

PROTECTING THE PRIVACY OF THE SOCIAL SECURITY NUMBER FROM IDENTITY THEFT

HEARING BEFORE THE SUBCOMMITTEE ON SOCIAL SECURITY OF THE COMMITTEE ON WAYS AND MEANS U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 21, 2007

Serial No. 111-33

Printed for the use of the Committee on Ways and Means



U.S. GOVERNMENT PRINTING OFFICE

63-017

WASHINGTON : 2011

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) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON WAYS AND MEANS

CHARLES B. RANGEL, New York, *Chairman*

FORTNEY PETE STARK, California	JIM MCCRERY, Louisiana
SANDER M. LEVIN, Michigan	WALLY HERGER, California
JIM McDERMOTT, Washington	DAVE CAMP, Michigan
JOHN LEWIS, Georgia	JIM RAMSTAD, Minnesota
RICHARD E. NEAL, Massachusetts	SAM JOHNSON, Texas
MICHAEL R. McNULTY, New York	PHIL ENGLISH, Pennsylvania
JOHN S. TANNER, Tennessee	JERRY WELLER, Illinois
XAVIER BECERRA, California	KENNY HULSHOF, Missouri
LLOYD DOGGETT, Texas	RON LEWIS, Kentucky
EARL POMEROY, North Dakota	KEVIN BRADY, Texas
STEPHANIE TUBBS JONES, Ohio	THOMAS M. REYNOLDS, New York
MIKE THOMPSON, California	PAUL RYAN, Wisconsin
JOHN B. LARSON, Connecticut	ERIC CANTOR, Virginia
RAHM EMANUEL, Illinois	JOHN LINDER, Georgia
EARL BLUMENAUER, Oregon	DEVIN NUNES, California
RON KIND, Wisconsin	PAT TIBERI, Ohio
BILL PASCARELL JR., New Jersey	JON PORTER, Nevada
SHELLEY BERKLEY, Nevada	
JOSEPH CROWLEY, New York	
CHRIS VAN HOLLEN, Maryland	
KENDRICK MEEK, Florida	
ALLYSON Y. SCHWARTZ, Pennsylvania	
ARTUR DAVIS, Alabama	

Janice Mays, *Chief Counsel and Staff Director*

Brett Loper, *Minority Staff Director*

SUBCOMMITTEE ON SOCIAL SECURITY

MICHAEL R. McNULTY, New York, *Chairman*

SANDER M. LEVIN, Michigan	SAM JOHNSON, Texas
EARL POMEROY, North Dakota	RON LEWIS, Kentucky
ALLYSON Y. SCHWARTZ, Pennsylvania	KEVIN BRADY, Texas
ARTUR DAVIS, Alabama	PAUL RYAN, Wisconsin
XAVIER BECERRA, California	DEVIN NUNES, California
LLOYD DOGGETT, Texas	
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

	Page
Advisory of June 14, 2007, announcing the hearing	2
WITNESSES	
Hon. Charles E. Schumer, a Senator from New York	6
Hon. Ed Markey, a Representative in Congress from Massachusetts	59
Hon. Joe Barton, a Representative in Congress from Texas	68

Hon. Patrick O'Carroll, Inspector General, Social Security Administration	63
Joel Winston, Director, Division of Privacy and Information Protection, Federal Trade Commission	74
Dan Bertoni, Associate Director, Education, Workforce, and Income Security, Government Accountability Office	96

Justin Yurek, President, ID Watchdog, Denver, Colorado	118
Stuart Pratt, President, Consumer Data Industry Association	123
James D. Gingerich, Director, Administrative Office of the Courts, Supreme Court of Arkansas, on behalf of the Conference of State Court Administrators, Williamsburg, Virginia	131
Annie I. Antón, Associate Professor of Software Engineering, North Carolina State University, Raleigh, North Carolina, on behalf of the Association for Computing Machinery	138
Marc Rotenberg, Executive Director, Electronic Privacy Information Center ...	158
Gilbert T. Schwartz, Partner, Schwartz & Ballen LLP, on behalf of the Financial Services Coordinating Council	169
SUBMISSIONS FOR THE RECORD	
LexisNexis, letter	183
Bruce Hulme, Legislative Director, National Council of Investigation and Security Services, statement	187
National Organization of Social Security Claimants' Representatives, statement	188
Property Records Industry Association, statement	190

**PROTECTING THE PRIVACY OF THE SOCIAL
SECURITY NUMBER FROM IDENTITY THEFT**

THURSDAY, JUNE 21, 2007

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

[The advisory announcing of the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

McNulty Announces a Hearing on Protecting the Privacy of the Social Security Number from Identity Theft

June 21, 2007
By (202) 225-9263

Congressman Michael R. McNulty (D-NY), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing to examine the role of Social Security numbers (SSNs) in identity theft and options to enhance their protection. **The hearing will take place on Thursday, June 21, in room B-318 Rayburn House Office Building, beginning at 10 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

As many as ten million Americans fall victim to identity theft every year. The effects of identity theft can be catastrophic to the lives of affected individuals. The reported costs are significant—according to the Federal Trade Commission, businesses lose \$50 billion and consumers expend another \$5 billion annually to recover from identity theft. The SSN is a critical tool for identity thieves looking to establish a credit account in someone else's name. And it is often the key that identity thieves use to gain access to other personal information such as bank accounts.

Because it is a unique piece of personal information that does not change over time, the SSN provides a convenient way to track individuals throughout public and private records. As a result, SSNs have become ubiquitous in these records, and they are being used for purposes far beyond their original role of tracking earnings in order to compute Social Security benefits. While the widespread use of SSNs can be advantageous to business and government, it is also useful for identity thieves and other criminals. Moreover, records containing the SSN are increasingly available in electronic form, and easily accessible over the Internet. Thus, the need for streamlined business processes and openness of public records must be balanced against the increasing risks of identity theft and other crimes.

Despite its widespread usage, there is no Federal law that requires comprehensive confidentiality protection for the SSN. An SSN may be found on display to the general public on employee badges and in court documents, or offered for sale on the Internet. Some limited protection of SSN confidentiality is provided by the Fair Credit Reporting Act (P.L. 91-508) and the Gramm-Leach-Bliley Act (P.L. 106-102), which restrict the use and disclosure of SSNs by financial institutions. Also, many states have enacted legislation to restrict the use, disclosure or display of SSNs. Still most private sector use of the number remains unregulated.

In the 108th Congress, the Committee on Ways and Means approved comprehensive legislation to enhance SSN privacy to protect against identity theft (H.R. 2971; H. Rept. 108-685). Among other provisions, the bill would restrict the use, sale, purchase or display of SSNs. Members of Congress concerned about the magnitude of identity theft and its devastating effects on victims have introduced similar legislation this year.

In announcing the hearing, Chairman McNulty stated **“there is no question that we need stronger protections for Social Security numbers to combat**

the growing crime of identity theft. Identity theft can destroy an individual's or family's financial well-being with a touch of a button. We must begin to place some common-sense limits on the use of the SSN by government and business in order to ensure the privacy of the information and prevent theft."

FOCUS OF THE HEARING:

The Subcommittee will examine what role the SSN plays in identity theft, and the steps that can be taken to increase SSN privacy and thereby limit its availability to identity thieves and other criminals. The hearing will examine how SSNs are currently used, what risks to individuals and businesses arise from its widespread use and options to restrict its use in the public and private sectors.

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://democrats.waysandmeans.house.gov>, select "110th Congress" from the menu entitled, "Committee Hearings" (<http://democrats.waysandmeans.house.gov/Hearings.asp?congress=110>). 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 **Thursday, July 5, 2007**. 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://democrats.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.

The Subcommittee met, pursuant to notice, at 10:00 a.m., in room B-318 Rayburn House Office Building, Hon. Michael R. McNulty (Chairman of the Subcommittee) presiding.

Chairman MCNULTY. The hearing will come to order. I want to welcome all of our witnesses and all of our guests. You will notice on the list of witnesses that we have three Members of Congress scheduled to be here today, Senator Schumer, Congressman Markey and Congressman Barton. They are involved in markups today so we do not know exactly what time they will arrive, but as they arrive, we will ask the indulgence of the other witnesses to accommodate their statements so that they can come in, make their statement, if they have time, answer a couple of questions and then get back to their markup.

Our hearing today will focus on the role that the Social Security number plays in the crime of identity theft and options to enhance the privacy and security of the Social Security number so that it is not as useful a tool for identity thieves.

Stealing or obtaining Social Security numbers through illegitimate means is a key part of identity fraud. Our Subcommittee is deeply concerned about identity theft and how to better protect the Social Security number. In fact, this is the 16th hearing on this topic we have held in the past 7 years. Identity theft is one of the fastest growing crimes in the United States. Research by the Federal Trade Commission suggests that almost 5 percent of the adult population of the United States, some 10 million people, were victims of some kind of identity theft in just a single 12-month period. Through its Web site and toll free hotline, the FTC receives between 15,000 and 20,000 contacts each week from those who have been victimized by identity thieves, as well as people seeking information about how to protect themselves from identity theft. Identity theft ruins individuals' good names and destroys their credit ratings. Identity thieves have stolen the homes of elderly retirees and have caused innocent persons to be arrested when crimes are committed under a falsified identity. It has even ruined the future credit ratings of young children.

The FTC reports that individuals spend \$5 billion a year attempting to recover their good names and credit histories. Annual surveys find that businesses lose more than \$50 billion per year to identity theft-related fraud. Victims also spend years cleaning up the damage done by such thieves. In fact, we have learned that a victim who testified before this Subcommittee in the previous Congress, Nicole Robinson, still has not been able to correct her credit record. Even though she testified before Congress and our staff intervened with the credit bureaus, she continues to experience problems relating from the theft of her identity 7 years after her identity was first stolen.

The Social Security Administration and its inspector general have worked diligently to increase the integrity and security of the Social Security number and the procedures used in issuing it. But SSA has essentially no control over how the Social Security number is used by other governmental agencies or the private sector.

Today, we will hear about the problem of identity theft from Government agencies who have studied it and representatives of those who suffer from it. We will hear from businesses and Government

agencies that use the Social Security and we will hear suggestions on how to better protect the Social Security number by limiting its use by Government and the private sector. I am committed to moving forward with legislation and of making it more difficult for thieves and other wrongdoers to obtain a Social Security number and use it to commit identity theft or other crimes. I welcome the testimony we will receive today that will help us better understand the nature of the problem and the potential solutions.

I am now pleased to yield to the Ranking Member of the Committee, a distinguished veteran and one of my heroes in life, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman. I appreciate Chairman McNulty for holding this hearing on protecting the privacy of Social Security numbers from identity theft. You know Americans are rightly worried about the security of their personal information, including their Social Security number. We hear reports on a daily basis about another data breach in the private or public sector where hundreds, if not thousands, of people's personal identity information is stolen.

According to the Privacy Rights Clearinghouse, the total number of known records that have been compromised due to security breaches beginning in January 2005 through last week was over 155 million. The fact is that even though Social Security numbers were created to track earnings for determining eligibility and benefit amounts under Social Security, these numbers are widely used as personal identifiers.

As we will hear today, Social Security numbers are vital to many commercial and Government transactions to verify identity and prevent fraud. Examples include enforcing child support, aiding law enforcement, compiling information from many sources to help ensure the accuracy of credit reports. Unfortunately, as pointed out by the GAO in testimony before this Subcommittee, Social Security numbers have become the identifier of choice and are used for everyday business transactions. In fact, in their April 2007 report, the President's Identity Theft Task Force identified the Social Security number as the most valuable commodity for an identity thief. So, it is no wonder that concerns about identity theft remain high.

According to the Federal Trade Commission, identity theft is the number one consumer complaint, amounting to 36 percent of complaints received in 2006. Americans are right to be concerned. According to the latest data provided by the FTC, over a 1-year period, nearly 10 million, or about 5 percent of the adult population, discovered they were victims of identity theft. Even worse, the true number of victims in this devastating crime is unknown since most victims do not report it. Losses due to these thefts were estimated to exceed \$50 billion. Also, it has been reported that ID theft victims spend roughly 300 million hours a year trying to resolve the negative effects of ID theft, including re-establishing their hard-earned good credit and clearing their good name. Even worse, identity theft continues to threaten our national security. As said in the 9/11 Commission Report, and this is a quote, "Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for board aircraft,

sources of identification are the last opportunity to ensure that people are who they say they are and to check whether or not they are terrorists.”

Our Subcommittee has been working on a bipartisan basis to protect the privacy of Social Security numbers and prevent identity theft since the 106th Congress when it first approved the Social Security number Privacy and Identity Theft Prevention Act to restrict the sale and public display of Social Security numbers. This legislation was introduced on a bipartisan basis by then Subcommittee Chairman Clay Shaw and then Ranking Member, the late Bob Matsui. We know that providing for uses of Social Security numbers that benefit the public while protecting their privacy is a complex balancing act. However, I believe we must act and with your help, Mr. Chairman, we will act to stop rampant abuse of Social Security numbers, help prevent ID theft and further protect American privacy.

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

Chairman MCNULTY. I thank the Ranking Member. Other Members will be allowed to insert opening statements for the record. We are pleased at this time to be joined by Senator Schumer, who is involved in another markup, and we are going to go to him right away. He is the senior Senator from the State of New York. He has a long history on this subject of trying to protect our constituents across the country from identity theft. He is a dear friend of mine and before he leaves, I am going to give him a little editorial from one of the local newspapers in my district because when he was first elected to the Senate back in 1998, many people in upstate New York were wondering how much they would see of the new Senator, and he made a pledge that he would visit each of the 62 counties in the State of New York every single year that he was in office. The editorial from the newspaper cites the fact that you have kept that pledge every single year that you have served in the Senate. Thank you for going over and visiting my friend John Redcliffe and the farmers over there, they deeply appreciate it.

Senator Schumer.

STATEMENT OF CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Well, thank you, Mr. Chairman. I very much appreciate the introduction. I am so glad to be here for a whole lot of reasons. First, it is great to call you “Mr. Chairman,” my good friend Mike McNulty, who does such a wonderful job both in the capital region and down here. Second, for the 18 years in the House, or at least the first 9 and 10, I really wanted to be on this Committee, and I never got on so I am glad to get here at least on this side of the table. I am now on Senate Finance. Things work a little faster in the Senate in terms of seniority.

I thought I might just tell a quick story in reference to the Chairman’s mention. It is true I visit every county every year, so I am pretty diligent. I go to the little counties and big counties. In 2004, when I ran for re-election, I carried 61 of the 62 counties. I did not

carry one, Hamilton County, not that far from where you are. Hamilton is a beautiful county. It is as large as Rhode Island. It is in the middle of Adirondacks, great forests and rivers and mountains, great hunting, great fishing, but it is our smallest county population-wise. It has a little bit fewer than 5,000 people. I had visited it six times since re-election, which was a lot. I asked my chief of staff, "Why do you think I lost Hamilton County," Martin Brennan. Martin Brennan said, "It is easy, Chuck, it is the only county where you actually met every single voter."

Anyway, it is good to be here. I want to thank all of my friends, so many of whom I served with in the House, and my friend, Eddy Markey, who was senior to me then and senior to me now, and I thank you for your leadership on this issue, Mr. Chairman. Let me thank Congressman Rangel, our colleague from New York as well.

We all know when it comes to identity theft, the Social Security number is the golden key that opens all doors. If you can get a person's Social Security number, you can impersonate him, steal his money, ruin his credit and literally devastate his life. In my testimony, I am going to focus on one particular risk of identity theft and what Congress can do about it. I am pleased that today the GAO, the Government Accountability Office, prepared at my request a report which focuses on the insidious problem of Social Security numbers displayed online in public records, and that report is being release coincident with this hearing.

Now, it used to be that when your tax lien or your divorce decree was filed as a public record, it sat in an office building. You had to go there in person to track down a record but in recent years, more and more Government agencies are putting public records on the Internet. In fact, the GAO found that in 40 out of 50 States, one or more offices are displaying people's public records right on the Internet. Anyone with a computer can now view these online records, often for free. The recordkeepers who put files online probably just want to provide more transparency and access to information and those are important values I think we all support, but we need to have public access in a way that does not expose people to identity theft.

In the words of the GAO, these online records provide "potentially unlimited access" to personal information, including Social Security numbers. It is not surprising that there are known cases where identity thieves use online public records to prey on their victims. Yet, the GAO reports that online display of public records is on the rise. We cannot let this practice continue unchecked. The report shows that online public records may be doing more harm than good. The world has changed but our laws are lagging far behind.

Here is what we can do about it, Mr. Chairman, and I look forward to working with you and Chairman Rangel to try and accomplish some good changes here. First, we need to have uniform standards for protecting Social Security numbers by hiding either the first five digits or the last four digits. The good news is that Federal agencies have started hiding the first five digits of Social Security numbers in public record documents. The very bad news is that data brokers and other entities are going in the opposite direction and hiding the last four digits. So, it is a classic case of the

Federal Government where one hand does not know what the other is doing. It makes it very easy to use public sources to get the whole nine numbers. It is sort of a little bit like an Abbott and Costello routine.

You get the first five from the Social Security records—you get the last four from the Social Security records, the first five from the others, the data brokers and others, and you sort of have straight flush for identity theft. It is like a slap stick routine, each group points the finger at the other but it is not a joke when ordinary citizens are paying the price. The GAO was able to piece together people's full nine digit numbers even though they were always hidden, one half or the second half, in just one hour from their desks. An identity thief could do this anywhere in the world. So, I am proposing legislation that would require the Social Security Administration to set standards, telling public agencies and private businesses what method of truncation to use so everyone will be protected. It is sort of a tragedy of errors, everyone is trying to help by masking part of the number but no one is paying attention to the big picture and that is where they need a Federal role.

Congress should act now because the numbers of records involved are growing everyday, a little coordination in this area will go a long way toward stopping identity theft and it seems to me that this simple bill should pass by a wide margin. I do not know who would oppose it.

Second, we need to make sure that state and local recordkeepers are never displaying full Social Security numbers on the Internet. I will be re-introducing my bill from the last Congress to ban these recordkeepers from showing complete numbers on the Internet. Again, I hope this bill can be passed quickly given the evidence of the report. The legislation is feasible and practical given the advanced technology we have today, like software to help find and hide Social Security numbers. County clerks and other public recordkeepers are public servants and they should be taking steps to protect people. They cannot say, "Well, it is not my problem."

So, if recordkeepers want to put documents online, they should but they should hide all or part of the Social Security number that appears in those documents. Under this bill, the Department of Justice will be able to enforce the ban by imposing fines on any office that ignores the law. It will also help recordkeepers by authorizing grants to their offices if they want to redact Social Security numbers from the older records because that takes a job to go back and do it, and we do not think that the local taxpayer should have to foot the entire bill for that.

Finally, the GAO reports that private businesses have been buying public records in bulk for years. We need to know more about this practice, and I have asked the GAO to investigate it. Currently, we have no idea how frequently our records are being sold or why or where they go. This report reveals there may be large sets of records that are overseas and that these Social Security numbers may be beyond the protections of American law. When the GAO reports back on their investigation, we should try to work together to close any loopholes. The buying and selling of our private information is not the kind of thing that should be happening in

the dark of night without any oversight even from people who are 10,000 miles away.

With the great power of today's technology, Mr. Chairman, in conclusion, comes a great responsibility to regulate that technology and avoid unintended harms. The measures I have mentioned today will address the risks uncovered in today's report, excellent report by the Government Accountability Office, great job, and I hope that my colleagues will join me in moving these measures forward to protect Americans from identity theft.

In conclusion, finally, I want to thank the Subcommittee and your leadership, Mr. Chairman, and the Ranking Member, Mr. Johnson, so that we can—this is an important step, this hearing, on rising to the challenge of protecting our Social Security numbers. I very much thank you for allowing me to be here today.

[The prepared statement of Senator Schumer follows:]

**Prepared Statement of the Honorable Charles E. Schumer
a Senator from New York**

Good morning, Chairman McNulty and Ranking Member Johnson. Thank you for inviting me to testify.

I want to commend Subcommittee Chairman McNulty and Committee Chairman Rangel, my esteemed colleagues from the New York delegation, for holding this important hearing on protecting Social Security numbers.

We all know that when it comes to identity theft, the Social Security number is the golden key that opens all doors. If you can get a person's Social Security number, you can impersonate him, steal his money, ruin his credit, and literally devastate his life.

In my testimony, I'm going to focus on one particular risk of identity theft, and what Congress can do about it. I am pleased to announce today's release of a new report, prepared at my request by the Government Accountability Office, that focuses on the insidious problem of Social Security numbers displayed online in public records.

It used to be that when your tax lien or your divorce decree was filed as a public record, it sat in an office building. You had to go there in person to track down a record. But in recent years, more and more government agencies are putting public records on the Internet.

In fact, the GAO found that in 40 out of 50 states, one or more offices are displaying people's public records right on the Internet. Anyone with a computer can now view these online records, often for free.

The record-keepers who put files online probably just want to provide more transparency and access to information, which are important values that I support.

But we need to have public access in a way that doesn't expose people to identity theft.

In the words of the GAO, these online records provide "potentially unlimited access" to personal information, including Social Security numbers.

It's not surprising that there are known cases where identity thieves used online public records to prey on their victims.

And yet the GAO reports that online display of public records is on the rise. We cannot let this practice continue unchecked.

This report shows that online public records may be doing more harm than good. The world has changed, but our laws are lagging far behind.

Here's what Congress can do about it, and I hope that my good colleagues here on the House side will lend their support to these measures.

First, we need to have uniform standards for protecting Social Security numbers by hiding either the first five digits or the last four digits.

The good news is that federal agencies have started hiding the first five digits of Social Security numbers in public record documents. The very bad news is that data brokers and other entities are going in the opposite direction of hiding the last four digits.

This is a case of classic Federal Government where one hand doesn't know what the other is doing.

This makes it very easy to use public sources to piece together a full nine-digit Social Security number that could be used for identity theft. The GAO was able to

do this in just one hour, from their desks. An identity thief could do the exact same thing—from *anywhere in the world*.

It's almost like a slapstick routine—each group is pointing the finger at the other. But it's not a joke when ordinary citizens are paying the price.

That's why I am proposing new legislation that will require the Social Security Administration to set standards telling public agencies and private businesses exactly what method of truncation to use.

It's a tragedy of errors—everyone is trying to help by masking part of the number, but no one is paying attention to the big picture. It's time for a federal role.

Congress should act now, because the numbers of records involved are growing every day. Just a little coordination here will go a long way toward stopping identity theft, and it seems to me that this simple bill should pass by a wide margin.

Second, we need to make sure that state and local record-keepers are never displaying full Social Security numbers on the Internet. I will be reintroducing my bill from the last Congress to ban these record-keepers from showing complete numbers on the Internet.

I hope that my bill can be passed quickly, given the new evidence in this report. This legislation is both feasible and practical given the advanced technology we have today, like software to help find and hide Social Security numbers.

County clerks and other record-keepers are public servants—they should be taking steps to protect people. If record-keepers want to put documents online, they are welcome to do so, but they should hide all or part of any Social Security number that appears in those documents.

Under this bill, the Department of Justice will be able to enforce the ban by imposing fines on any office that ignores the law. My legislation will also help record-keepers by authorizing grants to offices that want to redact Social Security numbers from older records, but need more resources.

Finally, the GAO reports that private businesses have been buying public records in bulk for years. We need to know more about this practice, and I have already asked the GAO to investigate it.

Currently, we have no idea how frequently our records are being sold, or why, or where they go. This report reveals that there may be large sets of records that are overseas, and that these Social Security numbers may be beyond the protections of American law.

When the GAO reports back on their investigation, the Congress should move quickly to close any loopholes. The buying and selling of our private information is not the kind of thing that should be happening in the dark of night, without any oversight.

With the great power of today's technology comes a great responsibility to regulate that technology and to avoid unintended harms. The measures that I've highlighted will address the risks uncovered in today's report, and I hope that my colleagues will join me in moving these measures forward to protect Americans from identity theft.

In closing, let me say that I appreciate the excellent work of the Government Accountability Office in preparing this study.

Again, I thank the Subcommittee for recognizing that we must rise to the challenge of protecting our Social Security numbers, and thank you for having me here today.

Chairman MCNULTY. Thank you very much, Senator Schumer. I know you are on the run but I just wanted to thank you for your testimony, to assure you that we will work together with you on legislation. I also want to thank you for a statement you made in another trip upstate recently about properly funding the Social Security agency so that we can start to cut back on this tremendous backlog that we have with regard to disability claims, which is not only a tremendous hardship on many of our constituents, it is a national embarrassment to every Member of Congress when someone comes in with a legitimate claim for a government benefit, and we tell them they have to wait a year and a half or 2 years before they even get an answer, so we really need to do something about that.

I want to thank you for your commitment in that regard. On the House side, we have taken some steps in moving toward that. We have got \$100 million over the President's request out of the Appropriations Committee, I asked for more than that but we got that far anyway. In recent years, the President's request has been under-funded, we are \$100 million over. I am hoping that on the Senate side you can help us get to at least that number, or hopefully higher, so that we can begin to make a serious dent in this backlog. I do not know if you have time, do you have time to take a couple of questions? Then we will get immediately to Ed Markey after that. Does any Member wish to pose a question to the Senator? Yes, Lloyd?

Mr. DOGGETT. Chuck, thanks so much for what you have been doing on this. Can you update us on where this legislation is in the Senate and how you think it is moving over there?

Senator SCHUMER. I think it is moving very well. We are just going to update it because of the GAO report, particularly the first thing I mentioned, but it seems to have support. The one place where there was objection, the old or the local officials who used and put these things online, we have dealt with their objections, and I think the new legislation should have smooth sailing. Thank you, Lloyd.

Chairman MCNULTY. I also want to ask unanimous consent that we insert into the record the new GAO report, which the Senator referenced in his testimony. Mr. Levin.

[The provided material follows:]

United States Government Accountability Office

GAO

Report to the Chairman, Subcommittee
on Administrative Oversight and the
Courts, Committee on the Judiciary,
U.S. Senate

June 2007

SOCIAL SECURITY NUMBERS

**Federal Actions Could
Further Decrease
Availability in Public
Records, though Other
Vulnerabilities Remain**



GAO-07-752

Contents

Letter		1
	Conclusions	3
	Recommendations for Executive Action	4
	Agency Comments	4
Appendix I	Briefing Slides	6
Appendix II	Comments from the Office of Management and Budget	40
Appendix III	Comments from the Internal Revenue Service	42
Related GAO Products		44

Abbreviations

DOJ	Department of Justice
IRS	Internal Revenue Service
OMB	Office of Management and Budget
SSA	Social Security Administration
SSN	Social Security number

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



June 15, 2007

The Honorable Charles Schumer
Chairman
Subcommittee on Administrative Oversight and the Courts
Committee on the Judiciary
United States Senate

Various public records in the United States, including some generated by the federal government, contain Social Security numbers (SSN) and other personal identifying information that could be used to commit fraud and identity theft. Public records are generally defined as government agency-held records made available to the public in their entirety for inspection, such as property records and court records. Although public records were traditionally accessed locally in county courthouses and government record centers, in recent years, some state and local public record keepers have begun to make these records available to the public through the Internet. While it is important for the public to have access to these records, concerns about the use of information in these records for criminal purposes have been raised. In 2006, these concerns were heightened when an Ohio woman pled guilty to conspiracy, bank fraud, and aggravated identity theft as the leader of a group that stole citizens' personal identifying information from a local public record keeper's Web site and other sources, resulting in over \$450,000 in losses to individuals, financial institutions, and other businesses.

Although we previously reported on the types of public records that contain SSNs and access to those records, less is known about the federal government's direct provision of records with SSNs to state and local public record keepers. Because of your interest in information on these issues, we agreed to answer the following questions: (1) Which federal agencies commonly provide records containing SSNs to state and local public record keepers, and what actions have been taken to protect SSNs in these records? (2) What significant vulnerabilities, if any, remain to protecting SSNs in public records?

To answer these questions, we gathered information from a variety of sources. Specifically, we interviewed cognizant officials from the Social Security Administration (SSA), Office of Management and Budget (OMB), Internal Revenue Service (IRS), and Department of Justice (DOJ). We interviewed these agencies because they are responsible for overseeing

federal use of the SSN or they were identified through our research as commonly providing records containing SSNs to state and local public record keepers. We also conducted interviews with public record keepers, their national associations, and stakeholder groups focused on privacy rights, open government, and the title insurance industry. To gather information on records access, we visited local public record keepers' offices in the District of Columbia, Maryland, and Virginia; reviewed several Web sites that provide information on state and local public records access; and used this work to guide our selection of state and local public record keepers' Web sites nationwide for additional review. In total, we reviewed at least one public record keeper's Web site per state. We also interviewed public record keepers in five Florida counties to examine implementation of recently enacted Florida statutes requiring Internet access to public records and the removal of SSNs and other information in those records. We conducted our work from November 2006 through May 2007 in accordance with generally accepted government auditing standards.

On May 10, 2007, we briefed your staff on the results of our analysis. This report formally conveys the information provided during that briefing (see app. I). In summary, we found:

- IRS and DOJ are the only federal agencies that commonly provide records containing SSNs to state and local public record keepers, and in recent years, both have taken steps to truncate or remove SSNs in those records. These agencies provide property lien records to public record keepers, on which they traditionally included full SSNs for identity verification purposes. However, both agencies have recently taken steps to better protect SSNs in these records. Currently, IRS mandates the use of a truncated version of SSNs on tax lien notices, which displays only the last four digits of the SSN. However, the agency does not mandate SSN truncation on all lien releases it issues. In addition, many of DOJ's districts have begun to truncate or fully remove SSNs on the lien records they provide to public record keepers. However, because DOJ's districts act independently to issue lien notices, some continue to display full SSNs in these records. Independent of IRS and DOJ efforts in this area, some states have begun to remove SSNs in all public records they maintain, though this approach can be costly and may not be fully effective at protecting SSNs.
- Both full and truncated SSNs in federally generated public records remain vulnerable to potential misuse, in part because different

truncation methods used by the public and private sectors may enable the reconstruction of full SSNs. While the display of truncated SSNs in federally generated public records is a step toward improved SSN protection, we previously reported that information resellers—companies that specialize in amassing personal information—sometimes provide truncated SSNs to customers that show the first five digits. Consequently, it is possible to reconstruct an individual's full nine-digit SSN by combining a truncated SSN from a federally generated lien record with a truncated SSN from an information reseller. In addition, while IRS and DOJ have recently taken actions to limit disclosure of full SSNs in records they generate going forward, full SSNs remain in the millions of lien records provided to public record keepers before the agencies implemented these changes. Increased access to these records through bulk sales to private companies and Internet access also creates the potential for identity theft. For example, public record keepers in some states have been selling complete copies of their records to private companies, such as title companies and information resellers, for many years. Because of this practice, current efforts to remove SSNs in records maintained by public record keepers do not apply to all copies of the record already made available. In addition, some public record keepers now provide potentially unlimited Web site access to personal identifying information in the records they maintain.

Conclusions

Federal agencies have taken actions to mitigate the availability of SSNs in public records by implementing the use of truncation for documents provided to state and local record keepers. While these actions provide some additional protection against using these records to perpetrate identity theft, our review demonstrates that identity thieves may still be able to reconstruct full SSNs by combining different truncated versions of the SSN available from public and private sources. Thus, truncation does not provide complete protection against identity theft. Yet despite this limitation, our analysis suggests that truncation provides better protection compared with records that display full SSNs. In this regard, as we noted in our May 2006 report, Congress may wish to further improve SSN protection by enacting truncation standards or assigning an agency to do so. In addition, Congress may wish to solicit input on promising truncation practices from the Commissioner of Social Security as part of this process. However, in the absence of such standards, federal agencies can still take steps to protect SSNs by further reducing their exposure in records they generate and provide to record keepers.

Recommendations for Executive Action

To the extent that truncation provides an added level of protection from identity theft, we are recommending that

- The Commissioner of IRS should implement a policy requiring the truncation of all SSNs in lien releases the agency generates.
- The Attorney General should implement a policy requiring, at a minimum, SSN truncation in all lien records generated by its judicial districts. Truncation should be in the same format as is currently used by IRS on lien notices.

Agency Comments

We provided a draft of this report to SSA, OMB, IRS, and DOJ for review and comment. SSA, IRS, and DOJ provided technical comments, which we incorporated as appropriate. We received written comments from OMB and IRS, which are reproduced in appendixes II and III. In its comments, OMB indicated its appreciation for the report's analysis of SSN use and vulnerability, in both full and truncated forms, and provided information on OMB's recent actions that require federal agencies to reduce the volume of sensitive information, including SSNs, they maintain.

Concerning our recommendations, SSA indicated that the agency fully supports our recommendations to IRS and DOJ because it believes that SSN truncation will greatly improve protection of the SSN. DOJ also agreed with our recommendation and subsequently issued a policy guidance memo that restricts all U.S. Attorneys' Offices from using full SSNs in any record submitted to state or local public record keepers. The memo requires offices to either remove the SSN entirely from these records or use a truncated version of the SSN, showing only the last four digits. While IRS generally agreed that the use of truncated SSNs on records submitted to state and local public record keepers provides an added level of protection against identity theft, the agency does not currently plan to implement our recommendation to truncate SSNs in all lien releases it generates, specifically those relating to pre-2006 lien notices. IRS indicated that truncating SSNs on lien releases for which the original lien notices show full SSNs may place a hardship on IRS's lien processing capabilities because it requires a change in how the agency's centralized Lien Processing Unit formats those lien releases. While we recognize that this change could potentially cause an administrative burden for IRS, we believe that the added level of protection against identity theft accomplished by truncating SSNs on lien releases outweighs these costs. IRS also indicated that truncating SSNs on lien releases for which the original lien notices show full SSNs may prove problematic for

record keepers. However, we do not believe that truncating SSNs on lien releases would prove problematic for most record keepers. Specifically, IRS includes key identifying information that corresponds to the original lien notice on most of the lien releases they submit to record keepers. Therefore, this identifying information can be used by record keepers to determine which lien notice corresponds to the newly submitted release, and IRS should not need to include a person's full SSN on the lien release for this purpose.

As we agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies of this report to relevant congressional committees, the Commissioner of SSA, the Director of OMB, the Commissioner of IRS, the Attorney General, and other interested parties and will make copies available to others upon request. In addition, this report will be available on GAO's Web site at <http://www.gao.gov>. If you or your staff have any questions about this report, please contact me at 202-512-7215 or bertoni@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report include Jeremy Cox (Assistant Director), Rachel Frisk (Analyst-in-Charge), and Ayeke Messam. In addition, Dan Schwimer provided legal assistance.



Daniel Bertoni
Director, Education, Workforce, and
Income Security Issues

Appendix I: Briefing Slides



**SOCIAL SECURITY NUMBERS:
Federal Actions Could Further Decrease
Availability in Public Records, though
Other Vulnerabilities Remain**

Briefing for Senator Charles Schumer
Chairman of the Subcommittee on Administrative
Oversight and the Courts
Committee on the Judiciary

May 10, 2007



Overview

- Key Objectives
- Scope and Methodology
- Summary of Results
- Background
- Findings
- Conclusions
- Recommendations for Executive Action

2



Key Objectives

We agreed to determine:

1. Which federal agencies commonly provide records containing Social Security numbers (SSN) to state and local public record keepers, and what actions have been taken to protect SSNs in these records?
2. What significant vulnerabilities, if any, remain to protecting SSNs in public records?

3



Scope and Methodology

To answer these questions, we:

- Gathered information from the Social Security Administration (SSA), Office of Management and Budget (OMB), Internal Revenue Service (IRS), and Department of Justice (DOJ);
- Interviewed public record keepers, their national associations, and stakeholder groups focused on privacy rights, open government, and the title insurance industry;
- Visited local record keepers' offices in the District of Columbia (D.C.), Maryland, and Virginia, reviewed several Web sites that provide information on public records access, and examined selected record keepers' Web sites nationwide; and,
- Interviewed record keepers in five Florida counties to discuss recently enacted state statutes related to public records access and the removal of certain personal-identifying information in those records.

4



Summary of Results

- IRS and DOJ commonly provide lien records containing SSNs to state and local public record keepers, and they have recently begun to truncate or remove SSNs in those records. While IRS mandates SSN truncation in all lien notices, it does not mandate truncation in all lien releases.¹ Because DOJ's districts act independently to issue lien notices, some truncate or remove SSNs in these records, while others continue to display full SSNs. Independent of these efforts, some states have begun to remove SSNs in all public records. However, this approach can be costly and may not fully protect SSNs.

¹ Lien notices are issued by government agencies to inform the public and creditors of a lien against a debtor's property. Lien releases are issued by agencies when a debt has been paid. 5



Summary of Results (continued)

- Both full and truncated SSNs in federally generated public records remain vulnerable to potential misuse, in part because different truncation methods used by the public and private sectors enable the reconstruction of full SSNs. In addition, the continued availability of SSNs in public records, as well as increased access to these records through bulk sales and Internet access, create the potential for identity theft.

6

Background 

SSNs: Use and Federal Regulation

- Although originally created to track workers' earnings and Social Security benefits, SSNs have become the identifier of choice for government agencies and private businesses and are currently used for myriad non-Social Security purposes.

7

Background 

SSNs: Use and Federal Regulation (continued)

- No single federal law regulates the overall use or restricts the disclosure of SSNs by governments. However, certain laws limit SSN use in specific circumstances.
 - For example, the Privacy Act of 1974 generally prohibits federal agencies from disclosing records containing SSNs without the consent of the individual whose records are being sought.
 - Exceptions authorized under the act include routine uses that are compatible with the purpose for which the SSN was collected, such as activities related to tax and debt collection.

8

Background

**SSNs: Use in Identity Theft**

- While the use of SSNs can be beneficial for identity verification and other purposes, SSNs are also a key piece of information used to create false identities for financial misuse or assume another individual's identity.
- Most often, identity thieves use SSNs belonging to real people. However, only 30 percent of identity theft victims know how thieves obtained their personal information.¹
- The Federal Trade Commission (FTC) estimated that over a 1-year period, nearly 10 million people discovered they were victims of identity theft, translating into estimated losses of billions of dollars.
- In response to this issue, the federal government and several state governments have passed identity theft legislation in recent years.

¹ This estimate is based on the FTC's identity theft victim complaint data. These data are self-reported and only represent crimes reported to FTC.

 GAO

Background

Public Records: Definition and Types

- Public records can generally be defined as records or documents that are routinely made available to the public by a government agency or the courts.
 - For example, local record keepers maintain public records that assist in the conduct of business, legal, or personal affairs.
- There are many types of public records, including birth, death, and marriage records; criminal and civil court case files; and records that concern property ownership, such as property liens.
 - Some documents in these records are created by government agencies, while others are submitted by private entities.
 - Some records contain personal identifying information, such as SSNs, dates of birth, credit card or bank account numbers, and children's names or mothers' maiden names.

10

Background 

Public Records: Storage and Access

- Record keepers store records in several formats, including paper copy, microfiche or microfilm, and electronic image.
- Traditionally, individuals accessed public records by visiting the government offices that maintained them, which provided practical limits on the volume of personal identifying information that could be disclosed.



The public, government agencies, attorneys, or businesses submit records to public record keepers

Public record keepers formally record submitted records

The public accesses records by visiting government locations where they are stored

Source: GAO analysis and Art Explosion (images)

11

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Records Containing SSNs to Record Keepers, and They Have Recently Begun to Truncate or Remove SSNs in Those Records

- IRS and DOJ commonly provide lien notices and releases containing SSNs to state and local public record keepers.
- IRS mandates SSN truncation in all lien notices but not all releases.
- DOJ's judicial districts act independently to truncate, remove, or include SSNs in lien notices.
- Some states are independently taking actions to remove SSNs from public records, but these approaches can be costly and may have a limited effect on protecting SSNs.

12

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Lien Notices and Releases Containing SSNs to State and Local Public Record Keepers

- We found that IRS and DOJ are the only federal agencies that commonly provide records containing SSNs to state and local public record keepers.
- Annually, IRS generates approximately 900,000 lien notices and releases for tax-related debts owed to the federal government.
 - IRS files lien notices and releases with state and local public record keepers through its centralized Lien Processing Unit.
- Annually, DOJ issues approximately 11,000 lien notices for criminal or civil court-related debts owed to the federal government.
 - DOJ lien notices are not generated through a centralized processing system. Instead, debt collection units for each judicial district file liens individually with the relevant public record keeper.¹

¹ While there are 94 districts, there are 93 debt collection units. These units also generate lien releases, but releases are typically provided directly to debtors rather than public record keepers.

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Lien Notices and Releases Containing SSNs to State and Local Public Record Keepers (continued)

- IRS- and DOJ-issued liens serve as federal government liens against property and are generally filed in the same manner.
- Neither federal statute nor regulations require that the SSN be included on notices or releases of liens. However, current federal law also does not prohibit SSNs from being included on these records. A lien record typically contains an SSN, name, address, and amount owed.
 - IRS and DOJ officials reported that SSNs traditionally have been included on lien records for identity verification purposes.

14

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Lien Notices and Releases Containing SSNs to State and Local Public Record Keepers (continued)

- While a significant number of federal lien records are generated annually, because they are distributed throughout the country, they do not always make up a significant portion of local record keepers' official records.¹
 - For example, the Palm Beach County, Florida, Clerk and Comptroller's Office reported that federally generated records account for only 3 percent of the county's official records.

¹ Official public records, or property records, generally include records related to property sale, ownership, or encumbrance, rather than vital records or court records unrelated to property. 15

Objective 1: Federal Provision of Records with SSNs



IRS Partially Mandates SSN Truncation, while DOJ's Districts Act Independently to Truncate or Remove SSNs in Lien Records

- In recent years, IRS and DOJ have taken steps to better protect SSNs in lien records they file with state and local public record keepers.
 - As of January 1, 2006, IRS mandates the use of a truncated version of the SSN on all tax lien notices. This truncated SSN displays only the last four digits of the nine-digit number.
 - Before implementing this change in policy, IRS conducted a survey of recording officials in 12 states who agreed that SSN truncation would be helpful in addressing privacy and identity theft concerns.
 - IRS stated that its SSN truncation policy still ensures identity verification with a high degree of certainty.

16

Objective 1: Federal Provision of Records with SSNs



IRS Partially Mandates SSN Truncation, while DOJ's Districts Act Independently to Truncate or Remove SSNs in Lien Records (continued)

- IRS's change in its SSN policy for lien notices does not apply to lien releases.
- Because the release is generated to match the original lien notice, lien releases sometimes still contain full SSNs.
 - For example, a lien release recorded in 2007 will show a full SSN if the corresponding lien notice was recorded before January 1, 2006.
 - However, lien releases recorded for notices generated after January 1, 2006, will contain truncated SSNs, like the corresponding notices.

17

Objective 1: Federal Provision of Records with SSNs



IRS Partially Mandates SSN Truncation, while DOJ's Districts Act Independently to Truncate or Remove SSNs in Lien Records (continued)

- Unlike IRS, DOJ has not issued a central policy regarding disclosure of SSNs in lien notices.
- Consequently, the 93 debt collection units for DOJ districts individually decide how to display SSNs in the lien notices they record with record keepers.
 - DOJ officials reported that 80 debt collection units currently include either a truncated SSN or no SSN in lien notices. Most include a truncated SSN showing the last four digits.¹
 - According to DOJ, the remaining 13 debt collection units currently include a full SSN on liens. However, several of these units told DOJ officials that they are considering removing SSNs on future liens.

¹ While DOJ could not confirm that all districts displaying truncated SSNs on lien notices show the last four digits, this is likely, due to similar changes in SSNs displayed in federal court records. 18

Objective 1: Federal Provision of Records with SSNs



Some States Are Taking Actions to Remove SSNs from Public Records, but These Approaches Can Be Costly and May Have Limited Effect

- Independent of IRS and DOJ actions, some states have recently considered removing SSNs in public records in order to better protect this information.
 - Florida and Nevada both passed legislation in 2005 requiring the removal of SSNs in public records. Record keepers have until January 1, 2008, to comply with the Florida law and January 1, 2017, to comply with the Nevada law.
 - Texas also passed legislation in 2005 that was interpreted by the Attorney General as prohibiting the disclosure of SSNs in public records. However, in response to that ruling, the Texas legislature enacted legislation that permits the disclosure of SSNs in public records and states that the SSN of a living person in Texas is not considered confidential in these records.

19

Objective 1: Federal Provision of Records with SSNs



Some States Are Taking Actions to Remove SSNs from Public Records, but These Approaches Can Be Costly and May Have Limited Effect (continued)

- Due to the 2008 deadline, public record keepers in Florida are currently taking actions to remove SSNs and several other personal identifiers from records. Officials in the five counties we spoke with are using a two-step process utilizing software that searches for and removes SSNs and a manual review of records by county or contractor staff.
- Florida record keepers reported that this approach is costly, with some funding provided by each county's trust fund for public records modernization.¹
 - For example, Palm Beach County, Florida's third largest county, paid over \$2 million to complete software and manual review and removal of SSNs and other personal identifiers in approximately 40 million pages of records.
- Due to software limitations and the potential for human error, this process may still not remove 100 percent of SSNs in these records.

¹ Recording fees have been accruing in county trust funds since Florida statute created these funds in 1987.

Objective 2: Remaining Vulnerabilities 

The Continued Availability of SSNs in Public Records, as well as Increased Access to These Records, Create the Potential for Identity Theft

- Both full and truncated SSNs can potentially be used to commit identity theft.
- Although IRS and DOJ have taken actions to better protect SSNs in the public records they commonly generate going forward, records they generated prior to these actions still contain SSNs.
- Some public record keepers provide potentially unlimited access to records and their content through bulk sales to private companies and online access.

21

Objective 2: Remaining Vulnerabilities

**Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft**

- Full nine-digit SSNs are key to the commission of identity theft.
 - For example, SSNs can be used as breeder information to create false identification documents, such as driver's licenses.
 - In addition, SSNs and other personal identifying information are used to fraudulently obtain credit cards, open utility accounts, commit bank fraud, file false tax returns, and falsely obtain employment and government benefits.
- Identity theft has been traced to personal identifying information accessed in public records.
 - For example, in recent years, criminals used personal identifying information contained in public records found on record keepers' Web sites in Hamilton County, Ohio, and Maricopa County, Arizona, to commit identity theft.
- However, the extent to which SSNs in public records have been used for this purpose is largely unknown.

