of crime. Such major issues should be resolved by elected officials and not delegated to the Department of Justice.

There are a number of bills before Congress which would ban the use of the Social Security number for any but its intended purpose. Many of these bills do not take into consideration the effect of removing the social security number as an identifier. We fully appreciate the incredible burdens faced by victims of identity theft. Many

of us have had to face these victims. When all other avenues of redress have fallen upon deaf ears and often as a last resort, identity fraud victims have turned to private investigators to redeem their name and restore their good reputation. In fact, many of us have assisted these victims for little or no remuneration.

The National Council of Investigation and Security Services holds the position that anyone who uses personally identifiable information or financial information for illegal purposes be subject to criminal sanctions and heavy fines. We favor the implementation of assessing enhanced penalties for aggravated cases, actual damages for willful violations, and additional damages allowed by the court for commercial purposes, disgorgement of profits, attorney's fees and costs, and additional sanctions upon the receiver of information that is obtained for unlawful purposes.

Taking away the tools from the civilian crime fighters and investigators serving the justice system is not the way to go about resolving identity theft. Congress needs to ensure that exemptions are provided for licensed private investigators on legitimate business. Our members have provided leads concerning rogue information providers to the FTC in the past. We would also like to see the FTC set up a formal liaison with our profession which would allow us to provide evidence on those who commit fraud and who tarnish our reputation.

Concerning this and similar legislation, we in the past surveyed our membership about how they have been able to assist victims of identity theft. The following examples demonstrate the benefits of permitting licensed private investigators to access essential information from "credit headers." HR 2971 would deny us this critical tool. These anecdotes should give this Committee some idea of the types of cases that require this information:

A past president of NCISS was retained by the New York courts in a guardianship proceeding to recover over $300,000 in assets stolen from a ninety-seven year-old retired Army officer by a neighbor caregiver. Through the use of credit headers he was immediately able to determine the identities and locations of the wrongdoer's relatives, properties and eventually their assets that had been taken from the victim. It was the initial header check on the suspect that uncovered a Myrtle Beach, South Carolina address for him. That information developed leads that the victim's assets had been used to purchase real property in South Carolina, expensive automobiles and increased the bank account balances of the subject under the guise that the 97-year-old victim, who was suffering from dementia, had given his life savings as gifts to the suspect. The suspect was to eventually plead guilty and was sentenced to three to nine years in state prison for second-degree grand larceny and ordered to pay $360,000 in restitution to the estate of the victim, who died a month before sentencing of the defendant.

In Coronado, California, an elderly woman whose apartment building had just been renovated suddenly began receiving bills for a credit card that she never used and kept in a desk drawer. When she complained to the contractor, he realized there were four possible suspect workers and hired a private investigator. The investigator verified the credit card was used by a man and wife fitting the description and in the neighborhood of one of the workers. The suspect was terminated while the other three were cleared and their jobs and reputations saved. No prosecution resulted.

In Tennessee, a show dog breeder was being stalked and threatened by e-mail from an unknown harasser. She was terrified because she had no idea what the suspect looked like and she was often exposed in public arenas. The police could not help without some identification. Using credit headers and other sources, the private investigator found addresses for the suspect who was using four names, four different social security numbers and who had a criminal record. The investigator's report was provided to the police. The same investigator reports she recently located and served process on a dead-beat dad and could not have located him without using credit headers.

In New York, a public utility hired our member to conduct a pre-employment background investigation for a high level position. A credit report, obtained under the FCRA contained two different social security numbers. Running a credit header check on the second number revealed a different name and addresses and the investigator discovered his true identity. The applicant had adopted the identity of one of his former college professors to keep his own less desirable background secret.

In Atlanta, Georgia, an auto dealership asked our investigator to help an applicant who claimed his identity had been stolen. An imposter had stolen this man's social security number and date of birth as well as the identity of four other people. His criminal record included nine felonies in Georgia and other multi-state offenses. The applicant couldn't understand why he had been turned down for several jobs until one potential employer leveled with him and he realized his identity had been stolen. Numerous law enforcement agencies told him they couldn't help him. Our

investigator arranged for the applicant to be fingerprinted and the Georgia Bureau of Investigation issued him a certificate stating he was not the same person as the imposter. He then carried the certificate to the three major credit bureaus to clear his name in their files.

The investigator says had he not helped the victim through this maze, he would surely have been arrested in Georgia or Florida where warrants had been issued.

An investigation in California found a middle-aged suspect had returned home after years away and stolen his elderly father's identity. He went on a spending spree in Oregon and California and was not called to answer before both his parents passed away. A private investigator was hired by the estate to try to apprehend the thief and obtain restitution. Most of his leads involve the use of credit header information.

A former Dallas police sergeant, now a private investigator, reported he was pursuing a physician who filed bankruptcy following loss of suit for a wrongful death. The doctor divorced her husband before the bankruptcy and is now remarried to a man with a similar name and date of birth and social security number. The suspicion is that this maneuver served to hide assets due to the victim's survivors.

In San Francisco, an investigator reports working a case for a successful business owner who started getting statements in the mail saying he owed tens of thousands of dollars on computers and other purchases, none of which he knew anything about. He found someone had hijacked his identity, opened credit card and store accounts in his name and had even opened a web page mirroring his web page and had an email address similar to his. The San Francisco Police said they would take a report, but would not investigate and suggested he go to the Secret Service. Although losses approached $80,000, the Secret Service said they would not handle the case until at least $100,000 is lost. The victim had a suspicion it was an ex-employee who lived in Salt Lake City and called the investigator. The agency used credit header information to learn that the ex-employee has three names, three or four social security numbers, and three different dates of birth on file.

Here is an investigator's story from Toledo, Ohio, in his own words, about how credit header information is used to locate lost heirs:

"One of my cases involved a woman whose name was Terri. She was left a sizeable inheritance by her uncle in the form of a trust. The family had not had any contact with her for a number of years, so the attorney handling the trust asked for my assistance. By using header information, I was able to eventually determine that Terri was recently married and was living someplace in Utah. I was able to locate her husband's relatives and learned that Terri and her husband were destitute and were living out of a pick-up truck either in Utah or Oregon. I sent the requisite documentation to Terri in care of her husband's relatives and she rightfully obtained her substantial inheritance. Without access to header information, I would not have been able to locate her."

The need for the continuation of the investigative profession's access to the SSN header search can be clearly seen from the following example. This example is from my own experience as a licensed private investigator attempting to assist a domestic maid whose son had been kidnapped by her husband. She had not seen her son in five years and had never contemplated hiring an investigator.

What she did do was mount a letter writing campaign which yielded many letters from various empathetic police officials and politicians expressing their regret but providing no real answers or concrete assistance. She showed me a stack two inches thick of such letters, including one to the president of the United States, her Congressman, county sheriff, local municipal police chief, etc.

When she told me that in addition to having her husband's date of birth, she also had his social security number, I became optimistic. I entered the SSN into my TransUnion database and immediately learned that the husband had used a West Palm Beach address within the previous six months when applying for credit. I checked directory assistance and they confirmed that there was a non-published telephone number in his name at that address. A five year journey of desperation, anguish and frustration was rewarded with success within a five minute period by simply having access to header information in the form of an inexpensive database search.

We believe that the identity theft laws recently enacted will help law enforcement to prosecute perpetrators once apprehended. But Congress should be aware that public law enforcement resources are stretched and crimes of this nature are not now a high priority. The losses, though devastating to the victims, are usually beneath the dollar threshold that many departments follow. And the mental toll on the victims is unquantifiable. The private sector will have to continue to augment public law enforcement. And it should be noted that the hapless victims of this crime often have very limited resources.

To the extent HR 2971 makes it easier for victims of identity theft to clear their credit files and restore their reputation, we commend it. But Congress should proceed very carefully before eliminating the very tools used to apprehend the stealers of the identities of others or the perpetrators of other criminal acts.

Chairman SHAW. Thank you. Mr. Buenger.

STATEMENT OF MICHAEL L. BUENGER, PRESIDENT, CONFERENCE OF STATE COURT ADMINISTRATORS, JEFFERSON CITY, MISSOURI

Mr. BUENGER. Thank you, Mr. Chairman. My name is Mike Buenger. I am the President of the national COSCA, and also the State Court Administrator for the State of Missouri. The COSCA represents the principal court administrative officers in each of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands and the Territories of American Samoa, Guam and the Virgin Islands. I am pleased to present testimony to you today as this Subcommittee examines and struggles with the issue of protecting privacy and preventing the misuse of SSNs.

Mr. Chairman, State courts handle 97 percent of all judicial proceedings in this country. Over 96 million cases are filed annually. I give you this statistic to frame the magnitude of the work of the State courts of our Nation and so that you can frame the impact of legislation such as H.R. 2971 on the courts. For the past several years, we have grappled with the issue of protecting privacy and private information as it relates to court documents. Although the immediate issue before the Subcommittee is protecting privacy of SSNs, privacy protection for information and court documents is part of a broader issue that involves balancing public access to government records and the openness of our courts with the legitimate privacy interest of citizens and, I might add, the capacity of courts to operationally accommodate both privacy and access concerns.

We have sought to provide guidance to the State court community through a project entitled Public Access to Court Records, both the Conference of Chief Justices and COSCA having issued guidelines for policy development by State courts. This guidance outlines the issues that courts should address in developing rules and policies governing access to court documents. It provides but one approach. However, Mr. Chairman, there is no doubt that SSNs are contained in many court documents and frequently as mandated by Federal and State law.

For example, Federal law requires us to collect SSNs to track deadbeat parents. Court orders and pleadings involving child support must bear the parties' SSNs, again a requirement of Federal law. Federal regulations require that garnishment orders for Federal postal employees bear the SSN of the garnishee. State courts use SSNs to identify parties to a case, to collect fines and crime victim restitution and to report criminal history to central repositories. Frequently, they are found in documents filed with the court for safekeeping, such as discovery documents and deposition testimony. They are, as noted, frequently used and for good reason. They are a needed and unique identifier used by virtually every

member of the justice community and the law enforcement community, not just the courts.

The most important message I can deliver to you today, Mr. Chairman, is that COSCA stands ready to work with you in crafting solutions to address the problem of identity theft. I think it is also important to understand that this is not a problem that can be resolved through a mandate. It is complex not only in terms of your responsibility to establish balanced public policy but also in terms of the ability of the States and in this particular case the State courts to actually implement that policy. The threat of identity theft is real, and we want to do our part to eliminate it.

Section 102 of H.R. 2917 is of particular concern to us because it would effectively require courts to redact or otherwise prevent the display of SSNs from most court documents. This section has serious implications for State courts in a variety of contexts. Given the volume of cases filed annually in the State courts, the task of redacting SSNs from existing documents or those to be filed would be daunting. In some circumstances, it puts us at odds with established Federal and State law.

The SSN may appear in a variety of documents, including financial documents that are filed with the court, for example, tax returns and child support cases, or are appended to official court documents such as motions for summary judgment. Restricting access to SSNs in such documents is difficult because often such information can be buried in a stack of documents generally not reviewed by the court or its clerks until the case is actually heard.

In conclusion, Mr. Chairman, we recognize the serious role of SSNs in incidents of identity theft and the fact that such information is readily available in a host of public records. The current state of affairs with regards to the treatment of SSNs provides lawbreakers a continuing opportunity to exploit the current system at the expense of ordinary Americans. However, there is no simple solution and certainly no cheap solution to this problem. Even the public policy coming from Congress evidences the complexity of the issue by requiring the collection, use and availability of such information and even its display on one hand, and then seeking to restrict its access in others.

We hope that you will also assist the State courts in dealing with the unfunded mandates that H.R. 2971 will present to us. I thank you for offering us the opportunity to offer our opinion on this important matter. As I said, COSCA stands ready to work with you collaboratively and cooperatively in crafting a solution. Thank you, sir.

[The prepared statement of Mr. Buenger follows:]

Statement of Mike L. Buenger, President, Conference of State Court Administrators, Jefferson City, Missouri

Mr. Chairman and Members of the Subcommittee,

The Conference of State Court Administrators (COSCA) is pleased to present testimony on today's hearing "Enhancing Social Security Number Privacy" as the subcommittee examines the issue of protecting privacy and preventing the misuse of Social Security Numbers (SSNs).

SUMMARY

Mr. Chairman and members of the subcommittee, for the past several years the state court community has been grappling with the issue of protecting privacy, and private information, as it relates to court records. Although the immediate issue for the committee is protecting the privacy of SSNs, privacy protection for information in court records is actually a much broader issue. The use of Social Security Numbers in court records is, thus, a subset of much larger issues that involve balancing public access to government records with the legitimate privacy interests of citizens with actual capacity of courts to operationally accommodate privacy and public access concerns. To this end, we helped develop guidance for state courts through a project entitled "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts." This guidance outlines the issues that courts must address in developing rules and policies governing access to court records. The *Guidelines* touch on the use of SSNs in court records and other private information. The text of the *Guidelines* can be found at http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf. Both the Conference of Chief Justices and COSCA adopted a resolution endorsing the *Guidelines* and urged the states to use them in developing their own standards, rules, and policies.

Mr. Chairman, SSNs are pervasive in state court documents, frequently as mandated by state and federal law. For example, federal law requires us to collect SSNs for various reasons related to tracking deadbeat parents. By federal law, SSNs must *appear* on pleadings and court orders related to child support. Even federal regulations require that a SSN must appear on garnishment orders involving postal employees. *See,* 39 CFR 491.3Along with other identifiers, courts use SSNs to associate parties to a case, i.e. to determine whether John Smith 1 is different from John Smith 2. We use SSNs to collect fines and crime victim restitution, to report criminal records to central repositories, and to aid in the enforcement and collection of child support. In addition, many SSNs appear in the public record in many types of court cases including, but not limited to, bankruptcy, divorce, paternity, and child support determination.

Mr. Chairman, the most important message I can deliver to you today is that the Conference stands ready to work with you in crafting solutions to address the problem of identity theft. But I think it is also important for the sub-committee and the Congress to understand that this is not a problem that can be solved through a simple mandate. It is complex not only in terms of your responsibility to establish consistent public policy but also in terms of the ability of states, and in this case state courts, to actually implement that policy. The threat of identity theft is real and we want to do our part to eliminate it. We are at the same time concerned about the effort to require us to redact or expunge SSNs that appear in public records. We feel that this type of requirement could impose an incalculable burden on the state courts in this country, both with respect to resources and funding to achieve that goal. The cost to fulfill this requirement would be high because many SSNs appear in paper documents as well as other hard-to-redact microfilm/microfiche.

ABOUT COSCA

Before I begin my remarks, I would like to provide some background on our group and our membership. I submit this testimony as the President of the Conference of State Court Administrators (COSCA). COSCA was organized in 1955 and is dedicated to the improvement of state court systems. Its membership consists of the principal court administrative officer in each of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and the Territories of American Samoa, Guam, and the Virgin Islands. A state court administrator implements policy and programs for a statewide judicial system. COSCA is a nonprofit corporation endeavoring to increase the efficiency and fairness of the nation's state court systems. State courts handle 97% of all judicial proceedings in the country, over 96 million cases annually. The purposes of COSCA are:

- To encourage the formulation of fundamental policies, principles, and standards for state court administration;
- To facilitate cooperation, consultation, and exchange of information by and among national, state, and local offices and organizations directly concerned with court administration;
- To foster the utilization of the principles and techniques of modern management in the field of judicial administration; and
- To improve administrative practices and procedures and to increase the efficiency and effectiveness of all courts.

Although I do not speak for them, I also would like to tell you about the Conference of Chief Justices (CCJ), a national organization that represents the top judicial officers of the 58 states, commonwealths, and territories of the United States. Founded in 1949, CCJ is the primary voice for state courts before the federal legislative and executive branches and works to promote current legal reforms and improvements in state court administration. COSCA works very closely with CCJ on policy development and administration of justice issues.

NATIONAL EFFORT TO CRAFT PUBLIC ACCESS GUIDELINES TO COURT RECORDS

Our project entitled, "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts" was a joint effort of CCJ and COSCA to give state court systems and local trial courts assistance in establishing policies and procedures that balance the concerns of personal privacy, public access and public safety.

The State Justice Institute (SJI) funded this project in 2001 and the project was staffed by the National Center for State Courts (NCSC) and Justice Management Institute (JMI). The project received testimony, guidance and comments from a broad-based national committee that included representatives from courts (judges, court administrators, and clerks), law enforcement, privacy advocates, the media, and secondary users of court information.

The *Guidelines* recommend the issues that a court must address in developing its own rules and policies governing public access to its records. The *Guidelines* are based on the following premises:

- Retention of the traditional policy that court records are presumptively open to public access
- The criteria for access should be the same regardless of the form of the record (paper or electronic), although the manner of access may vary
- The nature of certain information in some court records is such that remote public access to the information in electronic form may be inappropriate, even though public access at the courthouse is maintained
- The nature of the information in some records is such that all public access to the information should be precluded, unless authorized by a judge
- Access policies should be clear, consistently applied, and not subject to interpretation by individual courts or court personnel

The *Guidelines* Committee examined the use of SSNs in current court practices. They looked at the inclusion of SSNs in bulk distribution of court records, and information in other documents besides SSNs that courts traditionally protect, such as addresses, phone numbers, photographs, medical records, family law proceedings, and financial account numbers. Finally, the Committee examined various federal laws and requirements governing SSN display and distribution by state and local entities.

On August 1, 2002, CCJ and COSCA endorsed and commended "the Guidelines to each state as a starting point and means to assist local officials as they develop policies and procedures for their own jurisdictions."

STATE COURTS' INTEREST IN COLLECTING AND USING SOCIAL SECURITY NUMBERS

Why is this question of concern to state courts? Why do state courts need to require parties to provide their SSNs in the course of state court litigation?

Identification of parties. A growing number of court systems are using case management information systems in which an individual's name, address, and telephone number are entered once, regardless of the number of cases in which the person is a party. Such "party based" systems are rapidly replacing "case based" systems. The advantage of these systems is multifold: they enable courts to update an address or telephone number for all cases in which the person is a party by a single computer entry, they provide judges and court personnel with a fuller array of justice information, and they allow for cleaner information sharing with other justice community participants such as law enforcement, prosecutors, probation systems, and the like. Absent the use of unique identifiers such as SSNs, the entire justice community would come to a grinding halt and be unable to meet many state and federal mandates. SSNs provide a unique identifier by which court personnel can determine whether the current "John Smith" is the same person as a previous "John Smith" who appeared in an earlier case and whether this was the same "John Smith" reported to the central criminal records repository.

The need for SSNs in the future may be substantially reduced by the use of other "unique" identifiers, e.g., biometric identifiers in criminal cases. Moreover, the ability to mask SSNs becomes easier as state courts implement sophisticated case management systems. Certainly the move to "automate" state courts with high-end technology allowing such services as electronic filing can provide opportunities for greatly limiting access to personal information such as SSNs. However, the time and costs of moving to such systems necessarily means that the ability to mask or redact such information is, for many courts, a future event not something that can or will be done overnight simply because there is federal mandate to do so.

Collection of fees, fines and restitution by courts. SSNs are the universal personal identifier for credit references, tax collection, and commercial transactions.

When courts give a criminal defendant an opportunity to pay an assessment resulting from a criminal infraction in periodic payments, the court needs to be able to function as a collection agency. Having the convicted person's social security number is necessary for use of state tax intercept programs (in which a debt to the state is deducted from a taxpayer's state income tax refund) and other collection activities. Moreover, SSNs are often used for purposes such as enforcing criminal fines and restitution orders or denying of motor vehicle registration.

Creation of jury pools and payment of jurors. SSNs are a necessary part of identifying eligible jurors through a process by which multiple lists (for instance, registered voters and registered drivers) are merged to eliminate duplicate records for individual citizens in creating a master source list for the random selection of jurors. Duplicate records double an individual's chance of being called for jury duty and reduce the representativeness of jury panels. Some courts use SSNs to pay jurors as well.

Making payments to vendors. SSNs are used as vendor identification numbers to keep track of individuals providing services to courts and to report their income to state and federal taxing authorities.

Facilitating the collection of judgments by creditors and government agencies. Courts are not the only entities that need to collect judgements. Judgment creditors need SSNs to locate a judgment debtor's assets to levy upon them. Courts often require that the judgment debtor make this information available without requiring separate discovery proceedings that lengthen the collection process and increase its costs. Federal law now requires state courts to place the parties' SSNs in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgements in order to facilitate the collection of child support. On October 1, 1999, that requirement was extended to include the SSNs of all children to whom support is required to be paid.

Notification to the Social Security Administration of the names of incarcerated and absconded persons. The Social Security Administration cuts-off all payments to persons incarcerated in federal, state or local prisons or jails, and to persons who are currently fugitives from justice. The savings to the federal budget from this provision are substantial. To implement this process, Social Security Administration needs to identify persons who have been sentenced to jail or prison and persons for whom warrants have been issued. The agency has traditionally obtained this information from state and local correctional agencies. See 42 USC § 402(x)(3). The state courts of Maryland are involved in an experimental program to provide such information directly from court records. The Maryland program has two additional future advantages for state courts. First, the program offers the possibility of obtaining better addresses for many court records; social security and other welfare agencies have the very best address records because of beneficiaries' obvious interest in maintaining their accuracy. Second, cutting off benefits may provide a useful incentive to those persons subject to outstanding warrants without requiring law enforcement to expend resources to find and serve such persons.

Transmitting information to other agencies. In addition to the Social Security Administration, many states provide information from court records to other state agencies. A frequently occurring example is the Motor Vehicle Department, to which courts send records of traffic violations for enforcement of administrative driver's license revocation processes. These transfers of information often rely upon SSNs to ensure that new citations are entered into the correct driver record.

PROPOSED LEGISLATION

Mr. Chairman, your legislation, H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003, contains the following provision:

SEC. 102. RESTRICTIONS ON THE SALE OR DISPLAY TO THE GENERAL PUBLIC OF SOCIAL SECURITY ACCOUNT NUMBERS BY GOVERNMENTAL AGENCIES

"(x)(I) An executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof or trustee appointed in a case under title II, United States Code (or person acting as an agent of such an agency or instrumentality or trustee) in possession of any individual's social security account number may not sell or display to the general public such number."

This section has serious implications for state courts in a variety of contexts.

For example, *federal* law requires courts to enter SSNs on court orders granting divorces or child support or determining paternity. Some states' laws contain similar requirements in other types of cases. As noted previously, given that over 96 million cases are filed annually in state courts, the task of redacting SSNs from existing documents is not only daunting, it may actually violate federal law in some cases and certainly violates many state "sunshine laws" to the extent that access to documents is required.

SSNs appear in many financial documents, such as tax returns, which are required to be filed in court (e.g., for child support determinations) or are appended to official court documents, such as motions for summary judgments. Restricting access to SSNs in such documents is difficult because often such information can be buried in a stack of documents, which are generally not reviewed by courts or clerks until the case is actually heard.

Courts will have substantial increased labor costs in staff time to redact or strike the appearance of SSNs in paper records or in microfilm/microfiche if the above requirement is imposed.

In addition, we are unclear whether H.R. 2971 applies to newly made court records or all records in a court's inventory. Obviously, asking courts to retroactively expunge or redact social security from all court records would be time consuming and expensive. Given the extensive records retention policies applicable to court filings, retroactive redaction or masking could be an impossible task in some states.

Finally, in an effort to make courts and court records more open, many courts are now beginning to make available many public records on the internet either as text/character documents or by scanning and placing them online through imaging software (PDF files). While the removal of SSNs in text/character documents may be relatively easy in some computer generated records (XML), other scanned records, such as PDF files, will be harder to change necessitating more staff and an increase in labor costs.

COSCA RECOMMENDATIONS

We have recommended that state courts adopt the following policies, unless state law directs them otherwise:

Official court files. State courts should not attempt to expunge or redact SSNs that appear in documents that are public records, and certainly this should not be required on a retroactive basis. As was mentioned earlier, federal law requires state courts to place the parties' SSNs in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgement in order to facilitate the collection of child support. The purpose of placing that data on judgments is not just to provide it to child support enforcement agencies; it is also to provide it to the parties themselves for their own private enforcement efforts. Any other approach puts the courts in an untenable position—having an affirmative obligation to provide judgments in one form to parties and child support enforcement agencies and in another form to all other persons.

This same reasoning applies to income tax returns or other documents containing SSNs filed in court. It would be unreasonable, and expensive, to expect courts to search every document filed for the existence of SSNs. Further, court staff has no business altering documents filed in a case; the SSN may have evidentiary value in the case—at the very least to confirm the identity of the purported income tax filer.

Case management information databases. Data in automated information systems raises more privacy concerns than information in paper files. Automated data can be gathered quickly and in bulk, can be manipulated easily, and can be correlated easily with other personal data in electronic form. Data in an automated database can also be protected more easily from unauthorized access than data in paper files. It is feasible to restrict access to individual fields in a database altogether or to limit access to specific persons or to specific categories of persons. Consequently, state courts should take steps to restrict access to SSNs appearing in court databases. They should not be available to public inquirers. Access to them should be restricted to court staff and to other specifically authorized persons (such as child support enforcement agencies) for whose use the information has been gathered.

Staff response to queries from the public. When court automated records include SSNs for purposes of identifying parties, court staff should be trained not to provide those numbers to persons who inquire at the public counter or by telephone. However, staff may confirm that the party to a case is the person with a particular SSN when the inquirer already has the number and provides it to the court staff member.

In short, staff may not read out a SSN but may listen to the number and confirm that the party in the court's records is the person with that number. This is the same distinction applied to automated data base searches. This distinction is one commonly followed in federal and state courts.

CONCLUSION

Mr. Chairman, we recognize the serious role of SSNs in incidences of identity theft and the fact that such information is readily available in a host of public records. The current state of affairs with regard to the treatment of SSNs provides lawbreakers the continued opportunity to exploit the current system at the expense of ordinary Americans. The threat of identity theft is real and we want to do our part to eliminate it. However, as previously noted, there is no simple solution and certainly no cheap solution to this problem. Even the public policy coming from Congress evidences the complexity of the issue by requiring the collection, use and availability of such information on one hand and then seeking to restrict access to its use on the other. We also hope that you assist the state courts in dealing with the unfunded mandate H.R. 2971 presents.

I have presented several ways our courts utilize SSNs and finding solutions to protect an individual's privacy will be complex and difficult. Many state courts are already taking steps to fashion solutions in response to the problem. Washington state, for example, is pioneering an innovative solution where they are creating two sets of court records: a public and a private one. Other states are experimenting with different approaches.

Chairman SHAW. Thank you for your testimony. Mr. Cate.

STATEMENT OF FRED H. CATE, PROFESSOR OF LAW, UNIVERSITY OF INDIANA-BLOOMINGTON, BLOOMINGTON, INDIANA

Mr. CATE. Thank you very much, Mr. Chairman. I want to join the chorus of those thanking you for your steadfastness in having pursued both efforts to improve the integrity of the Social Security system and to fight identity theft. We are well-served by those efforts and well-served by this hearing today.

As you well know, SSNs are used throughout both the public and private sectors for two very important and closely linked roles. One is to accurately link information, if you will, connect information to the file. Maybe one example will be sufficient to suggest the daunting task this really is. In the credit reporting industry in this country, 3 major national credit reporting agencies process 2 billion pieces of personal data on 180 million active consumers every month. Getting the right data in the right file is a considerable challenge.

The second role is, of course, to facilitate identification of individuals; and, again, credit reporting may be a useful example. The 3 credit reporting bureaus generate 600 million credit reports, and one of the uses of SSNs is to link the individual to the file so that it is then possible for the retailer or lender or whoever is requesting that file to actually determine that the individual is who he or she claims to be. This system of ubiquitous, widely available national SSNs has yielded many benefits, and you have heard of many of these over the past years. These are not merely commercial, although the commercial ones are certainly quite important.

I would just take a moment to say we often think of the commercial benefits in negative terms, identifying people who have defaulted on loans or filed for bankruptcy, but the commercial benefits are also quite positive by allowing individuals to benefit from their own positive behavior, their good credit records, and it is protecting those good credit records that SSNs play a key role in, which are particularly important in helping to reduce frauds by linking the individual to the file so that it is possible to verify their identity.

We have already heard about the use for location. I would refer you to testimony before this Subcommittee 3 years ago in which you heard about the impact on pension beneficiaries, that the addition of the SSN to name and address information increased the likelihood of finding a pension beneficiary from 8 percent to 85 percent, a more than tenfold increase by virtue of having access to the SSN. Law enforcement, of course, for years has had access and made use of SSNs; and in the days and months since 9/11 we have discovered new security uses and available benefits that SSNs generate.

Let me be clear: when we think about the programs that Congress and the Administration have put in place or are considering for border security, for airline security and other forms of national security, the question of SSN availability is only goes to the question of making those programs more accurate. It may very well be that you do not wish those programs to go forward, but whether or not they go forward it is clear we want them to be as accurate as possible, and that, of course, is what SSNs help make possible.

This, then, reflects a problem with the current bill. Let me say there are many aspects of the current bill that are very desirable, very laudable: efforts to increase the penalties for the misuse of SSNs, to enhance the efficiency and oversight over the assignment of SSNs, to get SSNs off of identity documents where they do not belong. Nevertheless, the effort to restrict disclosure subject to certain exceptions in an effort to protect against identity theft, all of my research suggests will be not only ineffective but counterproductive. There are a number of reasons for this, and I will conclude by touching on those.

First, the issue is not just use of SSNs. It is fine to say that the Attorney General can adopt exceptions so that SSNs can be used in national security matters. However, of course, what most matters is that the SSNs were available when the data were collected so that the data were properly placed in the correct file. Second, the two-tier system seems unlikely to work. Maintaining records, whether in the public sector or private, in which SSNs are reflected in one version of the records but not in the others creates an extraordinary burden.

Third, it is not clear that most cases of identity theft would be in any way affected by this bill. The FTC's September 2003, study on identity theft indicated that 76 percent of identity theft cases involved a friend, family Member, coworker, neighbor or an employee of somebody who has lawful access to the SSN. Restricting the further transmission or the display of the SSN would not be relevant in those cases, the vast majority of cases.

Finally, there are far more important steps, far more urgent steps, that Congress could and should take to help protect against identity theft and to reduce the role of SSNs in identity theft. I would point, for example, to Ms. Foss's three suggestions, which strike me as excellent, that those who are responsible for identifying people in connection with their credit reports should be given incentives to make more certain identification, increased funding for enforcement, more funding for agencies like the SSA. At the end of the day, while Congress is concerned with passage of the FACT Act, about accuracy of credit reports and other databases and ensuring that those are used and applied as accurately as possible, restricting access to SSNs is likely to have the opposite effect. Thank you.

[The prepared statement of Mr. Cate follows:]

Statement of Fred H. Cate, Professor of Law, University of Indiana-Bloomington, Bloomington, Indiana

My name is Fred Cate, and I am a Distinguished Professor and director of the Center for Applied Cybersecurity Research at IndianaUniversity, and a senior policy advisor at the Center for Information Policy Leadership at Hunton & Williams. For the past 15 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and served as reporter for the recent Department of Defense Technology and Privacy Advisory Committee. A brief biographical statement is attached.

I appreciate the opportunity to testify today, and I am doing so on my own behalf. My views should not be attributed to Indiana University or to any other institution or person.

The Essential Role of Social Security Numbers

My research on information flows in both public and private sectors, and all of the other research in this field with which I am familiar, highlights the need for, and difficulty of, accurately identifying individuals and attributing information about them. At first glance, these may seem like straightforward activities, but they have proved exceptionally difficult. How do I know that the person presenting himself—to apply for instant credit, seek a government benefit, or board an aircraft—is who he claims to be? And how do I know that the data I have about him is correctly associated with the right person?

One example may suffice to suggest the magnitude of this challenge. The three national consumer reporting agencies process two billion pieces of personal data on 180 million active consumers every month to generate 600 million credit reports a year. Making certain that each of those two billion pieces of data is placed in the right one of 180 million files and that each file is provided only in connection with the individual it concerns is a daunting task.

The challenge is exacerbated by many factors, including:

- The frequency of common names (e.g., there are more than 60,000 John Smiths in the United States alone), and the fact that names are not constant, thanks in part to 2.3 million marriages and 1.1 million divorces every year.[1]
- The variety of addresses available to many people (e.g., home, office, vacation home, Post Office box), the fact that several people may share the same address, and the speed with which addresses and telephone numbers change: according to the U.S. Postal Service, approximately 17 percent of the U.S. population—about 43 million Americans—changes addresses every year; 2.6 million businesses file change-of-address forms every year.[2]
- The inconsistencies with which we record names (e.g., J. Smith, J.Q. Smith, John Q. Smith) and addresses (e.g., "123 Main," "123 Main Street," "123 Main St.," "123 S. Main Street," "123 Main Street, Apt. B").

---

[1] National Center for Health Statistics, *National Vital Statistics Reports*, vol. 51, no. 8, May 19, 2003, at 1, table A.

[2] United States Postal Service Department of Public Affairs and Communications, *Latest Facts Update*, June 24, 2002.

- The spread of first telephone and then Internet technologies, the increased mobility of the population, and the development of truly national competition mean that fewer transactions are conducted face-to-face, much less with people we know.

As a result of these and other factors, the need for a unique, ubiquitous, national, constant, and authoritative identifier has become inescapable. Many activities in which we engage in both public and private sectors are impossible or impractical without it. That is why the Social Security Number has evolved to fill this role: modern government and business activities required it to identify individuals, and ensure that information about one individual is not erroneously attributed to another individual. These two functions are often interrelated.

The identification function is often misunderstood. Obviously, the fact that an individual presents a Social Security Number does not prove that he or she *is* the person that the Social Security Number identifies. Rather, the Social Security Number provides an efficient, reliable way of locating a credit report or other record containing information that can then be used to verify the identity of a person. So, for example, if I apply for instant credit at a retailer, the retailer may ask for my Social Security Number as a way of locating a summary credit report about me. That credit report will list, among other things, my name, address, phone number, past addresses, and other identifying information. The retailer can then compare the information I have put on the instant credit application with the information contained in the credit report to determine if I am who I claim to be.

Two points are critical here: First, knowing my Social Security Number alone does not get me credit; it is merely a quick way of locating reliable information about me that then can be used to verify my identity. If you don't believe me, walk in to any Target or Wal-mart or other retailer and try to obtain instant credit by presenting your Social Security Number alone.

The second critical point is that the underlying data store must be accurate and reliable. Social Security Numbers play an essential role here as well by helping to ensure that data are linked to the right individuals and that subsequent users of those data have confidence in the accuracy and completeness of the data. When you apply for instant credit or an auto loan or a mortgage the lender wants to know that it is seeing an accurate and complete picture of your creditworthiness and that there will be reliable, affordable ways of determining if you declare bankruptcy or overextend yourself on credit in the future. Social Security Numbers facilitate the databases that do this.

Benefits of Ubiquitous Social Security Numbers

The availability and reliability of Social Security Numbers makes possible accurate and efficient national credit reporting and directly contributes to greater consumer choice, lower prices and interest rates, more widespread and affordable home ownership, and other benefits. Social Security Numbers facilitate commerce in other ways, for example, by making it easier to identify consumers remotely, thereby enhancing lender and seller confidence and reducing fraud.

The benefits of accessible Social Security Numbers are not limited to commerce. Social Security Numbers also play critical roles in identifying and locating missing family members, owners of lost or stolen property, heirs, pension beneficiaries, organ and tissue donors, suspects, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. Just as with credit reporting, Social Security Numbers—often combined with other information, such as name—make it possible to construct accurate, comprehensive public record and third-party databases and search them quickly and reliably. Paula LeRoy from Pension Benefit Information testified before this subcommittee in 2001 that the presence of a Social Security Number increases the chance of locating a pension beneficiary from less than 8 percent to more than 85 percent—a greater than ten-fold increase.[3] Moreover, Social Security Numbers can overcome inconsistencies in names or address or errors in the way this information is recorded.

Social Security Numbers are critical to identity verification and background checks required for airline employees, school bus drivers, child care workers, Defense Department and intelligence agency employees, and congressional staff. Post-September 11 programs for enhanced border, critical infrastructure, and passenger facility security all depend on being able to identify individuals and asses the risk they present by quickly connecting to accurate information about them. This is a

[3] Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers before the Subcom.on Social Security of the House Comm. on Ways and Means, May 22, 2001 (statement of Paula Leroy).

substantial challenge, as stressed by the recent final report of the Department of Defense's Technology and Privacy Advisory Committee.[4] Social Security Numbers are essential to this task.

The essential roles played by Social Security Numbers highlight the importance of today's hearing and of your longstanding efforts, Mr. Chairman, and those of this subcommittee to ensure the integrity and security of Social Security Numbers and to protect against their misuse. We must ensure that Social Security Numbers are accurate, unique, and available for responsible use. H.R. 2971 takes some important steps in this direction, for example, by getting Social Security Numbers off of identification cards and checks where they do not need to be displayed, and enhancing protections within the Social Security Administration for ensuring that Social Security Numbers are issued appropriately and securely. However, the breadth and importance of the roles played by Social Security Numbers raise concerns about some of the restrictions posed by H.R. 2971.

The Problem of Restricting Access Except for Specified Uses

H.R. 2971 would broadly restrict the "sale, purchase or display" of Social Security Numbers, subject to exceptions for certain uses—for example, credit reporting and national security. I applaud your attention to these critical needs. The problem, however, is that Social Security Numbers need to be associated with the underlying data from the start to ensure that they are included in appropriate databases and made part of the right files. So, for example, provisions authorizing the Attorney General to permit certain uses for national security purposes are important, but almost certain to be ineffective, because national security and law enforcement officials need—and regularly use—databases constructed for other purposes to access routine innocuous data to determine the risk that an individual may present. It is fine for the Attorney General to require that an individual entering a government facility or boarding an aircraft present a Social Security Number, but it will not matter at all if those numbers cannot be used to access properly segregated data in existing databases.

The FBI and other law enforcement agencies, for example, routinely access aggregate data collected and stored by Acxiom, ChoicePoint, LexisNexis, and other providers for many commercial uses. Allowing the FBI to use Social Security Numbers is important, but for the data to be reliable, the providers must have been permitted to use Social Security Numbers all along, and the government and private entities that supplied data to them must also have used them. Focusing only on the end user is inadequate.

The focus on use also ignores the fact that national security and law enforcement uses of Social Security Numbers frequently involve databases created for other purposes. Those other purposes subsidize the national security and law enforcement uses that the bill is likely to permit; if Social Security Numbers cannot be provided for those other purposes, they will not be available for the national security and law enforcement uses either.

The limitation of the display restriction to "the general public" is unlikely to ameliorate this risk, because of the breadth, vagueness, and circularity of the definition given the phrase "display to the general public": "to make such number available in any other manner intended to provide access to the general public." Moreover, as the General Accounting Office noted in its 1999 report to you, it is difficult to imagine that many data providers will undertake the cost and effort of maintaining two sets of data—one without Social Security Numbers for display to the general public and one without for other uses—or that data from which Social Security Numbers have been removed or obscured can be maintained, aggregated, and filed accurately.[5] In addition, because violation of this provision is made a crime, subject to five years imprisonment, it seems likely that most businesses will steer clear of any activity that might be considered "display to the general public," even if that means no longer providing valuable services that may very well continue to be legal.

The history of information flows is one of constantly evolving new and valuable uses. If those uses have to be approved one at a time through a legislative or regulatory process, they are less likely to evolve as quickly or to be as affordable when they do. Regulatory barriers might very well have restricted the unanticipated use of commercial records for locating parents delinquent with child support payments or retirees entitled to pension benefits. These uses were not anticipated when the

---

[4] U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 36–38 (2004).

[5] General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number is Widespread* (GAO/HEHS–99–28) (1999).

databases on which they rely were first created, but they are valuable and important today.

Rulemaking Authority and Lack of Preemption

The many and vital benefits that the public enjoys as a result of ubiquitous Social Security Numbers are also threatened by the broad discretion given the Attorney General as to whether, and if so how, he might create exceptions to the bill's restrictions. As we have seen, any meaningful exception would likely result in undercutting significant portions of the bill. Narrower exceptions run the risk of not achieving the goals they are designed to serve and/or placing private—and public-sector custodians in the untenable position of maintaining duplicate databases or supplying data that may not be accurate or complete. The broad discretion given the Attorney General also creates a new regulator, parallel with the FTC which has long had authority in this area.