22

Objective 2: Remaining Vulnerabilities 

Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft (continued)

- While the display of truncated SSNs—showing only the last four digits—in federally generated public records is a step toward improved SSN protection, this method of truncation does not fully protect SSNs because other sources may provide the first five digits of a person's SSN.
- In our prior work, we found that information resellers—private companies that specialize in amassing personal information—sometimes provide truncated SSNs showing the first five digits to customers with which they have accounts or to the public over the Internet.¹
 - For example, most customers of a prominent information reseller are able to access information containing truncated SSNs that show the first five digits.
 - Similarly, in our prior work on Internet-based information resellers, four resellers that gave our investigators truncated SSNs provided them in a form that showed the first five digits.

¹ See GAO-04-11 and GAO-06-495. 23

Objective 2: Remaining Vulnerabilities



Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft (continued)

The general public can purchase personal information, which may include truncated SSNs, from information resellers that provide services through the Internet.

General public

- Find a lost loved one
- Conduct your own investigation
- Screen your new tenant



Information report

Order information such as name, address, or SSN

Internet

Internet resellers

Public records

Publicly available information

Nonpublic information

Information report

Source: GAO analysis.

24

Objective 2: Remaining Vulnerabilities 

Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft (continued)

- Consequently, by combining a person's truncated SSN on an IRS- or DOJ-generated lien notice with that same person's truncated SSN obtained from an information reseller, it may be possible to determine an individual's full nine-digit SSN.
 - We tested this method and found that it can potentially be used by identity thieves to reconstruct full SSNs.

25

Objective 2: Remaining Vulnerabilities 

Although Federal Agencies Have Taken Actions to Better Protect SSNs in Records, Some Still Contain SSNs

- IRS and DOJ actions will generally limit disclosure of full nine-digit SSNs in records they generate going forward, but full SSNs remain in the millions of records these agencies provided to public record keepers before they began truncating and removing SSNs.
 - For example, in the 10 years prior to IRS enacting its policy requiring truncated SSNs on lien notices, IRS generated almost 9 million lien records containing full SSNs,¹ all of which currently remain in the public record.
- Once a record is officially recorded, the public record keeper is responsible for maintaining it in perpetuity. Therefore, although an IRS tax lien expires after 10 years, the lien notice remains in the public record even after expiration.

¹ The 9 million lien records include lien notices and releases. 26

Objective 2: Remaining Vulnerabilities

Some Record Keepers Provide Potentially Unlimited Access to Records and Their Content through Sales to Private Companies and Online Access

Public records were traditionally accessed by visiting government record centers. However, some record keepers currently sell records in bulk to private companies, and some provide access to records on their own government Web sites.

The public, government agencies, attorneys, or businesses submit records to public record keepers

Public record keepers formally record submitted records

The public may be able to access records:

- By visiting government locations where records are stored
- Through private businesses that have purchased records in bulk from record keepers
- By accessing public record keepers' Web sites

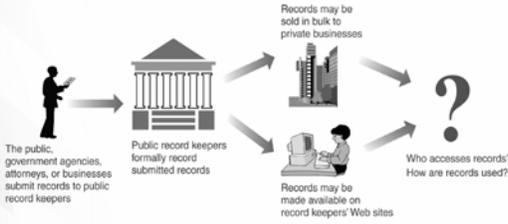
Source: GAO analysis and Art Explosion (images)

27

Objective 2: Remaining Vulnerabilities 

Some Record Keepers Provide Potentially Unlimited Access to Records and Their Content through Sales to Private Companies and Online Access (continued)

When records are sold in bulk or made available on the Internet, it is unknown how and by whom the records, and the personal identifying information contained in them, are used.



```
graph LR; A[The public, government agencies, attorneys, or businesses submit records to public record keepers] --> B[Public record keepers formally record submitted records]; B --> C[Records may be sold in bulk to private businesses]; B --> D[Records may be made available on record keepers' Web sites]; C --> E[? Who accesses records? How are records used?]; D --> E;
```

Source: GAO analysis and Art Explosion (images).

28

Objective 2: Remaining Vulnerabilities

**The Extent of Bulk Record Sales to Private Companies, as well as How Companies Use and Provide Access to Records, Are Unknown**

- Record keepers and others report that private businesses have been purchasing public records in bulk for years.¹ However, the extent of this practice and the ways in which private businesses use and provide access to these records are largely unknown.
 - For example, while title insurance companies may primarily use copies of property records to conduct related business, information resellers may use records for a variety of purposes. These purposes may include the provision of records that contain SSNs to customers and the general public.
 - In addition, the extent to which businesses provide access to these records, and their content, is unknown. Because some businesses use companies located outside of the United States for data entry and other purposes, records and the personal identifying information they contain may be accessible overseas. In these instances, it is unclear whether U.S. law would protect SSNs from potential misuse.

¹ This practice varies by state and locality. For example, some states require record keepers to sell records in bulk and only charge to recover the costs associated with record reproduction.

Objective 2: Remaining Vulnerabilities

**Online Access to Records Is Increasing, and May Result in Potentially Unlimited Access to Records and Their Content**

- Many record keepers and representatives of stakeholder groups we interviewed indicated that public records have become more available on the Internet in recent years.
- Across the country, record keepers provide different types of access to public records on their Web sites.
 - Some provide free access to a records index that includes information such as record type, person associated with the record, and recording date.
 - Others provide either free or paid access to both a records index and electronic record images. An electronic record image is typically a complete copy of the record and its contents.
- One organization that publishes public records information estimated that from 2004 to 2006, the proportion of all record keepers providing Internet access to a records index or electronic record images increased from 40 to 57 percent.¹

¹ This organization conducts research nationwide on entities that maintain public records and access to records. This estimate does not include public record keepers that maintain court records.³⁰

Objective 2: Remaining Vulnerabilities

**Online Access to Records Is Increasing, and May Result in Potentially Unlimited Access to Records and Their Content (continued)**

- Online access to electronic record images provides potentially unlimited access to the content of records, including SSNs and other personal identifying information, unless this information has been removed by the record keeper.
 - In our own review of record keepers' Web sites across the country, we found that at least 1 record keeper in 40 of the 50 states and D.C. (78 percent) provided free or paid online access to electronic record images.¹

¹ We reviewed the Web sites of state and local record keepers that maintain property records. Therefore, this figure does not include record keepers that maintain court or other public records. 31



Conclusions

- Federal agencies have taken actions to mitigate the availability of SSNs in public records by implementing the use of truncation for documents provided to state and local record keepers.
- While these actions provide some additional protection against using these records to perpetrate identity theft, our review demonstrates that identity thieves may still be able to reconstruct full SSNs by combining different truncated versions of the SSN available from public and private sources.
- Thus, truncation does not provide complete protection against identity theft.

32



Conclusions (continued)

- Yet despite this limitation, our analysis suggests that truncation provides better protection compared with records that display full SSNs.
- In this regard, as we noted in our May 2006 report, Congress may wish to further improve SSN protection by enacting truncation standards or assigning an agency to do so.¹ In addition, Congress may wish to solicit input on promising truncation practices from the Commissioner of Social Security as part of this process.
- However, in the absence of such standards, federal agencies can still take steps to protect SSNs by further reducing their exposure in records they generate and provide to record keepers.

¹ See GAO-06-495. 33

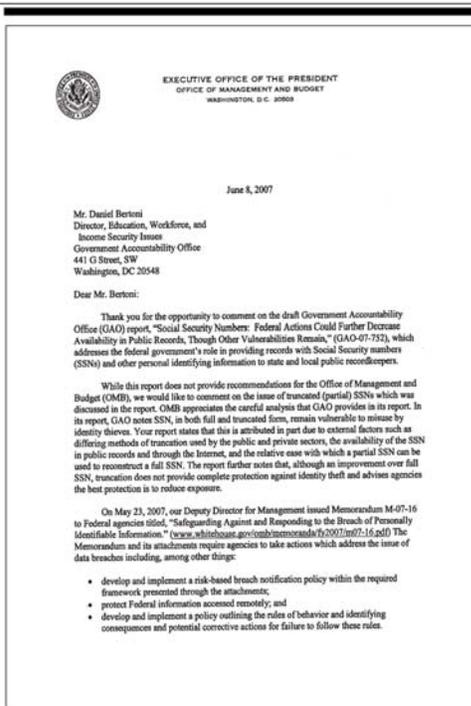


Recommendations for Executive Action

- To the extent that truncation provides an added level of protection from identity theft, we are recommending that
 - The Commissioner of IRS should implement a policy requiring the truncation of all SSNs in lien releases the agency generates.
 - The Attorney General should implement a policy requiring, at a minimum, SSN truncation in all lien records generated by its judicial districts. Truncation should be in the same format as is currently used by IRS on lien notices.

34

Appendix II: Comments from the Office of Management and Budget



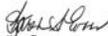
Appendix II: Comments from the Office of
Management and Budget

Additionally, this Memorandum requires agencies to reduce the volume of sensitive information maintained by agencies, including SSNs, to the minimum necessary. OMB further recognizes the path forward is for the Federal government to reduce its reliance on use of SSN. In this light, the Memorandum requires agencies to participate in government-wide efforts to explore alternatives to the use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.). The Memorandum goes a step further to require agencies to establish a plan within 120 days to eliminate unnecessary use of SSNs and implement the plan within 18 months.

The Memorandum does not distinguish between full and truncated SSNs. OMB has been providing informal advice to the agencies that the policy applies to both the full and truncated SSN. Specifically, agencies are required to safeguard SSN in any form with equal diligence. We will be providing more formal guidance to the agencies on this issue.

Thank you for the opportunity to review and comment on the draft report on this important issue.

Sincerely,



Karen Evans
Administrator
Office of E-Government and
Information Technology
Office of Management and Budget

Appendix III: Comments from the Internal Revenue Service



Appendix III: Comments from the Internal Revenue Service

Enclosure

Recommendation:

To the extent that truncation provides an added level of protection from identity theft, we are recommending that the Commissioner of IRS should implement a policy requiring the truncation of all SSNs in lien releases the agency generates.

Response:

The IRS agrees that truncating SSNs on documents filed with public record keepers adds a level of protection against identity theft. A multi-functional IRS task group contacted state and local recording officials, financial institutions, title and mortgage companies and credit reporting agencies, as well as attorneys and practitioners, and gathered data regarding truncation of SSNs. The group identified the most used truncation method as redaction of the first 5 digits of the SSN (i.e. xxx-xx-1234), the same method used by most recording officials and financial institutions. However, the data shows that truncating SSNs on lien releases, when original liens show full SSNs, may prove problematic for recording offices and may place an extreme hardship on lien processing capabilities. Based on the assembled data, IRS implemented changes to its automated lien system and provided guidance for manually prepared lien documents.

Effective January 1, 2006, in an effort to prevent identity theft and in recognition of the growing number of states requiring truncation, we began truncating SSNs on NFTLs. We will also truncate SSNs on lien documents that impact these filings (generated after 1/1/2006), such as certificates of release, withdrawal, and revocation.

Related GAO Products

Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs. GAO-06-495. Washington, D.C.: May 17, 2006.

Social Security Numbers: More Could be Done to Protect SSNs. GAO-06-586T. Washington, D.C.: March 30, 2006.

Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain. GAO-05-1016T. Washington, D.C.: September 15, 2005.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary in Private and Public Sectors. GAO-04-1099T. Washington, D.C.: September 28, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary. GAO-04-768T. Washington, D.C.: June 15, 2004.

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.

Social Security Numbers: Ensuring the Integrity of the SSN. GAO-03-941T. Washington, D.C.: July 10, 2003.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected. GAO-02-691T. Washington, D.C.: April 29, 2002.

GAO's Mission	The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."
Order by Mail or Phone	<p>The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:</p> <p>U.S. Government Accountability Office 441 G Street NW, Room LM Washington, D.C. 20548</p> <p>To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061</p>
To Report Fraud, Waste, and Abuse in Federal Programs	<p>Contact:</p> <p>Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470</p>
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548

Mr. LEVIN. Welcome.

Senator SCHUMER. Glad to be here, Sandy.

Mr. LEVIN. Both of you and everybody else. Just quickly, and I will ask the same of Ed Markey, what is the source of the hesitation or the resistance?

Senator SCHUMER. The only resistance, it is a good question, was from the local officials who said, "Look, we have an obligation to put it online, you do something about it." So, the fact that we are both mandating that in the future they treat things one way, that is not too hard for them to do. There is software that does that easily. For past records that are on display, which of course an identity thief anywhere in the world could go back to, we help give them some funding to cover those up because that is a little harder. You have got to go back in the records and re-enter them. I think now most of the opposition is gone.

Mr. LEVIN. By the way, I am not sure, as I look around, if everybody is old enough to remember Abbott and Costello.

Your reference to them—they are going into different doors.

Senator SCHUMER. Right.

Mr. LEVIN. But it sounds very much like these actions would be attributed to Abbott and Costello.

Senator SCHUMER. I find with my staff, and I am blessed, I have a great, great staff, but most of them are half of my age and I mention all these cultural things, and they look at me like I am from another planet. Now, I know how it feels, how my parents felt when we mentioned things like the Beatles or Elvis Presley or something like that.

Mr. LEVIN. Thank you.

Chairman MCNULTY. Well, I think most of them have seen the clips of “Who’s on first.”

[Laughter.]

Chairman MCNULTY. If there are no further questions, I want to thank the senior Senator from New York.

Senator SCHUMER. I thank you, Mr. Chairman, and all my colleagues. It is great to finally make it to the Committee on Ways and Means after all these years.

[Laughter.]

Chairman MCNULTY. Your staff has that editorial, Chuck.

Senator SCHUMER. Great, thanks.

Chairman MCNULTY. We would now like to go to our colleague from Massachusetts from Malden, Massachusetts, 7th District, the Honorable Ed Markey, who has been a real leader on this issue for a number of years.

**STATEMENT OF HON. ED MARKEY, A REPRESENTATIVE IN
CONGRESS FROM THE STATE OF MASSACHUSETTS**

Mr. MARKEY. Thank you, Mr. Chairman, very much and thank Mr. Johnson, and I thank each of you for inviting me here today. This is a very important issue. Mr. Barton of Texas and I have introduced legislation, the Social Security number Protection Act, in order to bring a halt to unregulated commerce in Social Security numbers. It does not establish an absolute prohibition on all commercial use of the number but it would make it a crime for a person to sell or purchase Social Security numbers in violation of rules promulgated the Federal Trade Commission. The Federal Trade Commission would be given the power to restrict the sale of Social Security numbers, determine appropriate exemptions, and to enforce civil compliance with the bill’s restrictions.

Why is this legislation necessary? Let me share with you just one story. Several years ago, a man named Liam Youens was stalking a 21-year-old New Hampshire named Amy Boyer. Youens reportedly purchased Amy Boyer’s Social Security number from an Internet Web site for \$45. Using this information, he was able to track her down, a process that he chillingly detailed on an Internet Web site that he named after his target. Finally, this demented stalker fatally shot Amy Boyer in front of the dental office where she worked. Afterward, he turned the gun on himself.

The terrible tragedy of Amy Boyer’s murder underscores the fact that while the Social Security number was originally intended to

be used only for the purposes of collecting Social Security taxes and administering the program's benefit, it has over the years evolved into a ubiquitous national personal identification number, which is subject to misuse and abuse. The unregulated sale and purchase of these numbers is a significant factor in a growing range of illegal activities, including fraud, identity theft, stalkings and tragically even murders. If you do the simple Internet search in which you enter the words "Social Security numbers," you will turn up links to dozens of Web sites that offer to provide you for a fee Social Security numbers for other citizens or to link up a Social Security number that you might have with a name, address and telephone number.

Where are the data mining firms and private detection agencies obtaining these numbers? In all likelihood, they are accessing information from the databases of credit bureaus, financial service companies, data brokers or other commercial firms. Unfortunately, this has become a business. The privacy of all Americans has become a business. It becomes valuable information, all of these secrets about American families. While there is a purpose to which all of that information can be placed, it just should not be a commodity that can be used by anyone that feels that if they can combine enough of it, it becomes a product valuable to someone who wishes to purchase it.

If someone actually obtains a Social Security number from one of these sites, they have a critically important piece of information that can be used to locate the individual, get access to information about the individual's personal finances or engage in a variety of illegal activities. By bringing to a halt, unregulated commerce in Social Security numbers, this bill, and what you are doing, Mr. Chairman, will help to reduce the incidence of pretext in crimes, identity thefts, and other frauds or crimes involving misuse of a person's Social Security number. We need to take action now if we are going to fully protect the public's right to privacy by preventing the sale of Social Security numbers.

Under the legislation which Mr. Barton and I have introduced, the Federal Trade Commission would be given rulemaking authority to restrict the sale of Social Security numbers, determine appropriate exemptions and to enforce civil compliance with the bill's restrictions. On May 10th of this year, that legislation passed through the Energy and Commerce Committee. This, of course, is the other key Committee in terms of dealing with this issue, and you have to take action in a way that reflects your expertise on the whole issue of Social Security since that subject is here in the Committee on Ways and Means. But together we should find a way of affording real protection to American families on this legislation. Taking action now can help us to prevent further Amy Boyer's from being victimized.

But even at a lower level, this whole idea that all of our information is now out there for anyone to be able to crack is wrong. These data miners have no regard for the personal privacy of us as a society. We are reaching a point now, to be honest with you, where some kid today who is googling some sites right now, unless we figure out a way of ensuring that that information is destroyed, 15 or 18 years from now, some employer will be saying, "Let's go back

and find out what that kid was googling to get some insight into who they are.” So all of this is becoming increasingly an important part of our society, to determine what kind of privacy we want to provide to American families. You are providing the leadership, Mr. Chairman, I thank you for that.

[The prepared statement of Mr. Markey follows:]

**Prepared Statement of the Honorable Ed Markey
a Representative in Congress from the State of Massachusetts**

Mr. Chairman, thank you for inviting me to testify at today’s hearing.

The Gentleman from Texas (Mr. Barton), and I have introduced H.R. 948, the “Social Security Number Protection Act,” in order to bring a halt to unregulated commerce in Social Security numbers. It does not establish an absolute prohibition on all commercial use of the number, but it would make it crime for a person to sell or purchase Social Security numbers in violation of rules promulgated by the FTC. The FTC would be given the power to restrict the sale of Social Security numbers, determine appropriate exemptions, and to enforce civil compliance with the bill’s restrictions.

Why is this legislation necessary? Let me share with you just one story. About six years ago, a man named Liam Youens was stalking a 21-year old New Hampshire woman named Amy Boyer. Youens reportedly purchased Amy Boyer’s Social Security number from an Internet Web site for \$45. Using this information, he was able to track her down, a process that he chillingly detailed on an Internet Web site that he named after his target. Finally, this demented stalker fatally shot Amy Boyer in front of the dental office where she worked. Afterwards, he turned the gun on himself.

The terrible tragedy of Amy Boyer’s murder underscores the fact that while the Social Security number was originally intended to be used only for the purposes of collecting Social Security taxes and administering the program’s benefits, it has over the years evolved into a ubiquitous national personal identification number which is subject to misuse and abuse. The unregulated sale and purchase of these numbers is a significant factor in a growing range of illegal activities, including fraud, identity theft, stalkings and tragically, even murders.

If you do a simple Internet search in which you enter the words “Social Security numbers,” you will turn up links to dozens of web sites that offer to provide you, for a fee, Social Security numbers for other citizens, or to link up a Social Security number that you might have with a name, address and telephone number. Where are the data-mining firms and private detective agencies that offer these services obtaining these numbers? In all likelihood, they are accessing information from the databases of credit bureaus, financial services companies, data brokers, or other commercial firms.

If someone actually obtains a Social Security number from one of these sites, they have a critically important piece of information that can be used to locate the individual, get access to information about the individual’s personal finances, or engage in a variety of illegal activities. By bringing a halt to unregulated commerce in Social Security numbers, my amendment will help reduce the incidence of pretexting crimes, identity thefts and other frauds or crimes involving misuse of a person’s Social Security number.

We need to take this action now if we are going to fully protect the public’s right to privacy by preventing sales of Social Security numbers. Under the Markey-Barton bill, the FTC would be given rulemaking authority to restrict the sale of Social Security numbers, determine appropriate exemptions, and to enforce civil compliance with the bill’s restrictions. As you know, on May 10th of this year, the Energy and Commerce Committee approved this legislation. The Speaker has now referred the bill to the Ways and Means Committee until July 20th, for consideration of such provisions that may fall within the Committee’s jurisdiction. I would strongly urge the Committee to approve this bill, so that this Congress can put in place stronger protections to restrict the purchase and sale of Social Security numbers. Taking action now will help us prevent a recurrence of tragedies like the Amy Boyer case, as well as the much more frequent incidences of misuse of the Social Security number to perpetrate identity thefts.

I look forward to working with you, Mr. Chairman, and with the Chairman of the full Committee, Mr. Rangel, and Ranking Members McCrery and Johnson as the Committee moves forward to consider this important legislation.

Chairman MCNULTY. Thank you, Mr. Markey. I want to thank you for your passionate activism on this issue for a long period of time. The part of your testimony I agree with the most is the time for talk should be over, and we should actually do something. I am in the process of putting together a proposal, which I am going to share with Mr. Johnson, hopefully get bipartisan support on this Committee, and then what I would like to do, Mr. Markey, is to talk to you and the gentleman from Ennis, Texas, Mr. Barton, and try to meld our proposals and get a united front and actually do something.

Does anyone wish to inquire of Mr. Markey? Yes, Ms. Schwartz?

Ms. SCHWARTZ. Thank you. Good morning. Just a question, you leave the question of exemptions or possible appropriate use in your legislation rather open, basically to be set later. I understand that is a little bit of a difference between your legislation and Senator Schumer's, is that correct? So, just to inquire about whether you think there are any appropriate uses that we ought to articulate in legislation and are you open to that?

Mr. MARKEY. Yes, well, what Senator Schumer I think was referring to is the fact that, for example, in the financial services industry, we have to find a way where they can use some of these identifiers so you can use the first five or the last four or some combination and so that there is some use that it can be placed but it doesn't unlock the whole key to who the individual is. We are actually working together on that for the financial services industry and others but only that a part of it is available, that the entire number is not made available unnecessarily because it is not necessary in order to provide an identification. All of us when we go down, and we punch in our little code when we are trying to take money out of the ATM machine, we only need four numbers, we do not need a nine number code. So, there is a way of doing it that can still protect the number.

Ms. SCHWARTZ. Okay, and I think this question has somewhat been asked, I am somewhat new to this Committee but I understand there have been quite a few hearings on this and it feels like this is an issue that has been around, and we just have not taken action on. As you move forward as we do, as the Chairman does, it certainly seems that it is time for us to do something about it, to reach some understanding and agreement about this and provide some of this protection. All of us are asked for Social Security numbers all the time. We had an interesting hearing actually, the full Committee, just about people being appropriately afraid to share their Social Security number because of such failure to protect it once you give it out. So, I look forward to working with you and, of course, working with the Senate as well to actually move this along. Thank you.

Chairman MCNULTY. Does anyone else wish to inquire? Mr. Markey, thank you very much for your testimony. We look forward to working with you on actually enacting some legislation.

Mr. MARKEY. Thank you, Mr. Chairman, and I thank all of you very much.

Chairman MCNULTY. We will now go to panel number two. Mr. Barton is on his way. When he gets here, because he is in another markup, we will accommodate him as well. Panel number two con-

sists of The Honorable Patrick O'Carroll, inspector general of the Social Security Administration; Joel Winston, associate director, the Division of Privacy and Information Protection of the Federal Trade Commission; and Dan Bertoni, the director of Education, Work force, and Income Security of the GAO.

I want to thank all of you for being here today. Your entire testimony will appear in the record. We ask you to summarize it in about 5 minutes so that we can have some time for some questions by the panel Members. If you could just keep your eye on the little indicator there, when the green light goes off and the amber light goes on, it is time to kind of wrap up. When the red light goes on, we would appreciate if you would try to conclude so we can get some questions in and also have time to get to the third panel.

We will start with the inspector general.

**STATEMENT OF HON. PATRICK O'CARROLL, INSPECTOR
GENERAL, SOCIAL SECURITY ADMINISTRATION**

Mr. O'CARROLL. Good morning, Chairman McNulty. Good morning, Mr. Johnson and Members of the Subcommittee. I want to thank you for your interest in protecting the Social Security number and for your interest in the work of the Office of the Inspector General. It is a pleasure to be here today to discuss this issue, which is at the heart of my office's mission: protecting the Social Security number. I suggest that in order to do so the time has come to strike an appropriate balance between convenience and security. You have my comprehensive written statement, and now I want to discuss some of its highlights.

Over the past decade, we have worked in partnership with the Social Security Administration and with this Subcommittee to bring about improvements in the process by which SSA issues Social Security numbers, new SSN cards and replacement cards. However, we believe the greatest vulnerability is the theft of the number. I assure you that it is harder than ever to obtain a SSN or a Social Security card based on fraudulent information or false pretense. Unfortunately, we cannot report the same degree of progress in protecting the SSN once it legitimately leaves SSA. Our audit and investigative work has taught us that the more SSNs are used unnecessarily, the higher the probability that they might become improperly disclosed and then used to commit crimes. We have highlight vulnerabilities and have suggested ways SSA can try to persuade organizations to limit their use of the number and better protect sensitive data.

However, legislation may be required to compel these organizations to forego the convenience the SSN represents. One of our most expansive reviews involved Federal agencies' controls over the access and use of SSNs by external entities. Recently, 15 Federal offices of inspectors general joined us with this review. We provided a comprehensive report with recommendations to improve the security the SSN at the Federal Government level. While we believe our work brought about improvements, recent OMB guidance makes it clear that the use of the SSN in Federal agencies will have to be further curtailed and security measures further improved.

Of course, the Federal Government is not the only repository of SSN information. Schools, hospitals, businesses and state and local governments request SSNs for a variety of purposes, very few of which are actually required by law. Many of these entities use the SSN simply as a matter of convenience and do not provide adequate controls to protect the data. For example, our auditors have studied by universities' and hospitals' use of the SSN. While these institutions may have a legitimate use for the number with respect to certain functions, we found that once collected, the number was used for other purposes and was not always given the level of protection it deserves.

In response to our audits, SSA's outreach efforts and their own experiences with data loss, many universities are now moving away from the SSN as a student identifier. In an audit currently underway, we are disturbed to learn though that 43 states still collect Social Security numbers for students in kindergarten through 12th grade despite the fact that only three of these states have laws that require it. Some of these schools and school districts still print the student's SSN on their attendance rosters, making it clear that they are placing convenience ahead of security. It may be the time for legislation barring the use of the SSN for all those but uses required by law.

Our Social Security Number Integrity Protection Team encouraged banning the display of SSNs on driver's licenses, and this is one example of legislation enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004 that we believe has made a significant difference in SSN integrity. We frequently remind people do not carry your Social Security card in your wallet, so having the SSN on their driver's license undermine these efforts. In the same vein, consider the wisdom of SSNs displayed on the Medicare card or other forms of identification. So, the IRTPA provided a degree of assistance but more is needed.

H.R. 745, introduced in the last Congress, and Senate bill 238, which was just discussed in the current Congress, each seek to address the display of SSNs and the sale of SSNs by information brokers, practices not currently prohibited by law. H.R. 948 would also prohibit the sale of SSNs under many circumstances, which would help reduce the largely unfettered trafficking in SSNs that are being done by information brokers.

Legislative action to limit the sale and display of SSNs is critical to the security of the SSN, and I applaud these efforts just as I applaud the Subcommittee's commitment to improving the integrity of the SSN protection for all. In summary, far from its original intent, the SSN has become a convenient tracking number, whose proliferation has significantly detrimental consequences. We cannot allow the public security to be jeopardized over a matter of convenience.

Thank you.

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

**Prepared Statement of the Honorable Patrick O'Carroll,
Inspector General, Social Security Administration**

Good morning, Chairman McNulty, Mr. Johnson, and members of the Subcommittee. Thank you for the invitation to be here today to discuss the Social Security number (SSN) and how we can better protect it and the American people.

The Office of the Inspector General (OIG) at the Social Security Administration (SSA) came into being in 1995, with the implementation of the *Social Security Independence and Program Improvements Act of 1994*. As a new entity charged with preventing and detecting fraud, waste, and abuse in SSA's programs and operations, we were well aware of the central role that the SSN played in American society, and the critical need for us to protect its integrity. With SSA, we have made significant strides towards that end since our early days. However, we are keenly aware that much more needs to be done. Today, I will provide you a brief history of our audit and investigative efforts, which have played an important role in strengthening SSN integrity—especially in the way these important numbers are assigned. But, more importantly, I will provide you with perspective on areas in which action is still needed—perhaps through additional legislation—to better protect SSNs from unnecessary collection and improper disclosure. I believe the American people expect and deserve our attention to address this vital matter.

Well before 9/11, and even before identity theft became as significant an issue as it is today, we knew we had much work to do to strengthen SSN integrity. We were especially aware of the broad uses of SSNs throughout U.S. society and their importance to noncitizens while they are in the U.S. We also recognized that SSNs are the cornerstone of SSA's programs and, therefore, before we could turn too much of our attention outward—to the use and misuse of SSNs—we first needed to make sure that everything was in order within SSA. As a result, much of our early SSN work was in the area of enumeration—the process by which SSA assigns SSNs. If SSA's enumeration processes were not sound, no amount of improvement to the use and security of the SSN after it was issued would be of much value.

Since 1999, when we issued a Management Advisory Report emphasizing the importance of proper SSN assignment and use, we have worked closely with SSA to improve controls in the enumeration process. Based on our recommendations, collaborative efforts and new legislative requirements, SSA has improved the enumeration at birth and enumeration at entry programs, heightened the awareness of SSA employees to fraudulent identification documents presented with applications for SSNs, tightened controls over the issuance of replacement Social Security cards, and otherwise made it much more difficult to obtain a valid SSN through the use of a fraudulent application.

During this period, my predecessors testified before this Subcommittee and other Committees and Subcommittees of both houses of Congress on SSN-related issues many times, presenting the results of our work, responding to requests from Members, proposing legislation, and seeking ways to further improve SSN integrity.

The September 11 attacks underscored the need to continue those efforts, but with respect to SSNs, did not teach us anything we did not already know about the critical role of the SSN in our society. In the months following 9/11, we worked with the FBI and other law enforcement agencies to provide critical information, and began a series of SSN-based Homeland Security initiatives. These projects sought to ensure, through review of SSNs and other information, that individuals with access to critical infrastructure sites such as airports, seaports, nuclear power plants, and similar locations, were who they claimed to be, and not imposters who would do us harm.

Even while working on Homeland Security matters, our investigators continued their day-to-day work on individual SSN misuse cases, bringing to justice scam artists, identity thieves, counterfeit document artists, and other criminals whose tool of the trade was the purloined SSN. On an annual basis, we receive about 10,000 allegations of SSN misuse a year, and investigate approximately 1,500 criminal cases of misuse. After years of increases, these numbers have now held steady for several years, indicating that not only our investigative work, but also our audit work, is having a significant impact.

Having completed numerous audits that helped SSA strengthen its enumeration processes, in more recent years our auditors have begun to address the far more challenging issue of SSN misuse. While SSA can implement controls to prevent the improper assignment of SSNs, it has very few mechanisms to curb the improper—or simply the unnecessary—use of an SSN. Our audit and investigative experiences have taught us that the more SSNs are used unnecessarily, the higher the probability that these numbers could be improperly disclosed and used to commit crimes throughout society. We read about these occurrences in the newspaper every day, but we've yet to develop meaningful ways to stem the tide.

As I'll discuss in a moment, our recent audit work has highlighted vulnerabilities and suggested some ways in which SSA can try to persuade organizations that use SSNs to limit this use and better protect this sensitive information. To some extent, these efforts, along with the users' own experiences with improper disclosures, have convinced some organizations to do as we and SSA have suggested. However, be-

cause it is such a convenient and unique number, and change may be costly, others appear to discount the risk and continue on with business as usual. To convince these parties, we believe SSA needs more help. Specifically, we believe the time has come to consider legislation limiting the collection and use of SSNs to those purposes mandated by Federal law, or otherwise reducing the use of SSNs as convenient identifiers.

In 2002, the Federal inspector general community joined with us to look more closely at one high-risk issue regarding SSNs: agencies' controls over access, disclosure, and use of SSNs by external entities, such as contractors, within their respective agencies. A total of 15 Offices of Inspector General participated in this effort, each conducting an audit within their respective Agencies. We combined our results and provided a comprehensive report, which included recommendations to improve the security of the SSN at the Federal Government level. While we believe that our work, and the work of our fellow inspectors general, brought about improvements in SSN security and heightened awareness of the issue, there is more to be done. Recent OMB guidance makes it clear that at least at the Federal level, uses of the SSN must be curtailed, and security measures enhanced. We will continue to monitor the Federal sector's progress in accomplishing this mandate.

Of course, the Federal Government is not the only source of SSN information. As I'm sure you're aware, schools, businesses, and State and local governments request SSNs for a multitude of purposes—very few of which are required by law. Rather, many of these organizations use the SSN as an identifier simply because it is convenient. For example, our auditors have looked at the use of SSNs by universities and hospitals as student and patient identifiers, respectively. While both of these types of organizations may have had some reason for collecting SSNs, such as financial aid or Medicare coverage, we found that once collected, the number was used too frequently for other purposes and not always given the level of protection necessary.

In response to our audits, SSA outreach, and their own experiences with data exposures, many universities are moving away from using SSNs as student identifiers. However, in an audit currently underway, we were disturbed to learn that 43 States collect the SSNs of students in kindergarten through 12th (K–12) grade. In only three of these States is the collection of these numbers required by law. The *No Child Left Behind Act of 2001* requires that each State implement an accountability program that measures the progress of students and schools through the collection and analysis of data. However, the law does not require that States use SSNs to identify and track students. Rather, we believe that some K–12 schools use SSNs as a matter of convenience. **For example, while we did not perform a statistical sample, we know of some schools and districts that still print the students' SSNs on attendance rosters. We would suggest that the security of individuals' personal information—in this instance, the personal information of children—not take a back seat to administrative convenience. For the 2004/2005 school year, the National Education Association estimated that there were more than 48 million K–12 students in over 15,000 school districts across the country. We believe that the collection and use of SSNs without proper controls is a huge vulnerability for this young population. Recent data indicate the number of children under age 18 whose identities have been stolen is growing. This is particularly troubling given that some of these individuals may not become aware of such activity until they apply for a credit card or student loan.**

We also found that State and local governments use the SSN as an identifier for other programs, such as prescription drug monitoring, when other identifiers such as drivers license numbers might be more appropriate. Additionally, these entities don't always provide sufficient protection of this data.

We even conducted an audit that looked at the access prisoners are sometimes given to SSNs while doing work in prison on State records or other documents containing SSNs and other personal information. The possibility of giving a convicted identity thief access to the tools of his or her trade *while in prison* is certainly alarming.

I'm proud of the work that has been done, and continues to be done, by both our Office of Audit and our Office of Investigations, but our focus on SSN integrity does not stop there. Several years ago, in order to keep track of our many-faceted effort to protect the SSN, we formed the Social Security Number Integrity Protection Team, or SSNIPT. That group, comprised of attorneys, auditors, and investigators, has had its own quiet—but important—successes. It was in part the efforts of the SSNIPT team that led to the eradication of the display of SSNs on Selective Service mailings and the Thrift Savings Plan website—two practices in which the Federal Government was itself putting the SSN at risk. The team has also worked to pro-

pose legislation, which was ultimately enacted as part of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), to eliminate the practice of displaying SSNs on drivers licenses. All of our exhortations over the years aimed at getting Americans to stop carrying their Social Security cards in their wallets would be of little value if the one document they were required to carry also displayed their SSN.

The OIG will not waver in our commitment to protect the integrity of the Social Security number through our timely audit, investigative, and other work, and we welcome Congress' help. Legislation has been, and will always be, a key factor in our ability to protect the SSN and protect the American people. Legislation has, to some degree, improved enforcement mechanisms in this area (the *Identity Theft Penalty Enhancement Act*), but legislation that would limit the display of SSNs on public documents or eliminate the sale of SSNs by information brokers has not yet been passed, with the exception of the IRTPA provision concerning drivers' licenses. Similarly, no law has been passed to address the unnecessary collection of SSNs by schools, hospitals, or other entities that use this number as a matter of convenience but fail to adequately protect this personal information.

There are, however, a number of bills that have been introduced. In the last Congress, H.R. 1745, as well as the current Congress' S. 238, each seek to address both the display and the sale of SSNs, and H.R. 948, while silent on the display of SSNs, would also prohibit their sale under many circumstances. Any legislative provisions that reduce the display of SSNs or limit or eliminate trafficking in SSNs by information brokers and others would be of great help to our efforts.

It is important, however, not only to stop intentional criminal behavior, but to place an onus on those who use the SSN—either because they are required to do so by law, or because the SSN is a convenient identifier—to protect the information they are holding.

Consider an investigation we recently concluded in which several people were convicted of SSN misuse on a large scale. The primary subject of the investigation was a manufacturer of fraudulent identification documents that he created using real names and SSNs that his co-conspirators obtained. The documents were then used to defraud banks, businesses, and individuals out of more than half a million dollars. The names, SSNs, and other data were stolen from banks and from a hospital where security measures were obviously inadequate to prevent or detect the theft.

This individual and his co-conspirators are being criminally prosecuted, but criminal prosecution is not always an option. One proposal we have made in the past is that the OIG's Civil Monetary Penalty authority be extended to include SSN misuse. Providing the authority to penalize those who misuse SSNs but are not criminally prosecuted, or to penalize institutions that collect, but fail to protect, SSNs could create a strong deterrent and an effective tool.

The OIG has proven its ability to administer such a program through its administration of the existing provisions of Sections 1129 and 1140 of the Social Security Act—and we are prepared to take on this new challenge.

Indeed, we are faced with new challenges on a daily basis, as we constantly find new ways to close gaps in the SSN's protection. We are currently examining the practice of assigning SSNs to noncitizens who will only be in the United States for a few months—but are allowed to obtain an SSN that will be good forever. Consider, for example, the practice of allowing noncitizens who enter the country with a fiance visa to obtain an SSN. While deciding whether they will marry, these noncitizens are allowed to stay in the United States for 3 months—after which time they must marry, leave the country or apply for a new immigration status with DHS. By approving their request for an SSN during this 3-month period, we might be giving those who have no intentions to marry a much-needed tool for overstaying their visas. We believe a wiser course of action would be to approve the SSN application after the marriage has occurred, but we may need a legislative remedy to implement such a policy. Additional opportunities exist to restrict SSN access to other populations that might take advantage of similar programs.

We've also just undertaken an audit concerning the display of the SSN on Medicare cards, a document that many Americans carry in their wallets. I mentioned earlier our attempts to remove the SSN from drivers' licenses; while the use of the SSN in the Medicare program may be necessary, the display of the SSN on the card is something we'll be taking a critical look at.

As we have stated before this Subcommittee on many occasions, the SSN was never intended to do more than track a worker's earnings and pay that worker benefits. As the uses of the SSN have expanded over the decades, through acts of Congress and through the SSN's adoption simply as a matter of convenience, its value has increased as a tool for criminals. The Social Security card itself, which states on its face that it is not to be used for identification, is frequently cited as needing

improvement. But spending billions of dollars to try and stay one step ahead of counterfeiters is not the answer. The answer lies in doing everything we can to ensure the integrity of the enumeration process; limit the collection, use, and public display of the SSN; encourage the protection of the SSN by those who use it legitimately; and provide meaningful sanctions for those who fail to protect it or who misuse it themselves.

We will continue our audit work in these areas, such as the fiancé visa audit I just mentioned. We will continue our investigations, such as those I've described today. We will continue working to ensure Homeland Security, as reflected in the role we played in the recent arrests of terrorists planning an attack on Fort Dix. We will continue to seek the prosecution of employers or others who knowingly provide false SSNs to employees otherwise not authorized to work in the United States, as we did just last week in the Pacific Northwest, where a staffing agency was allegedly providing illegal workers with fraudulent SSNs. And we will continue to work with SSA and with this Subcommittee in hearings such as this, and in seeking legislation to make our efforts still more effective.

Thank you, and I'd be happy to answer any questions.

Chairman MCNULTY. Thank you, Mr. O'Carroll. In accordance with my previous announcement, we want to accommodate Congressman Barton, who is in another markup. I want to thank you, Joe, for making the time to come over and at this time, I would like to recognize the gentleman from Ennis, Texas, Congressman Barton. His entire testimony will appear in the record, and we now invite him to summarize his testimony.

**STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN
CONGRESS FROM THE STATE OF TEXAS**

Mr. BARTON. Thank you, Chairman McNulty. I apologize for my tardiness. We do have a full Committee markup upstairs on nine bills to reauthorize and approve the Food and Drug Administration. I did not know Ways and Means had a hearing room in the Rayburn Building. I headed out to the Longworth Building, and I had to be turned around and brought back here, but this is pretty nice. We can make a trade or something. I also thank Ranking Member Johnson for his many courtesies over the years.

—I want to thank this Subcommittee for holding this important hearing on the vulnerability of the Social Security number and how we should protect our Social Security number. Twenty years ago, nobody gave a second thought to showing a Social Security number on a driver's license. Now times have changed. In the Internet age, the Social Security is the key to our personal, medical and financial history. If we do not protect it, other people can unlock our lives and steal both our money, our reputations and sometimes our identities. The thought of a universal identifier, like the Social Security number, falling into the hands of an identity thief strikes a chord of fear in every consumer in this country, as it well should.

The Federal Government is partly to blame for allowing Social Security numbers to morph into something so crucial. When Social Security was being invented, they needed a way to uniquely identify every participant. Since 1936, the government has issued roughly 420 million Social Security numbers. No one then imagined the ubiquitousness and the critical role that these numbers would assume because records were on paper, credit was a luxury for the elite, and identity theft was literally something out of science fic-

tion. Unfortunately, a Social Security number now can be used to wreck a person's finances. Our Social Security numbers are everywhere. They are vulnerable to abuse and the government largely has failed to do anything about it.

Last year, I applied for a cell phone at Radio Shack. I had to give my Social Security number to three different people in the course of getting that cell phone within a 30 minute period. That is simply unacceptable in my opinion.

Technology is part of the problem and fortunately technology is beginning to offer solutions. Businesses which use Social Security numbers as commercial identifiers can often authenticate customers effectively and in a flash with other identifiers. Moreover, there are numerous situations in which no benefit exists for the business to require a Social Security number at all. I think some of them simply do it out of habit. Once a business does have your Social Security number, can they share it? Can they sell it? For that matter, can a business buy your Social Security number from another business? None of that to me seems like a very good idea, and I hope this Subcommittee would agree with that. These are important questions and the answers are even more important.

Erasing the link between our Social Security number and our personal information I think and Congressman Markey thinks is the best idea. Lacking that, there are a few easy steps that each of us can take to cut the risk of our number falling into the wrong hands. H.R. 948, the Social Security Number Protection Act, is a good start. This bill accomplishes something so simple that it is hard to believe that it has not already been done. It makes the sale and purchase of our Social Security number illegal. Buying and selling people's Social Security numbers I think is intolerable in a modern society. Internet information brokers should not have the ability to sell information to anyone who walks in the front door and plunks down a few dollars. As additional protection, H.R. 948 restricts the display of Social Security numbers online and prohibits requiring your number on any identification or Membership card.

I am well aware of the benefits Social Security numbers provide in preventing fraud and protecting me from being a victim. Despite comments from the critics, the intent of H.R. 948 does not affect legitimate uses of Social Security numbers. The Federal Trade Commission has given rulemaking authority to exempt honest purposes from the prohibitions that protect consumers.

Mr. Chairman, Ranking Member, and Members of this Subcommittee, the Energy and Commerce Committee, on which I serve and Congressman Markey serves, voted unanimously to report H.R. 948 last month. That does not happen often on the Energy and Commerce Committee, let me tell you. Last night, we were up here until 11 o'clock and passed six bills, all on a party line vote, so an unanimous consent report of H.R. 948 is an accomplishment. I hope that your Committee will now take up either the bill that Mr. Markey and I are sponsoring or discharge it so that we can take this important step in protecting our consumers' identities and their privacy.

With that, Mr. Chairman, and Members of the Subcommittee, I yield back.

Chairman MCNULTY. Thank you, Mr. Barton, and thank you for your many years of work on this issue. I think most people have their own personal stories about being asked for their Social Security number. I have a similar one to yours. It was a retail purchase. My wife and I were out a few years ago, and we were buying a refrigerator. We made selection and filled out the paperwork, and I was paying by personal check. I know you have additional ID, so I had my driver's license, which is a picture ID, and the driver's license number, which is not the Social Security number, and I wrote that on the check and gave it to the cashier. She then asked me for my Social Security to buy a refrigerator. Now, the difference between you and me is I refused.

Mr. BARTON. Good for you.

Chairman MCNULTY. I still got the refrigerator, but how many people are in circumstances like that and they just freely give their Social Security number? So, I think before we even get to legislation, we have a tremendous job ahead of ourselves in educating people about the proper circumstances under which they should share their Social Security number. Thank you for that news about reporting the bill out of the Committee. Mr. Johnson reminded me that in the last Congress, we reported out a bill out of Committee on Ways and Means but for some reason or another, these bills never get enacted into law. I mentioned to your colleague, Ed Markey, and to Senator Schumer earlier that while everybody is grateful for what everyone has done in the past in focusing on this issue, now is the time we need to actually do something, to pass something and get enacted into law. I want to thank you for your continued commitment to see to it that that happens.

Does any Member wish to inquire of Congressman Barton? Ms. Tubbs Jones?

Ms. TUBBS JONES. Just an inquiry, Congressman Barton. I was reading a newspaper article from the Cleveland Plain Dealer, which is my hometown newspaper, and what happened in the state of Ohio was that an intern had a copy of a disk of a number of people who were receiving, I guess it was back-up checks and so it says that thousands of state workers rushed to sign up for identity fraud protection after learning their personal information was on a back-up computer tape stolen from an intern's car. There are all kinds of crazy things that happen that expose people's information to possible identity theft.

For the record, Mr. Chairman, I seek unanimous consent to have two articles from the Plain Dealer entered into today's record.

Chairman MCNULTY. Is there objection? The Chair hears none, so ordered.

The first provided article follows:



THE PLAIN DEALER

Thousands sign up for fraud protection State employees fear ID theft after computer data loss

Tuesday, June 19, 2007

Aaron Marshall
Plain Dealer Bureau

Columbus—Thousands of state workers rushed Monday to sign up for identity fraud protection after learning their personal information was on a backup computer tape stolen from an intern's car last week.