What is most surprising, however, in view of the need for a truly national identifier for national security, law enforcement, and commercial purposes is that the bill does not appear to expressly preempt state laws and regulations concerning the disclosure and use of Social Security Numbers. As Congress acknowledged last year with passage of the Fair and Accurate Credit Transactions Act, it is difficult to imagine anything more intrinsically national in scope than the creation of accurate, complete databases necessary to support national commerce, national security, nationwide law enforcement, and the fight against identity theft.

Incentives for Inaccuracy

Social Security Numbers are critical for maintaining data about individuals accurately. H.R. 2971, by restricting the use of Social Security Numbers, threatens to make databases less accurate. This is especially likely in the face of the proposed restriction on uses of credit header information, which is often the source of accurate, up-to-date data necessary to identify and locate individuals and which is already the subject of existing financial privacy law.

Nowhere is H.R. 2971's threat to accuracy more clear than in the provision prohibiting a person from doing business with an individual who will not provide a Social Security Number, unless federal law requires disclosure of the Social Security Number. The federal government has repeatedly acknowledged that it cannot maintain accurate records without access to Social Security Numbers; that is why the government requires them in such a wide range of settings even where no question of Social Security benefits is involved. But under this provision, the law would refuse to acknowledge that businesses face the same need; a business cannot refuse to provide a product or service to an individual who refuses to disclose his Social Security Number, even if that number is necessary to provide the product or service. The net result is certain to be data less able to be linked accurately with the individual it concerns—an ironic outcome at the same time as Congress has mandated the FTC and other regulators explore ways of improving accuracy in credit reports and other databases.

Social Security Numbers and Identity Theft

The motivation behind proposed new restrictions on the use and availability of Social Security Numbers is preventing identity theft. Identity theft is a growing scourge of modern life. It takes a toll not only on the economy and businesses, who bear the lion's share of economic loss associated with the crime, but also on individuals who struggle sometimes for years to correct false information—information wrongly placed—in their commercial or government records. It is certain that much more needs to be done to address the rising tide of identity theft; my research suggests that restricting Social Security Numbers in government and commercial records is not the right step.

While we do not know as much as we need to about identity theft, thanks to the efforts of FTC and others, one important fact we are learning is that much—perhaps most—identity theft is not committed by a stranger, but by a family member, friend, or co-worker. According to the FTC's Synovate study of identity theft, published in September 2003 and based on more than 4,000 interviews, of the one-quarter of identity theft cases in which the victim knew the identity the perpetrator, 35 percent involved a "family member or relative" and another 18 percent involved a friend or neighbor. Another 23 percent of cases involved someone who worked at a company or financial institution that held the victim's financial information.[6] Taken together, 76 percent of cases in which the perpetrator did identify the thief did *not*

[6] Federal Trade Commission, *Identity Theft Survey Report* at 28–29 (2003).

involve access to third-party data (e.g., commercial or public records) that appears to be the target of H.R. 2971.

In the remaining 24 percent of cases that might be affected by H.R. 2971, the role played by Social Security Numbers in identity theft is apparently the same as that played in other settings—namely, to link an individual to a database file (most often a credit report). Given the many valuable uses of Social Security Numbers and the many ways in which those numbers are available, it would be far more efficient, as well as more broadly effective, to focus on ways for improving the identification of the person with his file, rather than attempting to restrict access to the Social Security Number in the first place. So, for example, the law might creative incentives for credit grantors to take additional steps to ensure that the person is who he claims to be. This would held deter not only the 24 percent of identity theft cases that involve a stranger, but the other 76 percent that involve a friend, family member, or employee of a business with whom the victim has a relationship.

While our knowledge about identity theft is still developing, we do know that accurate Social Security Number information, attached to all financial information, is critical to fighting identity theft and to remedying it when it does happen. Social Security Numbers—if unique and reliable—are critical to preventing the granting of credit in somebody else's name. They are critical to keeping bad data out of innocent people's files. They are critical to identifying identity theft when it occurs and notifying victims. Yet H.R. 2971 seems intended and likely to diminish their availability.

The FTC study reports that businesses lost $47.6 billion due to identity theft.[7] We should certainly be hesitant before imposing restrictions on Social Security Numbers that could add to that cost, especially if we cannot identify clear specific benefits from those restrictions. In addition, countless hearings, interviews with identity theft victims, and studies have shown that the greatest burden most identity theft victims face is clearing their good names. We should be hesitant before doing anything that would make that already difficult process any harder.

Finally, I would just note there is some risk of getting caught in an unending cycle. The need for a ubiquitous, reliable, unique identifier is not going to go away. If legislation makes Social Security Numbers unavailable, government and industry will devise another system of numbers. If Social Security Numbers today play a significant role in identity theft—and I have not seen evidence that they do—what leads us to think that the identifying number of the next decade won't play that same role?

Conclusion

Ubiquitous Social Security Numbers help identify people and ensure that information is associated with the correct person. These two critical roles are essential to many valuable activities—from facilitating national competition to locating heirs and missing children to enhancing national security. Accessible Social Security Numbers are also critical to preventing, detecting, and remedying identity theft, yet they appear to play little if any role in contributing to most cases of identity theft. This subcommittee would be well advised to continue its careful study of these issues; to enlist the FTC, the Social Security Administration, and other appropriate agencies in carrying out the research identified in H.R. 2971; to enact those measures necessary to enhance the integrity of the systems by which Social Security Numbers are created and assigned; to strengthen criminal penalties against the deceptive or fraudulent use of Social Security Numbers; and to identify and adopt specific measures to help victims of identity theft reclaim their good names easily and quickly. But I would urge the greatest caution before proceeding with any restrictions on the productive and value uses of Social Security Numbers necessary to the benefits consumers enjoy today, our economic resiliency, the prevention and detection of crime, and our national security.

Chairman SHAW. Thank you. Mr. Mierzwinski.

STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PUBLIC INTEREST RESEARCH GROUP

Mr. MIERZWINSKI. Thank you, Mr. Chairman. It is a pleasure to be back before the Committee. On behalf of the State PIRG. I

[7] Id. at 7, table 2.

would like to offer our views on SSN privacy, identity theft, and related matters. Again, I also thank you for your long-time leadership on keeping these issues before Capitol Hill. I realize it is complex to enact a bill that has the jurisdictional breadth of your bill, but we think it is important, and we encourage you to keep going forward.

I want to make three points today, first on identity theft, then on Nation and its inadequacies and, third, on the need for your bill. Identity theft is not rocket science. Everyone agrees that anybody with no criminal skill and little physical risk, if any at all, can commit identity theft because of two factors, in my opinion, my professional opinion, I think that are agreed on by most experts in the field. The first factor is the ubiquitousness of the SSN. Your financial DNA is easily available out there.

The second factor is the sloppy practices of credit reporting agencies and creditors when they issue credit. They issue credit not based on a number of matching points of identity. As Mr. Beales pointed out the FTC will be looking at ways to increase the number of matches that are required as part of a study under Nation based, by the way, on California law, but because the instant credit context often involves merely a name and a social. They don't check for an extra address or whether the address matches or a previous address, and it is just very simple to obtain instant credit with a name, a social and any other address that you might have.

In our first studies done 8 or 9 years ago, we had no data on how extensive the problem was, but we did know that the problem was serious for consumers. We found in the year 2000, based on a survey, that consumers spent 175 hours clearing $17,000 worth of fraudulent credit off of their accounts and spent over $800 in out-of-pocket expenses trying to clear their names. That, of course, doesn't begin to measure the emotional distress.

So, the victims routinely tell us that they don't often know how the identity theft occurred. Some of them, to be sure, it happened because of a relative. Increasingly, identity theft, because it is such a simple crime, is being taught in the prison yards. I have been told recently that it is a business model for methamphetamine gangs. They like to stay up at night, as you might guess, and they often go dumpster diving and collecting financial DNA and other information.

Identity thieves also often take jobs—as part of gangs again, not relatives or brothers or friends. They will often take jobs as temporary administrative employees solely to harvest SSNs. So, the ubiquity of the SSN is out there. It is a big problem, and all the police that we have interviewed for our most recent reports, again, agree that the availability of the SSN is a significant problem. So, I would respectfully disagree with Professor Cate that the report suggests that it is not a problem. It is. The flaws in Nation, it is preemptive. We opposed final passage because it took away the laboratories of democracy, all the good ideas in fact that came from State law, yet Nation takes away the right of the States to enact most State laws.

Second, there is no private right of action in Nation for many of the new rights that consumers have gained. Third, some of the rights in Nation to restore and clear your name are only possible

if you file a police report. Many police don't take police reports. So, additional action is needed at the State level to give victims more ability to take advantage of Nation. Finally, the FACT Act doesn't protect SSNs; and that is why we need your bill. We need your bill to protect SSNs.

Also, I would disagree with the notion that we need credit headers in society today. We think section 108 banning credit headers is a very important section. I have outlined in my testimony in detail why we think that the credit bureaus are now using the notice and opt-out privileges or conditions of Gramm-Leach-Bliley to collect SSNs from individuals, because, in fact, our reading of Trans Union II, a case upheld by the D.C. Circuit Court, is that credit bureaus can no longer use SSNs in credit headers. They can use the old ones they previously collected, but unless they provide notice and opt out they cannot. So, we think that your bill will perpetuate and narrow even further what the agencies have done in the Gramm-Leach-Bliley rules which were upheld in that court decision.

The last point I want to make, I want to echo Mr. Hoofnagle's remarks on the refusal to do business provision. I know you have long stated that a video store should not be able to ask you for your SSN as a condition of renting a video. We agree, and we think that that is one of the most important sections of your bill. I think that if you tell the average American that you are going to put their SSN back in the box that Congress originally intended it to be in, that it can only be used for Social Security purposes, Medicaid purposes, tax purposes, they will be very happy with your legislation. Thank you.

[The prepared statement of Mr. Mierzwinski follows:]

Statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group

Chairman Shaw, Rep. Matsui and members of the committee: We are pleased to again present the views of the U.S. Public Interest Research Group on ways to improve citizen and consumer privacy by protecting the Social Security Number from misuse and misappropriation for fraudulent purposes, including but not limited to, identity theft. As you know, U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups, which are non-profit and non-partisan public interest advocacy groups active around the country.

Summary

U.S. PIRG believes that the widespread availability of the Social Security Number (SSN), the key to your financial identity, contributes to identity theft,[1] which is one of the nation's fastest growing white-collar crimes. According to a 2003 survey by the Federal Trade Commission (FTC), nearly ten million Americans in the past year and one in eight adult Americans in the last five years has been a victim of identity theft.[2] While the 2003 enactment of the Fair and Accurate Credit Transactions Act

[1] The state PIRGs have studied credit reporting and identity theft for fifteen years. See, for example, "Nowhere To Turn", Benner, Givens and Mierzwinski, CALPIRG and Privacy Rights Clearinghouse, 1 May 2000 at http://calpirg.org/CA.asp?id2=3683&id3=CA& We have released two previous reports on identity theft "Theft of Identity: The Consumer X–Files", CALPIRG and US PIRG, 1996 and "Theft of Identity II: Return to the Consumer X–Files", CALPIRG and US PIRG, 1997, as well as four reports on errors by credit reporting agencies since 1991, most recently "Mistakes Do Happen," 1998. For additional details, see testimony of Edmund Mierzwinski before the Senate Banking Committee, 31 July 2003, at http://www.pirg.org/consumer/pdfs/consumer31julymierzwinski.PDF

[2] See Federal Trade Commission "Identity Theft Report," released 3 September 2003, prepared by Synovate at http://www.ftc.gov/opa/2003/09/idtheft.htm

(FACT Act)[3] may reduce some of the sloppy credit bureau and creditor practices[4] that make it easy to open a fraudulent account in someone else's name, it is still incumbent on this committee to take additional steps to protect the Social Security Number. If the SSN is available in fewer places, on fewer documents and used for fewer commercial transactions or database identifiers when it shouldn't be, identity thieves as well as stalkers[5] and even terrorists[6] will be less able to harvest it for misuse. It is well-documented, for example, that identity thieves will often seek employment as temporary office employees, solely to harvest SSN and other bits of "financial DNA." Identity theft is a serious crime. It costs the economy billions and wreaks untold havoc on the lives of hard-working Americans who face the emotional distress and nightmare of clearing their names.

In addition, limiting the sale, purchase and display of the SSN in the private sector extends important privacy principles of the U.S. Privacy Act that have generally operated to protect privacy in government uses of information to also protect privacy in commercial uses of information, where consumers have generally only been protected by a patchwork of modest safeguards. As a result of the permissive availability of SSNs for use in the private sector, the SSN has leaked into use in all aspects of commercial transactions.

Your bill contains two important provisions we have long supported. First, it extends a strong anti-coercion provision that will limit private sector use of the Social Security Number by making it an unfair trade practice to refuse to do business with a consumer who refuses to provide an SSN. Second, your bill fully closes the court-narrowed credit header loophole, which has allowed secondary sale and use of Social Security Numbers without consent by credit bureaus, outside of the protections of the Fair Credit Reporting Act (FCRA).

In addition, your bill imposes important restrictions on the sale, display and use of the Social Security Number. For example the bill bans display on government-issued checks, on government or private sector employee and benefit ID cards and on drivers' licenses. It generally bans display, purchase or sale in the private sector. Your bill restricts use of SSNs by prison labor, following the well-publicized Metromail scandal involving a convicted felon who stalked a grandmother by tele-

---

[3] The identity theft epidemic was not the spark that kindled passage of the FACT Act. Congress had ignored identity theft for years Expiration of certain time-limited restrictions on state authority to enact stronger credit and privacy laws drove industry to support permanent extension of the preemption of state laws. Although the new law includes several elements of PIRG's long-sought reform platform, the bill's price was unacceptable, since Congress permanently restricted most state rights to enact stronger laws, even though the best parts of the law are based on recent state laws. Both the Fair and Accurate Credit Transactions Act of 2003 (PL 108–159, 12/04/03) and the FCRA as amended are available at the FTC website at http://www.ftc.gov/os/statutes/fcrajump.htm PIRG maintains an archive of FACT Act documents at http://www.pirg.org/consumer/fcra.htm

[4] Financial identity theft requires little criminal skill and no physical risk. Identity thieves armed with only your name and SSN exploit the creditor/credit bureau practice—extremely prevalent in the "instant credit" context, of matching only these two identifiers in the credit granting process. Conversely, since consumers are not trusted users, as are creditors, a credit bureau requires a consumer, to obtain his or her own credit report, to provide a full name, an SSN, an address, previous addresses for the past five year and, often, a xerox copy of a drivers' license or utility bill showing that same address. Of course, identity thieves are not seeking to obtain your credit report, merely to obtain credit in your name at their address. While certain FACT Act provisions are designed to increase creditor and credit bureau verification before account opening, limiting the availability of the SSN will make it harder to obtain your "financial DNA" and use it.

[5] Amy Boyer was the first known victim of an Internet stalker. A man named Youens tracked her with confidential information, including her Social Security Number, allegedly obtained through an Internet information broker. EPIC maintains an Amy Boyer archive at http://www.epic.org/privacy/boyer/ See PIRG's archived fact sheet at http://www.pirg.org/consumer/trojanhorseboyer.pdf

[6] According to recent news reports, a Kansas City man found out when he tried to purchase a car that his Social Security Number had been used by one of the suspected 9/11 hijackers' associates still at large. "Man Trying To Buy Car Finds Out 9/11 Terrorist Took ID," Omaha News Channel, 21 April 2004, last accessed at http://www.theomahachannel.com/news/3026399/detail.html on 13 June 2004. Further, one of the associates of the 9/11 hijackers, Lofti Raissi, had been reported to be using the Social Security Number of a long-dead New Jersey woman, suggesting one reason that the bill's protections for the SSNs of the deceased should be increased [See Title I, Section 101, exception VII of HR 2971 and Section 107(c)(2) of HR 2971]. Of course, nearly all the hijackers had one or more valid or invalid SSNs. See testimony of Social Security Administration Inspector General James Huse before the House Judiciary Committee, 25 June 2002, at http://www.house.gov/judiciary/huse062502.htm Also see the 8 November 2001 Joint Hearing on the Social Security Administration Death Master File of the Ways and Means Committee Subcommittee on Social Security and the Financial Services Oversight and Investigations Subcommittee archived at http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=83

phone. It also adds new safeguards when obtaining a Social Security Card, to prevent fraudulent use and protect the integrity of the Social Security Number system. Your bill also increasing criminal penalties for misuse of the SSN. We offer suggestions below to narrow the exceptions provided in the bill to better achieve its purpose.

Any legislation enacted should be simple, based on Fair Information Practices,[7] and contain as few loopholes and exceptions as possible. It is critical that new legislation not preempt or roll back existing privacy protection under either the Gramm-Leach-Bliley Act (GLBA) regulations[8] or the Shelby drivers' privacy amendments.[9] We urge you to resist business demands for exceptions and loopholes. You should especially challenge their specious arguments that so-called business-to-business uses will not pose privacy risks.

Unless credit bureaus and others are weaned from their over-reliance on the Social Security Number as a unique identifier, we will not succeed in protecting the SSN from misuse.

In addition to the problems created by theft of the SSN, its use in the credit system as a supposed unique identifier is flawed and leads to inaccuracy in credit reporting due to errors in data entry. Unlike credit card numbers, which contain a check-sum digit reducing data entry error rates, SSNs can be easily entered with transposed digits or other errors. Mistakes in credit reports lead to consumers either being denied credit or paying too much for credit.

(1) Principles of Social Security Number Protection: Simplicity, With Few, If Any Exceptions and Loopholes

Privacy expert Robert Ellis Smith, the publisher of Privacy Journal and author of "Social Security Numbers: Uses and Abuses" (May 2001) has proposed a simple Social Security Number protection scheme.[10] Your bill tracks much of it closely. Here is Smith's proposal, with his explanations in brackets:

1. "It shall be illegal to buy or sell the Social Security number of a person." [This is the source of much identity theft; it is always a secondary use of the SSN; and it is inconsistent with using the SSN as an AUTHENTICATOR of personal identity.]
2. "No person shall be required to provide a Social Security number on an application for credit or on a request for a copy of one's own credit report under the Fair Credit Reporting Act." [The FCRA merely requires satisfactory proof of identity to see one's own credit file. Use of SSNs to make a match between a requested credit report (by a credit grantor) and a credit report in a credit bureau's system has been the cause of confusion for credit grantors, nightmares for consumers, and identity theft. If credit bureaus did not rely on SSNs

---

[7] Fair Information Practices are discussed in numerous contexts in the Congress today. Unfortunately, many industry-supported bills and nearly all industry "studies" seek to dumb-down the comprehensive Fair Information Practices to unacceptable levels. As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices. Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. http://www.privacyrights.org/AR/fairinfo.html The document cites the version of FIPs in the original HEW guidelines, as well as other versions.

[8] The GLBA created a category of protected "non-public personal information." The final GLBA financial privacy rules issued by 7 federal financial agencies defined Social Security Numbers as non-public personal information (NPPI). A key provision is that the transfer of Social Security Numbers from financial institutions to credit bureaus is only allowed for regulated Fair Credit Reporting Act purposes (eg, for use in a credit report) but not for unregulated purposes, where the credit bureau would be considered a non-affiliated third party. The agencies correctly interpreted the law to prevent the sharing of Social Security Numbers unless consumers are given notice of the practice and a right to opt-out.

[9] Senator Shelby's 2000 amendments to the Driver's Privacy Protection Act were incorporated as Section 309 of the Transportation Appropriations bill (PL 106–346) signed by the President 23 October 2000. The amendment requires states to obtain express consent of drivers before the sharing or selling of a driver's "highly sensitive personal information," including Social Security Number, photograph, image, or medical or disability information. In 1999, Shelby had incorporated these provisions into law as part of the Appropriations bill, but only for one year, while the 2000 amendment amends the DPPA itself. In 2000, the Supreme Court upheld the constitutionality of the DPPA in *Reno vs. Condon*.