By 5 p.m., 11,000 employees had taken up the state's offer for free identity fraud protection. A panel of state lawmakers approved spending \$730,533 to pay for the protection and to design a computer security system that does not rely on an intern taking backup data home at night.

So many state employees were trying to sign up for fraud protection that the Web site of the Texas-based company offering the service - Debix - crashed for several hours Monday morning, said Ron Sylvester, spokesman for the state Department of Administrative Services.

The most sensitive information that is known to be on the stolen tape: Electronic fund-transfer banking information for 28,362 state employees who travel regularly.

The strange saga of the nabbed computer tape, which began Friday when Gov. Ted Strickland revealed the theft, took some new twists Monday, but no one reported any fraudulent accounts being opened.

Ohio taxpayers will put up the \$9.75 per person that Debix charges for identity theft protection. The State Controlling Board approved a \$630,533 contract with the company. Also approved by the Controlling Board: A pair of \$50,000 contracts for a company headed by a national computer security expert, Matt Curtin, to check the state's findings of what data was on the stolen tape.

IDA5

© 2007 The Plain Dealer

© 2007 cleveland.com All Rights Reserved.

The second provided article follows:



THE PLAIN DEALER

225,000 more taxpayers' data at risk

Files stolen from state intern's car

Thursday, June 21, 2007

Mark Rollenhagen
Plain Dealer Bureau Chief

Columbus- Nearly a quarter-million Ohio taxpayers Wednesday joined the growing list of people whose personal information was on a data backup tape stolen from a state intern's car last week.

The names and Social Security numbers of 225,000 taxpayers who hadn't cashed their state or school district tax refund checks that were issued in 2005, 2006 and through May 29 of this year were on the backup tape of state data stolen June 10, Gov. Ted Strickland said Wednesday.

People who cashed their checks after May 29 are also included in the data, the governor said.

The governor's announcement expanded the data debacle far beyond the 64,000 state workers whose information was already known to be on the backup tape.

Strickland said there is still no sign that anyone has accessed the information on the data cartridge that was swiped along with a radar detector from the car parked at the intern's apartment complex in Hilliard, a suburb of Columbus.

"We continue to believe that it is not likely that the data on the device can be accessed without specialized knowledge and specialized equipment," the governor said at a news conference in his Statehouse office.

Strickland said he was "encouraged" that there have been no indications of identity theft among the 20,000 state workers who signed up for ID theft protection offered by the state this week. The names and Social Security numbers of 64,000 state workers were on the tape.

Strickland said the same ID theft protection will be offered to the taxpayers.

The state Controlling Board earlier this week approved a \$930,000 contract with Debix to provide the state workers with protection on a per-person basis.

Strickland said that because only a fraction of the people signed up for the protection, he doesn't expect to have to ask the Controlling Board for more money.

Hugh Quill, director of the Department of Administrative Services, said his staff is also negotiating a lower per-person cost with Debix.

In addition to the taxpayers, state officials have also learned this week that the tape includes:

602 lottery winners who have yet to cash a check for lottery winnings;

2,488 Ohioans who have not cashed checks for unclaimed funds;

Up to 1,000 electronic fund transfers that were not completed because they bounced back from a bank.

Strickland said state officials and a consultant are close to completing a review of another backup copy of the same data and only then will they be confident that they know of everything that was on the stolen device.

"We think we are close to being able to tell you that," Strickland said. "I don't want to say we're finished."

Parl Sabety, director of the Office of Management and Budget, said the information on taxpayers with

uncashed refund checks was contained in a file used to reconcile the state's checkbook every month.

She and Strickland said the file contained names, Social Security numbers and check amounts but not bank account information or addresses.

The governor said there has been no indication that information for other Ohio taxpayers is on the stolen backup tape.

The intern had taken the tape home for the weekend as part of a data backup protocol that Strickland ended after the theft.

The State Highway Patrol is investigating the theft and the Ohio inspector general's office is investigating the management decisions that put the tape at risk.

Previously, state officials have said that in addition to the information about state employees, the tape contained data on about 75,000 dependents of state workers and 77,000 Medicaid providers. It also contained information about people who received Temporary Assistance for Needy Families.

To reach this Plain Dealer reporter:

mrolenhagen@pland.com, 1-800-228-8272

© 2007 The Plain Dealer

© 2007 cleveland.com All Rights Reserved.

Ms. TUBBS JONES. It ended up that the state decided that they would hire a company to provide identity theft protection for all these workers whose information had been lost in the process. But you think about it, this is a legitimate use of the Social Security number but being put in jeopardy as a result of some stupid activity, or maybe I should not say "stupid," someone not thinking about where they kept up with information on behalf of workers. Having coming from a criminal justice background, as a prosecutor, as a judge, sometimes I think we try and implement laws to protect a certain situation, it really may not be the criminal justice system that we need to implement but having to safeguard this place to make appropriate conduct for the use of information. I am like you, I have to call into the bank to get my information, I have to give them my full Social Security number to get the \$2 that I have in the bank. But it is really kind of a crazy situation.

Mr. BARTON. Can I borrow a dollar?

Ms. TUBBS JONES. Can you borrow a dollar? Let's see, maybe I can help you out.

Well, I want to thank you for the work that you are doing in this area and like to be supportive. Thank you, Mr. Chairman.

Chairman MCNULTY. Does anyone else wish to inquire? If not, we wish to thank Congressman Barton. Thanks, Joe.

Mr. BARTON. Thank you, Mr. Chairman.

Chairman MCNULTY. That concludes the testimony of panel one. We will continue on panel two with Mr. Winston.

STATEMENT OF JOEL WINSTON, DIRECTOR OF PRIVACY AND INFORMATION PROTECTION, FEDERAL TRADE COMMISSION

Mr. WINSTON. Thank you, Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee. I am Joel Winston, associate director of the Division of Privacy and Identity Protection at the Federal Trade Commission. I appreciate the opportunity to testify today about Social Security numbers and identity theft.

As we have heard, identity theft afflicts millions of Americans every year. One telling example illustrates the damage it can cause. A few months ago, a consumer from Los Angeles contacted the FTC Identity Theft Hotline. He reported that his employer had suffered a data breach in which the consumer's employee records, including his Social Security number, had been compromised. Soon thereafter, an identity thief opened five credit card accounts in the consumer's name, resulting in thousands of dollars of unauthorized charges. But the thief did not stop there, he also emptied the consumer's checking account of almost \$2,000. In the first month or so after discovering the theft, this consumer spent hundreds of hours trying to repair the damage.

The Social Security number is often the key item of information that an identity thief needs to commit his crime. It is therefore critical to make SSNs less accessible to identity thieves. At the same time, it is important to remember that SSNs serve legitimate and useful purposes in our economy, including their widespread use to match individuals to information about them. For that reason, any restrictions on SSNs should be carefully tailored to reduce disclosures or uses that are unnecessary without inadvertently eliminating or burdening those that are necessary.

Although SSNs sometimes are used for legal compliance or essential business purposes, too often they are used simply as a matter of convenience or habit. For example, some organizations still use SSNs on employee badges or ID cards when a different and less sensitive identifier would work just as well.

The President's Identity Theft Task Force, in its report issued this April, concluded that, "More must be done to eliminate unnecessary uses of SSNs, both in the public sector and the private sector." The government has already begun to address its own SSN policies. This week, for example, the Office of Personnel Management issued guidance to all Federal agencies on limiting the collection and use of SSNs for human resource purposes. With respect to the private sector, the Task Force calls for a comprehensive review of SSN usage, and this review has already begun. We will be looking at the extent to which SSN uses are driven by business ne-

cessity and what the benefits and costs would be of restricting them.

In the meantime, the Federal Trade Commission has taken, and is continuing to take aggressive action to address identity theft. The first priority is prevention, stopping thieves from obtaining SSNs or other sensitive information. Businesses must be vigilant in protecting sensitive data they collect from consumers. To re-enforce this message, the Commission has brought 14 law enforcement actions against businesses that fail to reasonably safeguard consumers' personal information.

Consumers, too, must be more careful about guarding their information and so consumer education is a key part of our strategy. The Commission reaches out to the public in a variety of ways, including our identity theft Web site and hotline, and our highly successful multi-media national education campaign named, "Deter, Detect, Defend."

But restrictions on SSN usage and disclosure and better data security are not enough. Some sensitive information inevitably will find its way to identity thieves. Therefore, we must make it more difficult for criminals to use SSNs once they obtain them. Creating better methods of authenticating consumers would further this goal.

When a thief steals personal data, he can use it to open an account only if he can convince the account provider that he is the person whose data he stole. In April, the Commission hosted a workshop on authentication. We learned some encouraging new techniques to authenticate consumers that are being developed and deployed, and we discussed how the government and private sector can encourage their adoption.

I would like to turn now briefly to the issue of legislation. As we have heard today, several bills have been introduced in Congress over the past few years that would restrict SSNs in various ways. Generally, these bills would prohibit the display, purchase, sale or use of SSNs, subject to several exceptions, such as for law enforcement, public health and credit reporting purposes. The Commission has not taken a formal position on these bills, but I believe that they have an appropriate objective: to eliminate gratuitous SSN transfers or use while recognizing that there are certain necessary and legitimate transfers or uses that should be permitted. The challenge is to draw the right line. As Mr. Johnson said, it is a complex balancing act.

As I stated earlier, the Task Force is in the process of developing a comprehensive record on the factors that impact on where that line might be drawn. We support the idea that rulemaking authority be granted to the appropriate Federal agencies to implement and flesh out these exceptions, and I note that H.R. 948 gives that authority to the FTC.

Identity theft is one of the most important consumer protection issues of our time and must be attacked at every angle. The Commission will continue to place a high priority on preventing this crime and helping victims to recover. We look forward to continuing our work with Congress in this effort, and I would be happy to answer any questions that you might have.

The prepared statement of Mr. Winston follows:]

**Prepared Statement of Joel Winston, Director, Division of
Privacy and Information Protection, Federal Trade Commission**

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

on

Protecting the Privacy of the Social Security Number from Identity Theft

Washington, DC

June 21, 2007

I. INTRODUCTION

Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee, I am Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s views on the role of Social Security numbers (“SSNs”) in identity theft and options to enhance their protection.

Identity theft is a pernicious crime and controlling it is a critical component of the Commission’s consumer protection mission. This testimony describes the nature and scope of identity theft and the critical role that SSNs play both in creating and solving the problem. The testimony also summarizes the recommendations of the President’s Identity Theft Task Force (“Task Force”) with respect to preventing misuse of SSNs and, more broadly, combating identity theft. Finally, the testimony describes the Commission’s law enforcement and education and outreach efforts on identity theft.

SSNs provide many valuable functions in our information-based economy. At the same time, they may help criminals to steal consumers’ identities. The Task Force has recommended comprehensive reviews of both private and public sector usage of SSNs, which are ongoing. Ultimately, the objective of any SSN restrictions should be to reduce *unnecessary* transfer or use of SSNs, without inadvertently burdening *necessary* transfers or uses. Identity theft must be attacked on other fronts as well, from improving data security to keep sensitive information out

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 individual Commissioner.

of the hands of criminals, to educating consumers to better protect their information, to developing more effective means of authenticating consumers so that criminals who do obtain sensitive information cannot use it to open new accounts or access existing ones.

II. THE IDENTITY THEFT PROBLEM

Millions of consumers are victimized by identity thieves every year, collectively costing consumers and businesses billions of dollars and countless hours repairing the damage.² Beyond its direct costs, concerns about identity theft harm our economy by threatening consumers' confidence in the marketplace generally, and in electronic commerce specifically. A Wall Street Journal/Harris Interactive survey, for example, found that, as a result of fears about protecting their identities, 30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking.³

There are two predominant varieties of financial identity theft: the takeover or misuse of existing credit card, debit card, or other accounts ("existing account fraud"); and the use of stolen information to open new accounts in the consumer's name ("new account fraud"). New account fraud, although less prevalent, typically causes considerably more harm to consumers.⁴

² See, e.g., Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary* (February 2007), http://www.javelinstrategy.com/uploads/701_R_2007IdentityFraudSurveyReport_Brochure.pdf.

³ See Jennifer Cummings, *Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft*, Wall St. J. Online, May 18, 2006, http://www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_PersFinPoll_2006_vol2_iss05.pdf.

⁴ In many cases, consumers suffer no direct monetary loss from existing account fraud. Federal law limits consumers' liability for unauthorized credit card charges to \$50 per card, if the consumer notifies the credit card company within 60 days of the unauthorized charge. See 12 C.F.R. § 226.12(b). Many credit card companies do not require consumers to pay the \$50 and will not hold consumers liable for the unauthorized charges, no matter how much time has

SSNs are valuable to identity thieves in committing both types of identity theft. Financial institutions generally require SSNs to open new accounts, either by law or because SSNs enable them to obtain creditworthiness information from consumer reporting agencies. In addition, SSNs often are used to control access to existing accounts by serving as internal identifiers to match consumers with their records, and for consumer authentication purposes.⁵

III. USES AND SOURCES OF SOCIAL SECURITY NUMBERS

SSNs play an important role in our economy. With 300 million American consumers, many of whom share the same name,⁶ the unique 9-digit SSN is a key identification tool for businesses, government, and others.⁷ For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file and that they are providing a credit report on the correct consumer.⁸ Businesses and other entities use these reports in making eligibility and pricing decisions for a variety of products and services, including credit, insurance, home rentals, or employment. Additionally, SSNs are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and

elapsed since the discovery of the loss or theft of the card. Different rules apply for debit cards and checking accounts.

⁵ For example, a financial institution may ask an account holder for his SSN to confirm his identity before providing access to his account.

⁶ According to the Consumer Data Industry Association, 14 million Americans have one of ten last names, and 58 million men have one of ten first names.

⁷ See General Accounting Office, *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information* (GAO 04-01) (2004).

⁸ See *Federal Trade Commission - Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 38-40 (2004), <http://www.ftc.gov/reports/facta/041209factarpt.pdf>.

other judgments. SSN databases also are used to fight identity fraud – for example, to confirm that an SSN provided by a loan applicant does not, in fact, belong to someone who is deceased. Federal, state, and local governments rely extensively on SSNs in administering programs that provide services to consumers,⁹ and businesses in many circumstances are required to collect SSNs.¹⁰

SSNs are available from both public and private sources. Public records in city and county government offices across the country, including birth and death records, property records, tax lien records, voter registrations, licensing records, and court records, often contain consumers' SSNs.¹¹ As these records are increasingly placed online, access to large stores of SSNs becomes easier and less costly. Improved access to public records has important public policy benefits, but at the same time raises significant privacy concerns. Some public records

⁹ For example, the Federal government uses SSNs to administer the federal jury system, federal welfare and worker's compensation programs, and military draft registration. See Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), available at www.ssa.gov/history/reports/ssnreportc2.html.

¹⁰ Employers must collect SSNs for tax reporting purposes, for example, and health care providers may need them to obtain Medicare reimbursement.

¹¹ As of 2004, 41 states and the District of Columbia, as well as 75 percent of U.S. counties, displayed SSNs in public records. Government Accounting Office, *Social Security Numbers: Government Could Do More to Reduce Display in Public Records and on Identity Cards*, at 2 (Nov. 2004), available at <http://www.gao.gov/new.items/d0559.pdf>. Some governmental offices have been reducing their reliance on SSNs for administrative purposes in response to identity theft concerns. For example, only a few states still use SSNs as driver's license numbers. See David A. Lieb, *Millions of Motorists Have Social Security Numbers on Licenses*, *The Boston Globe*, Feb. 6, 2006, http://www.boston.com/news/local/massachusetts/articles/2006/02/06/millions_of_motorists_have_social_security_numbers_on_licenses/. In some cases, however, governments still use SSNs as identifiers when it is not essential to do so. See Mark Segraves, *Registering to Vote May Lead to Identity Theft*, *WTOP Radio*, Mar. 22, 2006, available at <http://www.wtop.com/?nid=428&sid=733727>.

offices redact sensitive information such as SSNs, but doing so can be very costly, particularly when it involves records that already are contained within a system.

There also are a number of private sources of SSNs, including consumer reporting agencies that list name, address, and SSN as part of the "credit header" information on consumer reports. Data brokers also collect personal information, including SSNs, from a variety of sources and compile and resell that data to third parties for a variety of purposes.¹²

Although SSNs sometimes are necessary for legal compliance or business purposes, other uses are more a matter of convenience or habit. For example, some organizations use SSNs as internal identifiers or as identification numbers displayed on cards because they always have done so, even though they could generate alternate identifiers of their own. Many organizations are taking steps to switch to alternate identifiers, although changing systems and procedures entails costs.¹³

The widespread use of SSNs makes them readily available and valuable to identity thieves. The challenge is to find the proper balance between the need to keep SSNs out of the hands of identity thieves and the need to give businesses and government entities sufficient means to attribute information to the correct person.

IV. CURRENT LAWS RESTRICTING THE USE OR DISCLOSURE OF SOCIAL

¹² Some data brokers are voluntarily restricting the sale of SSNs and other sensitive information to those with a demonstrable and legitimate need. See *Social Security Numbers Are for Sale Online*, Newsmax.com, Apr. 5, 2005, available at <http://www.newsmax.com/archives/articles/2005/4/4/155759.shtml>.

¹³ See James Hilton, *U.Va.'s Vice President and Chief Information Officer, Issues Message About Security*, UVa Today, Jan. 17, 2007, available at <http://www.virginia.edu/uvatoday/newsRelease.php?id=1323>. Some health insurance providers have stopped using SSNs as subscriber identification numbers. See www.wpsic.com/edi/comm_sub_p.shtml?mm=3.

SECURITY NUMBERS

There are a variety of specific statutes and regulations that restrict disclosure of certain consumer information, including SSNs, in particular contexts. In addition, under some circumstances, entities are required to have procedures in place to ensure the security and integrity of sensitive consumer information such as SSNs. Three statutes that protect SSNs from improper access fall within the Commission's jurisdiction: Title V of the Gramm-Leach-Bliley Act ("GLBA");¹⁴ Section 5 of the Federal Trade Commission Act ("FTC Act");¹⁵ and the Fair Credit Reporting Act ("FCRA"),¹⁶ as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").¹⁷

A. The Gramm-Leach-Bliley Act

The GLBA imposes privacy and security obligations on "financial institutions."¹⁸ Financial institutions are defined broadly as those entities engaged in "financial activities" such as banking, lending, insurance, loan brokering, and credit reporting.¹⁹

1. Privacy of Consumer Financial Information

In general, financial institutions are prohibited by Title V of the GLBA²⁰ from disclosing

¹⁴ 15 U.S.C. §§ 6801-09.

¹⁵ 15 U.S.C. § 45(a).

¹⁶ 15 U.S.C. §§ 1681-1681x, as amended.

¹⁷ Pub. L. No. 108-159, 117 Stat. 1952.

¹⁸ 15 U.S.C. § 6809(3)(A).

¹⁹ 12 C.F.R. §§ 225.28, 225.86.

²⁰ See 15 U.S.C. § 6802; Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLBA Privacy Rule").

nonpublic personal information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.²¹ However, the GLBA includes a number of statutory exceptions under which disclosure is permitted without notice or a right to opt-out. These exceptions include for purposes of consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.²² Entities that receive information under an exception to the GLBA are subject to reuse and redisclosure restrictions of the GLBA Privacy Rule, even if those entities are not themselves financial institutions.²³ Specifically, the recipients may only use and disclose the information “in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received].”²⁴

2. Safeguards for Customer Information

The GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they

²¹ See 15 U.S.C. § 6809. The GLBA defines “nonpublic personal information” as any information 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, SSN, address, telephone number, mother’s maiden name, and prior addresses. See, e.g., Privacy of Consumer Financial Information, 16 C.F.R. Part 313 (“GLBA Privacy Rule”).

²² 15 U.S.C. § 6802(e).

²³ 16 C.F.R. § 313.11(a).

²⁴ *Id.*

receive from customers, whether directly or from other financial institutions.²⁵ The FTC's Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,²⁶ requires financial institutions to develop a written information security plan that describes their procedures to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires that security plans account for each entity's particular circumstances - its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps - for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers - in implementing their plans.

B. Section 5 of the FTC Act

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."²⁷ Under the FTC Act, the Commission has broad jurisdiction over a wide variety of entities and individuals operating in commerce. Under the Commission's deception authority, it is unlawful to make false claims about one's privacy procedures or security protections.²⁸

²⁵ 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

²⁶ The Federal Deposit Insurance Corporation, the National Credit Union Administration ("NCUA"), the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, and state insurance authorities have promulgated comparable information safeguards rules, as required by Section 501(b) of the GLBA. 15 U.S.C. § 6801(b); *see, e.g.*, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616-41 (Feb. 1, 2001). The FTC has jurisdiction over entities not subject to the jurisdiction of these agencies.

²⁷ 15 U.S.C. § 45(a).

²⁸ Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates*,

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.²⁹ The Commission has used this authority to challenge a variety of injurious practices, including companies' failure to provide reasonable and appropriate security for sensitive customer data.³⁰ The Commission can obtain injunctive relief for violations of Section 5, as well as consumer redress or disgorgement in appropriate cases.

C. The Fair and Accurate Credit Transactions Act of 2003

The FACT Act amended the FCRA to include a number of provisions designed to increase the protection of sensitive consumer information, including SSNs. One such provision required the banking regulatory agencies, the National Credit Union Administration ("NCUA"), and the Commission to promulgate a coordinated rule, requiring all users of consumer report information to have reasonable procedures to dispose of it properly and safely.³¹ This Disposal Rule, which took effect on June 1, 2005, helps reduce the risk of improper disclosure of SSNs. In addition, the FACT Act requires consumer reporting agencies to truncate the SSN on

Inc., 103 F.T.C. 110 (1984).

²⁹ 15 U.S.C. § 45(n).

³⁰ The Commission also has challenged as unfair the practice of imposing unauthorized charges in connection with "phishing," high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, SSNs, passwords, or other sensitive information. See *FTC v. Hill*, No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), available at <http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm>; *FTC v. C.J.*, No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), available at <http://www.ftc.gov/os/2003/07/phishingcomp.pdf>.

³¹ 16 C.F.R. Part 382 ("Disposal Rule").

consumer reports at the consumer's request when providing the reports to the consumer.³²

Eliminating the unnecessary display of this information could lessen the risk of it getting into the wrong hands.

D. Other Laws

Other federal laws not enforced by the Commission regulate certain specific classes of information, including SSNs. For example, the Driver's Privacy Protection Act ("DPPA")³³ prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to fourteen "permissible uses," including law enforcement, motor vehicle safety, and insurance. The Health Information Portability and Accountability Act ("HIPAA") and its implementing privacy rule prohibit the disclosure to third parties of a consumer's medical information without prior consent, subject to a number of exceptions (such as, for the disclosure of patient records between entities for purposes of routine treatment, insurance, or payment).³⁴ Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."³⁵

V. TASK FORCE RECOMMENDATIONS REGARDING THE USE OF SSNS

On May 10, 2006, the President established an Identity Theft Task Force. Comprised of

³² 15 U.S.C. § 1681g(a)(1)(A). The FTC advises consumers of this right through its consumer outreach initiatives. *See, e.g.*, the FTC's identity theft prevention and victim recovery guide, *Take Charge: Fighting Back Against Identity Theft* at 5 (2005), available at <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.pdf>.

³³ 18 U.S.C. §§ 2721-25.

³⁴ 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

³⁵ *Id.* at § 164.530(c).

17 federal agencies, including the FTC, the mission of the Task Force is to develop a comprehensive national strategy to combat identity theft.³⁶ The President specifically directed the Task Force to make recommendations on ways to improve the effectiveness and efficiency of the Federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution.

In April 2007, the Task Force published a strategic plan for combating identity theft.³⁷ Broadly, the plan is organized around the life cycle of identity theft – from the thieves' attempts to obtain sensitive information to its impact on victims – and identifies roles for consumers, the private sector, government agencies, and law enforcement.

The strategic plan also describes how identity thieves come into possession of consumers' SSNs and how they use them to steal identities. It concludes that "[m]ore must be done to eliminate unnecessary uses of SSNs."³⁸ Accordingly, several of the Task Force recommendations focus on SSNs and their use in the public and private sectors. With respect to the public sector, the Task Force recommended that:

- the Office of Personnel Management ("OPM") review its use of SSNs in collecting human resource data from federal agencies and on OPM forms, and take steps to eliminate, restrict, or conceal their use wherever possible (including assigning employee identification numbers where practicable).³⁹
- OPM issue guidance to federal agencies on how to restrict, conceal, or mask SSNs in employee records.

³⁶ Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

³⁷ The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("strategic plan") is available at www.idtheft.gov.

³⁸ Strategic Plan, at 25.

³⁹ *Id.* The OPM review has been completed.

- The Social Security Administration develop a clearinghouse of agency "best practices" for minimizing the use and display of SSNs.
- The Office of Management and Budget complete its analysis of responses to its survey on agency uses of SSNs.
- The Task Force work with state and local governments to explore ways to eliminate unnecessary use and display of SSNs.

The Task Force also recommended an analysis of private sector reliance on SSNs. As discussed in Section III, it is well-understood that the private sector uses SSNs in a many ways to match information with individuals. What is less clear is the extent to which such uses are driven by business necessity, as opposed to convenience or habit, and what direct and indirect costs would be entailed in requiring businesses to use alternate identifiers. Therefore, the strategic plan recommends that the Task Force develop a comprehensive record on the uses of the SSN in the private sector and evaluate their necessity. By the first quarter of 2008, the Task Force will make recommendations to the President on whether additional steps should be taken regarding the use of SSNs.

VI. COMMISSION ACTIVITIES TO COMBAT IDENTITY THEFT

As described earlier, to successfully combat identity theft, it must be attacked at several different points in its life cycle. First, SSNs and other sensitive data must be kept out of the hands of data thieves by, among other things, limiting the availability of such data and improving the manner in which those who collect such data safeguard it.⁴⁰ Second, it must be made more difficult for thieves to use data they steal to open or access accounts in the victims' names by,

⁴⁰ *Id.* at 22-42.

among other ways, improving methods to authenticate consumers.⁴¹ Third, identity theft must be deterred through more effective prosecution of criminals responsible for these acts.⁴²

Through its longstanding efforts to combat identity theft through law enforcement and consumer and business education, and its recent implementation of the Task Force recommendations, the Commission has and is continuing to act aggressively on each of these fronts.

A. Data Security

Public awareness of, and concerns about, data security have reached new heights as reports about breaches of sensitive personal information continue to proliferate. Recent breaches have touched both the public and private sectors. Of course, not all data breaches result in identity theft and, in fact, many may lead to no harm whatsoever. Nonetheless, some breaches - especially those that result from deliberate actions, such as hacking, by criminals - have led to fraud.

A number of bills have been introduced in the past two sessions of Congress that would require businesses that maintain sensitive consumer information to have reasonable protections in place to prevent unauthorized access, as well as to require companies that suffer a data breach to provide notice to affected consumers. At the same time, well over half of the states have enacted data security and/or breach notification laws. The Commission and the Task Force have recommended that Congress establish national standards for data security and breach

⁴¹ *Id.* at 42-45.

⁴² *Id.* at 52-71.

notification.⁴³

1. Law Enforcement

Pending the enactment of national standards, the FTC enforces several existing laws and regulations that, explicitly or implicitly, contain data security requirements, including the GLBA Safeguards Rule, the FCRA's "know your customer" requirements,⁴⁴ and the FTC Act. Since 2001, the Commission has brought fourteen cases challenging businesses that failed to reasonably protect sensitive consumer information that they maintained.⁴⁵ In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices.⁴⁶ In some cases, the alleged security inadequacies led to breaches that caused substantial consumer injury

⁴³ See Statement of Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft, at 7 (June 16, 2005) available at <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>; Strategic Plan, at 34-37.

⁴⁴ 15 U.S.C. § 1681 *et seq.* The FCRA specifies that consumer reporting agencies may provide consumer reports only for enumerated "permissible purposes," and requires that they have reasonable procedures to verify the identity and permissible purposes of prospective recipients of their reports.

⁴⁵ See generally <http://www.ftc.gov/privacy/index.html>.

⁴⁶ *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 23, 2007); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (March 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

and were challenged as unfair practices under the FTC Act.⁴⁷ Several cases involved alleged violations of the Safeguards Rule or the FCRA.⁴⁸

Probably the best-known FTC data security case was its 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including credit reports in some instances) on more than 160,000 consumers to data thieves posing as ChoicePoint clients. In turn, the thieves used that information in many instances to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of its information and ignored obvious red flags. For example, the company allegedly approved as purchasers individuals who lied about their credentials, used commercial mail drops and business addresses, and faxed multiple applications from nearby commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for violations of the FCRA and \$5 million in consumer redress for identity theft victims, and agreed to undertake substantial new data security measures.⁴⁹

⁴⁷ E.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (March 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

⁴⁸ E.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005). In the *Nations Title*, *Nationwide Mortgage Group*, and *Sunbelt Lending Services* cases, the Commission also alleged that the companies violated the GLBA's privacy provisions and the FTC's implementing Privacy Rule, which, among other things, require financial institutions to provide notices to their customers describing their information-sharing policies.

⁴⁹ See FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress* (Jan. 26, 2006), available at <http://www.ftc.gov/opa/2006/01/choicepoint.html>. The Commission has mailed more than

The Commission's most recent data security enforcement action involved Guidance Software, Inc., a marketer of software and related services for investigating and responding to computer breaches and other security incidents. According to the FTC complaint, Guidance, contrary to its claims, failed to implement simple, inexpensive, and readily available security measures to protect consumers' data, for example, by failing to defend against commonly-known or reasonably foreseeable web attacks, and by permanently storing credit card information in clear, readable text rather than encrypting or otherwise protecting it.⁵⁰

Although the Commission's data security cases have been brought under different laws, they share common elements: the vulnerabilities were multiple and systemic, and readily-available and often inexpensive measures were available to prevent them. Together, the cases stand for the proposition that companies should maintain reasonable and appropriate measures to protect sensitive consumer information. The Commission will continue to apply these principles in enforcing existing data security laws.

2. Consumer and Business Education

The Commission has made substantial efforts to increase consumer and business awareness of the importance of protecting data and taking other steps to prevent identity theft. The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives about 15,000 to 20,000 contacts each week through its toll-free hotline

5,000 claims forms to possible victims and has created a website at which consumers can download the forms and obtain information about the claims process.

⁵⁰ *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 3, 2007).

and dedicated website regarding identity theft recovery, or how to avoid becoming a victim in the first place. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft. The FTC's identity theft primer⁵¹ and victim recovery guide⁵² are widely available in print and online. The Commission has distributed over 2 million copies of the primer and has recorded over 2.4 million visits to the Web version.

Last year, the Commission launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend."⁵³ It includes direct-to-consumer brochures, as well as training kits and ready-made materials (including presentation slides and a video) for use by businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. The Commission has distributed over 3.5 million brochures and 40,000 kits to date. The Commission also has partnered with other organizations to broaden its reach. As just one example, the U.S. Postal Inspection Service recently initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

The Commission also sponsors a multimedia website, OnGuard Online,⁵⁴ designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudsters. OnGuard Online was developed in

⁵¹ *Avoid ID Theft: Deter, Detect, Defend*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth01.htm>.

⁵² *Take Charge: Fighting Back Against Identity Theft*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.htm>.

⁵³ See <http://www.ftc.gov/bcp/edu/microsites/idtheft>.

⁵⁴ See <http://www.onguardonline.gov/index.html>.

partnership with other government agencies and the technology sector, and since its launch has attracted more than 3.5 million visits.

The Commission directs its outreach to businesses as well. Recently, the FTC released a new business education guide related to data security.⁵⁵ Most companies have some information in their files - names, SSNs, credit card numbers - that identifies their customers and employees. The Commission has heard from some businesses, particularly smaller businesses, that they were not sure what data security measures they should take to protect such sensitive information from falling into the wrong hands. The Commission, therefore, developed a brochure that articulates the key steps that are part of a sound data security plan. The Commission anticipates that the brochure will be a useful tool in alerting businesses to the importance of data security issues and give them a solid foundation on how to address those issues.

B. Limiting Unnecessary Uses of SSNs

As described earlier, the Task Force recommended that agencies undertake a comprehensive review of the public and private sector uses of SSNs, with the goal of identifying unnecessary uses that could be eliminated. Efforts to evaluate and limit government collection, use, and disclosure through the OPM and OMB are well underway. At the same time, the Commission, assisted by other Task Force agencies, has begun implementing the review of private sector uses. Commission staff is developing a number of outreach opportunities to learn from stakeholders on this issue.

⁵⁵ *Protecting Personal Information: A Guide for Business*, available at <http://www.ftc.gov/infosecurity.htm>. Other business publications on data security and responding to data breaches are available at <http://www.ftc.gov/bcp/edu/microsites/idtheft.htm>.

C. Authentication

Restricting unnecessary uses of SSNs and better data security are not the only means of preventing SSN misuse. Even the most effective efforts cannot prevent thieves from obtaining sensitive information in all cases. For that reason, it is important to make this information less useful to thieves by making it more difficult for them to use it to steal an identity. To accomplish this goal, better methods of authenticating consumers - for example, proving that the individual is who she purports to be - must be developed.

To that end, the Task Force recommended holding a workshop on improving authentication methods, which the Commission hosted on April 23 and 24, 2007. The workshop was designed to facilitate discussions about the technological and policy issues surrounding the development of improved authentication procedures.⁵⁶ A number of themes emerged during the course of the two days of discussions. First, there is no single "right" way to authenticate individuals, but rather there are a number of promising techniques being developed and implemented that use multiple layers of security, including biometrics and smart cards. Identity thieves are increasingly sophisticated and adept at defeating authentication efforts, so that it is critical that new techniques continue to be developed to stay "a step ahead" of the thieves. Participants also agreed that consumer convenience and usability are critical - consumers will reject authentication procedures that are too burdensome. And, there was general agreement that the government can play an important role in this area by encouraging and facilitating the development of better authentication. Commission staff currently is drafting a summary report

⁵⁶ See *Proof Positive: New Directions for ID Authentication* at <http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml>.

of the workshop proceedings.

D. Criminal Prosecution

The Task Force strategic plan contains a detailed discussion of how identity thieves currently are investigated and prosecuted. The plan recommends numerous actions - from strengthening criminal statutes, to better coordinating domestic and international efforts, to more training of law enforcement investigators and prosecutors, to the establishment of an interagency National Identity Theft Law Enforcement Center to enhance information sharing among law enforcers. Although the Commission lacks criminal jurisdiction itself, it will play an active role in implementing these recommendations.

VII. CONCLUSION

Identity theft remains a serious problem in this country, causing enormous harm to consumers, businesses and ultimately our economy. Succeeding in the battle against identity theft will require the public and private sectors, working together, to make it more difficult for thieves both to obtain sensitive information and to use the information they are able to procure to steal identities. To prevent thieves from obtaining sensitive information, government and the business community should, first, limit the information they collect and maintain from or about consumers - including SSNs - to that necessary to meet clear legal or business needs, and, second, to better protect the data they do collect. In addition, to keep thieves from using the information they do procure to steal identities, consumer authentication techniques must be improved. The Task Force's strategic plan provides a blueprint for achieving these goals, and the Commission will continue to play a central role in the battle against identity theft.

Chairman MCNULTY. Thank you, Mr. Winston.
Mr. Bertoni.

**STATEMENT OF DAN BERTONI, EDUCATION, WORKFORCE,
AND INCOME SECURITY, GOVERNMENT ACCOUNTABILITY
OFFICE**

Mr. BERTONI. Good morning, Mr. Chairman, and Members of the Subcommittee. I am pleased to be here to discuss ways to protect the Social Security number, which was originally created as a means to track worker earnings and administer retirement benefits. Over time, the SSN has evolved beyond its intended purpose, become the identifier of choice and is now used for myriad non-Social Security purposes. This is significant because a person's SSN,

along with name and date of birth, are key pieces of information used to commit identity theft. Potential for misuse of the SSN has raised concerns about how the public and private entities are obtaining, using and protecting SSNs. My testimony today is based on our prior work, as well as the report issued today for Senator Schumer and will focus on describing SSN use in the public and private sector, as well as vulnerabilities that remain to protecting them.

In summary, a number of Federal laws and regulations authorize or require agencies at all levels of government to collect SSNs to administer their programs. For example, the Debt Collection Act 1996 requires any individual doing business with the Federal Government or applying for a grant or service to furnish a valid SSN. Certain state and local government agencies also collect SSNs as part of their responsibility for maintaining public records. In a prior work, we reported that 41 states and the District of Columbia display SSNs in public records, as well as 75 percent of all U.S. counties. SSNs were most often found in court and property records.

As noted earlier, in our report issued today, we found that the Internal Revenue Service and the Department of Justice are the only Federal agencies commonly providing records containing SSNs to state and local recordkeepers. IRS and Justice provide thousands of property liens annually to recordkeepers in which they have traditionally included full SSNs for identity verification purposes.

Historically, access to public records occurred by visiting local offices and search through electronic or paper records. However, today, more recordkeepers provide potentially unlimited access to sensitive information through bulk sales to private companies and to the public via the Internet.

Some states, however, have begun to restrict how they display or provide access to SSNs in such records. For example, Florida counties we recently visited are currently using special software to search for and remove millions of SSNs and other sensitive information from their records.

In the private sector, information re-sellers, credit bureau reporting agencies and health care organizations collect SSNs from various sources and use this information primarily for identification verification purposes. Large information re-sellers obtain SSNs from various public records, such as bankruptcy notices, tax liens, civil judgments and property transactions. In addition to their own direct use of SSNs, entities such as banks, securities firms, telecommunications firms and tax preparers also share this information—SSN information with third party contractors who perform services for them.

Although new Federal and state laws have helped restrict SSN use and display, vulnerabilities remain. For example, we are concerned that SSNs are still displayed on certain federally-issued cards. In particular, the Center for Medicare and Medicaid Services has not yet acted to remove SSNs from over 40 million Medicare cards despite our report citing this weakness. We are also concerned that current Federal laws restricting the sale of SSNs and other personal information applied to certain types of entities, such

as financial institutions, but not to information re-sellers, who are obtaining and using the same sensitive data.

However, recently proposed legislation, the Social Security Protection Act of 2007, as discussed by Mr. Markey earlier, if enacted, may help address this vulnerability by placing additional restrictions on the sale and purchase of SSNs. H.R. 1745, which was introduced in the last Congress, also includes provisions to address this issue.

Further, Federal oversight regarding the sharing of SSNs with contractors is less stringent for the telecommunications and tax preparation industries, which poses potential additional challenges for protecting SSNs and other sensitive data in those industries.

Finally, although Federal agencies have begun truncating SSNs on documents provided to state and local recordkeepers, different truncation methods between the public and private sectors have implications for identity theft. Current Federal lien records display the last four digits of SSNs, while private re-sellers often provide the first five digits of the SSN to the customer. Consequently, with minimal effort, our analysts were able to electronically access private sector databases, compare this information to Federal liens, and reconstruct full identity and SSN information for 10 liens for 10 individuals from 10 states. The entire process took less than an hour or about an hour or about 6 minutes per SSN and it was all done from their desks. In light of this finding, we continue to urge the Congress to consider enacting a single truncation standard or assign an agency to do so.

Mr. Chairman, this concludes my remarks. I will be happy to answer any questions that you or other Members of the Subcommittee may have. Thank you.

[The prepared statement of Mr. Bertoni follows:]

**Prepared Statement of Dan Bertoni, Director, Education,
Workforce, and Income Security, Government Accountability Office**

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss ways to better protect the Social Security number (SSN), which was originally created as a means to track workers' earnings and eligibility for Social Security benefits. Since its creation, the SSN has evolved beyond its intended purpose to become the identifier of choice for public and private sector entities and is now used for myriad non-Social Security purposes. This is significant because a person's SSN, along with name and date of birth, are the key pieces of personal information used to perpetrate identity theft. Consequently, the potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs.

Over the last several years, the Congress and some states have recognized the importance of restricting the use and display of SSNs by both the public and private sectors. As a result, federal and state laws have been enacted that to some degree protect individuals' personal information, including SSNs. However, the continued use of and reliance on SSNs by public and private sector entities, as well as the potential for their misuse, underscore the importance of identifying areas that can be further strengthened. GAO has issued a number of reports and testified before this Subcommittee about the various aspects of SSN use in both the public and private sectors. Accordingly, my remarks today will focus on describing the (1) use of SSNs by government agencies, (2) use of SSNs by the private sector, and (3) vulnerabilities that remain to protecting SSNs.

In summary, a number of federal laws and regulations require agencies at all levels of government to frequently collect and use SSNs for various purposes. For example, agencies frequently collect and use SSNs to administer their programs, link data for verifying applicants' eligibility for services and benefits, and conduct program evaluations. In the private sector, certain entities, such as information re-sellers, collect SSNs from public sources, private sources, and their customers and

use this information for identity verification purposes. In addition, banks, securities firms, telecommunication firms, and tax preparers sometimes share SSNs with their contractors for limited purposes. Although laws at both the federal and state levels have helped to restrict SSN use and display, and both public and private sector entities have taken some steps to further protect this information, several vulnerabilities remain. For example, federal laws addressing SSN use and collection in the private sector continue to leave SSNs maintained by certain industries vulnerable to misuse by identity thieves and others.

For this testimony, we primarily relied on information from our prior reports and testimonies that address public and private sector use and protection of SSNs. These products were issued between 2002 and 2006 and are listed in the Related GAO Products section at the end of this statement. We conducted our reviews in accordance with generally accepted government auditing standards.

Background

The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to manage the Social Security program, which 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. Today, SSA issues SSNs to most U.S. citizens, as well as non-citizens lawfully admitted to the United States with permission to work. Because the SSN is unique for every individual, both the public and private sectors increasingly use it as a universal identifier. This increased use, as well as increased electronic record keeping by both sectors, has eased access to SSNs and potentially made this information more vulnerable to misuse, including identity theft.

Specifically, SSNs are a key piece of information used to create false identities for financial misuse or to assume another individual’s identity. Most often, identity thieves use SSNs belonging to real people. However, the Federal Trade Commission’s (FTC) identity theft victim complaint data has shown that only 30 percent of identity theft victims know how thieves obtained their personal information. The FTC estimated that over a 1-year period, nearly 10 million people discovered they were victims of identity theft, translating into estimated losses of billions of dollars.

Federal Laws Affecting SSN Use and Disclosure

There is no one law that regulates the overall use of SSNs by all levels and branches of government. However, the use and disclosure of SSNs by the Federal Government is generally restricted under the Privacy Act of 1974. Broadly speaking, this act seeks to balance the government’s need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy. Section 7 of the act requires that any federal, state, or local government agency, when requesting an SSN from an individual, tell individuals whether disclosing the SSN is mandatory or voluntary, cite the statutory or other authority under which the request is being made, and state what uses it will make of the individual’s SSN.

Additional federal laws also place restrictions on public and private sector entities’ use and disclosure of consumers’ personal information, including SSNs, in specific instances. As shown in table 1, some of these laws require certain industries, such as the financial services industry, to protect individuals’ personal information to a greater degree than entities in other industries.

[Table 1: NOT AVAILABLE AT TIME OF PRINT.]

In 1998, Congress also enacted a federal statute that criminalizes fraud in connection with the unlawful theft and misuse of personal identifiable information, including SSNs. The Identity Theft and Assumption Deterrence Act made it a criminal offense for a person to “knowingly transfer, possess, or use without lawful authority,” another person’s means of identification “with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law.” Under the act, an individual’s name or Social Security number is considered a “means of identification.” In addition, in 2004, the Identity Theft Penalty Enhancement Act established the offense of aggravated identity theft in the federal criminal court, which is punishable by a mandatory two-year prison term.

State Laws Affecting SSN Use and Disclosure

Many states have also enacted laws to restrict the use and display of SSNs. For example, in 2001, California enacted a law that generally prohibited companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted. In our prior work, we identified 13 states—Arizona, Arkansas, Connecticut, Georgia, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas, Utah, and Virginia—that have passed laws similar to California’s. While some states, such as Arizona, have enacted virtually identical restrictions on the use and display of SSNs, other states have modified the restrictions in various ways. For example, unlike the California law, which prohibits the use of the full SSN, the Michigan statute prohibits the use of more than four sequential digits of the SSN.

Some states have also enacted other types of restrictions on the uses of SSNs. For example, Arkansas, Colorado, and Wisconsin prohibit the use of a student’s SSN as an identification number. Other recent state legislation places restrictions on state and local government agencies, such as Indiana’s law that generally prohibits state agencies from releasing SSNs unless otherwise required by law.

Government Agencies Collect and Use SSNs for a Variety of Purposes

A number of federal laws and regulations require agencies at all levels of government to frequently collect and use SSNs for various purposes. Beginning with a 1943 Executive Order issued by President Franklin D. Roosevelt, all federal agencies were required to use the SSN exclusively for identification systems of individuals, rather than set up a new identification system. In later years, the number of federal agencies and others relying on the SSN as a primary identifier escalated dramatically, in part, because a number of federal laws were passed that authorized or required its use for specific activities. For example, agencies use SSNs

- **for internal administrative purposes, which include activities such as identifying, retrieving, and updating records;**
- **to collect debts owed to the government and conduct or support research and evaluations, as well as use employees’ SSNs for activities such as payroll, wage reporting, and providing employee benefits;**
- **to ensure program integrity, such as matching records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments; and**
- **for statistics, research, and evaluation.**

Table 2 provides an overview of federal statutes that address government collection and use of SSNs. In some cases, these statutes require that state and local government entities collect SSNs.

[Table 2: NOT AVAILABLE AT TIME OF PRINT.]

Some government agencies also collect SSNs because of their responsibility for maintaining public records, which are those records generally made available to the public for inspection by the government. Because these records are open to the public, such government agencies, primarily at the state and local levels, provide access to the SSNs sometimes contained in those records. Based on a survey of federal, state, and local governments, we reported in 2004 that state agencies in 41 states and the District of Columbia displayed SSNs in public records; this was also true in 75 percent of U.S. counties. We also found that while the number and type of records in which SSNs were displayed varied greatly across states and counties, SSNs were most often found in court and property records.

Public records displaying SSNs are stored in multiple formats, such as electronic, microfiche and microfilm, or paper copy. While our prior work found that public access to such records was often limited to inspection of the individual paper copy in public reading rooms or clerks’ offices, or request by mail, some agencies also made public records available on the Internet.