[10] See the Privacy Journal website for more information. Smith's latest book is "Ben Franklin's Web Site: Privacy And Curiosity From Plymouth Rock To The Internet" http://www.privacyjournal.net/

to make a match, 80 percent of identity theft would cease. There is a long list of case law to support the need for this provision.]

3. "No person shall be compelled or coerced into providing a Social Security number for any transaction unless there are income-tax consequences in the transaction or there is relevance to Social Security, Medicare, or Medicaid benefits. No person shall be compelled or coerced into providing a Social Security number on an application of employment until there has been a firm offer of employment. Any application for employment shall state that the request for the Social Security number prior to a firm offer of employment is voluntary." [This would essentially freeze demands for Social Security numbers in a way least disruptive to organizations currently relying on SSNs. It would tie demands for Social Security numbers to the two original purposes (SSA administration and federal taxes) two uses that are at least anchored in long-standing law. Placing SSNs on job-application forms increases the risk of exposing them to fraudulent users of SSNs.]
4. "No institution of higher education or elementary or secondary school shall use a student's Social Security number as a student identification number." [An alarmingly high number of identity theft frauds originated from SSNs taken from universities. Deterring school systems from using the SSNs as a student ID number will permit parents to delay labeling their children with numerical IDs.]

(2) Principles of Social Security Number Protection And Analysis of HR 2971

U.S. PIRG concurs with the detailed testimony today from the Electronic Privacy Information Center (EPIC). We believe that the most effective way to protect Social Security Numbers would be to enact simple, straightforward legislation that reins in the widespread non-statutory uses of the Social Security Number as an identifier in the private sector.[11]

(A) Principal One: No Coercion By Businesses

The Social Security Number was originally intended for Social Security purposes. Its federal government uses have been expanded to tax and Medicaid purposes. No private sector business should be able to insist that a consumer provide an SSN as a condition of doing business, unless that firm is required to collect the SSN for official government purposes. Your bill (Section 109) makes coerced demand (refusal to do business) of a consumer's Social Security Number an unfair trade practice under Section 5 of the Federal Trade Commission Act. No one should have to give up his or her SSN to rent a video, as you have long pointed out.[12]

(B) Principal Two: Close The Credit Header Loophole

Your bill (section 108) also incorporates provisions long championed by its cosponsor Rep. Kleczka closing the so-called credit header loophole. Under an egregious 1994 decision of the Federal Trade Commission, consumer reporting agencies (credit bureaus) had developed a thriving business selling Social Security Numbers outside the Fair Credit Reporting Act[13] (FCRA), without consumer consent.

Credit headers include information ostensibly not bearing on creditworthiness and therefore not part of the information collected or sold as a consumer credit report. The sale of credit headers involved stripping a consumer's name, address, Social Security Number and date of birth from the remainder of his credit report and selling it outside of the FCRA's consumer protections. Although the information, marketing and locater industries contend that header information is derived from numerous other sources, in reality, the best source of credit header data is likely financial institution information, which is updated regularly.

---

[11] Ideally, such a bill would also narrow many of the government use exceptions that have been established over the years allowing the Social Security Number to be used as an identifier and matching element for secondary purposes unrelated to Social Security.

[12] This is essentially extending Section 7 of the Privacy Act of 1974, Public Law 93–579 (which protects the Social Security Number in government uses with an anti-coercion provision) to the private sector.

[13] 15 USC 1681 *et seq.* See the FTC's version of the FCRA as amended by the FACT Act at http://www.ftc.gov/os/statutes/fcrajump.htm

While the DC Circuit, U.S. Court of Appeals, has upheld the Gramm-Leach-Bliley Act privacy regulations[14] and thereby narrowed the credit header loophole,[15] more needs to be done. The regulations do however allow the harvesting of SSNs for secondary purposes if the law's notice and opt-out provision is complied with. A recent Washington Post[16] story notes that the credit bureaus are now adding a boilerplate notice to requests for credit reports or subscriptions to their over-priced credit monitoring services, which could allow them to bypass the court restrictions:

> "And the other "gotcha:" "There is an even higher price," the reader says. "Reading the privacy disclosure information, I was surprised that you were agreeing to let them use everything in your credit report for marketing—by them, by their affiliated companies and by others."
>
> Bad enough that many privacy policies state that they're going to share your name, address, phone, Social Security number, birth date, even credit-card number for marketing purposes—resulting in more junk mail, spam and telemarketing calls (yes, even if you signed on to the federal Do Not Call Registry, because now you have a business relationship).

In 1994, the Federal Trade Commission had granted an exemption to the definition of credit report when it modified a consent decree with TRW (now Experian). The FTC said that certain information would not be regulated under the Fair Credit Reporting Act. The so-called credit header loophole allows credit bureaus to separate a consumer's so-called header or identifying information from the balance of an otherwise strictly regulated credit report and sell it to anyone for any purpose.

(C) Principal Three: Restrict The Sale, Purchase and Display of the SSN

Your bill imposes important restrictions on the sale, display and use of the Social Security Number. For example the bill bans display on government-issued checks, on government or private sector employee and benefits ID cards and on drivers' licenses, and generally bans display, purchase or sale in the private sector. Your bill restricts disclosure to and use of SSNs by prison labor, following the well-publicized Metromail scandal. It also adds new safeguards when obtaining a Social Security Card, to prevent fraudulent use and protect the integrity of the Social Security Number system. Your bill also increases criminal penalties for its misuse.

(D) Principal Four: Not All Social Security Number Bills Are Created Equal

In previous Congresses, many worthy bills, in addition to your own, most recently HR 4857 (106th) and HR 2036 (107th), have been proposed by privacy champions. In the 107th Congress, meritorious proposals included HR 1478 (Kleczka), HR 220 (Paul) and S 324 (Shelby) to protect Social Security Numbers. Among other Social Security Number bills with positive features in the 106th Congress was a proposal by Rep. Markey (HR 4611).

However it is important to note that some well-intentioned privacy bills may actually increase the risk of sale or display of Social Security Numbers. For example, in the 106th Congress, the most prominent Senate proposal to ostensibly protect Social Security Numbers actually would have expanded commercial availability of Social Security Numbers. Originally intended to serve as a legacy for Amy Boyer, the first known victim of an Internet stalker, the Amy Boyer Law,[17] as very nearly enacted into law,[18] was actually a Trojan Horse and would have expanded commercial

---

[14] On 16 July 2002, the DC Circuit of the U.S. Court of Appeals, Case No. 01–5202 [See http://laws.findlaw.com/dc/015202a.html] upheld an April 2001 U.S. Court DC District ruling (Trans Union LLC v. Federal Trade Commission, Civil Action No. 00–2087, see http://www.dcd.uscourts.gov/00-2087.pdf) (the case now known as Trans Union II, consolidating Trans Union vs. FTC and IRSG vs. FTC) that the privacy rules issued under GLB are constitutional. [In *Trans Union I vs. FTC* the DC Circuit had upheld at FTC order that unregulated credit headers could not include dates of birth because of their use in credit scoring models and therefore, in credit decision-making. That case also upheld the constitutionality of the FCRA and that privacy protection serves an important government purpose. See (No. 00–1141, 13 April 2001, (cert denied, 10 June 2002 by Supreme Court), *Trans Union I vs. FTC,* http://laws.findlaw.com/dc/001141a.html

[15] For a discussion of the credit header loophole and the treatment of the SSN as protected non public personal information, see the GLBA Privacy Rule at pages 80–83, Federal Trade Commission, 16 CFR Part 313, Privacy Of Consumer Financial Information, Final Rule, available at http://www.ftc.gov/os/2000/05/glb000512.pdf

[16] See Oldenburg, Don, "Free Credit Reports That Cost You Your Privacy", The Washington Post, 17 Feb 04.

[17] See PIRG's archived fact sheet at http://www.pirg.org/consumer/trojanhorseboyer.pdf

[18] The Amy Boyer Law, introduced as S. 2554, (Gregg, 106th) was incorporated as Section 626 into the Commerce-Justice-State Appropriations (HR 4690 RS) and passed into law as Section 635 of HR 5548, which was included in HR 4492 as sent to the President, but then was re-

Continued

loopholes for obtaining Social Security Numbers, failed to protect Social Security Numbers on public documents and also would have preempted stronger state privacy laws. Subsequent proposals from the Amy Boyer Law's chief sponsor, Senator Gregg, and Senator Feinstein, have been better, but still deficient compared to your approach.[19]

(3) Suggestions To Improve HR 2971:

We concur with EPIC's detailed recommendations to strengthen the bill and narrow its exceptions. In particular, we agree that the Congress should limit the Title I exceptions for governmental sale of the SSN. Specifically, we recommend that subsection (V), which allows unlimited sale of SSNs to thousands of credit reporting agencies (CRAs), be removed from the bill. This exception is too broad and allows unrestricted transfers of government records containing social security numbers to CRAs, possibly for purposes unrelated to regulated credit reporting, including direct marketing. If it remains, it should be re-drafted in the manner of the credit header section, Section 109, which would only allow the use of the SSNs so provided for provision in a regulated credit report, not for any other purpose.

Second, as EPIC describes, additional procedural safeguards should be added to restrict the Attorney General's Section 102 prerogatives in granting additional sale and display exceptions. These include addition of a public comment period to the rulemaking, eliminating the "undue" qualifier and adding the crime of identity theft as a risk factor, and requiring any entity that gains use of the SSN through an exception to use technical means, such as encryption, to protect the SSN.

We also concur with EPIC that section 104 should also prohibit states from encoding the SSN on magnetic strips, barcodes, or smart cards on the driver's license, as we are aware that while some states do not print the SSN on the card, they may embed the identifier digitally on the card.

In addition, as we have pointed out above, unless steps are taken to wean the private sector of its over-reliance on the SSN, it will continue to use it. Therefore, we concur with EPIC that exceptions should be for limited and specific time durations. If the committee believes it is necessary to extend any exceptions at all allowing continued non-statutory collection of Social Security Numbers by the private sector, which has unfortunately come to depend on the Social Security Number as a crutch, then the committee should include technology-forcing time limits on private uses so that firms are forced to develop more accurate alternatives that do not pose the secondary use problems of continued use of the Social Security Number, which was originally intended only for Social Security and certain tax purposes. Expect the business community to argue that business-to-business uses are both necessary and protective of the SSN. Neither claim is true.

Conclusion

We want to thank you, Mr. Chairman, for your leadership on these issues and for offering us the opportunity to present our views on the need for strong privacy protections to protect Social Security Numbers from misuse. We look forward to working with you on this and other matters to guarantee the privacy of American citizens. Restricting the widespread availability of Social Security Numbers is one of the most important solutions to the identity theft epidemic. It also brings the use of SSNs more closely under the limited use principles embodied in the Fair Information Principles.

Chairman SHAW. Thank you. It wasn't too long ago this Committee had a hearing, and a military officer had undergone the same problem. The identity thief had taken his identity and SSN

scinded on the same day by language reversing its effect included in the Conference Report on HR 4577, the Consolidated Appropriations Act, (Labor-HHS Approps). Section 213 of HR 4577 amends HR 5548 by deleting a number of sections of HR 5548. Section 213(a)(6) of HR 4577 strikes the Amy Boyer Law (Section 635 of HR 5548). See page H12261 of the Congressional Record for 15 Dec 00.

[19] For example, under the law enforcement exception in S 848 (Feinstein, 107th) collection of delinquent child support would be a "law enforcement" purpose. Does that extend the exception to allow any private firm collecting child support to take advantage of the exception? It appeared to do so, despite well-documented circumstances where some private child support collection firms have abused debt collection laws. See "Problems At Child Support, Inc., Complaints Increase For Specialized Collection Firms" 18 May 2000, Washington Post, Caroline E. Mayer and Jacqueline Salmon.

and purchased a Jeep. On further reflection, he all of a sudden realized that, also, his Social Security was his serial number that was required on the back of the check at the PX. So, you never know how many hands these things are going to go through; and, Mr. Ladd, we have got a lag time in the bill of 2 years in order to get to conformity. As long as public documents are public documents, and, of course, these court files have to stay open to the public and particularly land records.

I practiced law for many years before coming to Congress. I can't remember a single time except in an estate situation where I had to inquire of the client of his SSN. Twenty some years can fog your memory, but I can't remember back then we ever needed them or wanted them, and that is back when we tracked land titles with abstracts instead of doing it online. We didn't know what online meant.

Mr. LADD. We would concur with that, that there is little purpose from the land records custodian's point of view for the inclusion of the SSN. However, because of some of the difficulties of identifying the correct Robert Jones, and in the land title business as well, that has become added to the record more and more frequently. We object to it, but we have no authority to refuse the record.

Chairman SHAW. My brother's name is John Shaw. Clay Shaw is not a very common name, unless you go to New Orleans. John Shaw is a common name. We own property together, and every time there is a title search his name pops up with about six judgments against it, which we cure with affidavits. We don't seem to have a problem with that because, of course, he doesn't have any judgments against him, but it is a common name. Still we have always done it without putting any SSNs on the record; and, quite frankly, I am not sure that would separate him from someone with a similar name because I don't recall the SSN ever being on a final judgment that was put on record.

Mr. LADD. Will that vary from jurisdiction to jurisdiction and then from financial institution to financial institution.

Chairman SHAW. You do have a problem as far as your State law is concerned? I think Mr. Cate, you spoke or one of you spoke about State rights. Either Buenger or Cate, I can't remember which one. The SSN is a Federal number issued by the Federal Government, and I don't see any States' rights problem in limiting the display of that. Ms. Foss, I wanted to go just a little further into your case. You certainly went through a nightmare; and, fortunately, the perpetrator showed up and was prosecuted and now is, I assume, still serving time in jail.

Ms. FOSS. The special agent with the Social Security Inspectors Office said that they couldn't track whether or not she was still in jail. So, they didn't know at this point in time.

Chairman SHAW. Well, we don't lose people in jail. Even in Baghdad we know who is in the can. I would think somebody could track that down. Was it in a Federal penitentiary? Or was it State?

Ms. FOSS. She was working out of Mail Boxes, Etc. on Wisconsin Avenue in D.C., so I believe it was the D.C. District Court that handled it.

Chairman SHAW. Do you live here in the District?

Ms. FOSS. I never lived in the District. I have lived in Maryland. At the time this happened to me, I was in Pennsylvania; and I never had anything stolen that I know of.

Chairman SHAW. How long ago was it?

Ms. FOSS. It was 1999 when I discovered it, and she had been going at it for about 6 months.

Chairman SHAW. Yes, I guess she is probably out. I hope she didn't write it down somewhere.

Ms. FOSS. I hope she forgets everything.

Chairman SHAW. You are smart to keep track of your record, because that stuff can pop up again. One of the terrible things with identity theft is once you get into that cycle you are very liable to get hit again. So, it is very important. I can see that you all disagree in a much more civil manner than we do here in the Congress, and I congratulate you. We very much appreciate your point of view. I am going to give the other Members of this Committee an opportunity to submit some questions which I intend to also submit to you in writing, and we would appreciate your answering those questions, and we will make that part of this record. Thank you so much for your time. The problem with the Members not being here is that the hearing went actually longer than we thought, plus we had an interruption of almost an hour in the middle of it, which got schedules all off kilter. Thank you. This hearing is adjourned.

[Whereupon, at 1:54 p.m., the hearing was adjourned.]

[Questions submitted from Chairman Shaw to Mr. Beales, Mr. O'Carroll, Ms. Bovbjerg, Mr. Maxwell, Mr. Ladd, Mr. Hoofnagle, Mr. Mierziwinski, Mr. McGuinness, Mr. Buenger, Mr. Cate, and their responses follow:]

Questions from Chairman E. Clay Shaw, Jr. to Mr. Howard Beales, III

Question: You mentioned that the Gramm-Leach-Bliley Act (GLBA) restricts financial institutions from sharing SSNs with unaffiliated businesses. When the FTC issued the final rule on privacy under GLBA, did you anticipate a greater level of protection for SSNs than has actually occurred, especially with regard to SSNs in credit headers? How has actual practice differed from what the FTC envisioned at that time? Would you agree we need stronger protection for SSNs?

Answer: When considering the need for greater protections for SSNs, it is important to keep in mind the reason that SSNs are valuable to identity thieves. SSNs are crucial to the proper functioning of our financial system. In particular, they are used by credit bureaus to match consumers to the appropriate credit information and are widely used by businesses to identify consumers. Thus, in a real sense, access to SSNs by legitimate users is an important tool in combatting identity theft. In my view, any restrictions on SSNs should be carefully tailored to balance the need to keep SSNs out of the hands of those who might use the information fraudulently with the need for businesses to have sufficient information—including SSNs—to spot fraud and attribute information to the right person. The best approach to achieving this balance is to limit access to SSNs to those purposes that are legitimate. This is the model used in other successful federal privacy laws, such as the Fair Credit Reporting Act, which allows information to flow without restriction to credit bureaus, who then may only disclose a credit report for a "permissible purpose" as specified in the FCRA. Any further regulation of SSNs should follow this same model.

With respect to the Gramm-Leach-Bliley Act, as discussed in the Commission's testimony, the GLBA Privacy Rule imposes certain restrictions on the disclosure of information collected by credit bureaus from financial institutions, including SSNs and other identifying information about consumers (sometimes called "credit header" information). Prior to the GLBA's passage in 1999, the disclosure of this information was not regulated under Federal law (including the Fair Credit Reporting

Act, which generally does not cover identifying information). Although I was not at the Commission when the GLBA Privacy Rule was enacted, it was likely anticipated that the disclosure of SSNs would be restricted under GLBA to a greater extent than existed prior to its passage. At the same time, it was recognized that GLBA did not place comprehensive restrictions on the sharing of SSNs. For example, GLBA covers only nonpublic personal information obtained from financial institutions, and is not retroactive (and therefore does not limit the sharing of information, including SSNs, that were collected prior to July 1, 2001).

With certain exceptions, such as for credit reporting, fraud prevention, and law enforcement, GLBA prohibits sharing of information to nonaffiliated third parties unless the consumer has been given a chance to "opt out." The Privacy Rule prohibits redisclosure of information received under an exception for purposes other than to carry out the activity covered by the exception. In practice, it appears that credit bureaus are redisclosing credit header information—including SSNs—for credit reporting purposes as well as for other purposes listed under certain GLBA exceptions, such as fraud prevention or law enforcement. *See* 16 C.F.R. § 313.14–.15 (2000). In my view, the Rule seems to assume that information will be disclosed for one purpose, but nothing in the rule expressly prohibits sharing information for more than one purpose, and it is unclear whether there is a statutory basis for such a prohibition. This broader interpretation has the result in many cases of furthering important policy goals, such as combating fraud, assisting law enforcement, ensuring public safety, and complying with judicial process. At the same time, it is important that the credit bureaus take care not to redisclose credit header information beyond the bounds of the GLBA exceptions.

Question: Do you agree with Mr. Fred Cate's interpretation of the FTC-sponsored Synovate survey's results, indicating the statistics prove commercial or public records are not the primary sources identity thieves use to obtain SSNs?

Answer: The Synovate survey indicated that the largest category of identity-related crimes within the preceding year involved the misuse of existing credit cards, which most likely can be committed without the victim's SSN. In those crimes where it is more likely that SSNs are used, such as when new accounts are opened or other frauds committed in the victim's name, it is difficult for victims of identity theft to know exactly when, where, how and by whom their personal information was compromised. Thus, the survey found that only 34 percent of victims who had new accounts opened in their name or whose information was used to commit other frauds ("Victims of New Accounts & Other Frauds' ID Theft") knew **who** had misused their personal information. Of these 34 percent who knew the identity of the thief, 53 percent said it was a family Member or relative; 12 percent said it was someone who worked at a company or financial institution who had access to the victim's personal information; and 10 percent of victims who could identify the culprit said it was a friend, neighbor, or in-home employee.

Further, the survey found that 58 percent of all victims of "New Accounts & Other Frauds" ID Theft indicated they knew **how** the identity thief obtained their personal information. Of that 58 percent, about 35 percent said their information was lost or stolen; 19 percent of those said their personal information was obtained during a transaction, such as a purchase; and 46 percent of those who knew how the information was obtained said the thief used "other" means of access (e.g., access via a family Member or from printed checks or bills.