In recent years, some agencies have begun to take measures to change the ways in which they display or provide access to SSNs in public records. For example, some state agencies have reported removing SSNs from electronic versions of records, replacing SSNs with alternative identifiers in records, restricting record access to individuals identified in the records, or allowing such individuals to request the removal of their SSNs from these records.

Private Sector Entities Collect SSNs from Various Sources for Identity Verification Purposes

Certain private sector entities, such as information resellers, consumer reporting agencies (CRAs), and healthcare organizations collect SSNs from public and private sources, as well as their customers, and primarily use SSNs for identity verification purposes. In addition, banks, securities firms, telecommunication firms, and tax preparers engage in third party contracting and sometimes share SSNs with their contractors for limited purposes, generally when it is necessary and unavoidable.

Private Sector Entities Collect SSNs from Both Public and Private Sources

Information resellers are businesses that specialize in amassing personal information, including SSNs, and offering informational services. They provide their services to a variety of customers, such as specific businesses clients or through the Internet to the general public. Large or well known information resellers reported that they obtain SSNs from various public records, such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, and real estate transactions. However, some of these resellers said they are more likely to rely on SSNs obtained directly from their clients, who may voluntarily provide such information, than those found in public records. In addition, in our prior review of information resellers that offer their services through the Internet, we found that their Web sites most frequently identified public or nonpublic sources, or both, as their sources of information. For example, a few Internet resellers offered to conduct background investigations on individuals by compiling information from court records and using a credit bureau to obtain consumer credit data.

CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Like information resellers, CRAs also obtain SSNs from public and private sources. For example, CRA officials reported that they obtain SSNs from public sources, such as bankruptcy records. We also found that these companies obtain SSNs from other information resellers, especially those that specialize in collecting information from public records. However, CRAs are more likely to obtain SSNs 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.

Organizations that provide health care services, including health care insurance plans and providers, are less likely to obtain SSNs from public sources. These organizations typically obtain SSNs either from individuals themselves or from companies that offer health care plans. For example, individuals enrolling in a health care plan provide their SSNs as part of their plan applications. In addition, health care providers, such as hospitals, often collect SSNs as part of the process of obtaining information on insured people.

Private Sector Entities Primarily Use SSNs to Verify Individuals' Identities

We found that the primary use of SSNs by information resellers, CRAs, and health care organizations is to help verify the identity of individuals. Large information resellers reported that they generally use the SSN as an identity verification tool, though they also use it for matching internal databases, identifying individuals for their product reports, or conducting resident or employment screening investigations for their clients. CRAs use SSNs as the primary identifier of individuals in order to match information they receive from their business clients with information on individuals already stored in their databases. Finally, health care organizations also use the SSN, together with information such as name, address, and date of birth, for identity verification.

In addition to their own direct use of customers' SSNs, private sector entities also share this information with their contractors. According to experts, approximately 90 percent of businesses contract out some activity because they find either it is more economical to do so or other companies are better able to perform these activities. Banks, investment firms, telecommunication companies, and tax preparation companies we interviewed for our prior work routinely obtain SSNs from their customers for authentication and identification purposes and contract with other companies for various services, such as data processing, administrative, and customer service functions. Company officials reported that customer information, such as SSNs, is shared with contractors for limited purposes, generally when it is necessary or unavoidable. Further, these companies included certain provisions in their standard contact forms aimed at safeguarding customer's personal information. For example, forms included electronic and physical data protections, audit rights, data

breach notifications, subcontractor restrictions, and data handling and disposal requirements.

Vulnerabilities Remain to Protecting SSNs in both the Public and Private Sectors

Although federal and state laws have helped to restrict SSN use and display, and public and private sector entities have taken some steps to further protect this information, our prior work identified several remaining vulnerabilities. While government agencies have since taken actions to address some of the identified SSN protection vulnerabilities in the public sector, private sector vulnerabilities that we previously identified have not yet been addressed. Consequently, in both sectors, vulnerabilities remain to protecting SSNs from potential misuse by identity thieves and others.

Government Agencies Have Taken Additional Actions to Address SSN Protection, yet Vulnerabilities Remain

In our prior work, we found that several vulnerabilities remain to protecting SSNs in the public sector, and in response, some of these vulnerabilities have since been addressed by agencies. For example, in our review of government uses of SSNs, we found that some federal, state, and local agencies do not consistently fulfill the Privacy Act requirements that they inform individuals whether SSN disclosure is mandatory or voluntary, provide the statutory or other authority under which the SSN request is made, or indicate how the SSN will be used, when they request SSNs from individuals. To help address this inconsistency, we recommended that the Office of Management and Budget (OMB) direct federal agencies to review their practices for providing required information, and OMB has since implemented this recommendation.

Actions have also been taken by some federal agencies in response to our previous finding that millions of SSNs are subject to exposure on individual identity cards issued under federal auspices. Specifically, in 2004, we reported that an estimated 42 million Medicare cards, 8 million Department of Defense (DOD) insurance cards, and 7 million Department of Veterans Affairs (VA) beneficiary cards displayed entire 9-digit SSNs. While the Centers for Medicare and Medicaid Services, with the largest number of cards displaying the entire 9-digit SSN, does not plan to remove the SSN from Medicare identification cards, VA and DOD have begun taking action to remove SSNs from cards. For example, VA is eliminating SSNs from 7 million VA identification cards and will replace cards with SSNs or issue new cards without SSNs between 2004 and 2009, until all such cards have been replaced.

However, some of the vulnerabilities we identified in public sector SSN protection have not been addressed. For example, while the Privacy Act and other federal laws prescribe actions agencies must take to assure the security of SSNs and other personal information, we found that these requirements may not be uniformly observed by agencies at all levels of government. In addition, in our review of SSNs in government agency-maintained public records, we found that SSNs are widely exposed to view in a variety of these records. While some agencies reported taking actions such as removing SSNs from electronic versions of records, without a uniform and comprehensive policy, SSNs in these records remain vulnerable to potential misuse by identity thieves. Consequently, in both instances, we suggested that Congress consider convening a representative group of federal, state, and local officials to develop a unified approach to safeguarding SSNs used in all levels of government. Some steps have since been taken at the federal level to promote inter-agency discussion of SSN protection, such as creation of the President's Identity Theft Task Force in 2006 to increase the safeguards on personal data held by the Federal Government.

In April 2007, the Task Force completed its work, which resulted in a strategic plan aimed at making the Federal Government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. The plan's recommendations focus in part on increasing safeguards employed by federal agencies and the private sector with respect to the personal data they maintain, including decreasing the unnecessary use of SSNs in the public sector. To that end, last month, OMB issued a memorandum requiring federal agencies to examine their use of SSNs in systems and programs in order to identify and eliminate instances in which collection or use of the SSN is unnecessary. In addition, the memo requires federal agencies to participate in governmentwide efforts to explore alternatives to agency use of SSNs as personal identifiers for both federal employees and in federal programs.

Vulnerabilities Persist in Federal Laws Addressing SSN Collection and Use by Private Sector Entities

In our reviews of private sector entities' collection and use of SSNs, we found variation in how different industries are covered by federal laws protecting individuals' personal information. For example, although federal laws place restrictions on reselling some personal information, these laws only apply to certain types of private sector entities, such as financial institutions. Consequently, information resellers are not covered by these laws, and there are few restrictions placed on these entities' ability to obtain, use, and resell SSNs. However, recently proposed federal legislation, if implemented, may help to address this vulnerability. For example, the SSN Protection Act of 2007, as introduced by Representative Edward Markey, would give the Federal Trade Commission (FTC) rulemaking authority to restrict the sale and purchase of SSNs and determine appropriate exemptions. The proposed legislation would therefore improve SSN protection while also permitting limited exceptions to the purchase and sale of SSNs for certain purposes, such as law enforcement or national security.

Vulnerabilities also exist in federal law and agency oversight for different industries that share SSNs with their contractors. For example, while federal law and oversight of the sharing of personal information in the financial services industry is very extensive, federal law and oversight of the sharing of personal information in the tax preparation and telecommunications industries is somewhat lacking. Specific actions to address these vulnerabilities in federal laws have not yet been taken, leaving SSNs maintained by information resellers and contractors in the tax preparation and telecommunications industries potentially exposed to misuse, including identity theft.

We also found a gap in federal law addressing SSN truncation, a practice that would improve SSN protection if standardized. Specifically, in our Internet resellers report, several resellers provided us with truncated SSNs showing the first five digits, though other entities truncate SSNs by showing the last four digits. Therefore, because of the lack of SSN truncation standards, even truncated SSNs remain vulnerable to potential misuse by identity thieves and others. While we suggested that the Congress consider enacting standards for truncating SSNs or delegating authority to SSA or some other governmental entity to do so, SSN truncation standards have yet to be addressed at the federal level.

Concluding Observations

The use of SSNs as a key identifier in both the public and private sectors will likely continue as there is currently no other widely accepted alternative. However, because of this widespread use of SSNs, and the vulnerabilities that remain to protecting this identifier in both sectors, SSNs continue to be accessible to misuse by identity thieves and others. Given the significance of the SSN in committing fraud or stealing an individual's identity, it would be helpful to take additional steps to protect this number. As the Congress moves forward in pursuing legislation to address SSN protection and identity theft, focusing the debate on vulnerabilities that have already been documented may help target efforts and policy directly toward immediate improvements in SSN protection. To this end, we look forward to supporting the Subcommittee and the Congress however we can to further ensure the integrity of SSNs. Related to this, we have issued a report on the Federal Government's provision of SSNs to state and local public record keepers, and we have also recently begun a review of the bulk sale of public records containing SSNs, including how federal law protects SSNs in these records when they are sold to entities both here and overseas.

Mr. Chairman, this concludes my prepared testimony. I would be pleased to respond to any questions you or other members of the subcommittee may have.

Chairman MCNULTY. I thank all of the witnesses. Thank you, Mr. Bertoni, especially for this new report, which you issued I believe today as a result of the inquiry by Senator Schumer.

Mr. BERTONI. Yes.

Chairman MCNULTY. That is now a part of the record of the Subcommittee, and we will certainly consider that in our deliberations. I want to thank Mr. O'Carroll for the time we spent together

recently to talk about issues generally regarding Social Security, and I want to thank you for your commitment to helping us to reduce the backlog, to keep the agency focused on its core mission and also the subject of today's hearing, protecting the American people from identity theft. I am glad to know we are on the same wavelength and working for the same purposes.

Mr. Winston, thank you also for your testimony. You mentioned this review of the Social Security number uses. Where are you on that, how long will that take, when can we expect to see some kind of a product on that?

Mr. WINSTON. As I mentioned, the Task Force issued its report in April, at which point we immediately put together a group of FTC and other agency employees to begin this review. In fact, this week, we are meeting with a number of officials from trade associations and business groups and others to try to find out more not only about how they use Social Security numbers but why and what it would cost in terms of money, as well as inconvenience of change.

Chairman MCNULTY. But just in line with my previous thoughts about this Congress actually doing something, when could we expect to see the results of your review?

Mr. WINSTON. The Task Force report calls for a report to the President by the first quarter of 2008. I suspect we will have information well before that that would be useful.

Chairman MCNULTY. Well, we would really appreciate any data that you could give us prior to that because some of us do not intend to wait around until 2008 to start moving legislation. At this time, I would yield to the ranking Member, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman. We are not going to wait until 2008, huh? Mr. O'Carroll, I remember some years ago the Social Security Administration was handing out new Social Security numbers to upward of 100 people—or 100 times to the same guy just by a phone call. Have we stopped that because we passed legislation to do it?

Mr. O'CARROLL. Yes, Mr. Johnson, that was one of the recommendations that came out after 9/11 when we started to ratchet down on the security of the number of it, and what we were looking at was multiple SSNs being reissued on it. We now have in the SSA systems because of our recommendations and because of your legislation, we are now being much more attentive to the number of cards going out, it is into the system. There are flags put up. We are taking a look at numbers of cards going to the same address, sort of the same type of similar thing with replacement cards. When 300 cards go to one address, it is what we call a "clue." So, we have been trying to plug up that hole.

Mr. JOHNSON. How do you do that?

Mr. O'CARROLL. Well, what we are doing with that is it is flagged, we get the information on it, and in our case we have been doing audit work on it where we actually go to the address what the address is. In some cases, it is legitimate in terms of it is a university or something where it is one entity but where it is an apartment building in some locale, we actually recommend that to our investigators and our investigators are going there, and we are

looking to find who is collecting those false cards and making arrests.

Mr. JOHNSON. Well, you mentioned your ongoing role to ensure homeland security, as reflected in the recent arrest of terrorists planning an attack on Fort Dix. Based on your experience to date, how are Social Security numbers and document fraud, how is that fraud being committed by potential terrorists or do you know?

Mr. O'CARROLL. Well, as we know with terrorists and in fact all criminals, everyone is trying to assimilate into the public. What happens is that we are finding in a lot of cases people trying to do that illegal assimilation are going to identity mills, and they are going to places where they are able to get immigration documents, Social Security cards, and we monitor that all the time and keep track in terms of the prices that going for it and just ways of monitoring. But we work very closely with Immigration, with FBI, in the case of Fort Dix, with the New Jersey State Police, all of them are a part of the Joint Terrorism Task Force up there, which we are a member.

What had happened in the case of Fort Dix was we found out that several of the suspects in it, in previous occasions in dealing with law enforcement, used false identities up to and including Social Security card fraud. I have got to tell you prosecutors use Social Security misuse, which is part of the legislation that came out this Congress, we use that as an enforcement tool, the misuse of the SSN to identify and arrest terrorist suspects.

Mr. JOHNSON. Good for you. Are you finding people from overseas asking for Social Security cards before they come over here?

Mr. O'CARROLL. Well, yes, and there are two stories to it. In terms of one, it is a good one because what is happening is before they get here, they go into an enumeration process where they are dealing with embassies overseas and they are being vetted by the embassy before they come here, which is a good technique. What we are finding, though, and we have done it in our audit reports, is that we find that only Social Security employees really put the due diligence into checking all the documentation, checking all the information, and we are finding that when SSA delegates that responsibility to other agencies to be doing it, we are not getting the same type of quality. So, in our audit report we recommended that Social Security work with State Department on making sure that the documents that are taken in those applications overseas are valid, are good and that they are legitimate needs for SSNs.

Mr. JOHNSON. Do we need to put anything in legislation to reaffirm that or is it clear enough now?

Mr. O'CARROLL. If you do not mind, let me check that and get back to you because I think at this point it does seem to be—it has been brought to State Department's attention, and I have got to tell you, it is a good program, and it is a fairly new one so we might be at a point now of monitoring it before we do any more recommendations for it. But I will check it and get back to you.

Mr. JOHNSON. Thank you, sir. I appreciate it.

Chairman MCNULTY. Thank you, Mr. Johnson. Mr. Levin may inquire.

Mr. LEVIN. Thank you, Mr. Chairman and Mr. Johnson, for having this hearing. When I read your opening statements, you mentioned, Mr. Chairman, this is the sixteenth hearing on this topic.

Chairman MCNULTY. It is time for action.

Mr. LEVIN. That the FTC receives between 15,000 and 20,000 contacts each week from those who have been victimized. Mr. Johnson, my pal, you say in your statement, according to the Privacy Rights Clearinghouse, since January 2005, that breaches have been over 155 million. So, the staff, as usual, has prepared some really incisive questions, but could I ask you this because this kind of jumps off the pages, what is the problem? What is taking so long? Why have we been having all these hearings and there are all these breaches and all these thefts? What is holding this up, what is holding you up? What is holding Washington up?

Mr. WINSTON. I guess I cannot answer the question about why you have had so many hearings but as far as what is holding up the FTC and the other agencies that have been working on this problem, we have been working diligently on it. We have done a lot of law enforcement. We have done a lot of outreach. I think additional legislation would be very helpful in making it easier for us to tackle this problem.

Mr. LEVIN. You are an active participant in crafting this legislation?

Mr. WINSTON. Yes, we have been involved. We have provided technical assistance to different Committees and the different sponsors. We have urged Congress to pass national data breach notification standards and national data securities standards. We think that is critical in this fight.

There are a lot of steps that are being taken but it is a complex problem and it is an ever-evolving problem. Identity theft is everything from your cousin going up in your bedroom and stealing your wallet to international crime rings hacking into computer databases and getting records. In tackling it, we need to tackle it from every angle, as I mentioned.

Mr. LEVIN. Okay, so it is complex but if we go home and talk to our constituents and we say about any problem, it is complex, it changes their complexion, they get kind of red. So, I will ask the two of you, Mr. O'Carroll and Mr. Bertoni, what is the problem? Why is it so difficult? Why haven't we acted besides its complexity?

Mr. BERTONI. As far as why you have not acted?

Mr. LEVIN. Congress and the Executive and all of you?

Mr. BERTONI. I think as far as the pressures on the Congress, there are interests on the other side of this issue that make the case that commerce and business to business information sharing and ultimately customer service will deteriorate. I think that argument has been heard. It points—it stalled forward progress in terms of making sure that other industries have similar protections in terms of their information security and disclosure similar to the financial services institutions, in particular the telecommunications and tax preparer industry. That bar is lower, and we have concerns that that bar is lower, and we believe at a minimum it should be raised at least to the level of the financial services community. So, I guess the roundabout answer is there are arguments on both sides and at some point which one will win or which compromise

will prevail, that is something for you all as policy-makers to work out.

Mr. LEVIN. I think that is a useful answer. Mr. O'Carroll, you get 30 seconds to explain why there has not been more action.

Mr. O'CARROLL. I guess I better talk quick. I think there has been a lot of action in terms of when I came to this inspector general's office 10 years ago, the Social Security number was out there, it was being used as the primary identifier on virtually every document up to and including the driver's license. In the time that I have been here, it is now off of the driver's licenses. The Social Security statement, which goes out every year to every citizen, has a truncated number on it now. When government checks went out, they had a Social Security number in the window on the check, that stopped. I got to say it has been a long haul doing it because of the convenience factor. Everyone used the Social Security number as a convenient tracking number, and it has been really our mission to try to get it back into the box through all this time. The Social Security Protection Act was some steps in the right direction, it took us a number of years with this Committee to get that through, and I think if you could do another act of this kind with more controls over the Social Security number, that would probably be the benefit of this Congress.

Mr. LEVIN. Thank you. Thank you.

Chairman MCNULTY. Thank you, Mr. Levin. Mr. Lewis may inquire.

Mr. LEWIS OF KENTUCKY. Thank you, Mr. Chairman. Going back to the balance that you were talking about there, Mr. Winston, in your testimony you stated that restrictions on the Social Security number should be reduced to unnecessary use without inadvertently burdening necessary use. Could you explain what you believe to be necessary and unnecessary use?

Mr. WINSTON. Yes, I think the H.R. 948 really goes at it the right way. It lists—it basically bans sale and purchase of the Social except for certain specific purposes, law enforcement, public health and safety, for credit verification, for fraud prevention. Then it says that the FTC should do rulemaking in order to flesh out those exceptions and add additional ones if it determines that it is appropriate. I think that is the right approach.

Mr. LEWIS OF KENTUCKY. Mr. Bertoni, would you want to comment on that too?

Mr. BERTONI. In terms of the balance, striking a better balance, as I said before, I think it is important that actions taken do not upset the free flow of commerce, the ability of businesses to share information. But as our report, as we continue to say in our reports, there are still industries that still fall we believe way out of the parameters in terms of a reasonable amount of regulation and control in terms of their information security and disclosure policies. Again, at a minimum, if you looked at what has happened in the financial services sector, that sector has not grinded to a halt. There have been changes made. We are asking the Congress to look at some of these other sectors to see if that bar could be raised. Again, there would be some compromises to be made, but we also believe there are soft spots and areas to be strengthened in several of those areas.

Mr. LEWIS OF KENTUCKY. Mr. Winston, of course all of you I think would agree that if we could authenticate the consumer or the customer, we would go a long way in stopping thieves. I know you have been looking at that, Mr. Winston. What have you come up with as far as finding a good way to authenticate the people who are out there?

Mr. WINSTON. We did hold a 2-day workshop on this subject with lots of people from all over the world coming in to talk about their experiences. I think what came out of that was that there is no panacea. There is no one perfect way to authenticate. If there were, thieves, who are very smart, would come up with a way to defeat it. So, what we are seeing more and more of are multiple layers of authentication, not just one piece of information but a biometric, a thumb print, an iris scan, plus an identification number or pin number. So, there is a lot of movement in that direction and government can facilitate that and encourage it. It probably is not a wise thing for government to come in and say this is how you have to authenticate consumers.

Mr. LEWIS OF KENTUCKY. Okay, thank you.

Chairman MCNULTY. Thank you, Mr. Lewis. Mr. Becerra may inquire.

Mr. BECERRA. Thank you, Mr. Chairman. Thank you all for your testimony. Let me ask a question. My understanding is if we were to try to re-issue the Social Security number to try to take care of discrepancies and to try to give people a new number that is not out there in the public domain, and if we were to try to give it some type of enhanced security, a photograph or some type of biometric, we are looking at somewhere in the order of about \$10 billion to do that. Is that—I know a rough estimate but is that still more or less an estimate, Mr. O'Carroll?

Mr. O'CARROLL. It is a moving target, Congressman, in that it depends on the type of—what features would go into the new card, whether it was a biometric.

Mr. BECERRA. Give me a rough estimate.

Mr. O'CARROLL. I say that just a rough off-the-top of my head number, that would be a good number, the \$10 billion but with a lot more "but's" to it.

Mr. BECERRA. I understand because I want to move off of that, I am just trying to get a rough sense of things, so about \$10 billion gives you a new card that might give Americans enhanced security. Right now SSA would swallow that cost, Congress would have to provide you with the money to do that, otherwise it would be impossible to actually administer because there will be tremendous cost trying to get folks to come in with their birth certificates and whatever else they will need to try to identify themselves for purposes of getting this new card. Okay, so let me ask this, who should pay for the establishment and maintenance of a new identity system, identification system, taxpayers or the users? Because right now the Social Security number imposes no cost on any consumer, any business if it is used solely for the purpose of identifying how much you have earned for Social Security purposes in the future.

That the taxpayers I think we are willing to bear because we are going to get the benefits of the Social Security system in the future. But as it is right now with identity theft, with business losses

mounting into the billions, tens of billions of dollars, there are lots of costs involved in trying to secure your identity or restore your identity or for a business to try to reclaim losses. I hear no talk about who is going to pay for giving us a more secure system, the taxpayers or all the consumers, meaning the businesses and actual individual consumers, who would utilize that increased security that would come from a new identification system that may be housed within Social Security?

Mr. O'CARROLL. Okay, not to be argumentative but why would Social Security be the vehicle for this new identifier?

Mr. BECERRA. That is a good question.

Mr. O'CARROLL. Be put back on to the management of the Social Security Administration when we have a good number now that is doing what it is supposed to do in terms of tracking wages and tracking benefits on it and the commercial half is the other one.

Mr. BECERRA. Let's take that path, say we say the Social Security number will be used only for Social Security purposes. Disability benefits, retirement benefits, death benefits.

Mr. O'CARROLL. Tax purposes.

Mr. BECERRA. That is not necessarily Social Security but we have ventured into at least taxes for purposes of the use of the Social Security number but for other reason, but then what would you suggest or does Social Security what would be used as that identifier that used nationally for whether it is consumer purposes or other types of purposes?

Mr. O'CARROLL. I thought I did a pretty good job of batting this away from Social Security.

[Laughter.]

Mr. O'CARROLL. I am thinking I might yield my time to one of my esteemed panel members.

Mr. BECERRA. Let me ask Mr. Bertoni that question is because what I am trying to get a sense—those must all be the folks from GAO who are laughing back there, I am just trying to get a sense, we are going to have do something but who should pay it? My sense is that the taxpayer should pay something because ultimately we are all taxpayers, most of us are taxpayers, and we want to have that security. But I am not out there selling my identification number to identity thieves. I am not the one that tells a particular business or government agency use my number for some other purpose, whether it is for purposes of registering a divorce or buying a refrigerator. So why should the taxpayer then foot the bill to make this card, if it is used for Social Security, to make it more secure?

Mr. BERTONI. Again, that is certainly a policy question. I can tell you how it is now. SSA has certainly—

Mr. BECERRA. I do not want to know how it is now, give me a sense, who should pay?

Mr. BERTONI. I think there are models out there where you could construct a different model where others could pay outside of the agency.

Mr. BECERRA. "Others," identify "others"?

Mr. BERTONI. I am just considering say the driver's, and I am not advocating, I am just kicking something around here, there are

models where people who are buying the card or buying the service, which is a driver's license, would be asked to pay a fee for that. I am not aware of any models where say beneficiaries of a particular card or identity card, such as a SSN, like an information re-seller, would have to pay. I cannot talk to that because I am not aware of that model. The only two models I am aware of are the agency footing the bill or the purchaser of the license or the card, historically that has not been something that SSA has wanted to do. Beyond that, again, I think that is an option, a policy option for Congress to consider.

Mr. BECERRA. A user fee of sorts?

Mr. BERTONI. There are models but I am not advocating that.

Mr. BECERRA. No, I understand and I thank you for your comments. Mr. Chairman, thank you very much. I know my time has expired.

Chairman MCNULTY. Thank you, Mr. Becerra. Mr. Ryan may inquire.

Mr. RYAN. Thank you, Mr. Chairman. I guess I will pick up where Mr. Becerra left off because this issue has so many sources, so many directions. It interweaves all of these problems we have got, terrorism, immigration, all of these things, so we have some no-brainers, unify the truncation standards, right, and some other easy low-hanging fruit things. At the end of the day, it seems like what we are headed to is how do we, A, authenticate people and, B, kind of clean up the database in Social Security and stop the mission creep of the number being used, these are pretty much the two issues here, right? So now we are being faced with this sort of fork in the road, do we do a Social Security card, do we just fix the Social Security card, put \$11.7 billion, \$10 billion, whatever this number is, and make the Social Security card better with biometrics and a centralized Federal database or do we go a different route? I guess that is kind of the fork we are in right now.

Let me ask just each of the three of you, if we go down this path of a better 21st Century Social Security card with the biometrics and all of this, do you believe that given the way the market works, given the way identity thieves work, that a Social Security card under today's technology can be implemented and can be successful for the long term from preventing identity theft and all that. I will just ask the three of you, just go down the line, however you want to start, Mr. O'Carroll?

Mr. O'CARROLL. I will tell you, Mr. Ryan, we have done a lot of looking at Social Security cards in terms of whether to use different type of stock for it, different printing for it, whether to put biometrics into it, everything else, and I have got to tell you what we have found by looking at just history in general is when whenever the government comes up with any type of a document, a form or whatever, especially if there is going to be some financial gain in figuring out a way of compromising it, the counterfeiters usually do figure out a way to compromise it. So, even when you say, if we come up with one, do you think we will get a few years out of it before somebody does it, then all of a sudden you are going to go back to the thought of another \$10 billion of coming up with a new card.

Mr. RYAN. Yes.

Mr. O'CARROLL. So, what we are advocating on this is that it is the number, it is not the card, and if we can put more time, effort, whatever into the system work on it, where we are getting good, positive hits on terms of when information is put in, is this the right person for it, and that is again what I am saying with this is that the first step on this thing is really with the government in terms of right now the agencies going to each other, basically work on that type of thing, the technology for it, that is a big step in the right direction.

Then at the time, which kind of goes back to what we were talking about before, is when you are talking in terms of the financial sector and all the other forms of identity that are being used, our recommendation is to use different numbers than the Social Security number for it. The one that I am always sort of cautious on with this thing is with the Social Security number, I think we have done a very good job about it, is keeping it, at least in terms of the government, for the government uses of it, and not having it become a national identity document, which is kind of the role where if you got into biometrics and hard cards and that, it is a whole other step.

Mr. RYAN. So, we could get ourselves on the slippery slope, but I want the other two of you to comment. Let me throw this at you as well. Tell me if I am wrong, we are at this fork, do we go down this sort of unifying national ID card route, which has all of the Orwellian and privacy and obsolete issues associated with it, or can the market produce ever upgraded standards on helping people authenticate who they are and give people the tools in the marketplace to be able to authenticate their identity and then you clean up the Social Security number itself and then people can operate through society by preventing identity theft and being able to authenticate who they are and the government does a job of basically saying this particular authenticating agency or company is correct, they do a good job. The government can do a job of making sure that a business that wants to market itself as an authenticating entity, has the Good Housekeeping Seal of Approval, can do that, is that the path that we go down, meaning instead of the national ID card, do we have institutions that are out there in the private sector that can be authenticators of people or not? Do you understand what I am trying to get to? I would like to just ask you to consider that as well and give me your take on that.

Mr. WINSTON. Sure. Mr. Ryan, I think what you are—

Mr. RYAN. Yes, I am not doing a good job of explaining myself.

Mr. WINSTON. No, actually you are.

Mr. RYAN. Okay.

Mr. WINSTON. What you are playing out I think is the very debate that is going on with the real ID act. There are certain advantages to that, of course, of having one ID card for everything. It is easy to use, hopefully it is secure, but there are down sides and there are privacy issues and there are cost issues that are very serious. My own view is that maybe another way to go is to further develop what is happening now, which is multiple forms of authentication, not having one form of authentication for every purpose but in different sectors having different forms of authentication. It can be a pin, it can be a biometric. That is much harder for an

identity thief to break into. There are convenience issues, of course. Consumers do not want to memorize 15 different passwords, but I think there is ongoing a development of better, useable forms of authentication that I think have a good chance of solving this problem.

Mr. RYAN. Mr. Bertoni.

Mr. BERTONI. There is a lot in that question. I think one thing we need to consider early on is given that we have real ID there, do we want to go forward with a parallel path of having a Social Security card with very similar secure features? I think you could create some redundancies that do not need to be there. So, there is an issue for the country to consider in terms of what will it be, will it be real ID, will it be the Social Security number? We issued a report last year that talked about the pro's and con's and options, and I can provide you some of that.

But, again, to step back, even before we talk about who does it and what we might use, there are real implementation issues to consider with just the Social Security Administration. With 300 million cards issued out there, how do we do it? Is it laddered? Is it all at once? Who gets it first? Prior to 1978, there was very little fraud verification for people seeking a SSN. These people could come forward now, get their Social Security card, and we really did not do a good job of verifying who they were in the first place. So, we have millions of people with these pre-1978 cards that they are going to walk away with an ID card that is going to be what most people conceive to be bullet proof, and they may not be who they say they are. That is an issue.

I think in terms of data cross-matching, we have gone on record at GAO that short of new cards, biometrics, there is a lot that the public and private sector can do in terms of data cross-matching, using various elements, not just the Social Security number. Truncation is a great protection. It should be part of the verification scheme, but there are new models out there where they use multiple data points to give the verifier a higher comfort level that you are who you say you are. So, that to us is certainly something that needs to be considered and moved on.

Mr. RYAN. I assume my time is up. Thank you, Mr. Chairman.

Chairman MCNULTY. Thank you, Mr. Ryan. Ms. Schwartz.

Ms. SCHWARTZ. Well, thank you. I am going to try and take us off the discussion of a national ID card. I am not sure we are anywhere near any agreement about the need for such a thing and who would do it and how we would pay for it and how we would protect people's identification. I think pulling us back if we could just a little bit to the use of the Social Security number and kind of risks we are already engaged in. It seems to me we ought to take care of that first, and we have not done that yet. So, let me just understand here, the feeling so far is that you do not, and I guess it would be the Social Security Administration, does not have the authority to restrict the use of Social Security numbers, I think that is a simple yes or no?

Mr. O'CARROLL. Yes.

Ms. SCHWARTZ. You do not have the authority, you do not?

Mr. O'CARROLL. Correct. There is no authority. Once it is outside of Social Security, it is out in the public, we have no authority to restrict.

Ms. SCHWARTZ. So, individuals ask for it, they give it—we all have, as you pointed out, hospitals, universities, schools—

Mr. O'CARROLL. But we can recommend people say no but we cannot enforce them not to ask.

Ms. SCHWARTZ. You do not also feel that you have the authority to set standards about its use? For example, you mentioned display, I think all of us have actually seen from what hospitals used it at some time or health centers might have used it as their patient chart number. It was on my Blue Shield insurance card for years, how hard was that to figure out, it said Allison Schwartz and my Social Security number, I think they would probably have assumed it was my husband's just out of sexism but it was actually mine, and I had my insurance. They only just recently have changed that, I assume, because of the concerns about identity theft. So, the question is do you feel like you could not even or you do not have the authority now to set standards about display or use or protection of a Social Security number used by any kind of private entity?

Mr. O'CARROLL. Correct. There is very limited use. One of the limits that is on it is that when it is falsely used in advertising, and we can enforce that. That is the one where you get in your mail a document that looks like it came from the Social Security Administration, it is using the logo, and that type of stuff. We can restrict that type of use but the other types of uses where Radio Shack is asking for your Social Security number, we cannot. That is where this is very difficult because once it got out of SSA and got into the economy, it started becoming that financial tracker.

Ms. SCHWARTZ. Hence, the need for us to take some action to—

Mr. O'CARROLL. Yes.

Ms. SCHWARTZ [continuing].—Limit the use in the private sector and attempt to set some standards or suggest who does set the standards on how they protect this very sensitive information.

One other question for you. The IRS, as you well know, has been subcontracting with private collection agencies to collect taxes. The first thing they ask is for the Social Security number. We had a hearing which revealed the fact that individuals are very hesitant, appropriately, to give someone who just says, "Hi, I am Susan, I cannot tell you why I am calling, I have to make sure I know who I am talking to first, would you give me your Social Security number?" It is just stunning actually that this is a government-authorized activity. Now, many people do not give their Social Security appropriately but some do. Now, do you know if you or the IRS has set very careful limits on the protection of those Social Security numbers once they get them, these are now private agencies?

Mr. O'CARROLL. Well, it is interesting that you bring that up. One is that you, as you noticed there, what we are saying is when somebody calls you up on the phone and asks for your Social Security number, do not give it, which reinforces that. But then with secondary information and back and forth, trust with information and know that what they are calling about is a transaction with

the government, there is that. But what we have done, and we have gone to the Department of Treasury, is that we have asked all other—we have asked 15 other inspectors general to take a look at their departments and the use that they have of Social Security numbers, up to and including contractors, which is what you are talking about, and in 2001, six years ago, there was very little control over that. There were no real limits on it, nothing was in the contract about safeguarding the Social Security information and that.

In a follow-up that we did about a year ago, those same 15 agencies were finding out—and they are all the biggest departments—were finding out that, yes, they are safeguarding their own information, one, they are too cautious on disclosures of it, so any of their documents, they are very cautious to not have Social Security numbers.

Ms. SCHWARTZ. The department is or the subcontractors are?

Mr. O'CARROLL. These are the departments and then each of the departments are asked at their subcontractors and whether the contractors were abiding by security of any Social Security number information, and we found that they were.

Ms. SCHWARTZ. So, you have done a study?

Mr. O'CARROLL. Yes, and so we keep doing that to make sure that the Federal agencies are looking at subcontractors and making sure, like in this instance, that there is protection on it. OMB, under the new PII guidance, is also reinforcing that. So, I have got to say at least government-wise and government contractor-wise, we are being very—much more astute or much more attentive to that issue.

Ms. SCHWARTZ. So, the concern is really much more in the private sector and the use of these numbers in the private sector.

Mr. O'CARROLL. Yes.

Ms. SCHWARTZ. We have had other hearings but we really need to do something to give you the tools and the authority, I am looking at both you actually, exactly how we will write all this legislation I guess remains to restrict the use of the Social Security number and to set very clear standards about its use. It is pretty stunning how it has been used. So, thank you very much. Mr. Chairman, I think my time is up.

Chairman MCNULTY. Thank you, Ms. Schwartz. Ms. Tubbs Jones.

Ms. TUBBS JONES. Thank you, Mr. Chairman. You do, sir, however the authority to restrict more than one person using the same Social Security number though, do you not?

Mr. O'CARROLL. Yes, we do.

Ms. TUBBS JONES. That is as big a dilemma in government as anything else is with regards to Social Security numbers, correct?

Mr. O'CARROLL. The misuse of the SSN and the legal use, yes.

Ms. TUBBS JONES. Yes, and so we have many employers who employ people in the United States of America and they in the same company and more than one person using the same Social Security card number, Social Security number, excuse me, not a card but the number?

Mr. O'CARROLL. Yes.

Ms. TUBBS JONES. What are we doing about that?

Mr. O'CARROLL. Well, we are working in terms with Immigration to be taking a look at what is called the basic pilot, which is the verification program, that when an employee applies for a job, we verify the SSN as being a legitimate SSN and a legitimate name and the basic information of male, female, date of birth on it. That is being done.

Ms. TUBBS JONES. So, what is your enforcement?

Mr. O'CARROLL. Excuse me?

Ms. TUBBS JONES. I am going to interrupt you because I do not have but 5 minutes.

Mr. O'CARROLL. Sure, hey, we are coming from the same place.

Ms. TUBBS JONES. So, what are your enforcement tools for that purpose?

Mr. O'CARROLL. Well, enforcement tools on it is the misuse of the SSN, we use that violation when people are misusing it, and as an example when we were talking about the Fort Dicks terrorist investigation, we worked with ICE every day of the year where people are misusing SSNs and where they are charged with it. Unfortunately, prosecutors are not the most thrilled with that type of a prosecution unless it is in large numbers.

Ms. TUBBS JONES. I am not talking about terrorists, I am talking about the employers who allow the use of more than one person to use a Social Security number, what are we doing about those employers and what are our enforcement tools and what have we done?

Mr. O'CARROLL. We are going after them. We just had a recent case in Massachusetts in which an employer was telling any new employee coming in if they did not have a Social Security number, go to this location and they will give you a Social Security number. They were getting counterfeit Social Security numbers going to work for this employer and the employer was arrested.

Ms. TUBBS JONES. Do you have any numbers? If you do not have them with you today, I would be interested on how many employers we have prosecuted for allowing employees to use—more than one employee to use the same Social Security number, I would be interested in having that?

Mr. O'CARROLL. I would have to respond back on that. I am not sure whether it is a large number but it is a number, and I will get it for you.

Ms. TUBBS JONES. I will tell you what, I am not sure either, but I bet money that it is a large number. I am laughing—not laughing but I just pulled out my Ohio Public Employees Retirement System prescription drug card, it has got my Social Security number on it, broad as day. That is my ID number. I guarantee you there are a whole lot of others out there that are using that.

It is easy for us to sit in this room, and I am not going to be a holier than thou person, but it is easy for us to sit in the room and have a discussion and be congenial in the course of our discussion about what we are going to do about Social Security numbers, and I have only been in Congress 9 years and I am sure, as we said, we have been sitting here having these nice little collegial discussions about the impact and that is why we end up where we are right now with the misuse and identity theft of Social Security numbers.

I just would hope that even in our collegiality, that in 2007, that we will move forward to accomplishing some real things because all of us sit here and say, "It is right here on my card. I call in to the bank, I want to get my bank account number. I have got to give my Social Security number, my mother's maiden name," and on and on. We have accepted it as just part of the living in the United States of America and accessing information, but we have got to get further ahead and be serious about how we involve this. After that nice little piece I have done, Mr. Chairman, I thank all of you for the work that you do, but tell us what you need, let's do it, let's not just sit here and allow people to continue to be put in harm's way as a result of misuse. I thank you, Mr. Chairman, for your time.

Chairman MCNULTY. I thank Ms. Tubbs Jones, and I want to assure her that Mr. Johnson and I have expressed our determination to move forward with some legislation rather than just talking about the issue. Mr. Ryan has an additional inquiry.

Mr. RYAN. Thank you, Mr. Chairman. Mr. O'Carroll, I wanted to follow-up on Ms. Tubbs Jones question, I want to ask you about these no-match letters. This happens to us all the time where we will have an employer that will call or write us and say they have received a no-match letter from the Social Security agency where they said, "Well, we have found that five people are claiming the same number, we do not know if your employee is the right person or the wrong person. You cannot fire the person, we are going to do the investigation." Then they typically have no follow-up from thereafter. So they are caught.

So can you just walk me through what is the process and the procedure at SSA, do you have what you need to do to find out who people are or who they are not? How do you do this, do you just do random audits of your database to see more than one claim on a Social Security number? What do you do when you find four or five people claiming the same number? What is the outcome? Can you just explain this briefly to me?

Mr. O'CARROLL. Well, when the tax information goes to SSA and that information is run against the SSA database, that is where the no-match's are coming out. It is all automated, it is automatic, a letter is automatically sent out to the employer.

Mr. RYAN. So, every no-match that comes in is identified?

Mr. O'CARROLL. Yes.

Mr. RYAN. Those that can be identified with an employer, a letter is generated on it to that employer. Really it is an automated process. On occasion, if there are a lot of them, SSA will contact employers with a liaison service to see if they can help them but for the most part it is a pretty passive action, where the letter goes out, the employer is notified, the employer knows that the information that he is given is incorrect and basically he or she is instructed to contact the employee and straighten it out. Then also the employee is recommended to go to Social Security and Social Security will then straighten it out with the employee.

Mr. RYAN. But since the employer just has an I-9 Form he or she has to fill out, which they have to have some document, one of what 29, I think thrown in front of them, they do not know whether the person is legitimate or not, whether they are illegal or

not, how then does the person proceed? They send the person to the local Social Security office and then it is up to the Social Security to use their best judgment to determine whether the person they say they are or not, is that basically how this follow-up occurs?

Mr. O'CARROLL. A lot of people follow up with the employee on it, yes. But I have got to tell you in most cases, it can be rectified at the employer/employee level in terms of the person does have the work documents, the other documents for the employer to look at and it can be resolved at that level. I have to tell you one of the down sides of this one is that in many cases by the time the employers are getting these no-match letters, especially in transient type industries, that employee is long gone and that is probably the biggest issue on this thing is that, and it is one of the biggest problems with misuse of SSNs in the application process of it is that if that person used false identification or purported to have a false identification, was turned away from SSA initially or whatever, we are never able to find that person because the information was all false that they had and they are gone into society.

That is probably the biggest problem with the no-match letters is that most cases are the biggest violators—or not violators, the biggest recipients of no-match letters are large industries are very transient. That is probably the biggest issue of it is that that employee is no longer there because it is a year later when the tax information comes in.

Mr. RYAN. But it also seems like the way the system is configured now, a person could still get away with possessing a wrong Social Security number even through this system, correct?

Mr. O'CARROLL. Yes.

Mr. RYAN. Even after the no-match letter person who really is not who they say they are, using some other Social Security number, could still continue using it?

Mr. O'CARROLL. That does happen, yes.

Mr. RYAN. All right, thank you. Mr. Bertoni?

Mr. BERTONI. Yes, we did some work on that last year, the electronic suspense file whereby wages that do not match, the name, date of birth, Social Security, end up in this file with billions of records and, yes, in fact we have seen Social Security numbers with all zeros, all 9s, all 8s, "ABCDEFGH" that are being used and people are working under them. We have recommended to IRS, DHS to pick up the enforcement effort.

Mr. RYAN. Thank you.

Chairman MCNULTY. Thank you, Mr. Ryan. If there are no further inquiries, I want to thank Mr. Bertoni, Mr. Winston and Mr. O'Carroll for your testimony. It has been very helpful. We do intend to try to move legislation. I would ask that the witnesses continue to be available to the Members and our staff as we try to move in that direction, thank you very much.

In the interest of time, while panel three is coming to the podium, I would just like to introduce the Members of the panel. We have Justin Yurek, president of ID Watchdog of Denver, Colorado; Stuart Pratt, president of Consumer Data Industry Association; James D. Gingerich, director, Administrative Office of the Courts of the Supreme Court of Arkansas, on behalf of the Conference of State Court Administrators; Annie Antón, associate professor of

Software Engineering, North Carolina State University, on behalf of the Association for Computing Machinery; Marc Rotenberg, executive director of the Electronic Privacy Information Center; and Gilbert Schwartz, partner of Schwartz & Ballen, LLP, on behalf of the Financial Services Coordinating Council.

I want to thank all the witnesses for being here and sharing your expertise today and for your patience in waiting for the other two panels to testify. All of your statements will appear in the record in their entirety. We would ask each one of you to summarize your statement in as close to 5 minutes as you can. Just keep an eye on the little device in front of you to give you an indication when you should wrap up. So with a summary of your testimony, it leaves a little bit more time for Members to make inquiries. I think we will start with Mr. Yurek and go right down the line and hear everyone's testimony first and then allow the Members to inquire. Mr. Yurek?

**STATEMENT OF JUSTIN YUREK, PRESIDENT, ID WATCHDOG,
DENVER, COLORADO**

Mr. YUREK. Thank you, Mr. Chairman and Members of the Committee. My name is Justin Yurek and I am the president of ID Watchdog Corp. ID Watchdog is an identity theft detection and resolution company that helps consumers to protect themselves from, and resolve issues related to, identity theft. Our firm experiences firsthand the pain and suffering of the consumer at the hands of identity thieves and it is this pain that I wish to highlight to do. Ultimately, the question of legislative reform comes down to an analysis of the expenses incurred by business and government and restricting access to sensitive data, such as Social Security numbers, versus the benefit such action would afford consumers. I wish to illustrate these benefits to consumer victims by way of case study. Rather than dealing with faceless statistics, I would like to tell the story of one of ID Watchdog's clients. I believe there is great benefit in looking at the specifics of his one case to determine general facts about all identity theft.

We first met our client, Charlie W., in April of 2006. Initially, Charlie asked us to perform a full background check to ensure that his personal data records were accurate. ID Watchdog pulled data from thousands of databases that cover 13 crucial areas of consumer information. The shocking results revealed the following incidents in Charlie's name which he was not responsible for. I apologize for the laundry list I am about to say, but I think all the details are important: Four traffic citations in Florida, Washington and Arizona; three felony arrests for assault and harassment in Washington; a conviction for assault where he served, supposedly, 144 days in jail in Washington; an active national warrant for arrest in Washington for bail jumping; an active warrant for arrest in Arizona for failure to appear; a newly issued driver's license in Florida; several thousand dollars of unpaid medical bills in Washington and Florida; and several thousand dollars of phantom 1099 income dating back to 1996.

A practicing Buddhist, Charlie had never had so much as a speeding ticket, let alone felony arrests for assault. Additionally, Charlie was a resident of Colorado and had never been to Florida,

Washington or Arizona. Dismayed, he immediately engaged us to assist in restoring his name.

A few weeks after Charlie engaged ID Watchdog to help him, his employer did a routine background check. As a result, Charlie was called into an office where he was to be fired, arrested and sent to Washington to face the active warrants there. We quickly intervened on Charlie's behalf and by providing photographs and fingerprints were able to save Charlie, termination, arrest and extradition.

Along side these very direct problems, Charlie also suffered significant secondary problems. First, his access to loans in order to finance and expand his business was limited due to his damaged credit reports. Second, he paid inflated car and medical insurance rates as a result of his damaged driving and medical records. Third, Charlie paid inflated interest rates on his mortgage and other lines of credit due to his unfairly lowered credit score.

A month later, the thief who was plaguing Charlie's identity was tracked to a car dealership in Louisiana where he was attempting to purchase a new vehicle using Charlie's identity. We immediately alerted the local sheriff's office who dispatched an officer to confront the thief. Once on the scene, the officer found that without an active warrant in Louisiana, he did not have proper cause to arrest the thief and planned to let him go. In response, ID Watchdog quickly called law enforcement officials in Washington state to have them fax over the active national warrant to the Louisiana authorities. After the Louisiana parish sheriff's office was able to verify that the warrant was still active, the thief was finally arrested.

The thief's real name was Hugh P. For more than 10 years prior, Hugh had stolen Charlie's wallet, which contained his driver's license and health insurance card. The health insurance card had Charlie's Social Security number printed on it. Over the years, Hugh had used Charlie's identity in every brush with law enforcement, whenever he needed medical treatment, and whenever he had 1099 income which he did not want to claim for tax reasons. In Hugh's own words, "It was very easy to use his ID and Social Security number. No one ever looks twice at them. To be honest, I never dreamt I would be caught."

The case of Hugh and Charlie illustrates the key problems with the system as it stands today. Social Security numbers are overexposed and overused, giving thieves too much access to sensitive data. Entities lack standard client authentication procedures leading to easy proliferation of the crime and law enforcement agencies lack multi-jurisdictional cooperation and effective laws leading to ineffective investigation and prosecution of the crime, as well as fearless criminals.

I applaud the Committee's commitment to this topic. As discussions continue, I would ask that you focus on the three previously mentioned areas when considering new legislation: Easily accessible Social Security numbers, lack of client authentication practices and lack of multi-jurisdictional cooperation and effective laws are at the heart of the crime's popularity with criminals and therefore must be at the heart of any legislation aimed to stop identity theft.

Finally, as the Committee continues to develop improved legislation, I would ask they keep in mind individual stories, such as Charlie's, and the trials and tribulation that he experienced. After all, hardworking, innocent, upstanding individuals like him will be the true beneficiaries of effective legislative change.

Thank you very much.

[The prepared statement of Mr. Yurek follows:]

**Prepared Statement of Justin Yurek, President,
ID Watchdog, Denver, Colorado**

Mr. Chairman and members of the Subcommittee,
My name is Justin Yurek. I am the president and co-founder of ID Watchdog, a Denver-based identity theft detection and resolution company. Since 2005, ID Watchdog has assisted identity theft victims in resolving identity theft related problems.

Our comprehensive process encompasses all aspects of identity theft from detection of the crime, to scoping and resolution. During the process, ID Watchdog takes a limited power of attorney and actually carries out the recovery process on behalf of our clients. Based on this experience, we believe that we have a unique perspective on identity theft as we have interfaced with all applicable entities involved in the problem—from law enforcement, to government, to creditors, to collection agencies, to reporting agencies, and so on. In addition, our diverse client base has given us the opportunity to deal with all types of identity theft—from financial, to criminal, to medical, to family identity theft, etc.

I appreciate the opportunity to share our broad-based familiarity with the topic of identity theft and am happy to speak today about the role of Social Security numbers (SSNs) in identity theft and about the need to enhance SSN privacy.

Introduction:

The purpose of my testimony is to underscore the plight of the consumer in the problem of identity theft. Often the problems of the consumer are overshadowed by losses sustained by business interests affected by the crime. Unlike the direct-losses absorbed by businesses, the effects of identity theft to an individual victim are consequential damages, and therefore less quantifiable. Nonetheless, the effects of identity theft to individual victims are devastating. The problem of identity theft is not a simple one and unfortunately continues to grow at an alarming rate. Identity theft is the fastest growing white collar crime in America; growing from fewer than 100,000 cases in 2000 to over 10 million new cases in 2006. At the same time that raw incidents of identity theft have grown, so has the scope and nature of the crime itself. While largely associated with financial consequences, identity theft crimes have gone well beyond credit reports into other more troubling areas. According to Federal Trade Commission statistics, only 30 percent of crimes reported last year were related to financial and credit report relevant matters. The newest and fastest growing segments of identity theft include medical, tax, and criminal related identity theft.

As the scope and nature of the crime broadens, we also see the time and energy required to recover from the crime increasing. We are now faced with a crime that is happening to more individuals and is simultaneously escalating in severity and consequence for the victims. With current protections, identity theft is not a matter of "if" for consumers; it is a matter of "when," as everyone will ultimately become a victim to some degree. These trends cannot be allowed to continue and the Subcommittee is in an excellent position to affect significant improvement on the current identity theft epidemic by enacting legislation that would directly affect the dissemination, use, and misuse of the social security number—undoubtedly the most important weapon in an identity thief's arsenal.

The Social Security number was not designed to serve as a universal, unique, personal identifier. However, it has developed over time to fill that role in government, military, public and private sectors. Despite becoming the de facto standard, there have been very few formal development efforts for the protection of this important identifier, resulting in a dangerous imbalance between the importance and accessibility of the SSN on one hand, and the protections afforded to the individual on the other.

I will detail a few case studies from ID Watchdog's own client base to show the problem of identity theft from a consumer point of view. I hope to illustrate the desperate need for legislative reform to ease the damage inflicted to a rapidly growing number of citizens.

Charlie W. realized that he was an identity theft victim when we performed a full background check on him in April of 2006. Analyzing thousands of reports in 13 crucial areas, ID Watchdog found the following fraudulent activity in Charlie's name: 2 traffic citations in Florida, several thousand dollars in medical bills in Washington, a traffic citation in Washington for driving with a suspended license, 3 felony convictions in Washington, a record of 144 days spent in jail in Washington, a warrant for his arrest for bail jumping in Washington, an arrest for DUI in Arizona, a second warrant for his arrest for failure to appear in Arizona, a new drivers license in Florida, a bill for an ambulance ride in Florida, and unaccounted-for 1099 income for work done in several states. Shortly after contracting with ID Watchdog to resolve these issues, Charlie's employer pulled a routine background check and found all of this data as well. Charlie was threatened with termination from his job, arrest, and extradition based on his active warrants. ID Watchdog intervened on his behalf and Charlie was neither arrested nor fired. However, it took several months of additional work to quash the outstanding warrants and to absolve him of the fraudulent debts.

Charlie's problems started a decade ago when the perpetrator of his identity theft stole his wallet. The thief used Charlie's identification documents including his Social Security number to perfect his impersonation of Charlie. Despite not realizing that he was a victim, Charlie suffered numerous damages during this 10-year period. First, he paid inflated car insurance rates as a result of his damaged driving record. Second, his access to loans in order to finance and expand his business was limited due to his damaged credit reports. Third, Charlie paid inflated interest rates on his mortgage and other loans and credit lines due to his erroneously negative credit reports. These monetary damages were then coupled with the emotional damage related to his close call with his employer as well as the stress of completing the restoration process.

Anita J. became a victim of identity theft after she began applying for mortgages online. Shortly after submitting her personal data to several mortgage brokerage sites, fraudulent activity began occurring within Anita's identity. Over the next several months, an industrious identity thief purchased four properties in Anita's name. The combined value of the mortgages attached to these properties approached \$1 million. Anita took a hiatus from her mortgage shopping and it wasn't until several months later, when she began investigating new mortgages again, that she realized she had been victimized. By the time she became aware of her problem, all four properties had been placed in foreclosure. Non-payment of the mortgages had dropped her credit scores more than 200 points. Collection companies eventually found Anita and began to demand payment for the delinquent accounts. Anita's credit card companies noticed the sudden drop in her credit scores and began to ratchet up her once low interest rates to above 20 percent. Appalled that all of this had occurred, Anita began the arduous process of repairing this damage and winning back her good name. Her efforts began to take a toll on her work. The long hours she spent writing letters to credit bureaus, dealing with title companies related to the properties, and phone calls made patiently trying to explain to unsympathetic collection agencies that "they had the wrong person," eventually raised Anita's stress to unhealthy levels. She began to log the time she was spending on the problem and surpassed 400 hours before finally enlisting our help.

Anita was quickly absolved of the debts that had illegally been acquired in her name. However, the rest of her case demanded more attention. Removing the delinquent mortgages and foreclosures from each one of her three credit reports presented a significant challenge—even with police reports and clear evidence of her innocence. Harder still was the removal of her name from public records related to the foreclosure and title work of the properties. This kind of straight forward "new account" ID theft is one of the most classic forms of the crime. Although the dollar amount involved is extremely high, this case and the steps required to solve it represent a very large portion of the 10 million cases of identity theft reported last year.

David H. realized that he was a victim of identity theft after he returned to the United States from Japan, where he served in the US Air Force. David was victimized not by one, but two separate thieves in different parts of the country. After receiving a couple of mysterious calls from collection agents, David checked his credit report to find over 20 fraudulent accounts in his name. David was shocked to find cell phone accounts, credit cards, utilities, and hospital bills that were in his name, but that he did not open. Not only did David have no prior knowledge of these accounts, he was not even in the United States when they had been opened. David's predicament quickly became worse when he was informed by his manager at work

that he was being fired because a background check found a felony drug conviction in Arizona. Once again, these alleged incidents occurred when David was abroad in the Air Force. After a long, drawn out process that involved filing extensive paperwork with the local magistrate in Arizona and reissuing a new driver's license, the arrest records were purged from David's background. Additionally, he was eventually reinstated to his old job; however, David's troubles were not yet over. Several months later, David received notice from the state of Illinois that 60 percent of David's wages were to be garnished due to unpaid child support payments. Not surprisingly, David had never met the woman who was receiving the payments, and was not in the country at the time the child was conceived or born. After two weeks of work and several in-person interviews with child services personnel, David was absolved from the payments.

Military personnel have traditionally been at high-risk for identity theft because of the military's use of Social Security numbers for identification. The number is often prominently displayed on ID cards and even on an individual's bunks in some cases. To date, David has spent one and a half years defending himself from false accusations and restoring his good name. He has been subjected to harassment from collection agencies, his credit score has been crushed, and he had to endure the humiliation of being fired from his job under the stigma of a false criminal conviction. He has been falsely accused of fathering illegitimate children and nearly lost 60 percent of his income as a result. Adding final insult to injury, these problems all occurred while David was actively serving his country during wartime. David's case is an example of how there is probably too much reliance by data brokers on the Social Security number to authenticate the identity of persons in records from many different sources. Today, the majority of David's problems have been resolved and deleted from his records, however he lives in constant vigilance, because the thieves could go back to work at anytime.

In the criminal world, identity theft continues to grow in popularity. It is our opinion that 3 driving factors have contributed to this rise in popularity, and that these factors need to be addressed by any new legislation. These factors are:

1. The availability of the Social Security number.
2. The ease of use of this data to commit fraud due to lack of effective authentication procedures.
3. The lack of legal consequences for a thief.

Identity thieves perceive identity theft as a low risk/high payoff crime. This perception will need to be altered to affect significant changes in the growth trends of the crime.

The Availability of the Social Security Number

Social Security numbers are simply used too much. Before using an identity to perform a crime, identity thieves must harvest personal identifying information such as name and Social Security number. The flow and availability of this information today affords thieves too many ways to obtain this data. Possible legislative changes to consider in order to improve this situation could include the following:

Companies should be restricted from using the Social Security number for customer identification purposes. The Social Security number should be removed from easily accessible public records. Social Security numbers should be removed from all forms of identification that might be lost or stolen. Social Security numbers should never be sold to unaffiliated 3rd parties for any reason.

The Ease of Use of This Data to Commit Fraud Due to Lack of Effective Authentication Procedures

Once a thief has harvested a victim's identifying information, he must now use it for his own benefit. In almost all cases, slight modifications need to be made to a victim's identity before a crime can be committed. For example, a thief opening a new credit card account would need to fill out a credit application. On this application he would write the victim's name and Social Security number, but his own address and telephone number. With his own address on the application, the thief is ensured that the new card will be shipped to him rather than to the victim himself. With his own phone number, the thief will be able to call to activate the card from a phone number that he controls. Additionally, the thief would sign the application with his own signature, rather than the victim's.

Standardized client authentication practices would greatly curtail potential identity thieves' ability to materially use identifying information to commit crimes and

should be considered for new anti-identity theft legislation. These practices should include both high-tech approaches such as cross matching address history and name against Social Security number; and low-tech approaches such as signature verification. Such standards should be implemented universally for all entities that maintain and use the Social Security number and should come with meaningful penalties for non-compliance and negligence.

The Lack of Legal Consequences for a Thief

Other than the potentially easy and lucrative payouts of identity theft, thieves are motivated to commit the crime due to a low prospect of facing prosecution. Two sub-factors contribute to this perception of safety. First, existing legislation is too vague and oftentimes too different from jurisdiction to jurisdiction to be effective. Further clarification of penalties for the misuse of Social Security numbers and identity theft along with stricter penalties should be considered in any new legislation. Second, thieves currently exploit an environment of non-cooperation and non-communication that exists among the many entities involved in the investigation of identity theft. The result is a very low arrest rates for identity thieves. The multi-jurisdictional nature of the crime is at the heart of this problem. It is imperative for an over-reaching entity such as the Federal Trade Commission or the President's Identity Theft Task Force to coordinate between the various entities and jurisdictions involved in the investigation and prosecution and to facilitate open channels of co-operation and communication. With identity theft the thief and the victim are seldom in the same place, and as such it is imperative that disparate law enforcement agencies have the means to share information and resources.

The statistics about identity theft are frightening. The sheer number of victims stands at an overwhelming 10 million per year. With such proportions, it is easy to become numb to these figures; however, it is a useful exercise to look at specific case studies to find general guidance for meaningful solutions. Additionally, it is vital for all of us to remain in tune with the specific pain and suffering that these crimes cause in order to maintain the proper motivation to find a solution. The Subcommittee has shown great leadership and tenacity over the past seven years in continuing to explore measures to limit identity theft. I implore you to continue your efforts and hope that when considering the costs associated with changes in legislation (especially costs to business), those costs should be weighed against the benefits that would be afforded to consumers such as Charlie W., Anita J., and David H.

Chairman MCNULTY. Thank you, Mr. Yurek.
Mr. Pratt.

**STATEMENT OF STUART PRATT, PRESIDENT, CONSUMER
DATA INDUSTRY ASSOCIATION**

Mr. PRATT. Mr. Chairman, Ranking Member Johnson, and Members of the Committee, thank you for this opportunity to appear before you today. My name is Stuart Pratt. I am president and chief executive officer of the Consumer Data Industry Association.

Let me start by saying that the CDIA supports efforts to limit the sale and display of the Social Security number to the general public. We also believe that sensitive personal information, like a Social Security number, should be secured. But we also believe in preserving the Social Security for legitimate uses for business to business and business to government transactions. Some context I think for that point is important. Forty million addresses change in this country every year. Three million last names change due to marriage and divorce. There are many other examples in our written testimony but in fact most identifiers change and our names are not unique. A unique identifier is important to fair information uses.

Consumers have expectations and the Social Security number plays a role in meeting these expectations. Consumers expect data about them to be accurate. Consumers want to be protected from fraud. Data about them should be protected and secured. There are Federal laws that exist today, and they are effective and the operation of these should be preserved. Some examples are the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act and there are other examples in our testimony. But these laws restrict the use and display of the Social Security number. They restrict how it can be used, who can use it, and under what circumstances.

Responsible uses of the SSNs do meet, I think, consumer expectations. This really just is not our view, the GAO concluded in a 2004 study that Social Security numbers are used to build tools that verify an individual's identity or match existing records since there is no widely accepted alternative, and we agree. The report further states that restricting business access to Social Security numbers would hurt consumers and possibly aid identity thieves, since it would be more difficult for businesses to verify an individual's identity. Again, we agree.

The Federal Trade Commission in its own testimony has stated that SSNs play a vital role in our economy, enabling businesses and government and others to match information to proper individuals. For example, consumer reporting agencies use SSNs to ensure the data furnished to them is placed in the correct file, that they are providing the right report for the consumer. SSNs are used for locator services, to find lost beneficiaries, witnesses, law violators, to collect child support, to enforce judgments.

But the SSN is not the final word on identity verification, and I think that this point is very important. The SSN plays a role, it is an important role, but data matching does not equate to identity verification or authentication. Our Members in fact produce one billion fraud likelihood assessments each year. We also produce 1.4 billion identity verification assessments each year. It is not just about data matching. Identity verification is much more. It is a risk assessment based on the deployment of a range of tools that consider matches of data, but they also consider application data. They also consider timing of application and various components of identity and whether or not they have been used previously in fraudulent applications.

We also recognize that the Social Security number has value in public records and this is important for this Committee's consideration. Public records play a vital role in our society. Bankruptcy records, tax liens and judgments are part of a credit report. Public records help in the location of missing and exploited children. Validating professional licenses is critical for the health care industry. Without an SSN to tie these records together, a consumer can simply alter an address, change a name and separate himself or herself from the record. Preserving the SSN in public records is essential, but our Members do support State Government efforts to redact the SSN from the display to the general public, and we think there is good progress being made on that front.

Finally, some building blocks of good public policy should include preemption. If you are going to establish a national standard, let's get it right and have a national standard and not a fifty-first state

law. Preserve the operation of current laws, like the Fair Credit Reporting Act, and I think this is where we may differ with some of the approaches thus far. The Fair Credit Reporting Act is a well-established statute, as is the Gramm-Leach-Bliley Act, including information safeguards. Ensure that the appropriate rulemaking authority is bounded and that it takes into consideration small business implications and the Regulatory Flexibility Act.

In conclusion, our Member's uses of the SSN meet consumer expectations. Data used is accurate, fraud can be prevented, identities can be better verified, public records are useful in our society. We appreciate this opportunity to testify, and we look forward to your questions.

[The prepared statement of Mr. Pratt follows:]

**Prepared Statement of Stuart Pratt, President,
Consumer Data Industry Association**

Chairman McNulty, Ranking Member Johnson and members of the subcommittee, thank you for this opportunity to appear before you today to discuss the importance of Social Security numbers. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.¹

Our members applaud this committee for the thoughtful and open dialogue that you have fostered regarding how Social Security numbers are used, to identify risks associated with such use, and to address these risks in a reasonable, targeted fashion.

As a preliminary matter, CDIA supports efforts to limit the sale and public display of Social Security numbers. CDIA's members do not publicly sell or display Social Security numbers to the general public, and we oppose such activity. However, as will be discussed below, such restrictions have to be carefully considered, balanced and bounded so that restrictions on use do not interfere with legitimate business uses of SSNs to detect and prevent ID theft and financial fraud and for other beneficial purposes.

• **The SSN is the only unique, individual identifier that follows a person throughout their lives, literally from the time they are born.**

SSNs are important to the smooth operation of today's economy because there is no other single identifier that serves the same purpose as effectively as the SSN.

Although there are other identifiers that may serve similar purposes in some contexts, there are no other identifiers that serve this role across all individuals and circumstances.

For instance, name and address can't be used because they are too common, change due to marriage and divorce, and, according to the U.S. Census Bureau, 42 million consumers move every year. Even for consumers who's address and name are constant, they do not always use their identifiers inconsistently (i.e., in some instances they will use a nickname, and may inconsistently use their generational designations (e.g., III, or Sr.)). There are also times where consumers themselves make mistakes when completing applications. Thus, a consumer's identifiers may be presented in different ways in different databases and, in some cases, the data may be partially incorrect. Further, personal identifiers such as name and birthday, are generally not as unique as we may believe they are.

Further, the use of other alternatives that could possibly serve as a substitute for an SSN, such as a cell phone number or driver's license number, is often restricted by law.

Thus, the SSN is a truly unique identifier.

As the only unique identifier, the use of the SSN has migrated beyond simply keeping track of social security payments, even within the Federal Government itself. For example, it is used for tax purposes, Selective Service registration, employment verification, the provision of government benefits and a host of other uses.

¹ CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, systems for insurance underwriting and also collection services. As we will discuss below, the secure and protected use of the social security number (SSN) is an important key to the effectiveness of these systems and services.

In addition, the use of the SSN is often mandated by the Federal Government. For instance, the Treasury Department regulations regarding PATRIOT Act compliance for financial institutions in many instances requires financial institutions to use the consumer's full SSN, as obtained from "trusted [private] sources," such as credit bureaus.

Additionally, many State laws require the use of the SSN for a wide range of important purposes dependent on accurate identification. For instance, to meet requirements of the law, government data often must be cross-checked or enhanced with data from private sector databases.

For the private sector, the role of the SSN is that it serves as a unique identifier that is permanent, so a consumer cannot voluntarily relinquish it in bad times, and it is consistent across various systems. For example, a financial institution, a wireless communications company and a hospital can all rely on the same identifier for widely divergent purposes, all to help ensure that the individual before them is the person they believe is before them. Said differently, after having verified that a consumer is legitimate, a bank, for example, can then create a unique identifier such as a customer or PIN number. But as long as the bank is dependent on third-party sources to cross-check applicant data, unique identifiers must cut across external data sources.

CURRENT LAW PROTECTS THE PUBLIC FROM INAPPROPRIATE USE

There are several federal and state laws and regulations that restrict the use or disclosure of SSNs, including: the Gramm-Leach-Bliley Act (15 U.S.C. 6826(b)) and its implementing regulations ("Privacy Rule"); the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); Section 5 of the FTC Act (15 U.S.C. 41–51); the Fair Debt Collection Practices Act (15 U.S.C. 1601 et seq.); the Health Insurance Portability and Accountability Act (Pub. L. 104–191); and the Drivers Privacy Protection Act (18 U.S.C. 2721 et seq.). Together, these laws restrict the use and display of SSNs, how they can be used, who they can (and can't) be shared with, and under what circumstances.

The use of the SSN by Credit Reporting Agencies (CRAs), for instance, is governed by both the FCRA and, in most instances, GLB as well. These statutes limit how and when CRAs can disclose SSNs, to whom, and under what circumstances.

For instance, many CDIA-member products are focused on helping consumers to gain access to the goods and services for which they apply—assisting a lender or other service provider in determining a consumer's eligibility. These products are regulated under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) as "consumer reports." Eligibility determinations include applications for any type of credit including unsecured credit, home purchases, auto financing, home equity loans, as well as for insurance of all types, employment, government benefits, apartment rentals, and for other business transactions initiated by the consumer.

The FCRA, enacted in 1970, has been the focus of careful oversight by the Congress, resulting in significant changes in both 1996 and again in 2003. There is no other law that is so current in ensuring consumer rights and protections are adequate.

Similarly, some fraud detection tools are regulated under GLBA, and the use of data regarding those products is similarly circumscribed.

Beneficial Uses of the SSN

Because the SSN allows for consistency across various systems and data bases, there are a number of ways that the SSN is used that benefits consumers. Further, without the availability of the SSN, many of the products and services that consumers take for granted today could become more scarce.

For instance, CDIA's members produce a range of critical consumer data products which bring great value to individual consumers, to society, and to the nation's economy. Our members design products used for determinations of a consumer's eligibility for a product or service, to prevent identity theft and fraud and to aid in the location of consumers for a variety of reasons.

(1) Proper File matching: Ensuring that data goes to the right file, and is reported about the right individual.

Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission, recently testified about the importance of Social Security numbers before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security:

"SSNs play a vital role in our economy, enabling businesses, government, and others to match information to the proper individual. For example, consumer reporting

agencies use SSNs to ensure that the data furnished to them is placed in the correct file, and that they are providing the right credit report for the right consumer. SSNs also are used in locator databases to find lost beneficiaries, witnesses, and law violators and to collect child support and other judgments. Employers must collect SSNs for tax reporting purposes, and health care providers may need them to facilitate Medicare reimbursement.” She went on to say that “the SSN is valuable in enabling entities to match information to consumers. With 300 million Americans, many of whom share the same name, the SSN presents significant advantages as a means of identification because of its uniqueness and permanence.”

Financial institutions and others rely on full and complete information from credit bureaus. Complete information is necessary if the appropriate information is to be placed in the proper consumer account. As an example, a financial institution may obtain information from a credit bureau on its customer named Tom Jones. As you can imagine, there are thousands of Tom Joneses in the country. In fact, it is likely that many Tom Joneses share the same last four digits of their SSN. Therefore, a report with information pertaining to Tom Jones with the last four digits of 1234 may not provide the financial institution with sufficient information to determine to WHICH Tom Jones the report refers.

SSNs, therefore, help to ensure that our members are more likely to load data to the correct file with a high degree of precision. This is particularly true where a new account has been opened and is being added to the consumer’s file for the first time. Consumer reporting agencies of all types have, under the Fair Credit Reporting Act, a duty to maintain reasonable procedures to ensure the maximum possible accuracy of the file; SSNs help them meet this requirement.

SSNs also help to ensure that the proper consumer’s file is produced when a consumer applies for a benefit under the FCRA. If a consumer reporting agency cannot, with precision, identify the proper file of the consumer, it returns a message to the creditor indicating that no record was found. This result would likely lead to far higher credit denials for consumers due to the inability of the creditor to review the consumer’s credit history. Said differently, the Fair Credit Reporting Act certainly does not contemplate the consumer reporting agency “taking a guess” as to which consumer’s file must be accessed and thus this current liability coupled with the absence of the SSN would seriously impinge on the way in which credit is granted in this country today.

(2) Identity Verification to Prevent Identity Theft and Fraud

A number of CIDA members produce products that are used by financial institutions, insurance companies and others to verify the identity of an individual and ensure that the person they are interacting with is who they say they are. These products are very effective in detecting and preventing identity theft and financial fraud before it happens.

The SSN helps businesses to prevent fraud by cross-checking applicant data against various other data sources in order to authenticate the consumers’ identity. Absent the use of an SSN, these systems will be far less likely to trigger security protocols, which prevent the crime of identity theft.

In 2004, the GAO conducted a study on Social Security numbers, and concluded that “information resellers, credit reporting agencies and health care organizations use social security numbers to build tools that verify an individual’s identity or match existing records since there is no widely accepted alternative.” The report further states that “restricting business access to social security numbers would hurt customers and possibly aid identity thieves since it would be more difficult for business to verify an individual’s identity.”

(3) Other specific products and services are enabled and enhanced through the availability of the SSN:

Access to home ownership: Every homeowner benefits from a credit reporting system that reduces the costs of all mortgage loans by a full two percentage points, thus putting literally thousands of dollars in disposable income into their pockets. Homeownership is no longer a luxury of the well-to-do, but is a truly democratized American dream enjoyed by nearly seventy percent of the population.² The SSN helps to facilitate the efficient operation of this system, as described above.

Child support payment enforcement: Access to SSNs dramatically increases the ability of child support enforcement agencies to locate non-custodial, delinquent parents (often reported in the news with the moniker “deadbeat dads”). For example, the Financial Institution Data Match program required by the Personal Respon-

² Kitchenman, Walter., U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns, Pp. 5 (1998).

sibility and Work Opportunity Reconciliation Act of 1996 (PL 104–193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly \$2.5 billion. Child support enforcement agencies report that their efforts are far more effective when they have access to the parent’s SSN. One agency reports that they are able to locate fully 80 percent more delinquent non-custodial parents when the SSN is available, and the Association for Children for Enforcement of Support (ACES), a private child support recovery organization, has stated that social security numbers are the most important tool for locating parents who have failed to pay child support.

Locator Services—SSNs are used routinely by law enforcement to locate missing children, fugitives and witnesses to crimes. The ability to conduct an information search using an SSN is essential. Restrictions on access to SSNs in government records would hamper the ability of law enforcement to obtain this vital information. Further a number of states report that use of SSNs to match across data bases has greatly reduced entitlement fraud. For example, Pension Benefit Information (PBI), a private company that locates former employees that are due pension benefits, has indicated that in many cases the SSN becomes the only link between an employer and their former employees with vested benefits. Employees move, marry and change their name, but the one thing that remains constant is their SSN.

Locating sex offenders—SSNs are used to locate registered and unregistered sex offenders. There are over 560,000 sex offenders in the U.S. Approximately twenty-four percent of these individuals fail to comply with address registration requirements mandated by law. Access to SSNs allows law enforcement to locate sex offenders even when the registration address has not been kept current.

Employment/security screening: As discussed above, SSNs serve as vital links among disparate records that help businesses verify prospective employees’ identities and conduct thorough, accurate background checks to ensure workplace safety and business security.

Small business B-to-B transactions: An SSN is the key business entity identifier to virtually all sole proprietorships or partnerships; as a result, SSNs are necessary to facilitate business-to-business transactions between small businesses.

Securitized credit markets: Confidence in the U.S. securities market is made possible by accurate financial histories compiled using the SSN as a key identifier. Restricting use of the SSN could undermine confidence in these securities, resulting in substantially higher consumer costs for credit, including mortgages and auto loans.

Insurance fraud prevention—Insurance companies use public record information compiled using social SSNs to detect fraudulent insurance claims. According to the National Fraud Center, the average American household pays \$200 to \$400 a year in additional insurance premiums to offset the cost of fraud. This cost would likely increase if companies do not have the information they need to detect and prevent fraud.

(4) Additionally, without the use of the SSN, consumers would suffer harm:

Incomplete data harms consumers: There would likely be an decrease in the ability of consumer reporting agencies to properly match incoming information to the correct consumer about whom the information relates. Think about the consequence to consumers of having a consumer credit report that does not contain all of the accounts that they pay on time and which makes them eligible for the lowest cost loans.

Incomplete data harms our banking system: The absence of the SSN would also put at risk the safety and soundness of lending decisions due to less information being included in consumer credit reports due to data matching problems.

Incomplete data prevents consumer access to goods and services: Think about the consequence for consumers when a consumer reporting agency cannot locate the proper file on a consumer and thus a lender, insurer or other service provider wanting to do business with the consumer has to deny the application, or the consumer has to pay higher rates.

INFORMATION SECURITY AND THE SSN

As discussed above, the use of data like the SSN actually helps to prevent fraud and identity theft, by enabling better authentication of consumers, so that a lender knows that a loan applicant is you, and not an identity thief.

However, concerns have been raised that the SSN is a “key,” and all a potential identity thief needs to “unlock” a consumer’s credit—that simply is not true.

There are 2 basic types of financial fraud that may be perpetrated against an individual. The first is fraud against a person's existing accounts, such as credit card fraud, where a thief obtains your account number or credit card, and charges items to that card or drains your existing bank account. While those instances are problematic, and may cause a consumer some stress while getting those problems rectified, they do not cause any long-term harm to the consumer; they suffer no financial liability, and such fraud does not impact their credit in any way. More than 2/3rds of all "identity theft," as identified by the FTC, falls into this category.

The second, and more serious type of financial fraud is what we term "real name" fraud, where a fraudster obtains a person's sensitive personal information, such as their SSN and other information, and somehow fools a lender into thinking that they are that person. This may enable the thief to open new credit accounts in a victim's name without the knowledge of the victim. While the victim is ultimately not responsible for the financial harm, this type of fraud can have serious repercussions for the victim.

As discussed, while obtaining a person's SSN may potentially make them susceptible to identity theft, it takes a lot more information, and the ability to use it in a way that thwarts the fraud detection tools in place, to commit "real" identity theft. Further, the SSN plays a major role in helping to stop such fraud, as well.

The availability of MORE information, rather than less, is the key to reducing reliance on the SSN. Database matching is often like finger-print matching—the more unique data points there are, the more ability there is to identify and authenticate an individual. Further, each piece of data reduces the reliance on every other piece. However, Congress has limited the use of alternatives, increasing the reliance on SSNs.

For instance, there are other unique identifiers that could help reduce the reliance on SSNs, such as Driver's License numbers, that do exist. However, the Driver's Privacy Protection Act (DPPA) has limited the ability of data base companies to utilize those to supplement, or even supplant, the use of SSNs.

Wireless cell phone numbers also have the potential to serve that purpose. However, while those numbers are not used for telemarketing, Congress has, in other contexts, considered limiting the utility of these numbers for identification and fraud detection purposes, as well.

PUBLIC RECORDS AND THE SSN

Public records play a vital in our society and bring value to the consumer. Bankruptcy records, tax liens and judgments are part of consumer "credit" reports used by lenders to make decisions that implicate safety and soundness. Records of eviction are critical to landlords who must themselves pay the bills and attempt to lease properties to consumers who will do the same. Validating professional licenses for employment screening agencies is yet another use of public records, as is accessing criminal histories.

Through the development of nationwide databases of public record information, our members have solved the problems inherent in having to search through tens of thousands of federal and state court houses and agency databases. In this way, the SSN is as important an identifier in a public document as it is in a private-sector database. It is a critical identifier for all of the data management reasons we discuss above. Without an SSN, a consumer can simply alter a few items of information, such as moving to a new address, or even changing a name and thus separate himself/herself from a bankruptcy record, a tax lien, a record of eviction and even a criminal history, in some cases. Clearly this is not a positive outcome for consumers or for American businesses which are on the front lines of making, for example, fair and accurate risk based lending and employment decisions, while at the same time fighting identity theft and fraud.

Some federal proposals have suggested that state agencies must limit access to the SSN. The concern of the CDIA's members is that this apparent unfunded mandate will drive under-funded state agencies to either stop requesting the SSN when processing vital records, or to simply deny all access to public records containing SSNs.

It is important that public records, including those records containing SSNs, continue to be made available. The open public records system is the cornerstone of the U.S. democracy and economy.

The debate about the presence of the SSN in public records has suggested a possible binary solution, where SSNs could be made available electronically for certain entities, but could possibly be redacted for publicly available electronic documents, though costs associated with such an unfunded mandate will have to be addressed.

It is encouraging to hear state court organizations discussing strategies for protecting SSNs, and CDIA will continue to engage in these dialogues.

However, while CDIA believes that disclosure of the SSN to the general public must be addressed, we also believe that public records must be made available, including SSNs, to those with an appropriate need. Ultimately, dialogue with state and federal agencies coupled with the advancement of technologies will address concerns about public records which contain SSNs. An unfunded mandate will destabilize the system of public records which is so important to our democracy.

- **Some Additional Notes on Other Important Issues:**

Finally, there are a few additional issues I would like to highlight before I conclude:

- **Legitimate business uses:**

It is important that any restrictions imposed on the sale or display of SSNs contain exceptions for legitimate business uses such as identity verification; detecting, preventing and investigating ID theft and fraud; locating individuals; collecting child support and other lawful debts; and for any purposes permitted under the Fair Credit Reporting Act and Gramm-Leach-Bliley Act.

- **Preemption:**

Ensuring that the Social Security number issue is addressed in a uniform fashion, so that all consumers are protected, is a vital component of this debate. Any legislation that would restrict the sale or display of SSNs must contain federal preemption so that businesses are subject to a single, national law rather than having to comply with various state laws all with differing and potentially conflicting requirements.

- **Exempt Current Law**

As discussed previously, SSNs are broadly covered by a whole host of current statutes. Instead of adding an additional compliance burden on top of those laws, we would urge the Committee to exempt practices already covered under existing laws.

- **Minimize Rulemaking Authority**

Because so many business practices rely on stable laws, CDIA would urge the Committee to codify any changes to current law, to the extent possible, rather than granting broad authority to the regulatory agencies.

- **Further Assisting Identity Theft Victims: Provide the Ability to “Ping” the SSN Database**

CRA's utilize very sophisticated tools to ensure the accuracy of their systems. However, in rare cases of identity theft, it would be useful for us to have the ability to cross-check our databases to determine if a particular SSN is associated with a particular person. This would be very useful in further helping ensure the accuracy of our databases, and could help contribute to the accuracy of our databases and the ability to help correct the records of Identity Theft victims.

CONCLUSION

In conclusion, you can see that the underlying theme in the discussion of SSN uses is that of balance and ultimately ensuring the security of the number. Law that imposes national uniform information security regulations on all who possesses the SSN in combination with a person's name and address, is the most responsible and constructive focus for Congress. In contrast, law that overreaches in attempting to limit use of the SSN is likely to merely take fraud prevention tools out of the hands of legitimate businesses at the expense of consumers.

Ironically, to prevent fraud you must be able to crosscheck information. To maintain accurate databases, you must be able to maintain a range of identifying elements. Absent the availability of the SSN, we will be less able to build accurate databases, to accurately identify records and to help prevent identity theft through the development of fraud prevention and authentication tools.

Ultimately consumers expect us all to accomplish the goals of protecting and securing the SSN, and also ensuring the accuracy and effectiveness of databases which contain information about them.

Thank you for this opportunity to testify.

Mr. JOHNSON. Thank you, Mr. Pratt.

Mr. Gingerich, you may testify.

STATEMENT OF JAMES D. GINGERICH, DIRECTOR, ADMINISTRATIVE OFFICE OF THE COURTS, SUPREME COURT OF ARKANSAS, ON BEHALF OF THE CONFERENCE OF STATE COURT ADMINISTRATORS, WILLIAMSBURG, VIRGINIA

Mr. GINGERICH. Thank you, Mr. Johnson and Members of the Committee. It is an honor to appear before you to have the opportunity to share with you some of the work which has already been done and is being actively considered in our Nation's state court systems in this very important area of balancing the public access to court records with privacy concerns of individuals.

As to the specific topic of the hearing today, our country's state court systems have been quite active, as this Committee has, in recognizing the serious threat to personal privacy which comes from public access to personally identifying information, such as the Social Security number. Previously, in hearings of this Committee, members of COSCA have testified about the work undertaken by the Conference of Chief Justices and the Conference of State Court Administrators in 2000 and 2001 to develop a recommended comprehensive policy on access to court records and suggested that those guidelines be adopted by every state supreme court in the United States. On August 1, 2002, CCJ and COSCA adopted the resolution endorsing the guidelines and encouraging their adoption.

I am pleased to report that since that testimony, 20 state supreme courts have adopted the guidelines, another eight states have made revisions to their previously adopted rules based upon the guidelines and five states have commissions currently underway considering adoption of the guidelines.

About 60 days ago, my own state of Arkansas became the most recent state to adopt a comprehensive policy after almost 2 years of study and debate. We utilized the recommended guidelines, as well as the good work which has been done in many of our sister states. As it relates to the Social Security number, let me just read you the rule that has now been adopted by the Arkansas Supreme Court. It applies to every court record in the state, whether it is a paper record or an automated record and whether it lies in the supreme court building or any rural courthouse in the state.

"The following information in case records is excluded from public access and is confidential absent a court order to the contrary . . . number four, Social Security numbers; number five, account numbers of specific assets, liabilities, accounts, credit cards and personal identification numbers; and number eight litigant addresses and phone numbers." Those three exceptions were all borne out of our concern about, and our many hours of debate about, the very real problem of identity theft. I have to suggest however that there were some things that we learned along the way to guide how we now implement that policy, which I think are consistent with your purposes.

First of all, the suggestion that we should simply ban the use of the Social Security number from any non-Social Security related activity is not good public policy and has serious negative consequences on the efficient and accurate operation of State court

systems. It also conflicts with many other important public policy goals, adopted both at the state level and at the Federal level, which require the use of a Social Security number. I will not go into all of the issues, but I think my written testimony recites the many, many ways in which courts legitimately and appropriately have need for that information to do the work of a court system; for example when judges need accurate and verifiable information in order to enter decisions about assets and income, especially in family law cases, and in some states for the accurate identification of parties. In Arkansas, we do not use the Social Security number at all in criminal cases but, for example, in our juvenile justice system, both in dependency and in delinquency cases we use it in order to accurately identify an individual. Our state public policy suggests that we are not going to fingerprint children and so it is the only way in which we can accomplish that. Those records are segregated and sealed but nonetheless it is an appropriate use of the Social Security number. There many other ways. So, for Arkansas it was not the case of barring the use of the Social Security number but in implementing policies to protect the information from unnecessary disclosure.

There is a second thing we learned; eliminating or restricting access to the Social Security number when the collection of the Social Security number has been required by the court or is otherwise required by state or Federal law in the future is an appropriate policy which we support and which we intend to implement.

As to the "in the future," our own rule adopted by the Supreme Court in Arkansas provides that the implementation date will apply only to records that are created after January 1, 2009. After looking at the scope of the issues for those files that resided in courthouses in millions of records in 75 county courthouses across Arkansas, it is simply impossible for us to expect that local officials in those courthouses were going to have any ability to go back and redact all of those records. So, we looked forward in terms of doing the best we could.

I should add, however, that our court specifically provided authority for the local court officials to redact earlier records if they are able to, and that will probably happen on a case by case basis. To the extent that collection of the Social Security number is required by the court, when courts are asking people for the information ourselves, we can control it, we can manage it; and so in Arkansas we will adopt a rule similar to that which already exists in Washington, Minnesota and North Dakota to separate that information in a separate court file, with only the main file being available to the public. The information like the Social Security numbers will be in a separate file and will be unavailable, either in paper or in the automated record. When the Social Security number is otherwise provided in a pleading, for example, or in something that is presented by a lawyer to the court, we have very little control over that; but Arkansas will adopt a rule that requires the attorneys or parties to protect that information.

I realize I am out of time, Mr. Chairman, and I would just say in conclusion that we recognize the problem. I think our state supreme courts are doing a pretty good job of trying to get to the im-

plementation of the policy which you desire, and we are looking forward to working with you and the Committee in that effort.

Thank you.

[The prepared statement of Mr. Gingerich follows:]

Prepared Statement of James D. Gingerich, Director, Administrative Office of the Courts, Supreme Court of Arkansas, on behalf of the Conference of State Court Administrators, Williamsburg, Virginia

Mr. Chairman and Members of the Subcommittee,
The Conference of State Court Administrators (COSCA) is pleased to present testimony on today's hearing on protecting the privacy of the social security number from identity theft.

SUMMARY

Mr. Chairman and members of the subcommittee, the state court community has been grappling with the issue of protecting privacy as it relates to court records for the past few years. We are taking a proactive stance in protecting the privacy of individuals and their social security numbers, while at the same time maintaining traditional open court access. Today, we will share examples of what state courts that are doing on this via the approval of court rules.

In collaboration with the Conference of Chief Justices (CCJ), we established a project entitled "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts," which outlines the issues that a jurisdiction must address in developing its own rules, and provides one approach. The *Guidelines* touch on the use of social security numbers (SSNs) in court records as well as other private information. The entire text of the Guidelines can be found online at <http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf>. Both CCJ and COSCA, adopted a resolution endorsing the Guidelines and urged the states to address them.

Mr. Chairman, SSNs are pervasive in state court documents and procedures. The testimony that follows gives the subcommittee numerous examples of how we use SSNs in day-to-day court proceedings. For example, we use SSNs to insure that judges have the best evidence available to them. We also use SSNs to collect fines and restitution. In addition, many SSNs appear in the public record in many types of court cases including, but not limited to, bankruptcy, divorce and child support cases. My testimony also details the federal requirements imposed on us to collect SSNs for various reasons, for example, to track parents who are not paying child support.

Mr. Chairman, we stand ready to work with you to craft solutions to address the problem of identity theft. 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 would impose an unfunded mandate on state courts in this country. 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 on behalf of the Conference of State Court Administrators (COSCA). The National Center for State Courts, of which I am President, serves as secretariat to 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. As you know, state courts handle 98 percent of all judicial proceedings in the country. 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 today, 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 U.S. territories. 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.

STATE COURTS ARE RESPONDING TO PRIVACY CONCERNS

Mr. Chairman, let me begin by informing you of the progress that many state courts are making to protect individual privacy rights, while maintaining the American tradition of open courts. Through court rules, state court systems are changing their procedures for viewing and accessing court records as they relate to the appearance of social security numbers. Washington State, for example, is establishing a procedure for “sealing” family case court records containing privileged information such as social security numbers and financial information. In effect, Washington is creating two sets of records: a public and a private one. Vermont is placing the burden on parties to expunge or redact social security numbers from papers filed with the court. Minnesota is requiring that parties in a divorce case fill out a confidential information sheet, which contains social security numbers, to be kept separate from the official record. South Dakota adopted a rule that protects SSNs and financial account number information by requiring these numbers to be redacted from documents and submitted to the Court on confidential information forms.

In addition to the proactive stance we are taking to this issue, we are also responding to some of the demands placed on our court systems by state legislatures and governors. In 2005, 53 bills were signed into law by governors dealing with social security number privacy. That’s 17 more than in 2004; an increase of 46 percent. These bills range from simple prohibition of displays of SSNs on public records to new expansive criminal and civil statutes that punish wrongdoers and those that traffic in social security numbers as a means to steal a person’s identity. In the 2006 sessions, state legislatures considered 176 measures dealing with social security numbers and privacy. Again, this number is an increase over the prior year.

At the direction of the CCJ and COSCA leadership, we established a special subcommittee of the CCJ/COSCA Court Management Committee to explore privacy protection innovations and share them with the Congress and the Administration. This committee meets twice a year at our annual and mid-year meetings. This subcommittee has been researching the issue and is responsible for compiling examples of best practices in this area that I am presenting today.

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/COSCA and the NCSC 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 it was staffed by the NCSC and the Justice Management Institute. 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 jurisdiction must address in developing its own rules governing public access. 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 in other private information 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

A question we are often asked is why do state courts utilize SSNs? What is the state court interest in collecting SSNs? Why do state courts need to require parties to provide their SSNs in the course of state court litigation? The following are some of the reasons we use them:

Accurate determination of assets/income Judges need the most accurate information on assets and income when making their decisions, especially in family law cases. In many instances this involves examining assets by a social security number. There are numerous examples of individuals giving a false social security number to avoid paying child support, for example. The same logic applies in dealing with divorce cases in dividing assets.

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. The advantage of these systems is to be able to update an address or telephone number for all cases in which the person is a party by a single computer entry. 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.

Courts have often used SSNs to identify criminal defendants as well as parties to civil cases. In the future, persons accused of crime will be identified by automated fingerprint identification systems (AFIS) which scan fingerprints and classify them electronically. The primary future need for SSNs as a means to identify individuals will therefore be in civil, not criminal, litigation.

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 litigant an opportunity to pay an assessment resulting from a judgment 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. Some states use additional means to enforce criminal fines and restitution orders, such as denial of motor vehicle registration; SSNs are often used for these purposes as well.