Not surprisingly, it is difficult to assess from these findings how and from where SSNs are obtained. Some of the information may have come from commercial records, or when the thief works for a company with the information, or in the course of a transaction. The survey results do not identify public records as a major source of information, but it is important to keep in mind that about 40 percent of victims of the most serious form of identity theft, the opening of new accounts, simply do not know how the thief obtained the information. Thus, the survey does not allow us to draw firm conclusions about the sources of SSNs for identity thieves.

Question: The Salt Lake Tribune reported this month that identity thieves are increasingly using their own names and somebody else's SSN to obtain credit. Can you confirm this? If yes, how could it happen? Don't credit bureaus check to see whether an individual's name and SSN match and refuse credit if it doesn't? The article also mentioned that if the name and SSN do not match, the credit bureau creates a "subfile." The subfile affects the victim's credit, but the victim cannot obtain a copy of the subfile when they request a copy of their credit report, so they cannot clear up the identity theft. Is this true?

Answer: The FTC staff is currently attempting to gain a fuller understanding of the facts and circumstances underlying the article's allegations. To that end, FTC

staff is following up with the government officials mentioned in the article to learn more about this issue. We have no information on the prevalence of this type of identity theft or whether it is increasing. The article does not disclose, and it may not be possible to determine, how the illegally used SSNs were obtained.

With respect to the types of information used by credit reporting agencies in their matching processes and information provided to creditors and consumers, Nation requires the FTC to study the methods and efficacy of credit reporting agency efforts in matching information to ensure that a consumer is the correct individual to whom a consumer report relates before releasing a consumer report to a user of that report. *See* Pub. L. No. 108–396, § 318 (2003). I anticipate that we will learn more about this issue in the course of our work on this study, which is to be completed by December, 2004. At this time, we do not know of any way that a "subfile" could impact a consumer's credit report or credit score without also being disclosed to the consumer upon request.

Question: This Subcommittee has heard from a number of victims of identity theft. A common, and frustrating, theme is that after individuals discover the theft and report it to credit bureaus and financial institutions, they continue to be victimized by identity theft. How can this continue to occur, given the anti-fraud programs the industry cites? In your judgment, is the private sector doing enough to combat identity theft and assist its victims? Are there more effective ways to assist victims of identity theft to correct their credit histories?

Answer: Victims of identity theft often must navigate through various bureaucratic procedures to recover from the crime. Nation has established a number of measures designed to simplify this process and reduce the incidence of identity theft. Identity theft account blocking will give victims certain rights to ensure that fraudulent information gets removed promptly from their credit reports, thereby preventing distortion of their credit records. Creditors or other businesses must give victims copies of applications and business records relating to the theft of their identity, which can assist victims in proving that they are, in fact, victims.

Other measures are designed to prevent or mitigate identity theft. The national fraud alert system will require creditors to take certain steps to verify the identities of consumers who have placed fraud alerts on their consumer reports before granting credit in the consumer's name. By means of the "Red Flag" rulemaking, financial institutions and creditors will have to analyze identity theft patterns and practices so that they can take appropriate action to prevent the crime. The Disposal of Consumer Report Information and Records rule will help to ensure that sensitive consumer information derived from consumer reports, including Social Security numbers, is disposed of properly.

We expect that these provisions should significantly improve victims' ability to recover from their identity theft with a minimum of trouble and help to reduce the occurrence of identity theft. It should be noted that the majority of these provisions will not take effect until December 1, 2004. At that time, we will be able to begin assessing their impact.

Generally, the private sector has been responsive in addressing particular problems in the system that can facilitate identity theft as those problems come to light. Combating this crime requires an ongoing effort by both the public and private sectors to identify new vulnerabilities and to implement new measures to protect thieves from exploiting them.

Question: If a private entity—for example, a consumer reporting agency, health care organization, or information reseller—has an individual's SSN in its possession, and this information is used in an identity theft or fraud, should that entity be held strictly liable for any harm done? Please comment on the advantages or disadvantages of this idea, as well as its feasibility and potential effectiveness in combating identity theft.

Answer: As demonstrated by the Synovate survey (see Q. 2 above), it is not often evident to victims how identity thieves obtain SSNs. Thus, a strict liability standard may not be the most appropriate means of curbing misuse of SSNs. A number of Federal laws mandate significant information security practices, which can protect SSNs from improper disclosure and use. Among these laws, the FCRA requires that consumer reporting agencies not disseminate consumer reports to entities unless they meet a statutorily permissible purpose to use the report. Nation amendments also require anyone with consumer information derived from consumer reports to dispose of that information properly. GLBA requires that financial institutions develop a program for taking reasonable steps to protect sensitive customer information and ensure that the program evolves to keep pace with new fraud trends. HIPAA and the Driver's Privacy Protection Act also require protection of sensitive information. I appreciate that certain entities or consumers are not covered by these

laws (e.g., retail customers, employers). The Commission, however, can and has brought enforcement actions for security breaches or potential security breaches under section 5 of the FTC Act (i.e., *In the matter of* Guess?, Inc. and Guess.com, Inc., http://www.ftc.gov/os/2003/06/guessagree.htm and *In the matter of* Microsoft Corp., http://www.ftc.gov/os/2002/12/microsoftdecision.pdf).

Questions from Chairman E. Clay Shaw, Jr. to Mr. Patrick O'Carroll

Question: You mentioned that one terrorist suspect in a case your agents helped investigate had two Social Security cards in his possession at the time of his arrest. Were they SSNs he obtained from the SSA using fraudulent documentation? Were they fake SSN cards? Were they cards he obtained or stole from somebody else?

Answer: At the time of his arrest, the subject had two genuine Social Security cards in his possession; one belonged to the subject, and the other belonged to the brother of the subject. The investigation revealed that both individuals were born in the United States. The SSNs/cards were legitimately obtained from SSA, and both the subject and his brother were properly enumerated.

Question: Are there other provisions you recommend for inclusion in the Social Security Number Privacy and Identity Theft Prevention Act of 2003, H.R. 2971, to further prevent terrorists from obtaining or using SSNs to abet their heinous crimes?

Answer: We recommend reviewing the implications of releasing information on deceased individuals and also recommend examining the potential for increased protection of this information.

The SSA should be permitted to cross-verify Social Security numbers against government and private databases to identify and fix inaccuracies which would limit the spread of false identification and SSN misuse. We also encourage more data matching opportunities under longer term agreements, some of which may require a change in the current legislation.

Question: You mentioned a couple of cases where SSNs were fraudulently obtained for nonexistent children. How did this happen?

Answer: The one case mentioned involved an elaborate conspiracy that included one man and eleven women. The women would visit Chicago and surrounding suburban area Social Security offices to apply for Social Security numbers for their supposedly newborn children. These individuals applied for the SSNs using counterfeit Illinois birth certificates, Department of Health immunization records and bogus employment identifications provided to them by the ringleader.

The names used on all the Social Security applications belonged to undocumented Nigerian citizens who paid the ringleader up to $5,000 each for a valid Social Security number, Illinois driver's license and U.S. Passport. The suspects would then visit local Social Security offices a month or two later with a second counterfeit Illinois birth certificate and their new identification to request a correction of their date of birth on Social Security records.

Question: Are the provisions in H.R. 2971 that your office recommended, which would require independent verification of all birth documents and improvements in the enumeration-at-birth process, sufficient to help prevent this from happening?

Answer: We believe that provisions 201 and 202 of HR 2971 will reduce the ease with which criminals may fraudulently obtain SSNs for non-existent children. A recent audit and numerous investigations indicate that because SSA does not verify birth records for children under the age of 1, criminals have inappropriately obtained SSNs for nonexistent children using invalid birth records. Accordingly, we recommended that the Agency close this loophole by verifying the authenticity of birth records presented by all U.S. citizens applying for original SSNs. We are currently awaiting the Agency's response to our recommendation. However, we commend the Subcommittee for taking proactive measures by including provision 201 in the proposed legislation—making it essential that SSA ensure the legitimacy of birth records submitted with original SSN applications.

Regarding section 202 of HR 2971, related to SSA's enumeration at birth program, we support the Committee's proposal that SSA tighten controls within this program. While our 2001 report Audit of the Enumeration at Birth Program (A–08–00–10047) concluded that generally the program was providing accurate and reliable data for SSA's enumeration of newborns, we recommended that the Agency implement additional controls to prevent those with criminal motives from submitting SSN applications for nonexistent children. The Agency has explored this idea and taken some action on our recommendations. However, we believe the provisions outlined in section 202 of the Social Security Number Privacy and Identity Theft Prevention Act

of 2003 would provide further incentive for the Agency and participating hospitals and States to implement our proposed corrective actions.

Question: You mentioned a case involving fraudulent acquisition of SSNs for unauthorized immigrants. Do you know what the unauthorized immigrants were doing with the fraudulently obtained SSNs? You stated the penalty some members of the scheme received was 2 years in prison.

Answer: Actually, certain subjects in the case mentioned above (Question 2) were given 2 year sentences. Other subjects in this case, who conspired to traffic in unauthorized immigrants, were sentenced as much as 71 months in prison. The fraudulent SSNs that were received by illegal immigrants were used to obtain employment, as well as for obtaining driver's licenses, credit cards, mortgage loans, and so forth.

Question: You have recommended new and enhanced penalties for fraudulently obtaining SSNs or SSN misuse which we have included in H.R. 2971. Are there others that are needed?

Answer: The OIG supports SSA's proposal requesting that the United States Sentencing Commission review and amend Federal sentencing guidelines to provide an appropriate penalty for any offense under sections 208, 811, or 1632 of the Social Security Act or any offense under 18 USC 1001 with respect to the Social Security, Special Veterans' Benefits, and the Supplemental Security Income programs. A primary purpose of sentencing guidelines is to reduce the disparity in sentencing between defendants who commit similar crimes. section 304 of H.R. 2971 proposes to amend sections 208, 811, and 1632 in order to obtain enhanced penalties, in cases of terrorism, drug trafficking, crimes of violence, or prior offenses, but it does not specifically direct the U.S. Sentencing Commission to consider amending Federal sentencing guidelines regarding these sections. In addition, the inclusion of the increased the penalties imposed for SSA employees who are convicted of selling SSNs will be a good deterrent in this area.

Question: You stated that you support cross-verification of SSNs through both governmental and private sector systems of records to identify and address inaccuracies. You said that all law enforcement agencies should be provided the same SSN verification services granted to employers. What does the SSA say regarding the proposal?

Answer: The SSA has not yet officially responded to this OIG proposal, and therefore we will defer to SSA to present its position.

Question: Why isn't information available from financial institutions, credit bureaus, and information resellers sufficient to prevent cases like the fraudulent home loan case you mentioned?

Answer: Although we believe that representatives from financial institutions, credit bureaus and information resellers may be in a better position to respond to this question, we will provide the Committee with one possible reason if their information is not sufficient to prevent cases like the fraudulent home loan incident. Specifically, most of these organizations currently do not have the ability to verify the accuracy of customer SSNs and names with SSA, the actual issuer of the number. Historically, the Agency has limited its verification services to employers.

Over the past several years, our organization has been a strong proponent of expanding SSA's authority to perform cross verifications service. Because the SSN has become a national identifier, we firmly believe that if the number is to be used as such, users should have correct information. For example, the Department of Housing and Urban Development had the ability to verify the name of SSN of the loan applicant, it would have discovered that an individual was using an incorrect SSN (one belonging to someone else) to obtain the loan.

Question: One of the witnesses at the hearing, Mr. Fred Cate, said that if we limit sale, purchase, and display of SSNs that it will affect the availability and reliability of data for law enforcement and other vital purposes. Do you agree or disagree, and why?

Answer: We believe there are alternative and reliable sources of data involving SSNs for law enforcement. For example, there are legal provisions that allow the sharing of SSN information among law enforcement agencies in appropriate circumstances. In addition, H.R. 2971 makes appropriate exceptions for law enforcement officials in the provisions that prohibit the sale, purchase or display to the general public of SSNs.

Question: If a private entity—for example, a consumer reporting agency, health care organization, or information reseller—has an individual's SSN in its possession, and this information is used in an identity theft or fraud, should that entity be held strictly liable for any harm done? Please comment on the advantages or disadvantages of this idea, as well as its feasibility and potential effectiveness in combating identity theft.

Answer: The concept of strict liability would confer liability on the consumer reporting agency, health care organization, or information reseller not based on actual negligence or intent to harm, but instead on the breach of an absolute duty to protect SSNs in its possession. This strict liability would benefit fraud victims. With the risk of this increased liability, there would likely be more motivations for these organizations to better protect SSNs. At the same time, the adoption of strict liability may be criticized by private industry for not considering the intent of these organizations or whether these organizations acted negligently.

This hypothetical illustrates the need for H.R. 2971 for those organizations not exempt from the H.R. 2971 limitations, such as the private resellers of information. The H.R. 2971 approach would limit the availability of SSNs to such entities, thus reducing the likelihood of their fraudulent use. A more feasible alternative might be the creation of a private cause of action on the part of victims against an individual or organization that did not exercise due diligence in the handling of their personal information.

Questions from Chairman E. Clay Shaw, Jr. to Ms. Barbara Bovbjerg

Question: You mentioned during your testimony that monitoring of the day-to-day release of information under the restrictions imposed by the Gramm-Leach-Bliley Act (GLBA) is essentially an "honor system." Could you elaborate on how it works? What is known about the degree to which businesses comply with the privacy requirements under the GLBA?

Answer: In my testimony, I observed that generally Federal laws have controlled the use and disclosure of the SSN in specific industries, but that secondary disclosure by clients of these firms is generally not closely monitored. GLBA is one of the laws that restrict disclosure and is illustrative of the point that businesses that are indirectly governed by these privacy laws are expected to adhere to them, but are not necessarily monitored for compliance. For example, GLBA restrictions apply to institutions that are considered to be financial institutions under GLBA, which covers a broad range of financial institutions. In addition, entities that receive consumers' financial information from a financial institution under GLBA are also subjected to GLBA's restrictions. However, companies such as some information resellers that fall outside of the purview of Federal regulators may or may not adhere to GLBA. However, Federal regulators enforcing GLBA compliance are not required to monitor entities that are not directly under their jurisdiction.

In our work for this Subcommittee, we found that some CRAs consider themselves to be financial institutions under GLBA. These entities are therefore directly governed by GLBA's restrictions on disclosing nonpublic personal information to nonaffiliated third parties. We also found that some of the information resellers we spoke to did not consider their companies to be financial institutions under GLBA. However, because they have financial institutions as their business clients, they complied with GLBA's provisions in order to better serve their clients and ensure that their clients are in accordance with GLBA.

FTC staff told us that GLBA also includes certain broad exceptions that are unspecific. For example, FTC officials said that they receive many inquiries from CRAs and information resellers concerning the application of GLBA's exceptions, such as whether the exceptions apply to certain circumstances. As a result, FTC officials said it is difficult to determine how and whether certain entities, such as information resellers, are appropriately interpreting the exceptions.

Question: You stated that court records are among those most often cited as containing SSNs in your survey on how government entities collect and store SSNs. Do you have any information on the percent containing SSNs because Federal, state, or local laws and regulations require them?

Answer: We cannot accurately calculate such a percentage until we have complied and verified all survey data from our ongoing work on SSNs in public records. Our work will be completed in September 2004.

Question: Some of the witnesses at the hearing asked for specific statutory exemptions from the restrictions contained in sections 101 and 107 of H.R. 2971, rather than relying on the Attorney General's regulatory authority provided in section 102. In your view, is the authority provided in the bill to the Attorney General sufficient to address these concerns?

Answer: H.R. 2971 would give the Attorney General discretionary authority to determine which entities could be exempted from the prohibition of engaging in the sale, purchase, or display of SSNs to the general public. As written, the bill provides for flexibility in determining which if any entities would be exempted, and offers a means to address concerns with such a prohibition once the law is passed that might not have been envisioned at the time it was drafted. Such an approach seems

designed to address changing circumstances rather than addressing existing concerns of specific entities.

If present concerns are deemed valid, the only way to assure that those concerns are addressed is to write them into the bill prior to passage, although such exemptions would still be subject to interpretation by courts.

Question: A witness representing the National Council of Investigation and Security Services requested the deletion of section 108 of H.R. 2971, citing the usefulness of credit headers in locating witnesses, criminal suspects, estate beneficiaries, and others. What other sources of information could be used to locate such persons if section 108 of H.R. 2971 were enacted into law?

Answer: Credit header information matches a persons' identifying information to their address, which is useful for purposes such as locating individuals. However, information is clearly available from other sources as well. Our current work shows that identifying information, such as name, addresses, and SSNs, can be found in public records and other publicly available information such as newspapers. In addition, entities willing to pay a fee can purchase such data from information resellers who specialize in amassing personal information.

Question: If a private entity—for example, a consumer reporting agency, health care organization, or information reseller—has an individual's SSN in its possession, and this information is used

Answer: Currently, identity theft victims are fully responsible for correcting problems caused by identity thieves. For example, victims must contact the major CRAs to have a fraud alert placed on their credit, file a report with the appropriate law enforcement entities, and if credit card misuse is involved they must report the misuse to their credit card company. Although private sector entities and the FTC have worked to lessen the burden on identity theft victims, identity theft victims can spend an average of 60 hours trying to resolve their problems.

Results from a recent FTC survey show that identity theft victims feel that the financial community could do more to help resolve their problems. Many identity theft victims reported that improved follow-up and assistance by the financial community, as they attempted to repair their records, would be beneficial. Identity theft victims also reported that financial institutions, including CRAs, could make greater efforts to monitor consumers' account activity and notify them when unusual transactions occur. They also reported some degrees of dissatisfaction with the way CRA's and credit card companies have handled their identity theft related reports. For example, 31% of victims were dissatisfied with all of the CRAs they contacted while 18% were dissatisfied with all of the credit card companies to whom they reported misuse of their credit cards.

CRAs, credit card companies and others are in a unique position to help identity theft victims resolve their problems. To the extent that these companies are made liable for losses, it is likely that more actions will be taken to protect SSNs and other personal information companies maintain. However, the benefits of assigning such liability to these companies must be balanced against the difficulty that these companies are likely to have in monitoring millions of individuals' accounts. In addition, holding companies responsible for identity theft victims' financial losses may not reduce the amount of time these victims spend trying to resolve their problems.

Questions from Chairman E. Clay Shaw, Jr. to Mr. Lawerance Maxwell

Question: You mentioned the Financial Industry Mail Security Initiative (FIMSI). Could you elaborate on who participates in the working group and the recommendations specifically made with regard to preventing use of SSNs? Why did the group believe a recommendation specifically dealing with SSNs was necessary?

Answer: The U.S. Postal Inspection Service sponsored the Credit Card Mail Security Initiative starting in 1993 in response to a dramatic spike in the theft of credit cards. Representatives from the credit card and retail Industries attended these meetings which were held on a quarterly basis in WashingtonDC.

The Postal Inspection Service decided in 2003 to expand the focus of the meetings to include presentations on money laundering, Internet fraud and bank fraud schemes. The attendee list was expanded to include both state and Federal prosecutors, investigators from local banks and credit unions, Federal and state law enforcement. Working groups include the Non Received Credit Card Working Group, the Bust-Outs Working Group, the Bank Fraud Working Group, and the Identity Theft Working Group. This new expanded group meets on a semi-annual basis. One of the more noteworthy accomplishments stemming from the credit card initiative

was the credit card activation "800" number which has become an industry standard for security.

The Identity Theft Working Group made recommendations dealing specifically with social security numbers (SSN's) in their consumer awareness campaign. Since the SSN is used as a personal identifier, it is the key piece of information needed to conducting Identity Theft. These recommendations included memorizing your SSN and passwords rather than carrying the cards with you; and, if possible, do not use your SSN as your identifying number on your driver's license.

Question: You mentioned cases involving rings of identity thieves, who obtained lists with the victims' names, dates of birth, SSNs, and other information. How easy would it be for these criminals to steal an individual's identity without the SSN?

Answer: The SSN is currently used as a personal identifier; this was never the intent when it was created. Without the SSN it would be much more difficult to take over an individual's identity. They would not be able to access or open financial accounts, instant credit accounts, or even cellular telephone accounts. The SSN is the key component to access and individuals credit history.