Creation of jury pools and payment of jurors SSNs are a necessary part of the process by which multiple lists (for instance, registered voters and registered drivers) are merged by computer programs to eliminate duplicate records for individual citizens in the creation of master source lists from which citizens are selected at random for jury duty. Duplicate records increase 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 and 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 prison or jails, and to person 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 §?1A402(x)(3) requiring Federal and State agencies to provide names and SSNs of confined persons to the Social Security Administration. 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 currency. Second, cutting off benefits may provide a useful incentive for persons receiving benefits to clear up outstanding warrants without requiring the expenditure of law enforcement resources to serve them.

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.

POTENTIAL LEGISLATION

Mr. Chairman, in the past, this subcommittee has considered various pieces of legislation that would, in some form or another, prohibit the display of a person's social security number on a public record. Blanket prohibitions like these will place courts in the position of trying to comply with conflicting public policies. We submit the following questions for your consideration:

The Welfare Reform Law requires courts to collect SSNs on court orders granting divorces or child support or determining paternity. State laws contain similar requirements in other types of cases in some states. What steps must a court take to restrict access to these documents, which are matters of public record in most states?

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. What steps must a court take to restrict access to these documents, which are also matters of public record in most states?

We were encouraged by language in the report accompanying HR 2971 (Rept.108-685, Part 1, p. 21) in the 108th Congress dealing with incidental vs. non-incidental appearances of SSNs in public records:

During Social Security Subcommittee hearings on the bill, court and other public records administrators testified they receive numerous documents filed by individuals, businesses, and attorneys that often include SSNs the government did not require to be submitted, and of which they are therefore unaware. They stated redaction of "incidentally" included SSNs would create a serious administrative burden, and it would require significant resources to review each document and redact such incidental SSNs . . . *With respect to SSNs submitted in court documents absent the court's requirement to do so, the individual communicating the SSN in the document, not the court, would be held responsible according to Section 108 of the bill.* (Emphasis ours)

In drafting social security legislation, we respectfully ask that you expand on the above sentiments in actual legislative language of any future bill.

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 a redaction requirement is imposed.

In the event you draft legislation dealing with redaction, we urge you to make a distinction between existing court records/documents and future documents. For example, requiring a court to retroactively redact or expunge old records would be a nightmarish task due to the cost in staff time and the actual compiling of said court records.

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.

OUR FUTURE COURSE OF ACTION

CCJ and COSCA have recommended that state courts adopt the following policies, unless state law directs them otherwise, to protect citizen privacy while providing service to litigants:

Official court files State courts should not attempt to expunge or redact SSNs that appear in documents that are public records. 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 interpretation 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 authority to alter documents filed in a case; the social security number 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 social security number when the inquirer already has the social security number and provides it to the court staff member.

In short, staff may not read aloud a social security number, but may listen to a social security 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 role of SSNs in the incidence of identity theft cases. The current state of affairs with regards 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.

I have presented several ways our courts utilize SSNs. 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. I remind you of the earlier mentioned approaches from Washington, Vermont, Minnesota and South Dakota. Other states are experimenting with different approaches.

Thank you for asking for our input on this important matter. The Conference of State Court Administrators stands ready to work collaboratively and cooperatively to craft solutions to this important issue. I will be happy to answer any questions you may have.



Chairman MCNULTY. Thank you, Mr. Gingerich.
Dr. Antón.

**STATEMENT OF ANNIE I. ANTÓN, ASSOCIATE PROFESSOR OF
SOFTWARE ENGINEERING, NORTH CAROLINA STATE UNI-
VERSITY, RALEIGH, NORTH CAROLINA, ON BEHALF OF THE
ASSOCIATION FOR COMPUTING MACHINERY**

Ms. ANTÓN. Good morning, Chairman McNulty, Ranking Member Johnson and members of the Subcommittee. Thank you for the opportunity to testify today. This statement represents my own personal position as well as that of the Association for Computing Machinery's U.S. Public Policy Committee.

By way of introduction, I am an associate professor at North Carolina State University and director of an academic privacy research center. In addition, I serve on several industry and government boards of technical advisors, including the DHS State of Privacy and Integrity Advisory Committee.

Right now, personal information about you, me and millions of Americans is being compiled, accessed, sold and exchanged among businesses and government agencies. Yet, we should all be concerned. Is that personal information protected? Is it being shared only among those with a legitimate need for it? Can criminals easily access our personal information? These concerns are compounded by three factors: First, the widespread use of Social Security numbers has made it a de facto national identification number; second, computing technologies enable us to collect and exchange and analyze personal information on an unprecedented scale; and, third, there are widespread problems with cyber security leading to frequent and large security breaches. In particular, technology allows personal information to be combined with Social Security numbers, thus creating a convenient way to track individuals across public and private records. This raises privacy concerns, and these concerns are exacerbated because many businesses use the Social Security number as both an identifier and an authenticator.

The terms "identifier" and "authenticator" have specific technical meanings that are often confused. An "identifier" is a label associated with a person. An "authenticator" provides the basis to believe that somebody is accurately labeled by some given identifier. So, authenticators might be something you know, like a secret password or a pin, something you have, like the key to your house, and something you are, such as a biometric. A Social Security number is an identifier. It is something that anyone can know, and many will, so it is not a secret. Hence, it is unuseable as an authenticator.

Even though many organizations use it in this way, and this is a very big problem. My passport picture coupled with a tamper evidence security seal is an authenticator because it links me, something I am, as embodied my photograph, with my identity. Using Social Security numbers for both identification and authentication makes them much more valuable to a criminal who is intent on stealing someone's identity. This is a problem of our own making and it is a problem that we can eliminate.

In the time remaining, I will highlight a few recommendations from my written testimony. First, we should move away from au-

thentication based on information that is easily compromised. Social Security numbers or mother's maiden names are poor choices for authentication.

Second, individuals should be empowered to control the dissemination of their Social Security numbers. Congress can support this by protecting citizens who prefer not to provide a Social Security number when conducting business that does not legally require it.

Third, we should reduce the exposure of citizen Social Security numbers by prohibiting their display on ID cards and in public records and by redacting them from existing public records. For example, Choice Point is now redacting Social Security numbers and other personal information from reports that it provides to its clients. This practice should be required at other companies and organizations, especially data brokers and credit bureaus.

Finally, we should require stronger security practices during the transmission and storage of Social Security numbers and all other personal information.

In conclusion, Congress is the only entity that can make meaningful changes to protect the privacy and identities of U.S. citizens. We are encouraged by your attention to these issues, and the computing professionals that I represent stand ready to help you in your efforts.

Thank you for your attention. I will be happy to answer any questions.

[The prepared statement of Ms. Antón follows:]

**Prepared Statement of Ana I. Antón, Ph.D. Associate Professor,
North Carolina State University**



Association for
Computing Machinery

Advancing Computing as a Science & Profession

**Testimony before the House Committee on Ways and
Means Subcommittee on Social Security on**

**Protecting the Privacy of the Social Security Number
from Identity Theft**

21 June 2007

**Statement of
Ana I. Antón, Ph.D.**

**Associate Professor
North Carolina State University**

**Director
ThePrivacyPlace.Org**

**On Behalf of USACM (the US Public Policy Committee
of the Association for Computing Machinery)**

Introduction

Thank you Chairman McNulty and Ranking Member Johnson for the opportunity to testify.

I am an associate professor at North Carolina State University in the Department of Computer Science in the College of Engineering. I am the director of a privacy research center named ThePrivacyPlace.Org, with collaborating faculty and students at NC State University, Purdue University and Georgia Tech. In addition to my role as a faculty member, I serve on several industry and government boards of technical advisors, including the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. A brief biography is in Appendix A.

This statement represents my own personal position as well as that of the Association for Computing Machinery's (ACM) Committee on U.S. Public Policy (USACM), of which I am a member of its Executive Committee. ACM is a non-profit educational and scientific computing society of more than 84,000 computer scientists, educators, senior managers, and other computer professionals in government, industry, and academia, committed to the open interchange of information concerning computing and related disciplines. The Committee on U.S. Public Policy acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. (See <http://www.acm.org> and <http://www.acm.org/usacm>.)

My statement today highlights two key policy and technology issues:

First, the Social Security number (SSN) should not be used as an identifier or authenticator. Such conflicting uses of SSNs confuse the role of identity and authentication, making the SSN valuable to for stealing someone's identity or committing fraud. Furthermore, because SSNs are so readily available, they are not an adequate means of identification or authentication.

Second, steps must be taken to reduce the use and exposure of SSNs. Reducing the use of SSNs helps protect individual information. The display of SSNs on ID cards and in public records should be prohibited, and SSNs should be redacted from existing public records. From a technical standpoint, we should require government and private entities to secure or encrypt records or documents containing SSNs in storage and during transmission.

Overview

Identity theft is no longer a rare crime impacting few and escaping the general public's attention. Since 2003, more than 36 million Americans have had their identities stolen¹ and since February 2005 over 155 million personal records² have been compromised, causing serious harm to those affected by these thefts and exposures. Massive data breaches, such as last year's stolen laptop containing the Social Security numbers (SSN) of 28 million veterans, are increasingly commonplace and will soon cease to be front-page news. With increasing public awareness of this epidemic, Congressional attention has followed, with no less than eight different committees conducting oversight hearings and proposing numerous bills.

Identity theft is a form of fraud that depends on two different factors, 1) information being improperly acquired, and 2) that information being used to facilitate fraud. The improperly acquired information is the enabler, but it is the fraud that does the damage.

A number of factors enable identity theft, but two key ones stand out for this committee's consideration. First, the use of the SSN is so widespread that it is a de facto national identification number. Businesses and government agencies collect the SSN to identify and then authenticate individuals. This has made it the primary instrument for stealing an individual's identity or creating a "synthetic identity," which is a new identity cobbled together using personal information from several sources. It is the key that unlocks access to credit, banking accounts and various other services for criminals.

Second, current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. As computing technology and storage continue to advance and become cheaper, and as more uses are found for information about people, we can only expect these collection activities to increase. Whereas paper records with personal information, including SSNs, used to require some effort to find, copy and disseminate, the spread of inexpensive computing technology has made it much easier to find, use and exploit such information – for good and for bad. Moreover, SSNs provide a way to easily link data records that should not be easily linkable — a key point in enabling data theft. Reducing the use of SSNs will make it more difficult for thieves to, for example, tie together medical and investment records.

Collectively, these trends suggest that it is a critical time for Congress to act to strengthen the privacy of Social Security numbers. The use of SSNs is widespread, and no amount

¹ Javelin Strategy and Research, "2006 Identity Fraud Survey Report", January 2006, <http://bbb.org/alerts/article.asp?ID=651> and Javelin Strategy and Research "2007 Identity Fraud Survey Report, data obtained from Privacy Rights Clearinghouse, "How Many Identity Theft Victims Are There? What Is the Impact on Victims?", accessed June 12, 2007, <http://www.privacyrights.org/ar/idtheftsurveys.htm>

² Privacy Rights Clearinghouse, "A Chronology of Data Breaches", accessed June 12, 2007, <http://privacyrights.org/ar/ChronDataBreaches.htm>.

of technology or law can “put this genie back in the bottle.” We can, however, construct sensible policies, combined with new business procedures, and deploy technology using best practices for privacy protection. Such measures will help protect SSNs and move us away from relying on them as the key to unlocking one’s identity.

In this testimony, I will touch on several issues that describe the nature of the privacy and security problems with SSNs. I will then discuss alternative approaches to managing identity and plausible technical solutions for protecting privacy. Finally, I will discuss some recommendations for this committee to consider as it moves forward with efforts to protect the privacy of SSNs.

Use as an Identifier and Authenticator

The U.S. government issues Social Security numbers to track taxes and benefits. Originally, the number was connected only with the Social Security program. Over time, governments and other entities have expanded the uses of the SSN. Issued to individuals for nearly three quarters of a century, each SSN is intended to be a unique number that people keep for life. The problem we face today stems from the fact that the SSN is so convenient for tracking individuals across public and private records that it is often used as both an identifier and an authenticator.

An *identifier* is a name or other label that can be used to uniquely select a particular person within a specific group or context. For example, my SSN identifies me within the group of U.S. Social Security participants. But someone who knows my SSN is not necessarily me. Many other people in many contexts have valid access to my SSN.

Authentication is the process of verifying that an identifier is valid and associated with a particular identity. There are three traditional categories of authenticators: knowledge-based (“what you know,” e.g., a password), object-based (“what you have,” e.g., an RFID token or a driver’s license), and ID-based (“what you are,” e.g., a biometric such as a fingerprint).³ There are strengths and weaknesses in each form of authenticator; these are discussed in more detail in USACM’s short tutorial on authentication, attached as Appendix B.

Companies and government agencies rely on the SSN as an identifier because it gives them some added degree of precision when disambiguating individuals. For example, when distinguishing between 20 different Sally Smiths in a database, the SSN is presumed to be unique and indicates exactly one individual. This holds true whether Sally enters her name as Sally Ann Smith, S. Smith, or uses her married name from one of several marriages. Clearly, this identification role is valuable to ensure that records are not mixed and duplicate records are not created. However, privacy problems ensue if access to those same personal records are provided when someone claiming to be Sally provides the SSN as an authenticator. Her family members, former college roommate and professors, employer, banker, former spouses and others likely know her SSN. So does

³ O’Gorman, L. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE*, Volume 91, pp. 2021-2040, 2003.

anyone with access to Sally's records at any organization that uses her SSN to identify her out of all the other Sally Smiths.

From a technical standpoint, the problem with SSNs is that some entities are using them as an identifier, others are using them as an authenticator, and yet others are using SSNs as both an identifier and an authenticator.⁴ For example, professors applying for some Federal grants via the Internet enter their social security numbers, last names, and a password to identify themselves. In this case, the SSN is used as an identifier and the last name as a form of secondary authentication. As another example, use of the SSN when opening a bank account is as an identifier, to indicate who is responsible for taxes. As a last example, if you call your credit card company to increase your credit limit they may ask for your SSN to authenticate you. These conflicting uses confuse the role of identity and authentication and thus make SSNs much more valuable for stealing someone's identity.

Remotely conducted business transactions that rely on the SSN as an identifier and authenticator are particularly risky. If someone is contacting his brokerage via the phone or Internet to purchase stock against a credit card, the brokerage needs to authenticate the identity of the customer as the holder of the credit card and the brokerage account. The customer also needs to authenticate that he is communicating with the real brokerage, and not with a criminal seeking to steal his credit card information. Furthermore, the authentication needs to be performed in a way that someone eavesdropping on the transaction cannot then masquerade as either party for any other operation. Knowledge of a SSN (or any other universal identifier) is not sufficient to reliably authenticate any party in this transaction, but this use is commonplace.

Ubiquity of SSNs

SSNs are so widely used that they are a de facto national identifier. Commercial entities and government agencies rely on their use, some states have them on driver's licenses, employers use them as medical plan IDs and employee IDs, and many colleges have long used them as student IDs. (In recent years universities have moved away from the use of SSNs). The military also uses SSNs as military serial numbers and has them exposed on the Common Access Card that every member the military carries for identification⁵.

In testimony before Congress⁶ in 2004, the General Accounting Office found that an estimated 42 million Medicare cards displayed entire 9-digit SSNs, as did approximately

⁴ S.L. Garfinkel. Risks of social security numbers. *Communications of the ACM* 38(10), pp. 146, October 1995.

⁵ B. Acochido & J. Swartz. "Military Personnel Prime Targets for ID Theft." *USA Today*, June 15, 2007, accessed June 18, 2007, http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-06-14-military-id-thefts_N.htm?csp=34.

⁶ Government Accountability Office, "Social Security Numbers: More Could Be Done to Protect SSNs", March 20, 2006, <http://www.gao.gov/new.items/d06586t.pdf>

8 million Department of Defense (DOD) insurance cards and 7 million Department of Veterans Affairs (VA) beneficiary cards.

As we have moved from paper-based systems to digital ones, the exposure of SSNs has increased. SSNs are often used as identifiers on public documents, such as property deeds. Before the widespread use of digital technologies, databases and networking, these documents represented little threat of being a source of large-scale identity theft. However, now such documents are digitally scanned and incorporated into massive databases often held by data brokers that share or sell this data. This facilitates identity fraud in dealing with other organizations that use knowledge of the SSN as a form of authentication. This secondary use and electronic transmission of this data creates an array of opportunities for the data to be intercepted and misused.

Data Security

Two weeks ago, before this subcommittee, Dr. Peter Neumann⁷ (an expert on privacy, security and trustworthy computing issues) discussed the security and reliability vulnerabilities of the existing computing infrastructure and the poor current state of practice in building trustworthy systems. These vulnerabilities can and have led to the exposure of personal information, particularly SSNs. Nearly two-thirds of the security breaches from January 1, 2005 to June 11, 2007 resulted in the exposure of SSNs.⁸ (There were more than 600 publicly reported data breaches during time period and, of these breaches, more than 400 potentially exposed SSNs.⁹)

Creating complex systems that are dependably trustworthy (secure, reliable, survivable in the face of many adversities) remains a grand challenge of computer science. Further, because many of the privacy problems are related to total systems, encompassing computers, communications, people, and procedures, they cannot be adequately protected by technological approaches alone. While better computer security is a worthwhile technical and policy goal, these factors suggest that a better approach is to move away from reliance on SSNs – at the very least, to avoid depending on them as means of authenticating identity.

Alternative Identifying Techniques

Reducing the use of SSN as both an authenticator and identifier will better protect privacy and security; however, the question is, what other techniques can we use that better protect identity?

⁷ Testimony of Peter G. Neumann For the Congress of the United States House of Representatives Committee on Ways and Means Subcommittee on Social Security Thursday, June 7, 2007, http://www.acm.org/usacm/PDF/EJVS_Testimony_Peter_Neumann_USACM.pdf

⁸ Privacy Rights Clearinghouse, "A Chronology of Data Breaches", accessed June 12, 2007, <http://privacyrights.org/ar/ChronDataBreaches.htm>.

⁹ Ibid.

A study by the American Journal of Public Health detailed the effectiveness of combinations of data used as identifiers instead of the SSN¹⁰. It found the SSA National Death Index could be used to identify people by certain data points (First Initial, Last Name, Day of Birth, Month of Birth, and Year of Birth) as accurately with or without the SSN. This means that adding the SSN falls within the margin of error when searching with only the first initial, last name and birth year. Adding full name, full birth-date, and possibly some other information such as birthplace would likely provide as complete and unique identification as the SSN.

We should not, however, replace one enabler of ID theft with another. Many of these data points are more readily available to strangers than SSNs. Thus, it is important that they not be used to *authenticate* identity for anything of value. Clearly, context for determining identity matters, but the larger issue is that we should move away from reliance on any system that creates universal identifiers, and especially from systems that use knowledge of those identifiers as authenticators of that same identity. It is more secure to use multiple factors to confirm an individual's identity. For data aggregators looking for a universal identifier, it may be more convenient – perhaps even more profitable – to work on ways to effectively sort and target their analyses to confirm that the information they collect is appropriate for their intended uses.

Designing Systems to Protect SSNs

Databases containing personal information often employ the SSN as the “primary key” or common identifier. This exacerbates the problems I have addressed as it presents yet another vulnerability by making it easier to match records from disparate data sources. Replacing SSNs as the primary key in these systems is not a large technical hurdle in most cases. Random 9-digit numbers would work for virtually every company in the U.S. and would not be difficult to generate. We can better protect individual privacy by using different, random numbers in each company database. This would prevent someone from easily correlating the personal data an individual held in several of those databases.

The technical challenge is in replacing the SSN in all those databases. First and foremost, if an SSN is being used in a database as an index, then replacing it will require updating the index. Indexes generally exist to make common selection operations faster in databases. The worst-case scenario would be a database that has a great many transactions per day and little to no downtime to update the index. For large, always-on databases, replacing the SSN and updating the index can be a difficult process, but it is possible.

The cost of cleaning up records in commercial databases is likely far from prohibitive for all but the smallest of commercial entities. Usually smaller entities have less expertise, time and money to scrub their records of SSNs. But, the smaller entities are also the least attractive targets for identity theft.

¹⁰ B.C. Williams, L.B. Demitrack, and B.E. Fries. “The accuracy of the National Death Index when personal identifiers other than Social Security number are used.” *American Journal Public Health*. 82(8): 1145-1147, August 1992.

The most vulnerable databases are employee records, which are typically not as secure as other business databases both because of insider threat and because they are often overlooked in audits of business assets.¹¹

Universities are increasingly discontinuing the use and storage of SSNs whenever possible, replacing them with university-specific ID numbers (i.e., a random 9-digit identifier that is not the SSN). In cases where SSNs must be collected and stored (e.g., for employment and financial aid), the SSN is no longer being maintained as the common identifier or primary key. In addition, universities are actively adopting technologies to protect SSNs. For example, devices containing SSNs are being protected by a password-based security system using encryption. This voluntary approach can serve as a model for other industries in the U.S. to similarly move away from the use of SSNs as primary identifiers.

Recommendations

There are several actions that can be taken to protect the privacy of SSNs. I present two sets of recommendations. The first set of recommendations address the purposes for which SSNs are used. The second addresses how SSNs are stored and transmitted.

Recommendations on the Purposes and Uses of SSNs

- No bank, credit agency, government agency, or other entity should verify the identity of a person based on weak authenticators such as knowledge of an SSN or mother's maiden name. Instead, they should require stronger authentication of identity when conducting business. Strong authentication can initially be provided by a passport, military ID or license with a photograph.¹² Once that is established, a secondary authenticator such as a secret, shared password or PIN can be used for subsequent transactions. While this requires additional effort, it provides extra layers of security, and should help assure the public that the security and privacy of their information is being taken seriously.
- Universities are voluntarily moving away from SSNs in an attempt to reduce their liability under the Family Educational Right to Privacy Act (FERPA) if SSNs are accidentally exposed. This has also led to improvement of their database security. Congress should consider making private institutions financially liable in a manner similar to universities: Consumers would have a civil right of action if their SSNs or other personal information is collected or exposed without a valid business need-to-know, whether intentionally or inadvertently.

¹¹ Stephanie Armour. "Employment records prove ripe source for identity theft," *USA Today*, January 23, 2003. http://www.usatoday.com/money/workplace/2003-01-23-idtheft-cover_x.htm

¹² There are other dangers to taking this approach to a logical conclusion: having some other form of national ID. We do not support this alternative.

- There should be no penalty or discrimination against someone who will not provide an SSN when conducting business, except where required by law to disclose that information. Moreover, entities that collect SSNs should provide notice that there will be not be a penalty for withholding the SSN. Within this context, it should be an unfair trade practice for private entities (e.g., utilities) to penalize or refuse to transact business with someone who declines to provide an SSN that is not required by law. Coupled with the previous recommendation, this provides a strong incentive to move away from the SSN. It is also consistent with advice from the Federal Trade Commission on protecting oneself from identity theft.¹³

Recommendations for Protecting SSNs in Storage and During Transmission

- The display of SSNs on ID cards and in public records should be prohibited. Further, SSNs should be redacted from existing public records. Redacting SSNs is, admittedly, complex because computers (and the Internet) are not good at “forgetting” things. Once something is stored in a computer, erasing it everywhere it is stored is difficult.

The National Security Agency has posted guides¹⁴ on how to redact data, but the reality is that redaction has a bad reputation as a workable solution. Paper redaction techniques such as covering a name or diagram with a blackened area do not work well in digital files. There are also so many different formats for digital files that the techniques that do work are generally not portable among formats. However, ChoicePoint, as one of its newly adopted business practices in the wake of its landmark \$16 million settlement for endangering the privacy of over 160,000 consumers in 2005, is now redacting SSNs and other personal data from the public records that it provides to its clients. This is a welcome development and one that could be required at other companies, especially data brokers and credit bureaus, as a matter of public policy.

There are other steps that can be taken to reduce the use and exposure of SSNs. They include:

- Require transmission of records or documents to be secure or encrypted if they contain SSNs and other personally identifiable information. Even basic Secure Socket Layer (SSL) encryption would help reduce the incidence of exposure and minimize the damage. SSL technology is readily available and is commonly used by almost every reputable e-commerce site. Properly encrypted data is usually protected even if it is stolen (e.g., on a laptop disk or thumb drive).
- Require electronic security for files and devices containing SSNs. Each instance of access to SSNs in databases should be logged for audit purposes and require a

¹³ Federal Trade Commission, “ID Theft: What’s It All About?”, June 2005.
<http://www.ftc.gov/bcp/online/pubs/credit/idtheftmini.pdf>

¹⁴ See both <http://www.fas.org/spp/othergov/dod/nsa-redact.pdf> and <http://www.nsa.gov/snac/>

secure session. These measures insert a level of security and accountability into the maintenance of these databases. With proper access controls (where individuals who access the database are controlled, recorded, and their specific access limited to a minimal number of records), individuals can be held accountable for breaches and exposures of SSNs that can be traced to a specific access of a database.

- Eliminate the SSN as primary key in databases containing SSNs. A primary key uniquely identifies each record in a database table. Instead of using the SSN, the primary key should be a unique number generated by the database management system. Universities and other large institutions have made this transition, and their example should be encouraged in other agencies, companies and organizations.
- USACM has a set of recommendations for enhancing the security, privacy and accuracy of personal data kept in databases. Those recommendations are attached as Appendix C. We encourage the committee to consider how these might be integrated and supported by any legislation crafted to protect SSNs and related personal information held either by government or by private organizations.

Conclusion

The increasing incidence of identity theft and data breaches requires that all entities, public and private, take steps to better protect information. Where this subcommittee can help is in encouraging a reduction in the use of the SSN in commercial and government transactions and in public records. The SSN is used much more than is necessary and the ubiquitous presence of SSNs makes them ideal targets for identity theft. Because these numbers are so readily available, they are not an adequate means of identification or authentication as many consider them to be. Reducing the use of SSNs helps protect individual information and encourages businesses, government and universities — some of which have already started to make changes — to move towards other means of identification. These alternate means in many cases can be as accurate, and more secure, than using the SSN. Increased privacy and security is not only a public good, but may make people more comfortable about conducting business online.

Acknowledgments

I am particularly grateful to Cameron Wilson (ACM Director of Public Policy), David Bruggeman (ACM Public Policy Analyst), Eugene H. Spafford (USACM Chairman, and Professor at Purdue University), Travis D. Breaux, Laurie A. Jones, Aaron K. Massey, Paul N.H. Otto, and many other members of ACM and USACM for their generous help in my preparing this testimony.

Appendix A – Biographical Information

Dr. Annie I. Antón is an Associate Professor of Software Engineering in the College of Engineering at the North Carolina State University. She received her Ph.D. in Computer Science in June of 1997 with a minor in Management and Public Policy from the College of Computing at the Georgia Institute of Technology in Atlanta. Her thesis co-advisors were Dr. Peter A. Freeman and Dr. Colin Potts. She received a BS in Information and Computer Science with a minor in Technical and Business Communication in 1990 and an MS in Information and Computer Science in 1992 (also from Georgia Tech). After one year at the University of South Florida, Dr. Antón joined the computer science department at NC State. She was awarded an NSF CAREER Award in 2000, named a CRA Digital Government Fellow in 2002, nominated and selected for the 2004-2005 IDA/DARPA Defense Science Study Group, and received the CSO (Chief Security Officer) Magazine "Woman of Influence in the Public Sector" award at the 2005 Executive Women's Forum. She is associate editor of *IEEE Transactions on Software Engineering*, the cognitive issues area editor for the *Requirements Engineering Journal*, and a member of the International Board of Referees for *Computers & Security*. She is a member of the International Association of Privacy Professionals, a senior member of the IEEE as well as a member of the ACM U.S. Public Policy Committee's Executive Committee. Antón currently serves on several boards: the NSF Computer & Information Science & Engineering Directorate Advisory Council, the Computing Research Association's Board of Directors, the CRA-W Board, an Intel Corp. Advisory Board, the Department of Homeland Security Data Privacy and Integrity Advisory Committee, the Berkeley TRUST Center Distinguished Advisory Board, and the Georgia Tech Alumni Association Board of Trustees. She is a former member of the Microsoft Research University Relations Faculty Advisory Board and the Georgia Tech Advisory Board (GTAB). Dr. Antón is director of ThePrivacyPlace.Org (<http://theprivacyplace.org>), and co-director of the NC State Electronic Commerce Studio. Her URL is: <http://www.esce.ncsu.edu/faculty/anton>.

About USACM

USACM is the U.S. Public Policy Committee of the Association for Computing Machinery (ACM). USACM members include leading computer scientists, engineers, and other professionals from industry, academia, and government. (<http://www.acm.org/usacm>)

About ACM

ACM, the Association for Computing Machinery (<http://www.acm.org>), is an educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

Appendix B – Understanding Identity and Identification**USACM**

The Public Policy Committee of ACM

Understanding Identity and Identification

Professionals who work with issues of security and control use some terms to precisely describe access to resources and naming. These same terms have usage in general language, but the words frequently are used imprecisely and even misleadingly. When describing how security in information systems operate, and when formulating regulations or laws, it is important that these terms are understood and used precisely.

The purpose of this short document is to describe these important terms for readers who are not familiar with the more formal definitions. These related terms are *identification*, *authentication*, and *authorization*. Related concepts include *uniqueness* and *biometrics*.

Terms

Identification is associating a distinguishing label (*identifier*) with something within a specific group or context. You can identify someone by getting both their label and the context of that label. An ID card can provide both the name (e.g. “John Smith”) and the context (e.g., “licensed driver”). Identification can also occur by providing only the context or group name, such as identifying oneself as a police officer, a student, a graduate of West Point, or a member of Congress by wearing an appropriate badge, uniform, or class ring. The reliability of an identification depends on the confidence that the distinguishing label and context actually apply to the individual in question.

Note that even when identification is reliable – and it often is not – it does not imply anything beyond being able to distinguish among items or people. Identification can be used to determine if someone is a member of a group or not, or among members of the group. If someone were to identify herself as “Snow White,” that is an identification if she uses it consistently. In the context of a Halloween party or an Internet chat room, that may be a logical label to adopt.

A key concept is that identification does not need to be a standard name. It can be a nickname, a login, or a simple description, such as “I am the tallest one here” or “I am the one with red hair.” Those are means to distinguish one person from another in a particular group context.

People are most often identified in social situations by their names. In the United States, these names are usually composed of a first (given) name, one or more middle names (usually), and a last (family) name. In other countries, names may be a single word, or

everyone may have a common family or middle name.

Uniqueness is when multiple items do not have the same identifier. Human names are seldom unique across a large enough population. For instance, there are many, many people named “John Smith” in the USA. If we also consider ancestors, then there may be even more individuals who have been associated with the same identifier (name).

We can further qualify an identifier to make it more specific and less likely to be a duplicate of another identifier. For instance, someone could be “John Smith who was born April 1, 1952 in Boise and whose mother was named Matilda.” However, we cannot always be certain this is unique, and it is unwieldy to use in formal documents. Thus, we commonly use an artificial identifier that is generated and assigned in a manner that ensures that it is unique within context. For instance, Social Security numbers are supposed to be assigned without reuse, making them theoretically unique. Other identifiers (e.g., driver’s license numbers) are similarly generated to provide uniqueness.

Authentication is the process of verifying – to some desired level of confidence – that a claimed identifier is valid and actually associated with a particular item or person. Often, this validation is performed by one or more persons inspecting the identification and authenticator(s). The authenticators can also be examined by some technical means, such as a login program or a badge reader connected to a computer.

Authenticators of people are typically some combination of “something known,” “something possessed,” and “something about (structural)” the person. These items have been previously registered with the persons or organizations performing the authentication. Additional factors can also be used, such as physical location, recognition by human or canine guards, and so on.

- *Something known* is a secret or a fact that is unlikely to be known to an impostor. Passwords, when properly chosen and protected, are this form of authenticator. In many old combat movies, the spy is exposed because he doesn’t know which team won the World Series the previous year – this is another form of “something known” as a group authenticator. Many companies use items such as “mother’s maiden name,” “birth date” or “social security number” as authenticators, but this is bad practice as those items are often easily discovered facts: Many of these items are public information as a matter of law or custom.
- *Something possessed* is a distinguishable token or a key that matches a counterpart. A license issued by a government agency is a form of token. Another example from an old movie is the dollar bill or playing card that is ripped raggedly in half – the two halves are kept and joined together to *mutually authenticate* two parties.
- *Something about* (structure) the object or person being authenticated. We can examine something physical about the person we wish to identify, such as a fingerprint, or the pattern of blood vessels inside the eye. If the comparison of a

person's distinguished characteristic is automated, then it is known as a *biometric*.

A current location may also be used for authentication, such as GPS coordinates, telephone caller-id or computer network address.

Using a combination of authenticators is known as *multi-factor authentication*.

Authorization is the granting of rights (verb) or the grant itself (noun). Generally, one authorizes an authenticated party. *Permission* is used by some people as a synonym for authorization.

An example

Consider a scenario involving a person who wishes to enter a guarded building. When the person approaches the building to enter, a guard stops him to verify that he can enter. The person produces an *identification* card (something possessed) issued by a trusted authority (the context). The guard compares the picture on the ID with the face of the person, and causes him to put his fingers on a scanner (a biometric). These checks confirm that the person is the one identified by the card. She has been instructed that anyone with a valid blue card is allowed to enter, but without a cell phone, so she allows the person to pass after determining that he does not have a cell phone.

Note that this is use of multi-factor authentication, and the identification is based on group membership ("people with a valid blue badge") – no specific name or ID number is required. Permission to enter is the authorization involved. A further element of access control that is not based on identity or authentication is also involved: there is no authorization to carry a cell phone in.

There are many potential weaknesses in this system as described. The system can be redesigned to prevent the weaknesses, but defensive measures may be too expensive or cumbersome to be worth the effort given both the likelihood of the threats occurring and the value of what is behind the door. Examples of weaknesses include:

- The picture on the card may be old and the guard makes a false negative authentication: she refuses to allow the authorized person to pass.
- The guard may be overpowered or bribed so that unauthorized people enter.
- The card has been altered from a valid card — the color has been changed, or the original holder's photograph and fingerprints have been replaced by this impostor.
- The cards are made to published standards without adequate safeguards: this is a forged card made by a well-informed and sophisticated attacker.
- The attacker has stolen the card, disguised himself as the cardholder, and donned fingerprint caps that fool the scanning machinery.

- The guard is unable to recognize a disguised cell phone.
- Someone pretending to be a law enforcement officer, in uniform, orders the guard to let him pass or he will arrest her for obstructing justice. She complies.
- If too many people arrive in a short time, the guard may not be able to process them in a timely fashion, and someone is either denied access incorrectly or slips in unnoticed.
- The guard may fall ill and leave her post, leaving the door locked or unlocked for subsequent visitors.
- A first-time visitor has no way of knowing that this is really a legitimate guard and the right door!

Additional Notes

1. As illustrated by the last point in the previous example, the problem of authentication is bidirectional — all parties in the transaction need some level of assurance that they know the identities of the other parties. This is one reason why *phishing* succeeds: the customers enter their authenticating information, but the other party (the purported merchant) is not strongly authenticated to the customer.
2. It is possible to have authentication and authorization without specific identification. For instance, producing an *authentic* \$20 bill provides authorization to make a purchase for something up to \$20 in cost. It is not a requirement to *identify* the purchaser beyond being a member of the group who has cash.
3. Knowing precise, authentic identity **does not disclose intent!** Knowing the name of everyone who enters a building or boards a plane does not mean that they will be well-behaved. Mohamed Atta's Florida driver's license and picture were legitimate and examined when he passed through airport security on 9/11/2001. Most identification checks instituted in the wake of 9/11 perform at most a weak security function because there is poor (or no) authentication, and even when the identity is known it does not prove anything about intent.
4. Social security numbers are not supposed to be reused. However, numerous recorded cases of SSN duplication make the use of these numbers as unique IDs problematic.
5. Most biometrics have been developed and tested for authentication of a claimed identity, not for performing the identification itself; fingerprints are a notable exception. Insufficient experience has been gained with both physical features and biometrics to know error rates over large populations. By example, given the data that John Smith is 6'1" tall, has brown hair and green eyes, we can determine with some confidence whether a person in the room claiming to be John is actually John.

However, given that same information and a crowd of people in a football stadium, we cannot be certain that we can uniquely identify John if he is present. Almost certainly, we will also make many false positive identifications. The same problems may exist with automated biometrics such as measuring facial features or hand geometry.

6. We know that every potential biometric has deficiencies. Not everyone has valid fingerprints over their entire lives, twins and triplets have the same DNA, and so on. People with special interests in some technologies have made unsupported claims about the performance of certain biometrics.
7. Most organizations use weak authenticators. In part, this is because most people are poor at remembering items such as long passwords and multiple ID numbers. As noted, use of authenticators such as mother's maiden name, social security number, or other such items is poor practice because those items can be easily found for many people.
8. Every instance where identifiers and authenticators are to be used should be carefully analyzed to determine strengths and weaknesses. This includes the value of what is being protected, and the consequences of false positives (authenticating an incorrect identity) and false negatives (failing to authenticate a valid identity).
9. As noted, identification and authentication mechanisms depend on context. Any security protocol is only as strong as the weakest element.

Appendix C – Privacy Policy Recommendations**USACM**
The Public Policy Committee of ACM
Policy Recommendations on Privacy
June 2006**BACKGROUND**

Current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. These technologies, which are widely used by many types of organizations, allow for massive storage, aggregation, analysis, and dissemination of data. Advanced capabilities for surveillance and data matching/mining are being applied to everything from product marketing to national security.

Despite the intended benefits of using these technologies, there are also significant concerns about their potential for negative impact on personal privacy. Well-publicized instances of personal data exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. Personal data — including copies of video, audio, and other surveillance — needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. Protecting privacy, however, requires more than simply ensuring effective information security.

The U.S. Public Policy Committee of the Association for Computing Machinery (USACM) advocates a proactive approach to privacy policy by both government and private sector organizations. We urge public and private policy makers to embrace the following recommendations when developing systems that make use of personal information. These recommendations should also be central to any development of any legislation, regulations, international agreements, and internal policies that govern how personal information is stored and managed. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and policy makers, but one of vital importance. For this reason, USACM has developed the following recommendations on this important issue.

RECOMMENDATIONS**MINIMIZATION**

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.
2. Store information for only as long as it is needed for the stated purposes.
3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.
4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.

5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

CONSENT

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (*opt-in*); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal information, including when appropriate, the deletion of that information (*opt-out*). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)
7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

OPENNESS

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.
9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).
10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.
11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.
12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.
13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

ACCESS

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.
15. Provide mechanisms to allow individuals to determine with which parties their information has been shared, and for what purposes, unless legally exempted from doing so.
16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

ACCURACY

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.
18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

SECURITY

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.
20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

ACCOUNTABILITY

21. Promote accountability for how personal information is collected, maintained, and shared.
22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.
23. Maintain *provenance* — information regarding the sources and history of personal data — for at least as long as the data itself is stored.
24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

USACM does not accept the view that individual privacy must typically be sacrificed to achieve effective implementation of systems, nor do we accept that cost reduction is always a sufficient reason to reduce privacy protections. Computing options are available today for meeting many private sector and government needs while fully embracing the recommendations described above. These include the use of de-identified data, aggregated data, limited datasets, and narrowly defined and fully audited queries and searches. New technologies are being investigated and developed that can further protect privacy. USACM can assist policy-makers in identifying experts and applicable technologies.

Chairman MCNULTY. Thank you, Dr. Antón.
Welcome back, Mr. Rotenberg.

**STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR,
ELECTRONIC PRIVACY INFORMATION CENTER**

Mr. ROTENBERG. I seem to have a technological problem but thank you, Mr. Chairman, Mr. Johnson and Members of the Subcommittee. It is nice to be with you this morning, and I appreciate the opportunity to testify on this issue. I have over the years appeared before the Subcommittee on the Social Security number issue. I have also litigated a number of the leading Social Security number privacy cases, one of which involved a resident in Virginia a number of years ago who was asked by the state secretary to provide his Social Security number when he went to register to vote. He did not object to that, what he objected to was the fact that the state of Virginia was publishing his Social Security number in the public voting rolls, and he said that that was a threat to his personal privacy. We wrote a brief for the Federal Appeals Court at that time, before people even used the phrase “identity theft” and we said if you make the Social Security number available, it will make it easier for people to commit the crime of financial fraud.

Fortunately, the court agreed with us. The state of Virginia and many other states changed their practices. Unfortunately, as you know, this problem has become quite a bit more severe over the last several years. I am going to say a few words about that today.

One of the key points I wanted to make this morning is actually I think the Privacy Act 1974 saw this problem coming and there is a provision in the Privacy Act that says very clearly that the Federal Government should try to minimize the collection and use of the Social Security number. It really should only be used for the original intended purposes, as well as a few others that have been authorized by law, including the use as a taxpayer identification number. But, as we all know, today the Social Security number is widely used across the Federal Government.

It is used also in the financial services sector, which for some of the reasons that Professor Antón has described, creates a particular problem for consumers in this country. The Social Security number is both an identifier and a password. If you have access to someone else's Social Security number, there is a very good chance that you are going to be able to pull up the records on that person and also use the number to get access to the content of those records, and that is precisely what identity thieves do when they use the Social Security number to get access to someone's credit record information.

Now, I describe in my testimony the problem has not escaped the notice of the White House. The President established a Task Force on Identity Theft, it was cochaired by the Attorney General, the chair of the Federal Trade Commission. We spent a lot of time on that task force, and we made some very specific recommendations. The task force rightly said that Social Security numbers were contributing to this problem but in our view, they did not go far enough to recommend strong solutions to diminish the problem. They wanted more enforcement authority to go after people who committed the crime of identity theft, but they did not do enough in our opinion to limit the collection and use of the Social Security number to really get to the problem at its source.

So the rest of my testimony talks about some of the specific suggestions and actions that I believe the Congress could take to limit the problems associated with the misuse of the Social Security number, not using it for example as a record identifier, particularly in the private sector, not publicly displaying it on Web sites, not putting it on identity cards. As I also describe, and it speaks to an issue that you raised earlier, Mr. Ryan, I think the more difficult we make it for people to use the Social Security number as a general purpose identifier, the more likely it is that businesses will come up with other systems of identification that are appropriate for a specific context.

If we think about it, this is actually our commonsense understanding of what an identifier should be. You have a bank account number for your banking relationship. You have a credit card number for your credit relationship. You probably have a number for your utility bill. That is actually a very good thing because if one of those numbers are compromised, it does not create a risk for you that all the other account information will be compromised. But part of the way to make that system work is to not let businesses

cut corners by using the Social Security number in place of their own record identifier. So, that is a very important part of our recommendation for you today.

Regarding the bill that has passed out of the Committee on Energy and Commerce, we think it is a good bill. It includes a lot of important provisions, but we do have a couple of specific recommendations that we think could make it a bit stronger. One issue we are particularly concerned about, and I know it is something that this Committee has considered in the past, and that is the issue of state pre-emption.

Now, you know if you pre-empt the states in this area, a lot of legislation that has already been passed that protects the privacy of the Social Security number will be effectively overwritten, and I think that could be very problematic, particularly in this area where things are developing so quickly. So, what I would urge you to do on that issue is to establish a Federal base line, make the national standard the floor. For the states where there is not protection, you will give them protection. But if it is a baseline, you allow the states that are doing more and trying to anticipate some of the new problems to go forward and maybe give you some material for the next bill.

So, thank you very much for the opportunity to testify.

[The prepared statement of Mr. Rotenberg follows:]

**Prepared Statement of Marc Rotenberg, Executive Director,
Electronic Privacy Information Center**

I. Introduction

Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee, thank you for the opportunity to testify on the misuse of the Social Security number and the escalating problem of identity theft

My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C.¹ Founded in 1994, EPIC has participated in the leading cases involving the privacy of the Social Security number and has frequently testified in Congress about the need to establish privacy safeguards for the Social Security number to prevent the misuse of personal information.²

Two weeks ago in testimony, I urged the Subcommittee to strengthen the privacy safeguards for the proposed Employment Eligibility Verification Systems and warned that the errors in the Basic Pilot will be exacerbated by the increased dependence on the SSN.³ And, about a year ago, I urged Members of this Subcommittee to reject the use of the SSN as a national identifier and to ensure the

¹EPIC maintains an archive of information about the SSN online at <http://www.epic.org/privacy/ssn/> ["EPIC SSN Page"].

²See, e.g., *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994) ("the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs"); Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), available at http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Chris Jay Hoofnagle, Legislative Counsel, EPIC, *Testimony at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the H. Ways & Means Subcom. on Social Security & the H. Judiciary Subcom. on Immigration, Border Sec. & Claims*, 105th Cong. (Sept. 19, 2002), available at <http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html>.

³Marc Rotenberg, President, EPIC, *Testimony at a Hearing on Employment Eligibility Verification Systems Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (June 7, 2007), available at http://www.epic.org/privacy/ssn/eevs_test_060707.pdf.

development of adequate privacy and security safeguards to address the growing crisis of identity theft.⁴

Today, my statement will focus on the dramatic increase in identity theft in the United States that has resulted directly from the misuse of SSN and the need to pass comprehensive legislation to limit the use of the SSN as well the need to develop better systems of identification that are more robust.

II. Summary of Social Security Number History

Social Security numbers have become a classic example of “mission creep,” where a program designed for a specific, limited purpose has been transformed for additional, unintended purposes, some times with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security.

These risks associated with the expanded use of the Social Security number and identification cards underscore the importance of the hearing today.

The SSN was created in 1936 for the purpose of administering the Social Security laws. SSNs were intended solely to track workers’ contributions to the Social Security fund. Legislators and the public were immediately distrustful of such a tracking system, which can be used to index a vast amount of personal information and track the behavior of citizens. Public concern over the potential abuse of the SSN was so high that the first regulation issued by the new Social Security Board declared that the SSN was for the exclusive use of the Social Security system.

Over time, however, legislation allowed the SSN to be used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the Social Security number that show a striking resemblance to the problems we face today. Although the term “identify theft” was not yet in use, *Records Computers and the Rights of Citizens* described the risks of a “Standard Universal Identifier,” how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted “prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes.”⁵

In enacting the landmark Privacy Act of 1974, Congress recognized the dangers of widespread use of SSNs as universal identifiers, and included provisions to limit the uses of the SSN. The Privacy Act makes it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN. Section 7 of the Privacy Act specifically provides that any agency requesting that an individual disclose his or her SSN must “inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it.”⁶ The Privacy Act makes clear Congress’ recognition of the dangers of widespread use of SSNs as universal identifiers.

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

But the reality is that today the SSN is the key to some of our most sensitive and personal information. The financial services sector, for instance, has created a system of files, keyed to individuals’ SSNs, containing personal and financial information on nearly 90 percent of the American adult population. This information is

⁴Marc Rotenberg, President, EPIC, *Testimony at a Hearing on Social Security Number High-Risk Issues Before the H. Ways & Means Subcom. on Social Security*, 109th Cong. (Mar. 16, 2006), available at http://www.epic.org/privacy/ssn/mar_16test.pdf.

⁵Dep’t of Health, Educ. & Welfare, Secretary’s Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 125–35 (MIT1973), available at <http://www.epic.org/privacy/hew1973report/>.

⁶Privacy Act of 1974, 5 U.S.C. §1A552 (a) (2006).

sold and traded freely, with virtually no legal limitations. In addition, credit grantors rely upon the SSN to authenticate a credit applicant's identity. Many cases of identity theft occur when thieves apply using a stolen SSN and their own name. Despite the fact that the names, addresses, or telephone numbers of the thief and victim do not match, accounts are opened and credit granted using only the SSN as a means of authentication.⁷

Even the government is susceptible to identity theft based solely on obtaining an SSN and the name associated with it. Stolen SSNs are used to file fraudulent tax returns and to seek refunds owed to other citizens. When the proper owner of the SSN files his tax return it may be rejected as a duplicate and he may be required to spend time fixing his records in order to receive his tax refund.⁸

III. President's ID Theft Task Force and Nexus Between SSNs and Identity Theft

The growing misuse of the Social Security number and the associated problem of Identity Theft have not escaped the notice of the White House. In May 2006, the President established an Identity Theft Task Force to "track down on the criminals who traffic in stolen identities and protect American families from this devastating crime."⁹ The Task Force, chaired by the Attorney General and the FTC Chair, was expected to protect the financial information of citizens and reduce the threat of identity theft, which the FTC now annually reports is the number one concern of American consumers.¹⁰

EPIC participated in the task force proceedings and provided extensive comments.¹¹ We supported the Task Force's recommendation to reduce reliance on SSNs at all levels of government. We said:

Reducing use of SSNs and limiting the amount of data collected by government bodies is fundamental to maintaining the security of consumer data. This is an especially critical limitation upon the public sector, since government has the power to compel individuals to disclose personally identifiable information. The personal data collected by government entities should never be disseminated in public records or sold to the private sector. The Task Force should curtail the publicly available sources of the SSN, including the Social Security Death Register; bankruptcy filings and other court records; birth and death records; and records of other life events.¹²

EPIC also pointed to the growing problem of the misuse of the SSN by businesses: The Task Force should also carefully investigate and analyze SSN use in the private sector, as there is evidence that private sector use of SSNs contributes substantially to the problem of identity theft. Restricting the sale, purchase and display of SSNs by private entities is a critical consideration in combating identity theft. The private sector must move away from using SSNs as identifiers, a goal which is feasible as demonstrated by Empire Blue Cross' transition from SSNs to alternative identification numbers for its 4.8 million customers.¹³

The President's Task Force recognized the connection between the misuse of the Social Security number and the crime of identity theft but failed to propose adequate safeguards. According to the President's Identity Theft Task Force, "the SSN is especially valuable to identity thieves, because often it is the key piece of information used in authenticating the identities of consumers."¹⁴ The SSN is also commonly used by the government and entities in the private sector to identify individuals. As the Task Force noted, "SSNs—are widely used in our current marketplace to match consumers with their records (including their credit files) and as part of

⁷See, e.g., *TRW, Inc. v. Andrews*, 534 U.S. 19 (2001) (Credit reporting agencies issued credit reports to identity thief based on SSN match despite address, birth date, and name discrepancies); *Dimezza v. First USA Bank, Inc.*, 103 F. Supp.2d 1296 (D. N.M. 2000) (same). See also *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003) (Credit issued based solely on SSN and name, despite clear location discrepancies); *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997) (same); *Vazquez-Garcia v. Trans Union De P.R., Inc.*, 222 F. Supp.2d 150 (D. P.R. 2002) (same).

⁸President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 21 (April 23, 2007) ["ID Theft Task Force Report"], available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

⁹Press Release, Office of the Press Sec'y, Fact Sheet: The President's Identity Theft Task Force (May 10, 2006), available at <http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html>.

¹⁰Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January–December 2006* (Feb. 7, 2007), available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>.

¹¹EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), available at http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf.

¹²*Id.* at 8.

¹³*Id.* at 8–9.

¹⁴ID Theft Task Force Report at 23, *supra* note 8.

the authentication process.”¹⁵ In short, SSNs function as both a username and a password—a single piece of information that both identifies an individual and authenticates that identification, a lock and a key rolled into one. Because of the way in which the SSN is used for identification and the prevalence of that use, much of your most sensitive information does not even have the same sort of rudimentary security as your email account.

As noted by the Task Force, “the SSN is a critical piece of information for the thief, and its wide availability increases the risk of identity theft.”¹⁶ Despite the problems associated with using the SSN as an identifier, the Federal Government routinely uses SSNs in order to identify individuals within governmental programs. SSNs have been included as part of Medicare’s Health Insurance Claim Number,¹⁷ and as part of a federal award identifier used by the USDA.¹⁸

IV. Identity Theft as a Result of Social Security Number Misuse

During the past fiscal year, the Department of Justice charged 507 defendants with aggravated identity theft. The DOJ highlighted a number of these prosecutions in a recent press release.¹⁹ A handful of the cases the DOJ put on display involved defendants misusing Social Security numbers for illegal purposes.

In one of the cases, a woman was sentenced to 75 months imprisonment for defrauding FEMA in the wake of Hurricane Katrina.²⁰ The defendant filed 28 fraudulent claims for disaster relief to FEMA using other people’s Social Security numbers. After receiving money from FEMA, the defendant went out to buy real estate, a mobile home, vehicles, electronics, furnishings, and other goods and services.

In another case, six defendants victimized AOL subscribers with a “phishing” scheme.²¹ The defendants “spammed” thousands of AOL users with emails containing fake electronic greeting cards. When the subscribers tried to open the friendly greeting, they were instead met with a software trojan that prevented the users from accessing AOL without entering sensitive information including bank account, address, and Social Security numbers. The defendants used the stolen information to make counterfeit debit cards, which they swiped at ATM machines to get cash, and used at online and retail stores to buy goods and services. It appears that we’ve gone from “Hello, you’ve got mail!” to “Hello, you got your identity stolen!”

Another defendant was paid to fraudulently use Social Security numbers and other confidential info to get personal phone records of reporters and Hewlett-Packard officials, as well as their family members.²² This case is a clear example of “pretexting” or posing as somebody else to obtain sensitive calling records. And these are just the cases the DOJ chose to highlight.

There’s also the case of 19 year-old Irving Escobar who bought stacks of \$400 gift cards from Wal-Mart and cashed them in to buy electronics.²³ Escobar went on lavish shopping sprees, charging as much as \$112,000 in goods at gift stores. Escobar purchased, in total, an estimated \$1 million in goods. Amy Osteryoung, assistant statewide prosecutor who handled the case for Florida Attorney General Bill McCollum referred to Escobar’s actions as “[m]odern day money laundering.”²⁴ Also, “Investigators believe it is the boldest tangible evidence of criminals cashing in on hacked data from TJX—the nation’s largest reported computer data breach, which TJX disclosed in January.”²⁵ TJX says it will pay for a credit-monitoring service to help avert identity theft for customers whose driver’s license numbers were the same as their Social Security numbers and were believed stolen. For others, the damage has already been done.

¹⁵ *Id.* at 44.

¹⁶ *Id.* at 42.

¹⁷ *Id.*

¹⁸ Ellen Nakashima, *U.S. Exposed Personal Data: Census Bureau Posted 63,000 Social Security Numbers Online*, Wash. Post, Apr. 21, 2007, at A05, available at <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/20/AR2007042002208.html>.

¹⁹ Press Release, Dep’t of Justice, Fact Sheet: The Department of Justice’s Efforts to Combat Identity Theft (Apr. 23, 2007), available at http://www.usdoj.gov/opa/pr/2007/April/07_opa_278.html.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ Jon Swartz and Byron Acohido, *TJX data theft leads to money-laundering scam*, USA Today, June 12, 2007, available at http://www.usatoday.com/money/2007-06-11-tjx-data-theft_N.htm.

²⁴ *Id.*

²⁵ *Id.*

V. Recent Social Security Number Breaches in the Federal Government

The Social Security Administration's Office of Inspector General said that 16 percent of the 99,000 fraud cases it investigated in the one-year period ending Sept. 30, 2006 involved the misuse of Social Security numbers.²⁶ Considering the following cases of breaches in Social Security number data storage, that number might be on the rise.

Recently, a woman named Marsha Bergmeier was bored and did an Internet search for her farm's name in Illinois.²⁷ She discovered a link to fedspending.org, a Web site created by OMB Watch to monitor federal spending. While clicking around the site, a searchable database popped up for her, containing information about her farm loan amount under an Agriculture Department program. Not only that, she also discovered the list of 28,000 SSNs, including her own. Published right there for everybody with an Internet connection to see.²⁸ The site had been up since 1996. And that's just the United States Department of Agriculture.

The Department of Defense uses Social Security numbers for just about everything;²⁹ from troop rosters to the dog tags dangling from soldiers' necks. Since 2006, data about almost 30 million active and retired service members has been stolen from four Veterans Affairs offices. That's approximately 30 percent of the 100 million total reported lost or stolen personal data in the United States.³⁰ That's a lot.

And that's a lot more than an active military service member needs to be dealing with. With increasing frequency, scam artists are setting their sights on military personnel. As USA Today reported, Marine Corporal Jacob Dissmore, 22, returned from Iraq in 2006 to learn that someone in San Diego had opened a credit card account, started a T-Shirt business and even purchased a house with Dissmore's money using his personal information.³¹

A retired Navy chief petty officer that keeps meticulous financial records suspects the theft of laptops from the Veterans Affairs office is directly responsible for suspicious activity on his accounts.³² Earl Laurie Jr. takes care of his private info very well; he uses a P.O. Box, shreds his papers, and avoids online banking. Mr. Laurie never had a problem until right after the laptop was stolen when he started getting phone calls asking him to confirm strange credit card applications on his account.

And the American Red Cross has even had to issue warnings to military families. Identity thieves have stooped to the lowest level. The families of active military officers have reportedly been receiving phone calls from scammers pretending to be with the Red Cross delivering unfortunate news about a soldier stationed in Iraq.³³ The scammers tell the families that their loved one is being airlifted to a hospital in Germany and will not receive medical treatment unless they offer up personal information immediately. One moment you'll think the Red Cross is helping you out, the next thing you know you're a victim.

It doesn't stop there. Residents in every state of every member of this Subcommittee have experienced massive data breaches in the past year.³⁴

- In Michigan, Congressman Levin, the details of a scientific study were lost on a small flash drive at the Michigan Department of Community Health in Detroit. The small flash drive contained the personal information and SSNs of 4,000 Michigan residents.³⁵
- The Medicare drug benefit applications of 268 residents from Minnesota and North Dakota were recently stolen from an insurance agent's unlocked car. The applications contained applicants' name, address, date of birth, SSN, and bank routing information.³⁶
- The Pennsylvania Department of Transportation's driver's license facility in Dunmore had computer equipment containing the Social Security of over

²⁶ *Id.*

²⁷ Ellen Nakashima, *U.S. Exposed Personal Data: Census Bureau Posted 63,000 Social Security Numbers Online*, *supra* note 18.

²⁸ *Id.*

²⁹ Byron Acohido and Jon Swartz, *Military personnel prime targets for ID theft*, USA Today, June 15, 2007, available at http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-06-14-military-id-thefts__N.htm?csp=34.

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ Jerry Carnes, *Scammers Target Soldiers' Families*, 11 Alive News, May 30, 2007, available at http://www.11alive.com/news/article_news.aspx?storyid=97757.

³⁴ Privacy Rights Clearinghouse, *A Chronology of Breaches*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

³⁵ *Id.*

³⁶ *Id.*

11,000 drivers. Also stolen were supplies used to create driver's licenses and photo IDs.³⁷

- In February of last year, Congressman Davis, a computer was stolen at the University of Alabama-Birmingham, containing nearly 10,000 Social Security numbers and the personal information of potential kidney donors and recipients.³⁸
- In California, it is difficult to figure out which data breach to highlight—there were just too many to pick just one. Last year, hackers gained access to a UCLA database containing the Social Security numbers and personal information for over 800,000 current and former students, applicants, parents, and staff members.³⁹
- And Texas. Everything is bigger in Texas, even the data breaches. Texas Guaranteed Student Loan Corp. announced last year that a total of 1.7 million people's information had been compromised.⁴⁰
- Congresswoman Tubbs Jones, Ohio was in the news just last week when an intern's car was broken into, and somebody made off with the Social Security numbers of approximately 75,000 state employees.⁴¹
- State employees in Kentucky received mail last year from Kentucky Personnel Cabinet. The mail had their Social Security numbers visible from the see-through plastic windows in the envelope.⁴²
- And, Congressman Ryan, documents containing the personal information of Wisconsin's state assembly members were recently stolen from a legislative employee's car while she exercised at a local gym.⁴³

Social Security numbers are being stolen in every state in this country.

VI. Solutions to the use of SSNs in Identity Theft

Although the Presidential Task Force on Identity Theft correctly identified many of the problems associated with SSN usage and identify theft, it failed to propose many of the obvious solutions. The Task Force noted that, as long as SSNs continue to be used as forms of authentication, thieves must be prevented from obtaining them, but it did not come up with any substantive improvement that could bring about that end.⁴⁴

The Task Force did note that unnecessary usage of SSNs in the public sector must be decreased⁴⁵ and suggested that the “[Office of Personnel Management] should take steps to eliminate, restrict, or conceal the use of SSNs (including assigning employee identification numbers where practicable), in calendar year 2007.”⁴⁶ Furthermore the Task Force suggested that “[i]f necessary to implement this recommendation, Executive Order 9397, effective November 23, 1943, which requires federal agencies to use SSNs in ‘any system of permanent account numbers pertaining to individuals,’ should be partially rescinded.”⁴⁷ Unfortunately, however, the Task Force did not propose that the SSN stop being used for purposes beyond its original intent. Instead, the Task Force conceded that “[t]he use by federal agencies of SSNs for the purposes of employment and taxation, employment verification, and sharing of data for law enforcement purposes, however, is expressly authorized by statute and should continue to be permitted.”⁴⁸

³⁷ *Id.*

³⁸ *Id.*

³⁹ Privacy Rights Clearinghouse, *A Chronology of Breaches*, *supra* note 35.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ ID Theft Task Force Report at 23, *supra* note 8.

⁴⁵ *Id.* at 24.

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

Although the Task Force recommended that the Office of Personnel Management take a leading role in issuing policy guidance on appropriate use of SSNs⁴⁹ and create a list of acceptable SSN practices in order to determine best practices,⁵⁰ the Task Force did not lay out any basic framework for this policy guidance or any suggested best practices. Furthermore, although the Task Force suggested that a comprehensive record on the private sector use of SSNs should be developed,⁵¹ it failed to detail how the information comprising this record ought to be recorded or what legislative changes would be necessary to reduce the crime of identity theft. The absence of a legislative recommendation on this key point is significant; in many other areas of the report, the Department of Justice recommend legislative changes to expand its own investigative and prosecutorial authority.

The task force recognizes the dangers of Social Security numbers' dual role in identification and authentication, but it fails to recommend that the Social Security number's role in authenticating an identity be completely eliminated and its use in the private sector limited. Although the Task Force adequately highlights some of the problems associated with SSN usage, it fails to provide a meaningful starting point for the government to act to correct the problems and it does not recommend, as it ought to, that the private sector immediately cease use of SSN for authentication purposes.

What else should be done?

- For starters, an effective law would limit the collection and the use of the SSN. It would be far preferable to reduce the crime of identity theft at its source than to create new enforcement authority for a problem that is clearly out of control.
- The use of the SSN should be limited to those circumstances that are explicitly authorized by law. For example, an employer should be permitted to ask an employee for an SSN for tax-reporting purposes (as long as the SSN remains the Taxpayer Identification Number), but a health club should not be permitted to ask a customer for an SSN as a condition of membership.
- Prevent companies from compelling consumers to disclose their SSN as a condition of service or sale unless there is a statutory basis for the request.
- Prohibit the sale and limit the display of the SSN by government agencies. It is simply inconsistent with Section 7 of the Privacy Act to allow the Federal Government to disseminate the SSN.
- Penalize the fraudulent use of another person's SSN but not the use of an SSN that is not associated with an actual individual. This would permit, for example, a person to provide a number such as the "867-00-0909" where there is no intent to commit fraud. (The number displayed could not be an actual SSN.)
- Encourage the continued development of alternative, less intrusive means of identification. We believe that the National Research Council should be funded to undertake further research on new techniques that enable records management while minimizing privacy risks.⁵²

It is also important not to preempt innovative state laws that reduce the risk of SSN misuse. Many states have enacted legislative protections for the SSN. They vary from comprehensive frameworks of protection for the SSN to highly-specific laws that shield the SSN from disclosure in specific contexts.

For example, a 2005 Arizona law 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.⁵³ The law also prohibits printing the SSN on materials mailed to residents of Arizona. Exceptions to 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.

In 2004 Ohio law limits the collection of the SSN and its incorporation in licenses, permits, passes, or certificates issued by the state.⁵⁴ The law requires the establishment of policies for safe destruction of documents containing the SSN. Insurance

⁴⁹ID Theft Task Force Report at 26, *supra* note 8.

⁵⁰*Id.*

⁵¹*Id.*

⁵²See also Nat'l Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Stephen Kent & Lynette Millett eds. 2003); Nat'l Research Council, *Engaging Privacy and Information Technology in a Digital Age* (James Waldo, Herbert S. Lin & Lynette Millett eds. 2007).

⁵³Ariz. Rev. Stat. § 44-1373.

⁵⁴Available at http://www.state.co.us/gov_dir/leg_dir/olls/sl2004a/sl_393.htm.

companies operating in the state must remove the SSN from consumers' identification cards. Finally, the legislation creates penalties for individuals who use others' personal information to injure or defraud another person.

In Georgia, businesses are now required to safely dispose of records that contain personal identifiers.⁵⁵ The Georgia law requires that business records—including data stored on computer hard drives—must be shredded or in the case of electronic records, completely wiped clean where they contain SSNs, driver's license numbers, dates of birth, medical information, account balances, or credit limit information. The Georgia law carries penalties up to \$10,000.

In the past year, Illinois has passed several laws to protect consumer privacy, including measures that address identity theft, limit the use of the Social Security number, require notification of security breaches, and allow state residents to put a security freeze on their credit report if they believe their personal information has been compromised.⁵⁶

Six state legislatures, in the past two months, have passed laws going against a new federal ID requirement.⁵⁷ The law would require 240 million Americans to get new licenses by 2013. The new identification cards would contain residents' SSN, home address, and that they are in the USA legally. Implementation of this new ID program would cost states more than \$11 billion,⁵⁸ according to the National Conference of State Legislatures. The Federal Government has estimated that REAL ID will cost \$23.1 billion.⁵⁹ Some state lawmakers have gone as far to call this federal effort an attempt to create a "papers-please" society.⁶⁰ Without all 50 states complying, it's not really a National ID card. In the end states will have their way.

The innovative solutions that state legislatures are developing to address privacy concerns should be encouraged. The states are laboratories of democracy, and are moving effectively on emerging issues. A federal privacy baseline ensures safeguards in those states where they do not currently exist, and leaves states free to develop better protection. Even a sensible national law will become outdated as technology and business practices evolve.

EPIC also favors technological innovation that enables the development of context-dependent identifiers. Such a decentralized approach to identification is consistent with our commonsense understanding of identification. If you're going to do banking, you should have a bank account number. If you're going to the library, you should have a library card number. If you're renting videos from a video rental store, you should have a video rental store card number. Utility bills, telephone bills, insurance, the list goes on. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number gets compromised, all of the numbers are not spoiled and identity thieves cannot access all of your accounts. All of your accounts can become compartmentalized, enhancing their security.

We believe that this is also the approach favored by businesses and cutting-edge technology firms that think carefully about the issue, though it has taken us some work to make this clear. EPIC filed a complaint with the Federal Trade Commission in 2001 about Microsoft Passport, an identity scheme proposed for the Internet.⁶¹ Microsoft was signing up users for a service that produced a single username and password for all of their Web services, including credit card information and a vast user profile. Microsoft Passport stored user information in a central database. The problem was that while Microsoft Passport claimed to enhance security, it actually had a lot of holes. And, if you accidentally left your user profile up on a public computer terminal or a malicious hacker gained access to one of your accounts, they would have access to everything associated with your user profile.

⁵⁵ Available at <http://www.epic.org/privacy/ssn/sb475.html>.

⁵⁶ Press Release, Office of the Governor, Governor Blagojevich calls on Veterans Administration to provide immediate protection to veterans whose personal information was stolen (May 24, 06), available at

<http://www.illinois.gov/PressReleases/ShowPressRelease.cfm?RecNum=4920&SubjectID=26>.

⁵⁷ Thomas Frank, *6 States defy law requiring ID cards*, USA Today, June 18, 2007, available at http://www.usatoday.com/news/nation/2007-06-18-id-cards_N.htm?loc=interstitialskip.

⁵⁸ *Id.*

⁵⁹ Dep't of Homeland Sec., Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10,819, 10,845 (Mar. 9, 2007), available at <http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm>; see generally, EPIC, Page on National ID Cards and the REAL ID Act, http://www.epic.org/privacy/id_cards/.

⁶⁰ Thomas Frank, *6 States defy law requiring ID cards*, supra note 57.

⁶¹ EPIC maintains an archive of information about Microsoft Passport at <http://www.epic.org/privacy/consumer/microsoft/passport.html>.

We urged the Federal Trade Commission to investigate, and the FTC eventually agreed with EPIC's position.⁶² Microsoft backed off Passport, developed an approach to identity management that allowed for multiple forms of online identification, and other companies, including open source developers, followed a similar approach.⁶³

I believe there is now consensus in the online community about the need to avoid single identifiers and to promote multiple identification schemes, and that this approach is best not only for privacy but also for security. The critical question is whether Congress can make physical identity systems similarly robust.

VII. The Social Security Number Protection Act, H.R. 948

H.R. 948, the Social Security number Protection Act of 2007, has passed before the Committee on Energy and Commerce and has been reported to the House. The purpose of H.R. 948 is to prohibit the display and purchase of Social Security numbers in interstate commerce pursuant to rules to be promulgated subsequent to the passage of the bill. Although we generally favor the bill, we believe it can be strengthened in several key areas. Most critically, there should be clear guidance to the FTC to limit the sale and purchase of Social Security numbers, there should be private right of action for individual citizens to ensure that the law is effective, and there should be no preemption of state law.

Sections 3(a)(1) through 3(a)(3) of H.R. 948 create a facially broad prohibition on the public display of Social Security numbers on the Internet, the requirement to use an individual's Social Security number as a password for access to any goods or services, and the display of Social Security cards on any membership or identity card. However, Section 3(c) grants the Federal Trade Commission open-ended authority to promulgate exceptions to the prohibitions contained within the bill. If exceptions concerning the display of Social Security numbers and requirement of their use as passwords are necessary, then they should be contained within the statute itself. Failing that, the authorization granted to the FTC should be narrowly tailored to areas in which exceptions are clearly needed. As currently formed, there is no way to know whether the exceptions will undermine the safeguards that are vitally important.

Although the purpose of the bill is, in part, to prohibit the sale and purchase of Social Security numbers, Section 4(a) only authorizes the FTC to create regulations to this end. Section 4(b)(1) requires the FTC to issue regulations but it provides little meaningful guidance on baselines standards the FTC should adopt. Furthermore, although Section 4(b)(2) appears to offer the Commission some substantive guidance, its language actually defines the ceiling for the FTC's rules rather than the floor. While the dual purposes of providing assurance that Social Security numbers are not to be used to commit fraud and to prevent undue harm are laudable, these should be the minimum requirements the FTC must meet under the act and should not define the boundary of the Commission's authority to regulate. Also troubling are the laundry list of required exceptions contained within Section 4(b)(3). Not only are the exceptions contained in Sections 4(b)(3)(A) through 4(b)(3)(F) requirements of any future FTC regulation, but also Section 4(b)(3)(G) gives the FTC open ended authority to create further exceptions pursuant to the general considerations in Section 4(b)(2). Despite its strongly worded purpose, the bill lacks adequate limitation on the sale or purchase of Social Security numbers and, instead, devotes more space to explicitly authorizing uses of Social Security numbers that were not originally intended.

Although it is laudable that the bill creates a right of action for states' attorneys general in Section 4(e)(2)(A), H.R. 948 fails to authorize a private right of action. Experience has shown that a private right of action is necessary in order to ensure vigorous enforcement of the law. While State and Federal Governments are often consumed with pursuing other issues and may be unable to pursue every indiscretion to the fullest extent of the law, individuals are always motivated to vindicate their own rights. The possibility of expansive litigation indicates the importance of this problem; it does not provide a reason to restrict an individual's ability to protect his identity.

I should add further that EPIC has had significant success bringing privacy complaints to the Federal Trade Commission. In fact, it was our complaint regarding the practices of the data broker ChoicePoint that led to the largest fine in the Com-

⁶²Fed. Trade Comm'n, *Agreement, In Re Microsoft*, FTC Docket No. C-4069 (Dec. 20, 2002).

⁶³Kim Cameron, *The Laws of Identity*, Identity Weblog, Dec. 9, 2004, <http://www.identityblog.com/stories/2004/12/09/thelaws.html>; Windows CardSpace, <http://cardspace.netfx3.com/>; OpenCard, <http://www.opencard.org/>.

mission's history.⁶⁴ Nonetheless, we would urge the Committee to include a private right of action, specifically where an individual or company misuses an SSN in violation of the Act. That will be critical to limit the problem of identity theft.

Finally, while a national standard may appear attractive, preempting state law will be a mistake. The preemption of state law will mean simply that certain practices that contribute to the crime of identity theft that are currently and appropriately outlawed by the states will become legal if this bill passes in its current form. Experience in other areas has made clear that a federal baseline for privacy protection is the best way to both create a national standard and to preserve innovation in the states.

VIII. Conclusion

There is little dispute that identity theft is one of the greatest problems facing consumers in the United States today. There are many factors that have contributed to this crime, but there is no doubt that the misuse of the Social Security and the failure to establish privacy safeguards are key parts of the problem. The Congress should pass strong and effective legislation that will limit the use of the SSN, that will provide effective means of oversight, that will not limit the ability of the states to develop better safeguards, and that will encourage the development of more robust systems for identification that safeguard privacy and security.

Thank you for your interest in this issue. I will be pleased to answer your questions.

Chairman MCNULTY. Thank you very much, Mr. Rotenberg.
Mr. Schwartz.

STATEMENT OF GILBERT T. SCHWARTZ, PARTNER, SCHWARTZ & BALLEEN, LLP, ON BEHALF OF THE FINANCIAL SERVICES COORDINATING COUNCIL

Mr. SCHWARTZ. Mr. Chairman, Ranking Member Johnson, and Members of the Subcommittee, I am Gilbert Schwartz, and I am pleased to appear today before the Subcommittee to present the view of the Financial Services Coordinating Council on the important issue of protecting the privacy of the Social Security number from identity theft.

FSCC is composed of the American Bankers' Association, American Council of Life Insurers, American Insurance Association, and the Securities Industry and Financial Markets Association. These organizations represent thousands of small and large banks, insurance companies and securities firms that provide financial services to virtually every household in the United States. As was mentioned by several witnesses today, Social Security numbers play an important and integral role in the daily operations of financial institutions.

They are used to make sound credit decisions, for underwriting insurance, for reporting to Federal and state authorities and they are a central element in customer identification programs required by the U.S.A. Patriot Act. Most importantly, Social Security numbers are used by financial institutions to prevent and detect fraud, root out identity theft, and to identify and report transactions that may involve money laundering, as well as activities involving terrorist financing.

The FSCC strongly supports efforts by the government and the private sector to protect Social Security numbers from being used

⁶⁴ EPIC, *Past FTC Review of ChoicePoint Privacy Practices*, <http://epic.org/privacy/ftc/google/#cpoint>; see generally EPIC, *ChoicePoint*, <http://www.epic.org/privacy/choicepoint/>.

to commit identity theft. However, in view of the important and essential role that they play in our financial system, legislation should avoid overly broad and unduly restrictive limitations on their use that could have unintended consequences. Banks, insurance companies and securities firms have robust systems to protect the security of financial transactions conducted by their customers and their personal information. Financial institutions have a long history of using Social Security numbers responsibly. It is important to underscore the fact that financial institutions do not sell or publicly display Social Security numbers to the general public.

Congress addressed the issue of consumer privacy and security safeguards for financial institutions in the Gramm-Leach-Bliley Act. That Act provides comprehensive and rigorous protections for consumers non-public personal information, which includes Social Security numbers. However, the GLB Act and implementing regulations specifically permit financial institutions to use Social Security numbers for specified legitimate business functions.

Federal regulators have also adopted guidance for depository institutions in the event of unauthorized access to consumer information. The guidance includes notification of customers if the institution determines that misuse of sensitive information has occurred or is reasonably possible so that they can take steps to protect themselves against possible identity theft.

In 2003, Congress also enacted the FACT Act to help consumers remedy the effects of identity theft. The FSCC believes that the continuing efforts of the agencies to implement the FACT Act has had a positive effect on reducing incidents of identity theft and will continue to do so as more and more regulations are implemented by the agencies.

In addition, many states have enacted legislation to protect sensitive customer information, such as Social Security numbers. This legislation provides strong protections for the use of personal information by financial institutions. We are concerned, however, that any Federal legislation could have unintended consequences if it restricts the ability of financial institutions to use Social Security numbers. It could disrupt the flow of credit and other financial services to consumers and hurt our ability to detect fraud and prevent identity theft. A prohibition on the sale and purchase of Social Security numbers could also affect securitization activities of financial institutions, as well as merger and acquisition activities because these numbers are embedded in the files that are required in connection with those securitization and mergers and activities.

Many institutions also use public records in connection with anti-fraud activities, as well as to identify and detect identity theft. Limits on access to public record information could jeopardize financial institutions' ability to protect customers' assets and prevent illegal activities. Many institutions are deeply involved in providing information to the public about how to prevent from becoming a victim of identity theft and how to assist victims of identity theft. We strongly support these efforts by financial institutions as well as by the government.

We also support, as I said, efforts by Congress to protect Social Security numbers in order to prevent identity theft. However, in view of the strong protections financial institutions have in place

to protect this information and existing Federal and state laws applicable to the use and disclosure of customer information, the FSCC believes that there is no need for further restrictions on the ability of financial institutions to use and disclose Social Security numbers.

Mr. Chairman, we appreciate the opportunity to appear before the Subcommittee today, and we will be glad to respond to any questions you may have.

[The prepared statement of Mr. Schwartz follows:]

Prepared Statement of Gilbert T. Schwartz, Partner, Schwartz & Ballen LLP, on behalf of the Financial Services Coordinating Council

Introduction

The Financial Services Coordinating Council ("FSCC") is pleased to present this statement to the Subcommittee on Social Security in connection with its hearing on "Protecting the Privacy of the Social Security number from Identity Theft." The FSCC is comprised of American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry and Financial Markets Association. The FSCC represents thousands of large and small banks, insurance companies and securities firms in the United States. Together, these financial institutions provide financial services to virtually every household in the United States.

How Financial Institutions Use Social Security Numbers

Social Security numbers are unique personal identifiers. While originally created as a means of tracking earnings and determining eligibility for Social Security benefits, they have evolved well beyond their original purpose. SSNs are the most effective means of identifying individuals and matching people with personal data. They are the identifier of choice for both the public and private sector, and are used widely throughout the economy and the financial system. They are a window into the financial and personal history of virtually every consumer. When combined with certain other personal information, SSNs can be used to create false identities and financial mischief. That is why SSNs are often sought by identity thieves.

The FSCC strongly supports proactive efforts by the government and the private sector to protect SSNs from the national problem of identity theft. However, it is also vitally important to our nation's financial system to avoid overly broad and unduly restrictive limitations on the use of SSNs that could have significant unintended consequences.

SSNs play an integral role in the operations of every financial institution in our country. Financial institutions use SSNs in conjunction with other personal information to make sound credit decisions, for underwriting and other insurance functions, and for screening in connection with customer identification programs. Our nation's credit reporting system relies on SSNs to gather information to compile consumer credit files. This information is used by financial institutions to make credit available to customers and to provide other services to consumers. Most importantly, SSNs are used to prevent and detect fraud, root out identity theft and to identify and report transactions that may involve money laundering and activities involving terrorist financing. They are also used by financial institutions to comply with reporting requirements of federal and state tax and securities laws; to transfer assets and accounts to third parties; to comply with "deadbeat spouse" laws; to verify appropriate Department of Motor Vehicle records when underwriting auto insurance; to obtain medical information used in underwriting life, disability income, and long-term care insurance policies; to locate missing beneficiaries to pay insurance proceeds; to locate insurance policies for owners that have lost their policy numbers; and to facilitate myriad administrative functions.

As you can see, SSNs play a critically important role in the daily functions of virtually every financial institution. The use of SSNs increases efficiency, reduces costs and makes it possible to offer innovative products and services that would not otherwise be available to consumers economically. Not only are SSNs critical to the smooth functioning of the financial system, they also serve as a means of detecting and preventing fraudulent transactions as well as combating identity theft. Any SSN legislation that may be considered must recognize the essential role that SSNs play in facilitating the delivery of financial products and services to consumers

throughout the nation. Restrictions on the ability of financial institutions to use SSNs for everyday business purposes could have significant unintended consequences on their ability to serve consumers. Moreover, limitations on the use of SSNs by financial institutions may have the unintended effect of increasing fraud and identity theft and impede law enforcement programs designed to thwart money laundering and terrorist financing.

How Financial Institutions Protect SSNs and Combat Identity Theft

Financial institutions take the problem of identity theft very seriously. We have long recognized the importance of protecting our customers' personal information, including SSNs. Public confidence in financial institutions is based in large part on the recognition that banks, insurance companies and securities firms are trusted intermediaries that have established robust policies, procedures and systems to protect the security of their customers' transactions, financial assets and personal information. Financial institutions have a long history of using SSNs responsibly and in a manner that protects them from abuse. It is important to underscore that financial institutions do not sell or display SSNs to the general public.

Congress formally addressed the issue of consumer privacy and financial institution security safeguards in 1999 when it enacted the Gramm-Leach-Bliley Act. The GLB Act was landmark legislation that expanded the ability of banks, insurers and securities firms to affiliate in order to provide more customers a full range of financial services more efficiently. The GLB Act requires all financial institutions throughout the nation to provide comprehensive, and rigorous protection of consumers' nonpublic personal information, including SSNs. The GLB Act establishes overarching Congressional policy that every financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of its customers' nonpublic personal information. Moreover, under the GLB Act, each customer has the ability to instruct his or her financial institution not to disclose the customer's personal information, including an SSN, to nonaffiliated third parties or to the general public.

In recognition of the fact that financial institutions have legitimate reasons to request, use and disclose personal information such as SSNs, the GLB Act and regulations of the federal agencies and state authorities charged with implementing the Act permit financial institutions to use such information for legitimate business functions, such as to effect, administer or provide a transaction requested or authorized by the consumer or in connection with servicing a customer's account. These laws also permit financial institutions to disclose such information in order to prevent fraud or unauthorized transactions, as well as to comply with federal, state or local laws.

Under the authority of the GLB Act, federal agencies require financial institutions to develop a written information security program that describes how they protect customer information. An institution must:

- **Designate one or more employees to coordinate its information security program;**
- **Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of safeguards for controlling these risks;**
- **Design and implement a safeguards program, and monitor and test it on a regular basis;**
- **Select service providers that can maintain appropriate safeguards;**
- **and**
- **Evaluate and adjust the program in light of relevant circumstances and changes in the company's business.**

Financial institutions have established information systems that maintain and store sensitive consumer information in a safe and secure manner. These facilities are subject to periodic audit by internal and external auditors as well as by state and federal examiners. Federal regulators also have adopted guidance relating to procedures depository institutions are to follow in the event of unauthorized access to customer information. The guidance includes notification of customers if the institution determines that misuse of sensitive customer information has occurred or is reasonably possible. Notice to customers under these circumstances enables them to take steps to protect themselves against possible identity theft.

Congress also enacted the Fair and Accurate Credit Transactions ("FACT") Act of 2003 which contains provisions intended to help consumers remedy the effects of identity theft. Many of the FACT Act's provisions have been implemented by regulations and guidance issued by the federal agencies. The FSCC strongly believes that

continuing efforts of the agencies to implement the FACT Act have had a positive effect on reducing incidents of identity theft.

In addition to the numerous state insurance laws implementing the GLB Act requirements, thirty six states and the District of Columbia have enacted security breach legislation. States have also enacted legislation that prohibits specific uses of SSNs, including the public display of SSNs. The FSCC believes that existing federal and state laws and guidance provide strong protections for the use of personal information such as SSNs by financial institutions. Accordingly, the FSCC believes that there is no need for Congress to enact legislation restricting the use and disclosure of SSNs by financial institutions.

Restrictions May Have Unintended Consequences

The FSCC is concerned about unintended consequences of legislation that restricts the ability of financial institutions to use SSNs. Unintended consequences have the potential to disrupt the flow of financial services to consumers and to harm the smooth operation of the U.S. financial system. Such effects could have serious consequences for the nation's economy.

Legislation could adversely affect the ability of financial institutions to use SSNs to verify the identities of consumers and customers. This could disrupt the flow of information creditors receive from credit bureaus and have adverse consequences for consumers seeking credit, insurance, securities and other financial services. It is essential that financial institutions obtain SSNs from consumers and disclose the SSNs to credit bureaus in order access their credit histories. If such access and use of SSNs is disrupted, the flow of credit, and other financial services will be undoubtedly be curtailed.

Prohibitions or restrictions on the sale or use of SSNs could seriously impede the ability of financial institutions to provide seamless administrative services to customers. For example, insurers use SSNs to verify the identity of an individual who requests a change to his or her insurance policy, such as a change in beneficiary. If an insurer is unable to verify the identity of the person making the request, the potential for fraudulent transactions and identity theft will increase.

Restrictions on the use and disclosure of SSNs could adversely affect the ability of financial institutions to detect fraud. Banks, insurance companies and securities firms rely on information they obtain from various sources to verify a consumer's identity. Financial institutions maintain sophisticated procedures, which are based upon SSNs as a means of identification, to accurately verify the identity of customers and to prevent and detect fraud or identity theft.

A prohibition on the sale or purchase of SSNs could be interpreted as restricting activities such as the sale of assets among financial institutions. Financial institutions often sell assets such as credit card and vehicle loans in connection with their securitization activities. Merger and acquisition activities may also result in a transfer or sale of all of the institutions' accounts and policies. SSNs are necessarily included in account and policy files that are transferred in connection with these routine business transactions. Of necessity, legislation that addresses the sale and purchase of SSNs must exclude these and other similar legitimate transactions from the scope of its coverage.

Restrictions on the ability to obtain SSNs could have an adverse effect on the ability of financial institutions to comply with anti-money laundering rules and anti-terrorism activities. Section 326 of the USA PATRIOT Act requires many financial institutions to obtain a taxpayer identification number, typically an SSN, before opening an account for an individual. The financial institution also must verify the identity of the individual. These measures are intended to prevent the ability of money launderers and terrorists to use financial institutions for illicit purposes. Limitations on the ability of financial institutions to use SSNs to verify the identity of customers could thwart their ability to prevent money laundering and financing of terrorist activities.

Access to Public Records

We understand that legislation may also address the use of SSNs that are available in public records. Many financial institutions use public records in connection with their anti-fraud activities as well as to prevent and detect identity theft. Public records facilitate the ability of financial institutions to verify consumer identities when opening accounts, issuing insurance policies and conducting various transactions. They also assist in verifying an employee's background. The ability to match SSNs ensures that the information included in these records matches the correct in-

dividual. Limits on access to public record information could jeopardize a financial institution's ability to protect its customer's assets and prevent illegal activities.

Customer Education

Financial institutions strongly support efforts to combat identity theft. Many institutions post extensive information on their websites, and distribute statement stuffers and brochures to inform consumers about steps they can take to prevent from becoming victims of identity theft. Financial institutions also maintain identity theft hotlines and participate in community outreach programs to spread the word about measures consumers can take to prevent identity theft. And financial institutions strongly support efforts by the federal agencies to educate consumers through various booklets, brochures and programs about preventing identity theft.

Conclusion

The FSCC strongly supports efforts by Congress to protect SSNs to prevent the national problem of identity theft. Under existing law, financial institutions have developed robust safeguards to protect the security of personal customer information such as SSNs. Financial institutions use SSNs in connection with normal business functions or to comply with critically important requirements established by Congress. In view of the strong protections currently in place, the FSCC believes that there is no need for further restrictions on the ability of financial institutions to use SSNs.

Chairman MCNULTY. Thank you, Mr. Schwartz. I want to thank all of the Members of the panel for their patience and for their excellent testimony. Some of us are a little bit under the gun as far as other commitments are concerned but before I yield to my colleagues to inquire, I just want to say that what I have heard from this panel and what I have heard from previous panels just strengthens my belief that obviously there are legitimate uses for the Social Security number, there are a lot of illegitimate uses. I just happen to think that the vast majority of entities that ask individuals for their Social Security numbers have absolutely no need to have that information.

I think part of the solution is education and doing what Nancy and I did when I related our own personal story about when we went to make a retail purchase, and we were giving them all kinds of information about us, then they asked for the Social Security number. They had absolutely no need to have it. I think more people need to do what we do, which was "Just Say No." However, I think we need to go beyond that and to have some legislation that further defines what are the legitimate reasons for seeking to know someone's Social Security number so that more people do not suffer the fate of Charlie W. and the others who have had these horrible experiences, which have disrupted their lives for years. With that, I will yield to the Ranking Member, Mr. Johnson.

Mr. JOHNSON. What was your question?

Chairman MCNULTY. I think what I gave was my conclusion. [Laughter.]

Mr. JOHNSON. I sense there is quite a difference between our people who testified out there and how you believe number use should be accomplished. It is interesting to me, we tried to get the military to stop using as a serial number the Social Security number, and they will not do it because it costs too much to change it all. So, having said that, in the financial industry, if we use private sources to verify a person's identification instead of going through

the government let's say, what would it cost to do that? You would use the Social Security number, I assume?

Mr. PRATT. Our Members make extensive use of the Social Security number for—I want to distinguish between, it was in the testimony, but between using the Social Security number to build a database to match information together, and I think the professor did a good job of explaining the difference between matching and building a database and authenticating, verifying the identity of the consumer. The SSN is used in part to build the database and you need consistency. Even a driver's license, for example, Mr. Chairman, if you move around the country, your number will change of course and not everybody moves, but we have at least 40 million consumers who are changing their addresses every year, so the SSN remains a good database matching tool, not perfect, and we use other matching elements of course to build the totality of the database. It is not unique to the Social.

On the authentication side, I think one thing that is very important that has been said several times, if every one of the transactions shared here had involved proper authentication, there would not have been records of arrest and there would not have been public records and there would not have been a driver's license issued in that individual's name. Maybe at the core of this hearing, I think it runs parallel with the discussion of the Social Security number, is that you must authenticate properly and it does involve using many different types of tests. What you do online to authenticate an identity is different than what you would do if I was in person speaking with you as a loan officer and that would be yet again different if I was on the phone.

Mr. JOHNSON. Well, focus for a minute on us having to have employer verification of legal residence, for example, can you do that?

Mr. PRATT. Again, identity verification is a risk assessment.

Mr. JOHNSON. That is what I mean.

Mr. PRATT. I do not think there is any way in this country to perfectly identify a consumer unless we are going to carry around identifying document, which will create a whole host of other problems, by the way, if we are carrying everything with us.

Mr. JOHNSON. We have got too many in our pocket now.

Mr. PRATT. Yes, sir. I was asked just today to provide a copy of my Social Security card in a lending transaction.

Mr. JOHNSON. You carry that around all the time, don't you?

Mr. PRATT. I do not have it and could not find it.

Mr. JOHNSON. Of course not.

Mr. PRATT. In fact, I recall it is a kind of fuzzy blue card that I received. By the way, my Social Security number matches up with my sister's almost perfectly because at my age the family obtained all of them sequentially at the same time and so there are two S. Pratts, and when we graduated from college, we lived in the same address, and so there were two S. Pratts at the same address with one digit difference in our Social Security numbers. So I think that explains why identity verification will never be solely the Social.

But, on the other hand, I think what Mr. Schwartz said is right, it is part of the tool box. For example, if we can identify in a fraud

database that a SSN has been used in other fraudulent transactions, that is not going to stop the transaction, but the user, the authenticator, should take additional steps and say, "I am sorry, we cannot push you through until we get to the point of knowing who you are, and we need to try to find a way to know who you are and we are going to ask you another question."

Mr. JOHNSON. So, all you are saying is it is just another ID method?

Mr. PRATT. It is part of the system but it is very important to database—

Mr. JOHNSON. But wants to get rid of them totally.

Mr. PRATT. I do not see any way that you can pull the Social Security number out of a, for example, a credit reporting database because every other data element is going to change. So if you pull the one stable identifier out of that database, we are causing another kind of problem that will be dealt with another Committee and that is the problem of inaccurate data being used to stop transactions.

Mr. JOHNSON. We are running out of time, but I would like to hear Dr. Antón's comment on that.

Ms. ANTON. Thank you, Congressman. We found a study in The Journal of Public Health that showed that we can identify people very accurately in the Social Security death master index by simply with their first initial, last name, date of birth and/or the birthplace, and that is without the Social Security number. So, it is possible to identify. This is why I was trying to make a point about not using the Social Security number as an authenticator as well. Our names and addresses and phone numbers have been published in the phone book for over 55 years, probably more than that, and we were not struggling with identity theft at that time.

Mr. JOHNSON. Well, the credit companies have to be more accurate than that, and I think it is just another source of identification for them. Is that true?