Questions from Chairman E. Clay Shaw, Jr. to Mr. Mark Ladd

Question: You mentioned the Property Records Industry Association's participation in the Records Access Policy Advisory Committee. What recommendations do you anticipate the Committee will make with respect to access to SSNs in public records?

Answer: The final four points outlined in the written testimony that we submitted comprise our recommendations to date. I do not anticipate any major changes in these recommendations.

Question: You suggested that the legislation be effective on a "day-forward-basis." This recommendation has been made before and was incorporated into the current bill's language, which establishes a timeframe of 2 years from the date of enactment for those who maintain public records to comply with the law. Is this enough time?

Answer: If documents that are on file with our office prior to the effective date of this legislation can be posted on our websites, even if they contain SSNs, then 2 years is more than enough time for compliance. Under this scenario, three to 6 months would be a sufficient grace period.

If, however, records that are already on file with our offices must have SSNs removed before they can be posted on our websites, then no length of time will suffice for most counties. A few large counties may be able to afford the cost of compliance, but most will not. Only documents presented after the effective date of this legislation could be posted on county websites under this scenario.

Question: You suggested giving public record keepers the authority to prohibit the filing of documents with SSNs, without requiring them to do so. Why is this important in your view, and would public records keepers implement such authority?

Answer: As I noted in my written and oral testimony, the shear volume of documents and the number of pages involved make prescriptive rejection authority extremely difficult to manage. However, permissive authority provides land records custodians the necessary tool to help protect the privacy concerns of the public if we discover a SSN included in a document during our normal review process.

Our members object to rejection authority being prescriptive, as do our commercial customers (title companies, abstract companies and attorneys). However, permissive authority empowers us to assist the public in protecting their privacy concerns without placing an impossible task on our shoulders.

It is my belief that most land records custodians would utilize permissive authority to protect the interests of their constituents.

Question: You said that given the hundreds of thousands of pages of documents a jurisdiction may receive in a year, and that the SSN could be placed anywhere on a document submitted by the parties involved, that responsibility for SSN removal is more properly placed on document preparers and individual customers. If the bill were modified so that public record keepers were required to remove the SSN on forms they require (or block it from display if it is collected), but the responsibility and liability for removing SSNs on all other materials submitted to the court rested on those who file the papers, would that enable you to support this bill?

Answer: Your proposal on this point is the most workable compromise that I have heard between agencies that require the SSN of necessity (such as the Court Ad-

ministrators testified) and those of us who receive the SSN without any desire or necessity for it.

Court Administrators who require SSNs could likely adopt rules regarding how documents are constructed that would make day-forward redaction manageable. By specifying a predetermined location that SSNs are listed in documents, they could reduce the effort required to redact. On the other hand, the burden to remove SSNs from documents that do not require them is correctly placed on document drafters.

I think PRIA members would support this proposal.

Questions from Chairman E. Clay Shaw, Jr. to Mr. Jay Hoofnagle and Mr. Edmund Mierzwinski

Question: Do you agree with Mr. Cate's statement at the hearing that knowing a Social Security number alone does not get an individual credit and that it is merely a quick way of locating reliable information about an individual that can be used to verify identity?

Answer: Mr. Cate's statement perfectly illustrates the *problem* of the Social Security Number (SSN)—it is used both as an identifier and as an authenticator. That is, some businesses use it as a record locator, a master identifier to associate and reference records. Other businesses use it for authentication, a process where a person proves he is who he says he is. Serious security problems are raised in any system where a single device is used both as identifier and authenticator.[1] It is not unlike using a password identical to a user name for signing into e-mail. Or like a bank routinely using the SSN as an account number and the last four digits of the SSN as a PIN for its automated teller machines.

It is because the SSN is used as both identifier and authenticator that identity theft has increased in incidence and prevalence. Because the SSN is relied upon so heavily by business, it is the personal identifier that impostors seek in order to commit crime. Congress' goal in addressing identity theft and privacy should seek to limit availability of the SSN generally and to induce businesses to rely upon alternative identifiers.

Question: Mr. Cate said that for data to be reliable, businesses and others must have been permitted to use SSNs all along, and that national security and law enforcement uses of SSNs frequently involve access to routine, innocuous data. Do you agree or disagree that prohibiting sale, purchase, and display of SSNs for unnecessary purposes would jeopardize use of SSNs for critical purposes?

Answer: We disagree with the proposition that businesses have been permitted to use the SSN. While Congress has approved government uses of the SSN, the identifier has never been approved for general private-sector use.

Restricting the sale, purchase, and display of SSNs for unnecessary purposes preserves their utility for more critical purposes while decreasing opportunities for imposters to obtain identities to hide behind. Additionally, maintenance of dual identifiers, or transitions away from SSNs as identifiers, is a very feasible and desirable goal as demonstrated by Empire Blue Cross's transition (4.8M customers), and existing requirements in many states prohibiting use of SSNs for student, driver, and other identifiers.

We also contest the notion that government uses of the SSNs frequently involve access to routine, innocuous data. The SSN plays an unparalleled role in aggregation of information, and thus information once thought to be innocuous can take on greater significance. For instance, a document EPIC obtained under the Freedom of Information Act from the United States Marshals Service highlights the amount of information that can be aggregated around identifiers:

With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes. The profile includes personal identifying information (name, alias name, date of birth, Social Security number), all known addresses, drivers license information, vehicle information. . . . telephone numbers, corporations,

[1] The driver's license is used as both identifier and authenticator, but it is a superior device because it includes a picture, address, signature, and basic physical information. It expires regularly and must also be renewed. A SSN lacks any of these additional features; *see also* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problemem,* 80 Tex. L. Rev. 89, 100 (November 2001) ("In particular, Social Security numbers and mothers' maiden names are inherently poor passwords because they are widely known and difficult to change. Knowledge of a Social Security number supports only a weak inference that the knower is the person to whom that Social Security number was assigned.").

business affiliations, aircraft, boats, assets, professional licenses, concealed weapons permits, liens, judgments, lawsuits, marriages, worker compensation claims, etc.[2]

In many cases, collection of the SSN is not necessary, and Congress should act swiftly to curb these uses of the SSN. In January 2002, a statewide grand jury empanelled by the Florida Supreme Court found in its first report that:

We have identified that the government and business take in much more information than necessary to conduct business. For example health clubs require members to disclose their Social Security numbers on applications for membership; video rental stores ask for social security numbers on applications; and life insurance companies ask for social security numbers of beneficiaries; local governments ask for Social Security numbers on routine transactions. We were distressed to learn from the Interim Project Report by the Committee on State Administration and Committee on Information Technology that 96.3% of state agencies do not even have a written policy relating to the collection of Social Security numbers. This same report indicates that 63% of these agencies disclose Social Security numbers on some public record requests.

Medical service providers and insurance companies routinely substitute Social Security numbers for patient or policy numbers, unnecessarily exposing this sensitive information to scrutiny on such documents as health and insurance cards. Unsecured mailboxes and trash containers provide thieves with easy access to this personal information.[3]

The body found that personal information was being collected by government entities and disseminated in public records. It recommended that State law be amended to require consent of the citizen, a court order, or a compelling need before identifying information of citizens was included in the public record. It also found that the "public and private sectors routinely use and rely on the consumer's Social Security number for use as an identifier and an account number." The body recommended that the State legislature "prohibit the use of Social Security numbers for independently generated identifiers to track customers, patients, policies, and so forth., unless required by law."[4]

Finally, we note that Mr. Cate's previous testimony supports limits on government collection of personal information.[5] In testimony to the House Energy and Commerce Subcommittee on Consumer Protection, Mr. Cate wrote:

The government plays many critical roles in helping to protect individual privacy. One of the most important responsibilities of the government is assuring that its own house is in order. Only the government has the power to compel disclosure of personal information and only the government operates free from market competition and consumer preferences. As a result, the government has special obligations to ensure that it complies with the laws applicable to it; collects no more information than necessary from and about its citizens; employs consistent, prominent information policies through public agencies; and protects against unauthorized access to citizens' personal information by government employees and contractors. Similarly, there are many steps that only the government can take to protect citizens against privacy-related harms, such as identity theft: Make government-issued forms for identification harder to obtain; make the promise of centralized reporting of identity thefts a reality; make it easier to correct judicial and criminal records and to remove permanently from one individual's record references to acts committed by an identity thief. The government alone has this power.

We agree that a large part of protecting privacy in the context of SSNs involves the government reducing the collection and disclosure of personal information. H.R. 2971 has many provisions that would promote these goals.

Question: Some of the witnesses at the hearing asked for specific statutory exemptions from the restrictions contained in sections 101 and 107 of H.R. 2971, rather than relying on the Attorney General's regulatory author-

---

[2] Sole Source Justification for Autotrack (Database Technologies) (n.d.) (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02j.pdf; *see also* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement,* 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004).

[3] Identity Theft in Florida, First Interim Report of the Sixteenth statewide Grand Jury, SC 01–1095 (Fla. Jan. 2002), available at http://myfloridalegal.com/pages.nsf/4492d797dc0bd92f85256cb80055fb97/758eb848bc624a0385256cca0059f9dd!OpenDocument.

[4] *Id.*

[5] *Hearing on Privacy in the Commercial World, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection,* U.S. House of Representatives, Washington, D.C., Mar. 1, 2001 (statement of Fred Cate), at http://www.law.indiana.edu/directory/publications/fcate/cate010301.pdf.

ity provided in section 102. In your view, is the authority provided in the bill to the Attorney General sufficient to address these concerns?

Answer: The authority provided to the Attorney General is sufficient, provided that the asked-for exceptions satisfy the statutory standard requiring a compelling interest that cannot be served through the employment of alternative measures. We think that this standard has enough flexibility to address legitimate needs for the SSN while avoiding the codification of exceptions. If exceptions are codified, it is unlikely that qualifying industries will ever transition to alternative identifiers. We therefore suggest that all exceptions sunset after a given number of years to encourage a transition to alternative identifiers.

Question: This Subcommittee has heard from a number of victims of identity theft. A common, and frustrating, theme is that after individuals discover the theft and report it to credit bureaus and financial institutions, they continue to be victimized by identity theft. How can this continue to occur, given the anti-fraud programs the industry cites? In your judgment, is the private sector doing enough to combat identity theft and assist its victims? Are there more effective ways to assist victims of identity theft to correct their credit histories?

Answer: We think that creditors, in order to obtain new accounts and compete vigorously, are employing lax identification and authentication procedures that make identity theft easy to commit.[6] In a typical scenario, an impostor will gather personal information of the victim and apply repeatedly for credit until they get a "hit." Impostors can rely upon a creditor's alacrity to open new accounts in victims' names.

In passing the Fair Credit Reporting Act in 1970, one of Congress' prime goals was to place fairness and privacy duties on credit reporting agencies (CRAs). This was necessary because competition did not produce competent or even decent credit reporting activities.[7] CRAs were not subject to adequate market pressure to ensure accuracy and fairness because the customers of CRAs are creditors, not individual members of the public. Congress thus created duties on the CRAs, users of credit reports, and furnishers of personal information. Those duties are now inadequate. For instance, under the FCRA, credit reporting agencies only are required to "maintain reasonable procedures designed" to prevent unauthorized release of consumer information.[8] In practice, this means that credit reporting agencies must take some action to ensure that individuals with access to credit information use it only for permissible purposes enumerated in the Act. The FTC Commentary on the FCRA specifies that this standard can be met in some circumstances with a blanket certification from credit issuers that they will use reports legally.[9]

This certification standard is too weak. It allows a vast network of companies to gain access to credit reports with little oversight. It treats credit issuers and other users of credit reports as trusted insiders, and their use of credit reports and ultimate extension of credit as legitimate.

Even where fraud is suspected, creditors only have minimal authentication duties. Once the individual does suspect wrongdoing and triggers an alert, new protections in the Fair and Accurate Credit Transactions Act (FACTA) require that creditors use "reasonable policies and procedures to form a reasonable belief that the user [creditor] knows the identity of the person making the request."[10] It is somewhat troubling that a tradeline can be extended without at least "reasonable policies and procedures" to verify the credit applicant's identity. It seems only reasonable that such protections be in place by default, rather than when fraud is actually expected.

We think that more accountability could be encouraged in this area if creditors were held liable to victims for extending credit to impostors. However, courts have been reluctant to recognize a right of action for negligent extension of credit. Most recently, the South Carolina Supreme Court rejected the tort of "negligent enablement of imposter fraud."[11] In that case, the plaintiff identity theft victim alleged that banks owe a duty to identity theft victims when they negligently extend

---

[6] *See e.g.,* Jeff Sovern, *The Jewel Of Their Souls: Preventing Identity Theft Through Loss Allocation Rules,* 24 U. Pitt. L. Rev. 343, 358 (Winter 2003) (arguing that "[g]reater vigilance on the part of the merchants involved would have prevented many identity frauds").

[7] Robert Ellis Smith, Ben Franklin's Web Site, Privacy and Curiosity from Plymouth Rock to the Internet (Privacy Journal, 2000).

[8] 15 U.S.C. § 1681e(a).

[9] The FTC is statutorily barred from promulgating regulations on the FCRA. 15 U.S.C. § 1681s(a)(4). The agency issues a non-binding commentary on the Act. Credit, Trade Practices, 16 CFR § 600, 607 (1995).

[10] Pub. L. No. 108–159 § 112 (h)(1)(b)(i). FACTA amended the Fair Credit Reporting Act, 15 U.S.C. § 1681.

[11] *Huggins v. Citibank,* 585 S.E.2d 275 (S.C. 2003).

credit in their name. The defendants argued that no such duty existed because the victim was not actually a customer of the bank. Focusing on the requirement that an actual relationship exist between victim and tortfeasor before a legal duty arises, the court rejected the proposed cause of action:

"We are greatly concerned about the rampant growth of identity theft and financial fraud in this country. Moreover, we are certain that some identity theft could be prevented if credit card issuers carefully scrutinized credit card applications. Nevertheless, we—decline to recognize a legal duty of care between credit card issuers and those individuals whose identities may be stolen. The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.[12]

Congress could assist victims greatly by creating an enforceable duty so that creditors were more responsible with victims' credit.

Question: We have heard a recommendation that Congress consider creating a nationwide system of cross-verification of SSNs among public agencies and private businesses. What is your view of this recommendation? Are there other ways to increase the security and integrity of the SSN that would not unnecessarily compromise privacy?

Answer: In passing the Privacy Act 1974, Congress was specifically reacting to and rejecting calls for the creation of a similar idea, a one-stop "federal data center" for personal information. A 1977 report issued as a result of the Privacy Act highlighted the dangers and transfers of power from individuals to the government that occur with centralization of personal information:

In a larger context, Americans must also be concerned about the long-term effect recordkeeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between government and the rest of society. Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's recordkeeping capability poses the risk that existing power balances will be upset.[13]

Creation of a nationwide system of SSN verification across public agencies and private businesses will upset balances of power described in the 1977 report and reduce individuals' autonomy from both government and commercial entities.

Promoting the use of the SSN also hardens the number as a de facto national identifier. The creation of a national ID runs counter to public sentiment and recent congressional action.[14]

This concern is not new; it was voiced at the creation of the SSN and has since been raised repeatedly. The SSN was created in 1936 for the sole purpose of accurately recording individual worker's contributions to the Social Security fund. The public and legislators were immediately suspicious and distrustful of this tracking system fearing that the SSN would quickly become a system containing vast amounts of personal information, such as race, religion and family history, that could be used by the government to track down and control the action of citizens. Public concern over the potential for abuse inherent in the SSN tracking system was so high, that in an effort to dispel public concern the first regulation issued by the Social Security Board declared that the SSN was for the exclusive use of the Social Security system.

The use of the SSN as the means of tracking every encounter between an individual and the government will expand the treasure trove of information accessible to the unscrupulous individual who has gotten hold of another's SSN. The use of the SSN as the mandatory national identifier will facilitate linkage between various systems of governmental and private sector records further eroding individual privacy and heightening surveillance of each American's life.

There are ways to strengthen integrity of the SSN without implicating privacy. For instance, the format of the SSN could be changed to include a "checksum," a formula that allows one to immediately verify whether the number has a proper form. Credit card numbers already are issued in this fashion so that they cannot be guessed or faked easily.

Question: A witness representing the National Council of Investigation and Security Services requested the deletion of section 108 of H.R. 2971, citing the usefulness of credit headers in locating witnesses, criminal sus-

---

[12] *Id.* at 334.

[13] Privacy Prot. Study Comm'n, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission (1977), available at http://www.epic.org/privacy/ppsc1977report/c1.htm.

[14] For instance, the Department of Homeland Security is expressly prohibited from developing National ID systems. 6 USCS § 554 (2004).

pects, estate beneficiaries, and others. Do you share this view? Are there other sources of information that could be used to locate such persons if section 108 of H.R. 2971 were enacted into law?

Answer: Under H.R. 2971, credit headers could still be accessed by private investigators where they have a "permissible purpose" under the FCRA. The FCRA would allow access where the private investigator had a court order, where it is used for employment purposes, or where it is used for collection of an account. In the contexts listed above, it seems that a court order would be readily obtainable, thus satisfying the FCRA requirement, as location of witnesses, criminal suspects, and estate beneficiaries are all activities likely to occur within the context of a court action. As a fairness measure, the law would require the CRA to note on the credit report that the information had been accessed by the private investigator. We think that this is an appropriate standard for access to credit headers, which contain all the personal identifiers necessary for the commission of fraud or harassment.

Investigators did exist before the credit header system was created. They are resourceful and can call upon different resources to obtain personal information. The current system, where a network of private investigators can obtain credit headers on any person, is unfair and privacy invasive. Individuals do not even receive notice that their personal information has been obtained under the current framework. Furthermore, in some states, private investigators are not even licensed to practice. In others, licensure is merely a pro forma activity. Serious accountability concerns are present, most notably exemplified by the Amy Boyer case, where private investigators used credit headers and pretexting to locate a young woman for a stalker who killed her.[15]

We also suspect that the private investigators may be putting on "their best face" for maintaining access to credit headers. No one wants to impede the function of a private investigator when they are finding individuals in order to give them inheritance from an estate. We question what percentage of credit header access is performed for this function.

If Congress chooses to maintain access, it should limit the purposes for which investigators can obtain credit headers. When access is obtained, a notation should be entered onto the credit report so that the individual can find out who has been purchasing access to their personal information.

Question: One witness at the hearing testified that an FTC study on identity theft indicated that the SSN does not play a major role in identity theft. Do you agree with this interpretation of the study?

Answer: We strongly disagree with the proposition advanced by Mr. Cate in oral and written testimony on June 15, 2004 that the Social Security Number (SSN) does not play a major role in identity theft. Common sense, the experience of identity theft clearinghouses, identity theft litigation, and the academic literature support the proposition that the SSN plays a primary role in identity theft. It is almost impossible to obtain credit without a SSN, making possession of the identifier a necessary condition for commission of identity theft. Under Federal law, states must collect SSNs in order to issue driver's licenses; therefore the identifier is always involved in cases where an impostor seeks credentials in a victim's name. Mr. Cate may be correct that the SSN is not a major factor in credit card fraud, but that form of identity theft is less serious from the victim's perspective, and legislative effort to prevent the crime should focus on impostors who obtain new accounts or credentials in the victim's name.

This common-sense problem of SSN being linked to fraud was identified by a Florida statewide grand jury devoted to exploring problems of identity theft: One of the most valuable pieces of information that an identity thief is searching for is the Social Security number, because the American financial industry has placed great reliance on it as the primary means of identifying individuals. Universities identify students with it. Providers of medical care and insurance coverage use it to identify their patients and clients.[16]

The Florida grand jury made strong recommendations for limiting disclosure and use of the SSN in order to address identity theft . . . the sale of Social Security numbers must be stopped. The Federal proposals must be adopted and Florida must continue its efforts to enforce the recently enacted laws that make social security numbers confidential within public records and prohibit its release. Florida must also continue to minimize the requests for Social Security numbers to be included

---

[15] Electronic Privacy Information Center, Amy Boyer, available at http://www.epic.org/privacy/boyer/.

[16] Identity Theft in Florida, Second Interim Report of the Sixteenth statewide Grand Jury, SC 01–1095 (Fla. Nov. 2002), available at http://myfloridalegal.com/pages.nsf/4492d797dc0bd92f85256cb80055fb97/f6995a8304fb723685256cca0059975f!OpenDocument.

on documents that will become public record, where the number is of little relevance to the government function.[17]

The experience of the major identity theft clearinghouses point to the central role that the SSN plays in fraud. A visit to the Web site of the Privacy Rights Clearinghouse, a leading provider of direct assistance to identity theft victims, reveals a number of cases where SSNs were the key to fraud: It's just a number, a nine-digit sequence issued by the U.S. Government. Every American must have one. It becomes your identity for life.

But most Americans take it for granted. I did—until my Social Security number, along with other personal information, fell into the wrong hands a couple of years ago. Since then, my number—my identity—has been hijacked several times for use in stealing thousands of dollars in goods and cash. Each time, I'm left to sort out the mess—Recently, I saw an entry blank for a drawing for a house. I stopped to look it over, but the instant I saw that the entry required disclosure of Social Security number, I threw it away. That number has become too precious.[18]

Individuals who serve in the military are at particular risk of identity theft, in part because of the government's use of the SSN as an identifier: I have been an identity theft victim for 1 year and I've yet to find an agency or organization that has brought any relief or words of comfort that can make this nightmare seem like it will have an end. I retired from the U.S. Army in 1999 after 20 years. July of 2001, Jerry Wayne Phillips, was able to get a military ID from Ft. Bragg, NC with my name and SSN. From there, you probably know the rest of the story. With that ID and my good credit history, he was able to buy cars, motorcycles, open credit card accounts, checking accounts, and get credit at virtually every department store that offers credit. I never came in contact with him, I didn't lose a credit card, and I wasn't careless with my Social Security number. The accounts he opened had no relationship to any of my accounts.[19]

Another victim testified:

How can this be possible? How can someone else actually open accounts or borrow money in your name? Well, it's quite easy, as we belatedly found out. All that person needs to do this is a close approximation of your first and last name and your SOCIAL SECURITY number. Spelling or accuracy doesn't matter. Nothing else about you is relevant. Different addresses various spouse names, birthday, any random place of employment, and spelling of this information is irrelevant. Age or any other personal information doesn't matter. All that is required is a first and last name that almost matches a Social Security number. The credit agencies readily verify an application if the Social Security number presented shows a good credit payment record. It doesn't matter if a different address, birthday, spouse's name or any variation to their recorded data is submitted with the application for their verification. The false data submitted by their customer now becomes your information. Again every transaction that involves your credit records is based on only one major piece of identification, your social security number.[20]

The Identity Theft Resource Center explains in a publication on the crime that: It is also clear that in the majority of identity theft situations victims were not responsible for the loss. Most of these situations started because a business or governmental entity allowed the thief access either directly or indirectly to personal identifying information. This includes databases, cards carried in wallets that included one's SSN or via items mailed to victims with account or SSN information (allowing access through mail theft, dumpster diving or theft), or unsafe information gathering or handling practices. The reality is there are only two things that a victim can do to directly facilitate identity theft: carry a Social Security card in one's wallet or fall victim to a telephone or Internet scam. In all other situations direct links to a business entity can be drawn.[21]

Identity theft litigation also shows that the SSN is central to committing fraud. In our written testimony, we detailed several identity theft lawsuits where it is clear that the SSN was the key to the impostor's success in the commission of iden-

---

[17] *Id.*

[18] Kerry Hill, *It All Starts with the SSN: Your Social Security Number Provides Avenue for Thieves,* Wisconsin State Journal, Sept. 13, 1998, at 1B, available at http://privacyrights.org/cases/victim13.htm (accessed June 29, 2004).

[19] *The Military ID Was too Easy to Get: System Failures Aided the Thief,* at http://privacyrights.org/cases/victim22.htm (accessed June 29, 2004).

[20] *Legislative Testimony of John and Jane Doe,* available at http://privacyrights.org/cases/victim5.htm (accessed June 29, 2004)

[21] Identity Theft Resource Center, Identity Theft: The Aftermath 2003, at http://www.idtheftcenter.org/idaftermath.pdf

tity theft.[22] In fact, the SSN plays such a central role in identification that there are numerous cases where impostors were able to obtain credit with their own name but a victim's SSN, and as a result, only the victim's credit was affected.[23] Last month, the Salt Lake *Tribune* reported: "Making purchases on credit using your own name and someone else's Social Security number may sound difficult—even impossible—given the level of sophistication of the nation's financial services industry—But investigators say it is happening with alarming frequency because businesses granting credit do little to ensure names and Social Security numbers match and credit bureaus allow perpetrators to establish credit files using other people's Social Security numbers."[24] The same article reports that Ron Ingleby, resident agent in charge of Utah, Montana and Wyoming for the SSA's Office of Inspector General, as stating that SSN-only fraud makes up the majority of cases of identity theft.[25]

Because creditors will open new accounts based only on a SSN match, California has passed legislation requiring certain credit grantors to comply with heightened authentication procedures. California Civil Code § 1785.14 requires credit grantors to actually match identifying information on the credit application to the report held at the CRA. Credit cannot be granted unless three identifiers from the application match those on file at the credit bureau.

We are aware of no academic literature that supports Mr. Cate's position. Instead, even a cursory review of the identity theft academic literature reveals that the SSN is understood as a principal tool for fraud.[26] In a recently published article, R. Bradley McMahon explains the key role that the SSN plays in identity theft:

The easiest and most common way for a thief to steal someone's identity is by acquiring that person's Social Security number and other private information. Social Security numbers are attractive to identity thieves because the numbers are abundant and provide access to a victim's private information. Social Security numbers commonly are used as a national identifier for everything from car rentals to credit card applications. Often a thief needs only a name and a Social Security number to open up a credit card account or to access an existing account.

A recent study reported that identity theft occurs mainly because information was either stolen or released from a company that compiles personal information. Over one thousand companies compile comprehensive databases of personal information and transfer this information every 5 seconds. Two of the largest compilers of personal data are the health care and the financial industries. Often, thieves look to these two sources for obtaining personal information. The liberal sharing policies of companies allow personal information to flow far beyond primary compilers. Once a person's information is released to one of these central sources, the dissemination of the personal information is completely out of the person's control. The extent to

---

[22] *See e.g. Nelski v. Pelland,* 2004 U.S. App. LEXIS 663 (6th Cir. 2004) (phone company issued credit to impostor using victim's name but slightly different Social Security Number); *United States v. Peyton,* 353 F.3d 1080 (9th Cir. 2003) (impostors obtained six American Express cards using correct name and Social Security Number but directed all six to be sent to the impostors' home); *Aylward v. Fleet Bank,* 122 F.3d 616 (8th Cir. 1997) (bank issued two credit cards based on matching name and Social Security Number but incorrect address); *Vazquez-Garcia v. Trans Union De P.R., Inc.,* 222 F. Supp. 2d 150 (D.P.R. 2002) (impostor successfully obtained credit with matching Social Security Number but incorrect date of birth and address); *Dimezza v. First USA Bank, Inc.,* 103 F. Supp. 2d 1296 (D.N.M. 2000) (impostor obtained credit with Social Security Number match but incorrect address).

[23] See e.g. TRW Inc. v. Andrews 534 U.S. 19 (2001) (patient's data was stolen by receptionist who successfully applied for credit with a matching SSN but different addresses in a different state, a different first name, and different date of birth).

[24] Lesley Mitchell, New wrinkle in ID theft; Thieves pair your SS number with their name, buy with credit, never get caught; Social Security numbers a new tool for thieves, The Salt Lake Tribune, June 6, 2004, at E1.

[25] Id.

[26] See e.g. Harry A. Valetk, Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies, 2004 Stan. Tech. L. Rev. 2 (2004) (describing problems caused by the " Nine-Digit Key to Identity Theft"); Peter C. Alexander, Identity Theft and Bankruptcy Expungement, 77 Am. Bankr. L.J. 409 (Fall 2003);Lynn M. LoPucki, Did Privacy Cause Identity Theft?, 54 Hastings L.J. 1277 (April 2003) (noting that of the identifiers on a credit application, " most important will be Consumer's Social Security number"); Christopher P. Couch, Forcing the Choice Between Commerce and Consumers: Application of the FCRA to Identity Theft, 52 Ala. L. Rev. 583 (Winter 2002); Erin M. Shoudt, Identity Theft: Victims "Cry Out" For Reform, 52 Am. U.L. Rev. 339 (October 2002); Jerilyn Stanley, Crimes Identify Theft: Supporting Victims in Recovering From the Crime of the Information Age, 32 McGeorge L. Rev. 566 (Winter 2001); Stephanie Byers, The Internet: Privacy Lost, Identities Stolen, 40 Brandeis L.J. 141 (Fall 2001); Kurt M. Saunders and Bruce Zucker, Counteracting Identity Fraud In The Information Age: The Identity Theft And Assumption Deterrence Act, 8 Cornell J. L. & Pub. Pol'y 661 (Spring 1999); Kristen S. Provenza, Identity Theft: Prevention and Liabilityty, 3 N.C. Banking Inst. 319 (April 1999).

which this information proliferates into third party networks is not known. The information shared by corporate America is one of the principal sources for identity theft.[27]

Professor Daniel Solove of the George Washington Law School similarly argues that: SSNs are a key piece of information for identity theft. SSNs can unlock a wealth of other information held by the government and the private sector—SSNs are used as passwords to obtain access to a host of personal records from banks, investment companies, schools, hospitals, doctors, and so on. The SSN is a powerful number, for with it a person can open and close accounts, change addresses, obtain loans, access personal information, make financial transactions, and more——

In short, the SSN functions as a magic key that can unlock vast stores of records as well as financial accounts. The SSN is the identity thief's best tool.[28]

The link between SSNs and identity theft is so well established that most academics include reference to the identifier when describing the crime:

The cases described earlier in this article merely hint at the range of actions that may constitute bankruptcy-related identity theft. Forms of bankruptcy-related identity theft include, without limitation:n:

Filing for bankruptcy using the name and/or SSN of another known person, such as a parent, sibling, child or other relative; a spouse, ex-spouse, "significant other" or ex-significant other; a current or former business partner, co-employee, cosigner on a debt, friend, neighbor or fellow student; or even a deceased person.

Incurring debt under a false name and/or SSN and then filing for bankruptcy, using that name and/or number to discharge the debt. Sometimes this debt is owed to the government via a farm loan, small business loan, student loan or similar obligation.

Transferring property into the name of a relative or friend, then filing for bankruptcy using that person's name and/or SSN to avoid foreclosure. Typically the transferee agrees to the transfer "to help out," but does not understand the legal ramifications.

Filing for bankruptcy using a false name and/or SSN that was apparently randomly chosen, because it does not belong to a person known to the perpetrator——

Using a false SSN when identifying oneself as a bankruptcy petition preparer.[29]

Finally, we take issue with Mr. Cate's characterization of the Identity Theft Survey Report that appears on page 6 of his testimony. On that page, Mr. Cate suggests that 76 percent of identity theft cases involved family members, friends, or financial institutions, and did not involve third party data. This is not a careful analysis of FTC's findings. Mr. Cate's 76 percent figure is not based on all identity theft victims. Instead, it is based on the *minority* of identity theft victims who knew the actual identity of the impostor ("in 26% of all cases, the victim knew who had misused their personal information").[30] The correct figure certainly is not 76 percent, as Mr. Cate suggests. Rather, the FTC very clearly wrote that:

"35% of the 26% of victims who knew the identity (or, in other words, 9% of all victims) said a family member or relative was the person responsible for misusing their personal information—23% of the 26% of all victims who knew the identity of the thief (or 6% of all victims) said the person responsible was someone who worked at a company or financial institution that had access to the victim's personal information—Of the 26% who knew the identity of the person who took their information, 18% said the thief was a friend, neighbor, or in-home employee, while 16% said the thief was a complete stranger, but the victim later became aware of the thief's identity. (These figures represent 5% and 4% of all victims respectively.)[31]

Mr. Cate would be correct in stating that in 25 percent of cases, the victim knew the impostor. However, that does not lead to the conclusion that H.R. 2971 or restrictions on third-party SSN sale is unjustified. H.R. 2971 could still reduce identity theft in cases where a friend, family member, company, or financial institution has access to SSNs. Instead of dumpster diving or stealing SSNs from computers, these impostors rely upon the appearance of the SSN in their acquaintances' mail or other personal belongings. For instance, in the college context, identity theft is facilitated by institutions that print the SSN directly on the student identity card.

---

[27] R. Bradley McMahon, Note: After Billions Spent to Comply With HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America?, 49 Vill. L. Rev. 625, 627 (2004).

[28] Daniel J. Solove, Identity Theft, Privacy, and the Architecture of Vulnerability, 54 Hastings L.J. 1227, 1252 (2003)

[29] Jane E. Limprecht, Fresh Start or False Start? Dealing with Identity Theft in Bankruptcy Cases, American Bankruptcy Institute Journal, December 200, 2000 ABI JNL LEXIS 192.

[30] Federal Trade Commission, Identity Theft Survey Report 28, Sept. 2003, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[31] Id. at 28–29.

Accordingly, a roommate can very easily copy or take the victim's student identity card and then have the identifiers necessary to commit identity theft. Contrary to Mr. Cate's conclusion, H.R. 2971 would address these risks of identity theft. As SSNs are removed from checks, ID badges, and other materials, individuals will be less likely to be victimized by strangers or by their roommates, family members or friends.

Question: If a private entity—for example, a consumer reporting agency, health care organization, or information reseller—has an individual's SSN in its possession, and this information is used in an identity theft or fraud, should that entity be held strictly liable for any harm done? Please comment on the advantages or disadvantages of this idea, as well as its feasibility and potential effectiveness in combating identity theft.

Answer: EPIC has argued that collection of the SSN should be limited, but where it is allowed, it should be subject to a full set of "Fair Information Practices," rights and responsibilities in data that ensure accuracy, access, and accountability. As part of the accountability responsibility, a strict liability standard would encourage companies to avoid unsafe practices. In particular, when a safer alternative activity exists, strict liability encourages use of the safer alternative while negligence offers no such additional incentive.

Social Security number usage is a good fit for this standard. There are clear and equally effective alternatives to SSN use (alternative identifiers, avoiding SSN use altogether if unnecessary, and so forth.), and there is a far greater interest in avoiding identity theft altogether rather than simply preventing any identity theft that is not cost-effective to prevent in the first place, which negligence provides.

Also, given the relatively small number of SSN aggregators, it is likely to be more efficient and less expensive to provide insurance against identity theft for such aggregators, rather than for individual potential victims who are likely to be less able to gauge their relative risk. The main disadvantage to a strict liability standard is that it may impose damages for losses that are unforeseeable or that would be too costly to prevent. Additionally, liable entities may draw attention to particular cases where significant damages are imposed in the absence of obvious fault.

By encouraging companies to avoid using SSNs at all, rather than simply providing certain protections for unnecessary SSN use, a strict liability standard would be more effective at combating identity theft by decreasing the availability of and dependence on SSNs.

We also suggest that Congress consider as an accountability measure a "security breach notification" law. California enacted such a law that took effect in July 2003. It requires all entities to notify individuals when their unencrypted SSNs are acquired by an unauthorized person.[32] Under current law, a company could suffer a severe security breach and not notify any individual affected (except Californians). We think that a notice requirement is a fair condition for continued use of the SSN.

Questions from Chairman E. Clay Shaw, Jr. to Mr. Brian P. McGuinness

Question: How many states do not have a specific licensing requirement for private investigators? For those states that do have licensing requirements, how uniform are those requirements? Describe the oversight performed of licensed investigators' activities? What would prevent an investigator from becoming licensed, or having a license renewed?

Answer: There are currently seven states that do not require licensing of private investigators. In my state of Florida investigators are subject to extensive criminal history background checks. We are stringently regulated with requirements for records retention, insurance, training (if armed) and subject to disciplinary action. The Department of Agriculture and Consumer Services takes its job seriously. Requirements do vary among the states but include background checks. Details about the various requirements may be found through the website of the International Association of Security and Investigative Regulators at www.iasir.org. As in my state, investigators are subject to penalties including the loss or suspension of a license. Serious violations of state regulations would prevent an investigator from renewing a license. Mandatory background checks prevent unqualified applicants from obtaining one. Let me add that there are very few instances of private investigators misusing identifying data. As proposed, the restrictions on our ability to access critical information puts the public at far greater risk than do the handful of cases where an investigator may have inappropriately used the data.

---

[32] California Senate Bill 1386, available at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

Question: You mentioned that information providers audit the users of the data to ensure compliance with their contract (i.e., that the data is being used only for purposes authorized under the law). Do both licensed and unlicensed private investigators have access to credit header data? What percent of transactions would you say information sellers audit? How many times have you been audited? What checks are there in the system to prevent a private investigator (licensed or unlicensed), or a member of the staff of a private investigator, from accessing credit header information for an unauthorized purpose?

Answer: We are not aware that the bureaus publish the number or extent of their audits. I have never been audited personally, but some of our members have and report that TransUnion, for example, has conducted stings to verify our members comply with the requirements to know their client and verify the purpose for which a report is used.

Question: You recommended deletion of section 108 of the bill, which would authorize the release of SSNs by credit bureaus only under the terms required for a full consumer report. That provision in the bill is not the jurisdiction of this Committee, but rather the Committee on Financial Services. However, we are interested in hearing your feedback about the provision. Since the bill's provision only restricts release of the SSN, why couldn't other parts of the credit header, like name, address, and telephone number still be used to locate witnesses? In what percent of cases overall is the SSN needed to help differentiate between records? Rather than eliminate the provision altogether, is it possible to modify it in a way that balances SSN privacy with necessary uses?

Answer: With regard to jurisdiction, we realize that any changes to the FCRA would be done by the Financial Services Committee, however, though you are not representing that Committee, Chairman Shaw is the author of the bill and we presume would have the authority to make recommendations for amendments. Because HR 2971 has been referred to multiple committees we expect that the vehicle that will ultimately be considered on the floor would in all likelihood be the product of a negotiation among these committees and the House Rules Committee. Recommendations of the sponsor and the Ways and Means Committee will be important.

Name and address information is not sufficient to assure that an individual is the person whom we are attempting to locate. The Social Security Number is essential for distinguishing among numerous people with the same name. In many instances we are seeking persons who share a name with thousands. Even if we had John Smith's birth date it wouldn't be sufficient because he would share it with many other John Smith's.

There are two ways requests for credit header information are made:

One is by submitting a social security number to the credit bureau provider. While that appears to be permissible under the current structure of section 108, under section 107 (a), it would be unlawful for an investigator acting as a Consumer Reporting Agency to submit a Social Security number to the provider or anyone. Under the Fair Credit Reporting Act, and pursuant to the FTC, investigators conducting investigations for a "permissible purpose" are considered to be Consumer Reporting Agencies. A substantial percentage of investigations by our members fall under the purview of the FCRA.

It should also be pointed out that the credit bureaus only sell header information to entities with whom they have contracted and who have executed those contracts which contain detailed limitations on the way that information may be used. I am unaware that credit headers are being sold directly to the general public.c.

Investigators are also required to indemnify the provider unconditionally for any liability incurred or alleged. The contracts spell out that the providers will conduct periodic reviews of "subscriber activity" and random audits. Violators are subject to termination of the account, legal action and being reported to Federal and state regulatory agencies.

The second way header information is requested is by submitting a name and date of birth to the provider. However, under section 107 (b)(1), the provider would be prevented from providing the Social Security number to the investigator thereby preventing a positive identification cross check.

With regard to modifying section 108, that could be done by inserting exemptions. However, we feel it should best be eliminated.

Following are our suggestions for amending section 107:

In section 107, after (c) strike (A) and insert the following new subsection:

i. to the extent necessary for law enforcement, including (but not limited to) the enforcement of a child support obligation, as determined under regulations of the Attorney General of the United States issued under section 205(c)(2)(I);
ii. if the display, sale, or purchase of the number is for a use occurring as a result of an interaction between businesses, governments, or business and government (regardless of which entity initiates the interaction), including, but not limited to——
a. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court,
b. or the prevention of fraud (including fraud in protecting an employee's right to employment benefits);
c. the facilitation of credit checks or the facilitation of background checks of employees, prospective employees, or volunteers;
d. the retrieval of other information from other businesses, commercial enterprises, government entities, or private nonprofit organizations

Question: You said you believe Congress should spell out all the appropriate uses of SSNs in the private sector, rather than allow the U.S. Attorney General to provide exceptions through regulations to the bill's prohibitions on sale, purchase, and display of SSNs to the general public, as H.R. 2971 requires. The activities you listed that private investigators provide are laudable. Why do you believe that you would not be able to convince the U.S. Attorney General during the process of developing and receiving comment on regulations that the SSN is needed for these purposes and that the costs do not outweigh the benefits?

Answer: HR 2971 includes several exceptions to the restrictions on the use of SSNs in section 107. These include exceptions for law enforcement, child support, national security, public health, emergencies, research and where the Attorney General determines appropriate. We believe investigations in anticipation of litigation, due diligence, insurance claims, civil and criminal fraud, criminal defense, identity fraud, stalking and other violations of law are just as deserving of exception. Not clearly listing these investigations in the statute sends a message to the Department that they are of less concern to Congress. Our industry has had recent experience with administrative interpretations of statute. Until corrected by statute last year, the FTC had interpreted the Fair Credit Reporting Act to require the consent of employees suspected of workplace misconduct before we could institute an investigation! We want to avoid repeating that experience.

The FTC is statutorily barred from promulgating regulations on the FCRA. 15 U.S.C. § 1681s(a)(4). The agency issues a non-binding commentary on the Act. Credit, Trade Practices, 16 CFR § 600, 607 (1995).

Questions from Chairman E. Clay Shaw, Jr. to Mr. Mike Buengerer

Question: What did the guidelines developed by the Conference of Chief Justices and Conference of State Court Administrators recommend with regard to display of SSNs, particularly on the Internet? What were the considerations that went into that recommendation? Didn't the draft version of the guidelines recommend excluding all but the last four digits of the SSN from display to the general public? Why did the group back off that recommendation?

Answer: With respect to the display of documents containing SSNs on the Internet or available electronically, the Guidelines recommended that courts consider whether those documents be accessible only on computer terminals within a court's facility. This proposal could be costly to implement as it would require court staff to examine documents to see if the contained SSNs and other sensitive information.

The preeminent consideration in the development of this recommendation was addressing the twin goals of protecting an individual's privacy and maintaining public access to the courts, which includes access to court documents. Many state constitutions possess so-called "open court" provisions that have generally been interpreted to mean that not only the courthouse doors but also the records of the court must be made available to the public. Other factors included: costs (both staff time and technology expenses), future technological advances, differing resource levels from court to court, inconvenience to court customers, and measuring the effectiveness of this approach.

Question: Court systems may sell copies of their records, individually or in a batch, to information resellers and others, correct? How does this

process work? How much revenue is raised by such sales? Would information resellers seek to purchase those records as frequently or at the same price if they did not contain SSNs?

The FTC is statutorily barred from promulgating regulations on the FCRA. 15 U.S.C. § 1681s(a)(4). The agency issues a non-binding commentary on the Act. Credit, Trade Practices, 16 CFR § 600, 607 (1995).

Answer: The interaction between information resellers and state courts vary widely from jurisdiction to jurisdiction. Generally, some resellers do pay for court records in bulk, especially in larger court systems, and these transactions are governed by court rules and procedures. In my experience, courts do not generally gain or make a "profit" from the bulk sale of court data. The money generated from such transactions pays for staff time, computer equipment usage/programming costs, paper, and cost of media. This is due in no small measure to the provisions of many state open record laws that allow state governments (including courts) to make public information available at cost but which generally limit the ability of state government entities to make information selling a "profit center." Most court rules governing these transactions stipulate that courts can reject a request from a reseller if that interferes with their ability to effectively serve the public. I would be glad to share examples of those court rules with the Subcommittee.

I have checked with the National Center for State Courts, the premier research institution dealing with state courts, and they report that there has not been a survey or study done on the amount of nationwide revenue generated by sales of bulk information to the courts.

I would theorize that information resellers would still purchase those records in bulk if they did not contain SSNs. Zip code marketing, home mortgage sale information, addresses and phone numbers are some of the valuable commodities to resellers that can still be garnered from court records.

Questions from Chairman E. Clay Shaw, Jr. to Mr. Fred Cate

Question: You stated that SSNs help locate information that can be used to verify the identity of a person. Why then is identity theft increasing at such a rapid pace despite the fact that creditors and others can use SSNs to link to information that helps verify an individual's identity and when they have a financial incentive to do so?

Answer:

1. As I testified, according to the most recent research conducted for the FTC, most identity theft is not committed by strangers, but rather by family members, friends, co-workers, and employees of organizations with whom the victim has contact. Social Security Numbers play a very limited role in these types of identity theft, and so the value of Social Security Numbers to help prevent identity theft and other frauds is limited.

In other situations, where a stranger uses a Social Security Number as one tool to help open a fraudulent account in a third party's name, Social Security Numbers have been very effective in helping to deter many incidents of identity theft. They would be even more effective (a) if they were more widely used by retailers, credit grantors, and others, and (b) if those same parties were more diligent in matching the identifying information in the credit file which the Social Security Number references to the individual seeking credit. In their haste to provide speedy service to a customer, some retailer and credit grantor may appear not to be diligently matching address, telephone number, and other available information that could be used to better verify identity..

Two caveats are important here. First, the problem of matching information is especially great in online and telephone commerce, where the applicant and credit grantor are not located in the same place. Nevertheless, many Internet and telephone businesses have been very successful in requiring extensive matching information and thereby holding down fraud. (Consider many airlines, for example, which require not only a valid credit card number, but also an address and telephone number that match the information in the credit card issuer's file.)

Question: You have said that ubiquitous SSNs help identify people and ensure that information is associated with the correct person. Why then have the FTC, the SSA IG, and the Postal Inspection Service identified it as a prime tool for terrorists and identity thieves?

Answer:

2. Social Security Numbers are a tool for many identity thieves for precisely the same reason that they are valuable to legitimate merchants, service providers, and consumers: they help provide a necessary link with a payment mechanism (e.g., whether a credit file that indicates likely ability to pay or a credit card).

We cannot have the positive benefits of instant credit, national commerce, and Internet and telephone business, without also having the risk that the same tools that make that possible will be used for identity theft. None of the government authorities to which you refer in your question has to my knowledge voiced any contradictory conclusion.

This is why I believe all of the available research suggests that the long-term solution to identity theft is not to restrict the use of Social Security Numbers, but to enhance their integrity and availability. If retailers and credit grantors were given greater incentives to check the file indicated by the Social Security Number presented by the customer and then match the information there with information presented by the customer, identity theft could be significantly reduced.

However, again, it must be reiterated that such incentives will be far less effective if consumers, in turn, are not given incentives to protect their Social Security and credit card numbers, avoid disclosing PINs and passwords to colleagues and family members, and check their account statements regularly for irregularities. It is easy, and therefore tempting, to focus only on the business side of the equation, but many of the most critical steps to help guard against identity thieves are uniquely in the hands of consumers. Moreover, as the FTC's recent work in this area demonstrates, the speed with which incidents of identity theft are detected is critical to reducing the losses they cause, yet a third of all consumers studied by that report never informed anyone of the theft, even after they discovered them. This suggests that reports of identity theft are exaggerated or that consumers wren to doing there part to help protect themselves.

Question: This Subcommittee has heard from a number of victims of identity theft. A common, and frustrating, theme is that after individuals discover the theft and report it to credit bureaus and financial institutions, they continue to be victimized by identity theft. How can this continue to occur, given the anti-fraud programs the industry cites? In your judgment, is the private sector doing enough to combat identity theft and assist its victims? Are there more effective ways to assist victims of identity theft to correct their credit histories? Should we require the credit industry to give priority status to help victims restore their records and good credit?

Answer:

3. You highlight a critical issue: the difficulty consumers face in getting their reputations restored after they have been the victims of identify theft. This is the single most consistent refrain from virtually all identity theft victims. Interestingly, many victims report that their primary frustration is when dealing with the government (e.g., getting the police to even take a report of an incident of identity theft, clearly up arrest records and traffic offenses resulting from an identity theft, finding consistency across the jurisdictions in which an identity thief may operate). I would urge you to focus on the government first, because there is nothing the public can do if the government fails in its duty.

The most recent research suggests that identity theft victims find it easier to deal with businesses, especially national credit bureaus and credit card issuers. Through measures adopted voluntarily by industry and those required by law, often facilitated by the FTC and other federal government agencies, it is getting easier to report identity theft and to get errors in financial records caused by identity thieves corrected. There is still more to be done. One measure that many industry representatives suggest would be useful would be a standardized identity theft police report, taken under oath, which could be made available electronically to retailers and credit grantors. It is important to remember that consumers often mislead businesses in an effort to avoid paying the debts that they have in fact incurred. Representatives of major credit card companies have long testified before Congress that many consumers—according to some companies, a majority—who call to object to a charge or other expense actually were responsible for it and either forgot it (or forgot lending their card to a family member or friend) or were deliberately trying to avoid paying it. It is not surprising that businesses might have some hesitation in accepting a consumer's word about an incident of identity theft in the absence of a police report.

Finally, I would encourage the Subcommittee staff to be as precise as possible when categorizing the complaints of identity theft victims. My understanding is that of those consumers who do have complaints with businesses—as opposed to the government—most focus on credit grantors, not credit bureaus or other aggregators of information.

Question: If a private entity—for example, a consumer reporting agency, health care organization, or information reseller—has an individual's SSN in its possession, and this information is used in an identity theft or fraud, should that entity be held strictly liable for any harm done? Please com-

ment on the advantages or disadvantages of this idea, as well as its feasibility and potential effectiveness in combating identity theft.

Answer:

4. The concept of liability for misuse of information by a third party has been discussed for some time, but so far avoided as a matter of law for what, I suspect, are good reasons. First, the proof problems are vast. How do we know where an identity thief got the information that he used in his crime? Second, causality is not at all clear. As I have noted before, the Social Security Number only provides a link to a credit or other file. It cannot—by itself—be used to commit identity theft.

Third, and closely related, there are almost always critical intervening factors that are far more important than the Social Security Number. The merchant who fails to verify information presented by the customer with that in the credit file, the business who accepts fraudulent identification that the thief obtained from the government, the consumer who fails to review his credit card statement—how is the law to assign responsibility to the possessor of the Social Security Number as opposed to these other parties.

Fourth, liability creates great risks for consumers—risks that merchants will be persuaded to invest in protecting Social Security Numbers at the expense of focusing scarce resources on other anti-identity theft measures, and risks that the additional costs of defending against such liability will undercut valuable services, interfere with consumer convenience, and contribute to increasing prices. Let me be perfectly clear, as a matter of both law and economics, I believe that broad-based liability for Social Security Number misuse by a third party is wholly unworkable.

That does not mean that there is no role for increased liability at all. When Congress limited consumer liability for credit card fraud to $50 (thereby effectively imposing that liability on merchants or card issuers, but without creating an invitation for expensive and wasteful class actions), it helped drive the greatest expansion of consumer credit the world has seen. There may be similar steps that Congress should be considering today—modest, targeted, highly focused efforts to create incentives for preventing and fighting identity theft. For example, Congress could provide that losses from identity theft will presumptively be the responsibility of any merchant whose failure to follow reasonable procedures to verify the identity of the customers is exploited by an identity thief.

As I have indicated, I believe the Subcommittee should think about focusing any new liability not only on businesses, but also on individuals, who are often in the best place to prevent and detect identity theft. For example, if you legislated a uniform identity theft affidavit, subject to a civil or criminal penalty for anyone who knowingly lies when completing one, it would then be far more feasible to expect retailers and credit grantors to rely on it and to do so quickly.

I would caution against too great of a focus on liability at this time, however. Congress has just put new tools into the hands of consumers and businesses that may prove very valuable in the fight against identity theft. Free credit reports, fraud flags, and other measures adopted last year as part of the Fair and Accurate Credit Transactions Act hold great promise. While the FTC is implementing those and we wait to see their impact, I would encourage you to focus on:

a. educating consumers about the new tools available to them to fight identity theft;
b. ensuring that government is doing its part in that fight by making incidents of identity theft easy to report, by improving the systems by which government records are cleansed of the deeds of identity thieves, and by improving the identity verification process that the government uses when issuing driver's licenses and other forms of identification on which we all rely; and
c. continue with those portions of the pending bill that would eliminate the wholly inappropriate use of Social Security Numbers (on envelopes and checks) and toughen penalties against providers of illicit Social Security Numbers and identification documents.

[Submissions for the record follow:]

June 16, 2004

The Honorable Clay Shaw
Chairman, House Ways & Means Subcommittee on Social Security
B–316 Rayburn 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 remain 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.

As public and private employee benefit plan sponsors, we provided detailed analysis of possible legislative proposals on July 24, 2003, to address our concern that such legislation could unintentionally hinder the delivery of benefits from, and the efficient administration of these plans. In that testimony, we stated that 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.

In working with you and your staff over the past year, much of this concern has subsided. We appreciate the bill you introduced in the 108th Congress, H.R. 2971, the "Social Security Number Privacy and Identity Theft Prevention Act of 2003." Although the bill treats public and private sector entities somewhat differently, it specifically recognizes the importance of voluntary employee benefit plans. Section 208A(a)(2)(B)(ii) (Section 107(a) of H.R. 2971) ensures that the provision of and administration of these plans will not be hindered by the legislation.

As you know, public and private employee benefit plans generally use SSNs because they enable the accurate and timely administration of benefits for a highly mobile workforce, and because use of the SSN 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"). We believe that Section 208A(a)(2)(B)(ii) would allow these important processes to continue as well.

Also, 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. Again, we believe this section, like the allowable legitimate uses of SSNs for national security, law enforcement, public health and advancing public knowledge purposes, permits this effective health process to continue.

As further evidence of your intent to protect the employer-employee relationship, Section 109 of H.R. 2971 provides for the continued use of SSNs when expressly required under Federal law, such as for W–2 income tax reporting. We applaud this effort as well.

We look forward to continuing to work with you and 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. To this end, we urge you to retain the important provisions described here without change as the Committee continues to examine legislative proposals. Please do not

hesitate to contact us should you require additional information or wish to discuss this issue in more detail.

Sincerely,

Jim Klein
American Benefits Council
Brian Graff
American Society of Pension Actuaries
Tony Lee
College and University Professional Association for Human Resources
Janice Gregory
ERISA Industry Committee
Bob Shepler
Financial Executives International's Committee on Benefits Finance
Jeannine Markoe Raymond
National Association of State Retirement Administrators
Cindie Moore
National Council on Teacher Retirement
Chris Stephen
National Rural Electric Cooperative Association
Ed Ferrigno
Profit Sharing/401(k) Council of America
Mary Huttlinger
Society for Human Resource Management

First Data Corporation
Englewood, Colorado 80112
June 14, 2004

The Honorable Clay Shaw
Chairman, Subcommittee on Social Security
1102 Longworth House Office Building
Washington D.C. 20515

Dear Chairman Shaw,

On behalf of First Data Corporation, I am submitting this testimony for the record. Serving approximately 3.5 million merchant locations, 1,400 card issuers and millions of consumers, First Data makes it easy, fast and secure for people and businesses to buy goods and services, using virtually any form of payment: credit, debit, smart card, stored-value card or check at the point of sale, over the Internet or by money transfer. First Data believes that protecting consumers from the misuse of Social Security Numbers (SSN) is an important goal. However, it is equally important to ensure that restrictions on the use of SSNs do not disrupt financial activities that consumers expect to occur or increase fraud, identity theft, and other criminal activities. As a leader in the financial services industry, we offer the following perspective on the positive uses of Social Security Numbers and exemption language that we believe should be considered in any legislation restricting the use of SSNs.

POSITIVE USES—While no one should profit from the display, sale or purchase of SSNs, restricting the use of the number may have the unintended consequence of increasing fraud and identity theft, making it harder for consumers to obtain the important services they have come to expect and rely upon from financial service companies, or increasing both the time and cost of obtaining such services. The following are examples of positive Social Security Number uses:

1. ***Authenticating individuals involved in financial accounts and transactions*—**Consumers engage in a wide variety of financial transactions and often have numerous financial accounts. Currently, the Social Security Number is the most reliable piece of personal information used to verify the identity of the consumer. Consumer names, addresses, phone numbers and account numbers often change over time. Both the date of birth and mother's maiden name are often easily accessible from public records. In contrast, a Social Security Number remains constant over time and is not, by itself, a public record.
2. ***Fraud and Identity Theft*—**Using a Social Security Number to authenticate a consumer is a valuable tool used by the business community to detect fraud and identity theft. Unfortunately, it is this same value that makes the Social Security Number such a precious commodity to criminals. The goal of any So-

cial Security Number legislation should be to limit criminal access to Social Security Numbers while preserving its use to stop identity theft.

PROPOSED EXEMPTIONS—We believe that legislation restricting the use of SSNs should include exemptions forthe collection or use of an individual's SSN in connection with the following activities:

a. To approve, guarantee, process, administer or enforce a financial account or transaction involving the individual, including authenticating the individual and any information provided by the individual in connection with the account or transaction.

[For example, the SSN is used to ensure that a deceased individual's Social Security Number is not used for fraudulent purposes and that future communications addressed to the deceased can be stopped.]

b. To evaluate, detect or reduce risk, fraud, identity theft or possible criminal activities.

[For example, the SSN is used to locate possible victims of such criminal activities.]

c. To report to or obtain information from a consumer reporting agency pursuant to the Federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq), or where the collection and use of the individual's SSN is required by any state or federal law, rule or regulation.

[For example, the SSN is a critical element for creating accurate credit reports which allow consumers efficient access to credit and other financial transactions.]

Sincerely,

Joe Samuel
Director of Government Relations

Statement of Stephen B. Copeland, Professional Investigators and Security Association, Vienna, Virginia

Mr. Chairman and Members of the Subcommittee:

My name is Stephen B. Copeland, and I am President of the Professional Investigators and Security Association (PISA). I want to thank you for the opportunity to submit testimony on the important issue of identity theft and how to effectively combat it. PISA was established in 1984 to represent the private investigation and security industries of the Commonwealth of Virginia. PISA's membership includes hundreds of professionals, many of which would be impacted by H.R. 2971.

In Virginia, these industries are regulated and monitored by the Private Security Services Section of the Commonwealth's Department of Criminal Justice Services. Extensive training, registration, certification and licensing requirements, coupled with criminal background checks, help ensure a high degree of competence and adherence to ethical standards. The Department of Criminal Justice Services also conducts investigations and audits of firms, individuals and training schools in the private security industry to ensure compliance with the requirements of Virginia law and regulations.

PISA is supportive of federal legislative efforts to prevent identity theft and assist victims of this fast-growing crime. Many of our members have been on the front lines of the battle against identity theft, assisting companies and individual identity theft victims by investigating, documenting, and exposing identity theft and fraud. In these efforts, Social Security Numbers and credit header data are critical investigative tools when used appropriately by law enforcement and licensed private investigation and security businesses.

Private investigation and security professionals use this data for a variety of other purposes as well, including child support enforcement, locating missing persons and heirs, fraud prevention, and employee background investigations.

Currently, access to Social Security Number and credit header data is not limited to credentialed professionals, but is also being made available to the general public, especially through the Internet. This access creates many opportunities for abuse by potential identity thieves. However, as noted recently by the General Accounting Office, restricting legitimate use of identified data by businesses could hurt con-

sumers and in fact make identity theft easier by making identity confirmation and background investigations more difficult.

To best serve the interests of the public, Congress must balance restricting access to Social Security Numbers and credit header data with the legitimate needs of law enforcement, businesses, and investigation and security professionals. While the objectives of H.R. 2971 are laudable, sections 107 and 108 would have a serious negative impact on the ability to investigate cases of identity theft and confirm the accuracy of background information provided by individuals.

We urge Congress to help prevent and combat identity theft by ensuring that any additional limitations on access to Social Security Number and credit header data preserve appropriate access by credentialed private investigation and security professionals.