Mr. PRATT. That is true. By the way, we have also done a death master file analysis where you can have more than 90 John Smith's with the last four digits of a Social Security number that match, so our challenge is in fact to use the Social in combination with an address, again 40 million of them changing every year, in combination with marriages and divorces where last names change. Candidly, our hit or miss ratio in the financial services space may be very different than in a retail space that does not have to deal with the Fair Credit Reporting Act or Gramm-Leach-Bliley Act or a USA Patriot Act, Section 326 obligation.

Ms. ANTON. Not to be argumentative, but you do not need those four digits of the Social Security number to be able to accurately identify those people in a database.

Mr. JOHNSON. Thank you. I am out of time. I appreciate your comments.

Chairman MCNULTY. Ms. Tubbs Jones may inquire.

Ms. TUBBS JONES. Thank you, Mr. Chairman. I want to get a "shout out" to an organization. In case you all do not know what a "shout out" is, that means you are saying something about somebody you know. It is done over the radio more often than not, it is a slang term that my son has taught me, he is 24. But I am

going to get a “shout out” to Axiom from my congressional district, who is a Member of Mr. Pratt’s organization. Thank you, Mr. Pratt, for your testimony.

Let me also say to Mr. Gingerich I am a former common pleas judge out of Kyle County, Ohio, and I want to celebrate the great work that the Center for State Courts does because it is through the work that you do that we have continually improved the level of the judiciary in the United States of America. So, that is a “shout out” for the Center for State Courts.

I am interested, I would love to be in a courtroom and let two or three of you all really debate this in-depth because it is very clear that there are differing opinions. Dr. Antón, so when I go to Macy’s and I am getting ready to buy something and I do not have my credit card with me and they say, “Okay, put your name in there,” and then this little machine says, “Put in your Social Security number,” is that authentication?

Ms. ANTON. Yes.

Ms. TUBBS JONES. Okay, all right, just checking to see if I am on the same terms. But I should not have to do that? What should I have to do if I really want—no, I am kidding, what should be the way in which they would know who I am, what else should they be using, my birth date, not my mother’s maiden name?

Ms. ANTON. On every single one of my credit cards, I have not signed one of them, it always says, “See ID.” So, if someone steals my card, they have to see the picture on my driver’s license to make sure that it is me.

Ms. TUBBS JONES. I am with you, Dr. Antón, I do not sign my credit cards either.

Ms. ANTON. That is how I authenticate.

Ms. TUBBS JONES. Okay, all right.

Mr. JOHNSON. But you should put on the back, “Ask for ID.”

Ms. TUBBS JONES. I should write that on it?

Mr. JOHNSON. Yes, you should.

Ms. TUBBS JONES. Okay, I will remember that one. I have just about thrown them all out the door though. I really do not have a lot of questions, I am interested in spending some time reading your testimony and having a little more opportunity to address it, but I want to say on behalf of all the people that I represent, we need your input in trying to walk through this dilemma that we are in. We are in a true dilemma because, as Mr. Pratt and Mr. Gingerich said, the Social Security number has become such an integral part of whatever it is we are doing, that to yank it immediately would cause havoc. But, on the other hand, we really need to be doing something to prohibit its use.

I thank you, Mr. Chairman, for the time. I know my friend, Mr. Ryan, down there really wants to talk, so I yield you my time.

Mr. RYAN. Yes, sure, thank you. I appreciate it.

Chairman MCNULTY. Thank you, Ms. Tubbs Jones. Mr. Ryan may inquire.

Mr. RYAN. Well, I will just pick up where you left off then. I like making these conversations flow. Boy, this is a good hearing, Mr. Chairman, again another good one. Correct me if I am wrong, Dr. Antón, I liked your testimony, it was very interesting, it helped logically set this up. Using the cart in front of the horse or the

horse in front of the cart analogy, we have to come up with authenticating system and then an identifier, right, so first authenticate, then operate through society by identifying, correct? If you cannot authenticate who you are, all the rest is academic.

Ms. ANTON. In most transactions it seems that your first identified and then authenticated.

Mr. RYAN. Right.

Ms. ANTON. So, you do not use your name to authenticate yourself, and you should not use your Social Security number and you should not use your mother's maiden name. These are all weak authenticators.

Mr. RYAN. Right.

Ms. ANTON. That is the problem.

Mr. RYAN. So, to prevent all these problems we have in society, whether it be terrorism, illegal immigration, identity theft, we have to have a better system for authenticating our identity?

Ms. ANTON. Yes.

Mr. RYAN. Okay, so now what we are trying to figure out, what should government do to do this? What is it that we can do to facilitate this, to make that happen in the 21st century? Then whatever we do, will it be obsolete in a couple of years, will we throw money down a hole with ID cards that are going to be obsolete, which we saw on the last panel, what path should we put ourselves on so that people can get their IDs—get themselves authenticated so that the system can work, what do you recommend? Mr. Rotenberg, I know that you have put a lot of work into that too, as well?

Mr. ROTENBERG. Well, thank you, Mr. Ryan, I am going to put something on the table, which Professor Anton will understand, but it is going to sound a little confusing. It does answer your question, however. I think the long-term solution to this problem, and it is an enormous problem, is to separate authentication from identification.

Mr. RYAN. Right.

Mr. ROTENBERG. Let me give you an example of what I mean. A young person walks into a liquor store to purchase alcohol. There is one thing that the owner of that store needs to know in most states, is this person over the age of 21? To have a legal transaction in that context, there needs to be a way to authenticate the fact that person is over the age of 21. It turns out that his actual identity is irrelevant and in truth from a privacy perspective and a security perspective, it would be best if his identity was not disclosed because that information does not need to be made available.

Mr. RYAN. Can I have my time now, Mr. Chairman?

Chairman MCNULTY. Yes.

Mr. ROTENBERG. As I said, and we have done a lot of work on this issue over the years, it comes up a lot, particularly in the Internet economy where you have people on Ebay, for example, relying on the reputation of others, whose actual identity is not known. But the reputation value of the pseudonym they use is extraordinarily useful. If someone's reputation is high, they will do business with them online. It does not matter who they actually are.

I think we are going to need to get a handle on this problem. You see what has happened is that the Social Security number is actually at the opposite end of the ideal system. The Social Security number is both an identifier and authenticator and it fails completely. A good identity system actually separates these functions. You would agree with this, would you not?

Ms. ANTON. Yes, absolutely.

Mr. ROTENBERG. Yes.

Mr. RYAN. Now, we have the two financial services and consumer data people, so we are going to have to figure out here as legislators what is the way to go, what is the happy median, where is it that you really do not need the Social Security number even though it may be convenient and easy to use, where do you really not need it? For instance, my bank, just a small community bank in Wisconsin, just sent out—I do my online banking and at first you needed to use your Social Security number as your password, as your ID and then you had your own password. They just sent out an email, if you want to get back on, no more, we are getting rid of this, you come up with your own ID and password and then that will from now on henceforth get you access to your bank accounts.

So, it seems to me, just using that one little example, that financial services firms and other firms can, if they choose to do so, change this data that is required to ID and authenticate who you are. So, where is it that, and I know each of you are going to have a different answer to this question, where is it that you absolutely have to have the Social Security number and where is it that you would like to have it but you really do not need it? I would just like to ask the four of you who are involved in this your answer to that question?

Mr. PRATT. I believe at the front-end of every transaction, when you are in the process of authenticating, and I think to that extent we agree, you must have a system of authentication, not the same as do you have a Social Security number. Using the Social Security number though as part of the complete set of data that is gathered at the point of the opening of the transaction is important because later you may close that account and open up another account and that bank may use a different authenticating system. Later you may close that account and open up a different account with a different authenticating system.

Mr. RYAN. This presumes that you cannot really authenticate who you are, right? This presumes that there is no other better authenticating method, right?

Mr. PRATT. Well, no, actually what it presumes is there is no silver bullet to authentication and paralleling authentication strategies will be criminals chasing down the strategy, trying to pull it apart and to defeat it. That will always happen, always has, always will. So, paralleling authentication will be the need to have a definitive identifier. I have authenticated you through a variety of means, which could include using data off your consumer report to say tell me about your mortgage, you can get this online, for example, with whom do you have a mortgage, and you can identify that. Approximately what is the payment you make per month, and you

can authenticate that. By doing that, you actually end up closer to authenticating the identity of that consumer.

But with the Social, no matter which financial institution you are doing business with, I will be able to say that account is going to go into this record in the Credit Bureau database. The irony of what we have heard with some of the testimony is I was in a hearing a floor up and was being criticized, we were being criticized where a data match might use just an initial, so one of the challenges is I have other Committees with other opinions in other contexts, such as the Fair Credit Reporting Act, where if we do not use full and complete identifying data, I have excerpts from Federal Trade Commission reports on data matching.

Mr. RYAN. I want to hear these other folks.

Mr. PRATT. So, I just want you to know that it is—you need data to match and build accuracy and you need authentication strategies to authenticate.

Mr. RYAN. Dr. Antón, Mr. Rotenberg, Mr. Schwartz.

Ms. ANTON. I would just like to note that if we published everyone's Social Security numbers in the phone book along with their name and telephone number but never used it as an authenticator, we could eliminate some identity theft in this country.

Mr. ROTENBERG. I think that would be a risky strategy.

[Laughter.]

Mr. ROTENBERG. Until everybody got on board with that plan but food for thought. I do think we need to move away from the Social Security number as an identifier. As I described in my testimony, Congress understood this problem. They saw what was happening. What preceded the Privacy Act was a very good detailed report that said the SSN is going to become a universal identifier if we do not put some brakes on it, and we are living with the consequences. It is not cost-free for the financial services to be using the SSN. It is the number one complaint that consumers have to the FTC and the cost is over \$50 billion.

Mr. SCHWARTZ. Mr. Ryan, I would say that it would be very difficult for the financial services industry to move away from Social Security numbers. First, obviously, for tax reporting purposes, the Social Security number is required. Under the USA Patriot Act, one of the requirements of a customer identification program is to get a Social Security number to make certain that that person is a legitimate person, that a Social Security number has been legitimately issued.

I agree that the authentication—and that is the reason why your bank has moved away from that—the authentication issue is an important one and because of the proliferation of Social Security numbers and the availability of them, many financial institutions are now requiring other types of vehicles for getting access to your account.

Mr. RYAN. So, you might need it to open up the account to begin with, but you do not need it to proceed thereafter as an identifier?

Mr. SCHWARTZ. Well, sometimes, too, for example, if you call and you wanted to find out what your balance is in your account or to find out if a check has been paid or to transfer funds, there are many Mr. Ryan's in this world who are dealing with banks, and you do not remember your account number, for example, I

have no idea what my account number is, but that would be one element that you would be asked for, your Social Security number, and that—

Mr. RYAN. But it could be something else other than the Social Security number?

Mr. SCHWARTZ. Well, what are you going to use, the bank would not know what your account number is because you do not know what your account number is, so that is at least one way of getting the first level of information. Then they will ask you, for example, what has been a recent transaction or give me your address, your date of birth, there are other identifiers.

Mr. RYAN. All these other things.

Mr. SCHWARTZ. You do not know your date of birth?

Mr. RYAN. No, I said you could use all these other things other than the Social Security number.

Mr. SCHWARTZ. They are, they are. If you call a bank, they will not give you—most institutions will not give you access to your account simply by giving your name and your Social Security number, there will be other questions that they will ask you to verify that you are who you say you are.

Mr. RYAN. The challenge for the industry is going to be, it may be easy, it may be the path of least resistance to use the SSN, but clearly not necessary. Maybe to open up an account, maybe for taxes but not necessarily as an identifier or as an authenticator, I guess I am using these words correctly. You could move forward with other pieces of information that people could navigate to use as identifiers and authenticators prospectively once an account is opened, could you not?

Mr. SCHWARTZ. I think it would be very difficult in many industries to do that. For example, if you have many accounts at a bank and have many different numbers, one thing that ties them all together is your Social Security number so that, for example, if you call and say, “How much do I have in my checking account, when is my CD going to be maturing, what is the balance on my credit card?” If you do not know the numbers on those accounts and you cannot give them to the person that you are talking to. Your Social Security number is a way in which the central information files of many institutions tie all these accounts together.

Mr. RYAN. That is just the way the programs are running right now.

Mr. SCHWARTZ. Excuse me?

Mr. RYAN. It is the way the programs are running right now.

Mr. SCHWARTZ. But then for each institution, you would have separate identification numbers and then we would have the same problem we have now, every time you go online, who can remember what your passwords are? Most people are now using of course their birth dates because it is easier to remember.

Mr. RYAN. I know I am being liberal with the time, but I can see you are shaking ahead a thousand times, Dr. Antón.

Ms. ANTON. In my written testimony, I would just like to point out that I talk about the dangers of using Social Security numbers as primary keys in a database and that that is another problem area, and so I just encourage your staff to look at that.

Mr. RYAN. Thank you.

Chairman MCNULTY. Thank you very much, Mr. Ryan. If there are no further inquiries, I want to thank our staff for the tremendous work they did in preparing the Members for this hearing. I want to thank all of the witnesses, all of the guests who have been so patient for the past three hours. I especially want to thank Senator Schumer, Congressman Barton and Congressman Markey for leaving other markups to come here today and to testify.

When Senator Schumer was here, he was talking about old phrases and sayings that people might not relate to, let me use one more, it seems to me that there are legitimate reasons why in certain cases people should reveal their Social Security number. They, in my opinion, are finite in number. The old phrase I am going to use is that it seems to me today that "every Tom, Dick and Harry" is asking people across the country to reveal what their Social Security number is. We heard many individual instances today that people went through. Mr. Barton related the story about purchasing a cell phone and being asked for his Social Security number. Ms. Tubbs Jones had one and I mentioned the time Nancy and I were going out to buy an appliance.

Now, think for a moment about the information, which we gave to this retailer. We gave them our names, our address, our zip code, our home telephone number, a picture identification card, and our driver's license number to buy a refrigerator. This must stop.

After we did that, the clerk, who recognized me, asked me for my Social Security number, and I said, "No." Before I said "no," I said, "I do not think you should be asking me for that information. Why are you asking me that information?" She said, "We ask everybody." I said, "No, I am not going to do that." I said, "Check with your supervisor." She went and checked with her supervisor and came back and said, "No, we do not really need to have that." So I just hope that reason can prevail as we go forward.

I hope two things as a result of today's hearing as we move on. Number one is that before we get to any legislative fixes at all, that people within the sound of my voice will be a bit more careful about giving out this very sensitive information and doing basically what Mr. O'Carroll suggested, that unless you really know there is a legitimate reason why that person has to have that information, "Just say no." The second thing we need to do, beyond that, is just because it has proliferated to the point where it is really quite a crisis and has really destroyed some lives, we need to take some legislative action to restrict the ability of some folks to be asking for this very sensitive information. We are going to move forward on that.

I thanked the folks before who have been working on this issue for years but, in my opinion, the time for talk has ended and the time for action is now, and we intend to move forward.

Again, I want to thank all of you for your expert testimony, for spending so much time with us today. This hearing is concluded. [Whereupon, at 12:50 p.m., the hearing was adjourned.]

[Submissions for the Record follow:]

LexisNexis, Letter

LexisNexis
Reed Business
July 3, 2007

The Honorable Michael R. McNulty, Chairman
Subcommittee on Social Security
Committee on Ways and Means
1102 Longworth House Office Building
Washington, DC 20515

Dear Chairman McNulty:

Reed Elsevier Inc., on behalf of its LexisNexis division, appreciates the opportunity to submit comments for the record on Social Security number (SSN) privacy. We would like to commend the Subcommittee for its leadership on this important issue over the years, and hope that our experience in this area will be useful as you develop legislation regarding SSNs and identity theft.

Reed Elsevier is one of the world's leading publishing and information companies, employing more than 20,000 people in the United States. LexisNexis leads the information industry with the largest online information service, providing critical information to legal, business, and government professionals. Products and services provided by LexisNexis help businesses and government manage risk through fraud detection and prevention, identity authentication, and intelligent risk scoring and modeling.

LexisNexis' identity authentication products help detect and prevent identity theft and fraud by allowing financial institutions, insurance companies, government agencies, and others to determine whether people are who they say they are. In addition, LexisNexis provides products and services that are used to help professionals locate people and assets, support national security initiatives, and facilitate background checks on prospective employees. LexisNexis staff includes subject matter experts in identity theft, identity management, and identity authentication.

One of the distinguishing aspects of the LexisNexis service is our extensive collection of public records information. Use of our public records information is an indispensable tool for gathering information and providing accurate answers to prevent and detect fraud, verify identities, locate individuals, perform due diligence searches, and provide risk management solutions and employment screening for businesses and governments worldwide. The overwhelming majority of the information sources on the LexisNexis service are public in nature, all of which are available to the general public through their public libraries, the local newsstand or bookstore, or from government offices. Many of these public records contain SSNs, which we use for indexing, matching and verifying data to help ensure the accuracy of the information in our databases.

LexisNexis is committed to the responsible use of information and has been at the forefront of the privacy debate, leading industry efforts to balance consumer privacy interests with responsible uses of information for important and socially beneficial purposes. We recognize that key to the SSN issue is striking the appropriate balance between protecting consumer privacy and ensuring that important uses of this information can continue. We share the Subcommittee's concern about the potential misuse of data for identity theft and other harmful purposes. Indeed, in the fight against identity theft, where verifying an individual's identity is crucial, information from commercial databases such as LexisNexis is absolutely essential.

Due in large part to the efforts of members of the Subcommittee and the important record built through hearings it has held, there has been increased recognition of the importance of striking a proper balance between protecting privacy and ensuring continued access to SSNs by business and government for important and socially beneficial uses. There have been other legislative proposals before this committee and other committees to restrict SSNs in a way that would limit many of the critical and societally beneficial uses of SSNs. Ironically, such restrictions would actually inhibit many of the tools critical to fighting identity theft and fraud. We urge the committee to ensure that such uses are not restricted as it considers legislation in this area.

We appreciate the opportunity to provide you with the following comments that we hope will be useful to the Subcommittee as it considers legislative options. Our comments below focus on the following two main areas: First, we will highlight the many important business-to-business and business-to-government uses of SSNs. Second, we will discuss several important issues that should be considered in developing any legislation in this area.

I. Important and Beneficial Uses of SSNs by Business and Government

Government agencies, businesses, researchers, and others rely on information contained in commercial databases to do their jobs. Commercial database companies like LexisNexis play a vital role in this effort by collecting information from numerous sources and creating comprehensive data collections that allow users to easily search and locate information. Without this critical public records information, the effectiveness of these government agencies, businesses, and researchers would be dramatically reduced.

The use of SSNs is essential for person identification and record matching purposes and is critical in ensuring the accuracy of the information in these databases. SSNs allow persons to be identified accurately and ensure that records for different individuals do not get co-mingled, providing a false result. There are more than 43,000 Robert Jones' in the U.S. today. How else can someone distinguish one from another? A unique identifying number like the SSN is important to ensure that information collected about individuals is pertinent and accurate.

The following examples describe some of the important ways in which commercial database services, such as LexisNexis, are used by our customers to help people, protect consumers, locate missing children, prevent fraud, and assist law enforcement efforts:

- **Locating sex offenders**—SSNs are used to locate registered and unregistered sex offenders. There are more than 560,000 sex offenders in the U.S. Approximately 24 percent of these individuals fail to comply with address registration requirements mandated by law. LexisNexis provides products to law enforcement entities to help them locate registered and unregistered sex offenders. Use of SSNs for record matching and retrieval allows law enforcement to locate sex offenders even when the registration address has not been kept current.
- **Preventing and investigating terrorist activities**—The use of commercial databases like LexisNexis is an important tool in the global battle against terrorism. Information provided by LexisNexis was instrumental in locating suspects wanted in connection with the September 11 terrorist attacks. Since September 11, the Department of Justice found that LexisNexis public records were mission critical in bolstering cases against terrorists. As a result, agents, investigators, attorneys, and analysts have full access to LexisNexis public records and other information. The SSNs contained in the LexisNexis database are a critical tool used by the FBI and other federal law enforcement agencies to locate suspects and witnesses and in investigating and building cases against suspected terrorists.
- **Locating and recovering missing, abducted and exploited children**—LexisNexis has partnered with the National Center for Missing and Exploited Children to help that organization locate missing and abducted children. Locating a missing child within the first 48 hours is critical; after that time, the chance of recovering the child drops dramatically. In many of these cases, it is the non-custodial parent who has taken the child. The use of SSNs is critical in quickly locating the non-custodial parent and recovering the missing child.
- **Identifying and preventing fraud**—Banks and other financial institutions routinely rely on SSNs to accurately match and retrieve public record information contained in LexisNexis' databases to detect fraudulent credit card applications. Through the use of LexisNexis, credit card companies have significantly reduced losses due to fraud. Insurance companies have experienced similar successes through the ability to use SSNs in data matching and retrieval. The use of SSNs in public records and other sources is key to preventing fraud.
- **Locating witnesses and helping make arrests**—Lawyers are major users of person locator databases. Use of SSN information in these databases, even when it is not displayed, is critical to tracking down witnesses in connection with civil litigation. Law enforcement agencies also are major users of commercial databases. For example, in 1998, the FBI made over 53,000 inquiries to commercial online databases. This information led to the arrests of 393 fugitives and the location of nearly 2,000 suspects and more than 3,000 witnesses.¹

¹Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the U.S. Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State and the Judiciary and Related Agencies, March 24, 1999.

- **Preventing and investigating financial crime**—LexisNexis provides information to the Financial Crimes Enforcement Network (FinCEN), which supports federal, state and local law enforcement agencies in financial investigations and is heavily reliant on SSNs in these investigations. In addition, LexisNexis worked with the American Bankers Association to develop best practices to be used by banks and other financial institutions to prevent money laundering and ensure compliance with the USA PATRIOT Act. The use of SSNs by financial institutions to verify and validate information about prospective customers is critical to the success of that program.
- **Recovery of child support and other debts**—Public and private agencies rely on SSNs and other information contained in information solutions and services products to locate persons who are delinquent in child support payments, other lawful debts, and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for Enforcement of Support (ACES), a private child support recovery organization, has stated that SSNs are the most important tool for locating parents who have failed to pay child support. ACES has had tremendous success using LexisNexis products to locate nonpaying parents.
- **Helping locate pension fund beneficiaries**—The task of locating former employees is becoming increasingly difficult. Americans move on average every five years, particularly when they change jobs. Their names may change as a result of marriage or they may list slightly different names (e.g., leaving out a middle initial) on employment documents. To ensure that pension fund beneficiaries receive the money owed them, plan administrators and sponsors are required by federal law to use a commercial locator service, such as LexisNexis, to search for missing pension beneficiaries. These services are by far the most cost-effective and efficient way to find these former workers. Pension Benefit Information, a leading service locating these workers, reports that searching with a retiree's SSN results in an 85–90 percent success rate in locating an individual, compared to a success rate of only 8 percent without use of this information. Loss of SSNs from public records and commercial locator services would dramatically increase the costs of locating former employees. Moreover, in many cases, employers would be unable to find former employees, resulting in a loss of pension benefits to the individual.

II. Important Issues To Be Considered in Developing Legislation

We applaud members of the Subcommittee for recognizing legitimate business and government uses of SSNs, and we will continue to work with the Subcommittee to help ensure that any legislation accomplishes its important objective of preventing the misuse of SSNs, while ensuring the continued use of SSNs for legitimate business and government uses. There are several important issues that should be considered by the Subcommittee in developing any legislation in this area. Our specific comments are focused in the following four areas:

A. Business-to-Business and Business-to-Government Exemptions

It is critical that any legislation restricting access, use or display of SSNs contain exceptions for important business-to-business (B-to-B) and business-to-government (B-to-G) uses. Among the exemptions needed are those that would preserve uses permitted under the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). It is critical to ensure the continued use of SSNs consistent with GLBA for identity authentication and verification to assist in fraud detection, prevention, and investigation efforts, to perform an array of background checks, and to effectuate and enforce transactions requested by the consumer. Similarly, an exception should be included to ensure the continued use of SSNs for the permissible purposes under the FCRA.

Moreover, it will be important to ensure that any legislation clarifies the scope of exemptions for law enforcement or national security purposes to ensure that information service providers, such as LexisNexis, can continue to access and acquire this information to be able to provide information tools to its law enforcement customers, as well as to users who, although not government officials, undertake law enforcement activities. Groups with which LexisNexis works, such as the National Center for Missing and Exploited Children, would be severely hampered if they could no longer access databases containing SSNs to do their jobs.

If the law enforcement/national security exemption included in legislation is too narrowly crafted to only include government law enforcement agencies, many of the important law enforcement and national security applications performed by non-gov-

ernmental entities will be excluded. Finally, exceptions should be included for locating individuals, pension fund beneficiaries, missing heirs, and individuals delinquent in the payment of child support or other debts.

B. Public Records

The issue of SSNs in public records is highly complex, and legislation in this area will have far-reaching implications. As explained above, public records are an important source of information used by LexisNexis in compiling data for our online service. We routinely use SSNs in public records to accurately match records from disparate data sources and to enhance the accuracy of record retrieval. In addition, our clients, including financial institutions, insurance companies, government agencies and others routinely rely on our public record databases containing SSNs for identity verification and validation purposes, to identify, prevent, and investigate identity theft and fraud and for other important purposes.

When we refer to public records, we mean government records that typically and historically have been made available to the public. Examples of public records include titles to real property, real property tax assessor records, bankruptcy records, judgments, liens, state professional licenses (and their suspension and revocation), corporation filings, and death records. This information traditionally has been available to members of the general public upon request.

As the General Accounting Office confirms in its June 2007 Report to Congressional Requesters on Social Security numbers, redacting SSNs from public records would be a difficult and challenging process.² The summary of results reports that removal or truncation of SSNs in all public records may be “costly and may not fully protect SSNs.” For example, the report states that it cost Palm Beach County more than \$2 million to complete software and manual removal of SSNs and other identifiers in approximately 40 million pages of records (Report at 25). In small cities or towns that do not have the resources to remove or truncate SSNs in public records, many may choose to simply cut off access to these records.

Public records are a unique class of information that historically has been made available for public inspection. Therefore, we are concerned about any limits on the dissemination of this information. Any legislation being considered should provide an exception for an SSN that is incidental to the sale or provision of a document lawfully obtained from the Federal Government or state or local government made available to the general public, or from a document that has been made available to the general public via widely distributed media. This is the approach taken in S. 1208 and S. 1178.

C. Rulemaking

The proposed rulemaking provisions in some of the proposals being considered provide only limited guidance and wide discretion that could result in excessively restricted access to SSNs. Legislation should clearly delineate the restrictions on the sale and purchase of SSNs and provide a complete list of exceptions. To the extent that any rulemaking language is included, any discretionary authority should be limited, and the factors to be considered in promulgating the regulations limited to those specific factors necessary to balance restrictions on use and continued use of SSNs by legitimate businesses.

D. Preemption

Given the uniquely federal nature of SSNs and their importance to businesses engaged in interstate commerce, legislation regulating the use of SSNs should preempt state laws. It is important that a single, national law governing the sale, purchase, and display of SSNs be applied consistently on a nationwide basis.

LexisNexis is committed to the responsible acquisition and use of SSNs and other personally identifiable information. LexisNexis shares the Subcommittee’s concern about the potential misuse of this information for identity theft and other harmful purposes. Nevertheless, as many of the Subcommittee members and witnesses recognized during the June 21 hearing, legitimate uses of SSN information are absolutely essential in the fight against identity theft and fraud and other important uses. Congress should not take any steps that would jeopardize the usefulness of such services. We thank the Subcommittee for having held this hearing on these important issues, and look forward to working with the members of the Subcommittee and others to develop an appropriate solution.

²See GAO Report 07–752 on Social Security Numbers (June 2007) (“Report”).

We appreciate the opportunity to submit comments and hope that our comments will help the Subcommittee as it considers these issues and develops legislation. If you have any questions, please call me at 202/857-8253 or Steve Emmert of my staff at 202/857-8254.

Sincerely,

Steven M. Manzo
Vice President, Government Affairs

Bruce Hulme, Legislative Director, National Council of Investigation and Security Services, statement

Thank you for the opportunity to provide testimony on protecting the privacy of the Social Security number from identity theft. I am Bruce Hulme, Legislative Director of The National Council of Investigation & Security Services (NCISS) which represents professional private investigators and security officers across the nation.

Our members agree that personal data, including Social Security numbers (SSNs), should not be readily disseminated and available to anyone with an Internet connection and a few dollars. We support efforts to limit the sale of the SSN except where there is a legitimate need for it. NCISS supports prohibitions on the display of Social Security numbers on checks, drivers' licenses and employee ID badges. These provisions were in legislation previously considered by the Ways and Means Committee.

We support the prohibition of the sale of personal data over the Internet to the general public. Such a prohibition, along with limitations on the use of the number on the documents cited above, would solve many of the issues related to identity theft. It is critical, however, that care be taken to provide clear exceptions for purposes that serve the public good. The exceptions in Section 3, as reported by the Energy and Commerce Committee, are insufficient and would result in unintended consequences.

Financial institutions, schools, state and local governments and others have used the SSN as an identifier because it is uniquely attached to an individual. Private investigators have utilized the SSN for the same reason. It is the best way to assure that the John Smith we're attempting to locate is the correct John Smith, and not one of 50,000 others.

There are many John Smiths sharing the same birthday and living in the same town. Often the Social Security number is the only way to distinguish people sharing a name and other identifiers.

Section 3 of HR 948 would deny private investigators access to this unique identifier by making it unlawful to sell or purchase the number. This will affect the accuracy of databases we access to locate the right John Smith. The SSN is also critically important for identifying women who often change surnames through marriage and divorce. The SSN does not change and allows us to locate these otherwise difficult to find witnesses. In California, database searches led directly to witnesses who recanted testimony and helped free a man *wrongly imprisoned for twenty years*. Without the ability to use the database, it is unlikely these witnesses would have been located.

Due Process Issues

The exceptions listed in *Section 3(b)(3)* include one for law enforcement. The absence of an exception for private investigators denies a critical tool to persons accused of crime. This is particularly important for indigent defendants because of the small expense budgets available to public defenders and appointed counsels. They need a cost effective way to locate witnesses. They don't have the resources of the state. The lack of such an exception provides an obvious due process issue where the police have access to a database not available to defendants.

Civil Trials

These disparities can exist in civil cases as well. An individual consumer considering a lawsuit against a major corporation will be disadvantaged if this inexpensive tool for locating witnesses is made unavailable. Some meritorious cases would likely never be brought.

In both civil and criminal trials, justice is served best by all parties getting access to all possible witnesses. Access to a fair trial is a fundamental right of American

citizens. Without the ability to identify and locate all witnesses, that right is threatened.

Investigators do not have access to the central criminal history database that law enforcement officials do, so it is essential to have addresses when seeking information about prior convictions. With prior address data, investigators know which courthouse records to search. Without the address, we may not even know in which states to look. This information is important for more than pre-employment purposes. In both civil and criminal trials, attorneys need to know the backgrounds of witnesses and potential witnesses.

In testimony before this Subcommittee last year, I described how I was able to solve a case in which a 97 year old New Yorker was robbed of hundreds of thousands of dollars by a caregiver who attempted to hide his ill-gotten gains with relatives in South Carolina. Had I not been able to use a database, I never would have known to look for records in that state in which the funds were used to purchase real estate and for other purposes.

Fighting White Collar Crime

It is no secret that law enforcement does not have all the resources it needs to fight white collar crime, including identity theft. That crime is difficult to solve and often involves multiple jurisdictions. Many victims turn to investigators for assistance. In some instances, when accessing databases investigators have discovered that the criminal is using multiple SSNs. Under HR 948, we would be denied that information, which can assist other victims besides our client. In one instance we cited in testimony last year, a private investigator solved a case that authorities would not investigate because the client's \$80,000 in losses did not meet or exceed the law enforcement agency's minimum threshold to investigate. Using the SSN, the investigator discovered that a former employee had stolen the client's identity and had three aliases and at least three SSNs.

The SSN is critical to investigators for conducting other fraud investigations as well. It can be particularly important for matters involving theft of intellectual property, ranging from copyrighted music and motion pictures to design of computer chips.

These databases, using the SSN, have also been important for locating lost heirs and enforcing child support orders. Last year, the committee also heard from a witness about how critical the information can be for assisting in finding pension beneficiaries.

We urge that a new exception be added to HR 948 in Section 3(b)(3):

“to identify or locate missing or abducted persons, witnesses, criminals and fugitives, persons suspected of fraud, persons who are or may become parties to litigation, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries, missing heirs and persons material to due diligence inquiries.”

During consideration of S-1178, the Senate Committee on Commerce, Science and Transportation adopted an amendment including similar language. Such an exception would permit appropriate uses of databases. NCISS supports strong sanctions for anyone who would misuse this data.

Our association stands ready to assist the Committee as it develops legislation to protect Social Security numbers.

National Organization of Social Security Claimants' Representatives, Englewood Cliffs, New Jersey, statement

I am the Executive Director of the National Organization of Social Security Claimants' Representatives (NOSSCR). Founded in 1979, NOSSCR is a professional association of attorneys and other advocates who represent individuals seeking Social Security disability and Supplemental Security Income (SSI) disability benefits. NOSSCR members represent these individuals with disabilities in proceedings at all SSA administrative levels, but primarily at the hearing level, and also in federal court. NOSSCR is a national organization with a current membership of nearly 3,900 members from the private and public sectors and is committed to the highest quality legal representation for claimants.

As demonstrated by the testimony at the Subcommittee hearing on June 21, 2007, the impact of identity theft on individuals can be catastrophic. The cost of recovering from identity theft has the potential to be astronomical and it can take years

to repair the damage. Given the repeated warnings from agencies, including the Social Security Administration (SSA), our Statement for the Record describes what we believe is an unnecessary requirement by SSA that attorneys and others who represent claimants repeatedly disclose their own Social Security numbers (SSNs).

BACKGROUND

The Internal Revenue Service has advised SSA that it must set up a procedure to issue Forms 1099-MISC to attorneys and eligible non-attorneys who receive direct payment of fees for representation from SSA.

The IRS Forms 1099-MISC will first go out in January 2009, covering fee payments made in calendar year 2008. SSA plans to issue Forms 1099-MISC to all appointed claimants' representatives who receive payment of aggregate fees of \$600 or more in a calendar year. Generally, the payment amounts will be reflected in Box 7 (Nonemployee compensation) on Form 1099-MISC. This includes representatives who are sole proprietors and those who have made the election to the IRS to be classified as a single-member Limited Liability Company (LLC) or single-member Limited Liability Partnership (LLP).

In those situations where SSA is notified that the representative is an employee or partner, and the firm or other entity provides the necessary taxpayer information via this registration process, SSA will issue two Forms 1099-MISC:

- One Form 1099-MISC will be issued to the representative reflecting aggregate payments made to the representative in his or her capacity as an employee or partner in Box 14 (Gross Proceeds Paid to an Attorney).
- The other Form 1099-MISC will be issued to the firm or other entity reflecting aggregate payments made to its employees/partners in Box 7.

The IRS has indicated to SSA that, while it performs a matching process for amounts reported in **Box 7** of the Form 1099-MISC, **it does not match against the amounts reported in Box 14**. Box 14 might be termed "nonactionable" and is not used by the IRS to match with income reported on that individual's tax return. NOSSCR has urged SSA to work with the IRS to eliminate this "nonactionable" reporting, which seems to serve no purpose.

THE REGISTRATION PROCESS

Starting January 1, 2007, SSA will make direct payment (through fee withholding) only to those attorneys and eligible non-attorneys who have completed the registration process.¹ As described below, there are three forms that must be filed. Two forms are filed one-time only. However, one form, SSA-1695, must be filed for every new client and it is this form that requires disclosure of the representative's own SSN.

STEP ONE: All attorneys and eligible non-attorneys who want to receive direct payment of fees must complete and submit Form SSA-1699, "Request for Appointed Representative's Direct Payment Information." In addition, law firms, partnerships, corporations and multi-member LLCs/LLPs that have attorneys and/or non-attorney representatives as partners or employees who receive direct payment should provide tax ID information for that business entity, using Form SSA-1694, "Request for Business Entity Taxpayer Information." Both of these forms, the SSA-1699 and SSA-1694, are submitted one time only. They also can be submitted online through a secure site.

STEP TWO: In contrast, attorneys and eligible non-attorneys must submit the new Form SSA-1695, "Identifying Information for Possible Direct Payment of Authorized Fees," in **every case** where they become the representative on or after January 1, 2007.

This form is completed by the individual representative, not the firm, for each client. It must be filed in the SSA field office and in paper form only. Unlike the other two forms (which are submitted one time only), Form SSA-1695 cannot be filed online. The form requires not only the client's Social Security number (SSN), but also the representative's SSN. In addition, the firm's Employment Identification Number (EIN) must be included. The instructions which appear at the bottom of the form state, "To SSA Staff: After the information on this form is entered into the appropriate system(s), immediately shred the form. Under no circumstances should this form be scanned, placed in a claims file or otherwise retained."

¹SSA provides an explanation of the new registration process at its website: http://www.ssa.gov/representation/direct_payment_of_approval_fees_forms_1099.htm.

Our main concerns with the new registration process relate to use of the Form SSA-1695. Attorneys and eligible non-attorneys are understandably uneasy about the prospect of their SSNs appearing on the SSA-1695s. We have contacted SSA about our concerns regarding confidentiality and the increased potential for identity theft and have recommended alternative ways to deal with the process.

- First, we believe that there is no reason to require the representative to include his or her SSN. In most cases, the law firm employing the attorney (as a solo practitioner, partner or associate) is the entity that is responsible for payment of income taxes on the fees received. And, the attorney is required to provide that law firm's EIN on the SSA-1695.
- Unlike the other two new forms in the new registration process (Forms SSA-1694 and SSA-1699), the SSA-1695 cannot be completed online and only a paper copy can be submitted to the SSA field office. While SSA instructions state that district office workers must shred the forms after processing the information, we have received reports from some NOSSCR members that mistakes are being made and that, in some cases, these forms are appearing in claims folders.
- In our interactions with SSA, we have maintained that the form should require only the submission of the EIN for the firm that is liable for payment of the taxes. We also have proposed an alternate individual identifier, such as a PIN.

CONCLUSION

We believe that these repeated disclosures of a representative's SSN on Form SSA-1695 are unnecessary and, potentially, an invitation to identity theft. We are constantly bombarded with warnings from many sources, including SSA, about privacy concerns and protection of our SSNs. From attorney bar rosters to health insurance to state departments of motor vehicles, we are told not to maintain records according to SSNs and to use other identifiers. Because of concerns with possible SSN misuse, many NOSSCR members have now opted to sign up for credit protection service.

Questions for SSA regarding this process include:

- Why must the SSN be submitted in every case, through an unsecure process, when in fact SSA already has this information from the secure one-time filing?
- If SSA must have this information on this particular form, why can't this information be submitted in a secure manner?
- How can SSA guarantee that the representatives' SSNs will not be subject to identity theft?

Property Records Industry Association, Morrisville, North Carolina, statement

As you most assuredly are aware, the hottest buzzwords of the millennium include "Identity Theft" and "Personally Identifiable Information." Everyone is wrestling with what is the solution to the problem of protecting individual privacy rights while at the same time encouraging commerce and improving compliance with government regulations.

When serious consideration is given to the various facets of this topic, it quickly becomes clear that there is no easy, "one-size-fits-all" solution. There are many factors to be considered. However, there is little disagreement that something needs to be done to counter the abuses that undermine faith in existing institutions.

The Property Records Industry Association (PRIA) is a coalition of public and private participants of the property records industry, cooperating to formulate positions on issues of common interest. Among other objectives, the Association works to identify problems, opportunities and solutions that will make property records systems more efficient, effective and responsive to the public. The Association also works to identify areas of consensus within the industry, leading to recommendations for national standards pertaining to recordable documents.

PRIA began seriously engaging the issue of social security numbers appearing in real estate documents in early 2003. As part of its Winter Conference in March 2003, PRIA hosted a "Privacy/Access Roundtable" in Washington DC. At the conclu-

sion of the Roundtable, PRIA moved to establish a Privacy/Access Workgroup. The workgroup then initiated an email listserv discussion around a number of privacy-in-public-records topics. Those discussions led to various presentations and open forum sessions at PRIA conferences in 2003 and 2004. In July of 2004, PRIA was invited to testify before the House Ways and Means Committee Social Security Subcommittee regarding HR 2971, the Social Security number Privacy and Identity Theft Prevention Act of 2003. Both PRIA Winter and Summer conferences in 2005, 2006 and 2007 include presentations and open forum discussions of this privacy and information security dynamic. PRIA wrote a White Paper in January of 2006 titled, "Privacy and Public Records: Making Practical Policy" and drafted Model Legislation called the "Social Security number and Privacy Protection Act" (SSNAPP Act) in July of 2006 (see Appendix A). Our focus is on the importance of social security numbers to the real estate and public record industry.

Identity theft

Before the turn of the last century, one would have to take a ride on horseback to the county seat to pull the original Deed books to find information about a parcel of real estate. This is the concept of "practical obscurity" of public records—personal information could be found in a public record, but there was little risk of harm to an individual because someone had to take the time to search the records at the recorder's office.

Technology undeniably has had a significant impact on access to public records. Technological developments raise concerns about how much information is too much information and whether there should be global access to public records.

It is a common misconception that easy access to public records has facilitated identity theft or land fraud. While posting documents that contain certain key information on the Internet, such as credit card numbers, social security numbers, and signatures, can provide a criminal with some of the information needed to commit identity fraud or theft, there is no evidence to support any claim that this is systematically being done to perpetuate identity theft crimes. There are many easier, and far more efficient, ways for identity thieves to obtain this information in today's world, as opposed to combing through public records and hoping to find something—a "needle in the haystack" approach.

That being said, a proactive approach to apply greater discretion to what public land record information is disclosed online is a reasonable approach to discourage the use of public land records to perpetuate identity theft and fraud. An accommodation between information privacy and access is appropriate and necessary.

It is important in any discussion involving the protection of social security numbers that legislators consider the full impact of these actions on their constituents as well as the industries that serve them. Public land records contain information critical to the economy of the United States because much of the information collected by the private sector comes from public records and that information is key to the proper function of the real estate industry. Both the public custodians and the private business sectors that use the public records to facilitate critical functions within the real estate transaction; i.e. listings, mortgages, title insurance, closings, escrows and others; need to be considered when deciding how best to protect social security numbers from identity theft.

The Role of Public Records in Combating Identity Theft and Fraud

It is important to understand that access to public records data is actually a very effective weapon in combating identity fraud and theft. Social security numbers compiled from public records (including court records) have proven to be the most reliable tool in verifying an individual's identity, which helps prevent the rapid increase in identity fraud victims. Commercial databases compiled using public records for identity authentication are routinely used to detect fraud, including credit card application fraud, insurance application fraud, and other types of fraud. Thus, efforts to restrict the collection and use of personal information contained in public records, though well intended, actually may hinder efforts to prevent identity theft by depriving businesses, government and law enforcement officials of valuable data that is used to authenticate identities and protect the public. Security must be balanced with access.

Prohibiting Complete Social Security Numbers on Public Land Records

As you review testimony to enhance the privacy of your constituents, most are more than likely looking to prohibit the use and disclosure of an individual's social security number in public records. However, it is important to understand for which

purposes and how social security numbers are used by government and the private sector, as well as what impact redaction and truncation have on record custodians, business, and the public.

Privacy Focus: Social Security Numbers

A number of privacy advocates warn that the display of social security numbers in public records must be reduced as they are a primary piece of information in the commission of identity theft crimes. At least forty-one states and the District of Columbia maintain at least one record that displays an individual's social security number, according to a U.S. Government Accountability Office (GAO) study conducted in November 2004. Given the nature of the social security number as a unique identifier for important records and services, advocates are concerned that display of the numbers in public records makes it easier for identity thieves, both domestic and international, to obtain new credit and bank accounts in the names of their victims.

As outlined in a white paper created by the PRIA, "Privacy and Public Land Records: Making Practical Policy" available for your review at www.pria.us, under a section entitled "Identity Theft," at this time there does not appear to be evidence supporting the claim that information derived from public records, including social security numbers, is systematically used to perpetuate identity theft crimes. That being said, it is reasonable to expect that government should, and must, institute reasonable safeguards to protect citizens from becoming victims of identity theft as a result of public land record abuse.

Legitimate Business and Government Uses of the Social Security Number

Several legitimate business and governmental uses exist for social security numbers. These include preventing and investigating terrorist activities, locating and recovering missing children, identifying and preventing fraud, locating witnesses and helping make arrests, preventing and investigating financial crime, enforcing child support obligations and government assistance programs, helping locate pension fund beneficiaries, helping locate blood, bone marrow, and organ donors, contributing to important medical research efforts, notifying families about environmental hazards. The benefits gained from the legitimate use of a social security number need to be balanced with the potential for abuse.

Balancing Benefits Versus Abuse of Public Records/Access to Social Security Numbers

The Federal Government, states and businesses are either legally obligated, or choose to voluntarily control, the disclosure of records containing social security numbers. While privacy advocates call for greater control of access to social security numbers in public records, such a restrictive approach would threaten the ability of the government and businesses to accurately and efficiently verify the identification of citizens or consumers and authenticate that they are who they say they are.

Identity thieves are using a number of methods to obtain personal identification information, including "phishing" scams in which thieves send bulk or targeted emails to consumers impersonating legitimate businesses asking consumers to provide personal information such as social security numbers. "Phishing" has recently been expanded to include "spear-phishing." "Spear-phishing" is where identity thieves send bulk or targeted emails falsely appearing as a commanding officer, in the case of military personnel, or as a superior or executive within an organization. These thieves ask that the employee email the supervisor or executive, at the false email address, their personal information to update records or to confirm their personal information. Another new scam is "pharming," where identity thieves redirect visitors from legitimate websites to "spoofed" websites (websites which look legitimate, but are not), and then collect personally identifiable information from these visitors.

It is important then that any legislative or regulatory attempts to restrict the access to, the display of, or use of social security numbers in public land records should carefully weigh the actual threat of identity theft with the efficient and current use of social security numbers in public land records by state and local governments, business and citizens.

Considerations for Federal Legislation

Prior to the development of federal legislation that affects the use of social security numbers and other data elements in public records policymakers should consider the following points:

- Before exempting any specific data element from collection by a government entity or from disclosure to the public, policymakers should first set out to understand what records contain that data element and the reason for its presence in that record. Data elements are necessary in certain records and have a clear purpose. For example, without complete social security numbers in certain critical documents, such as tax liens, government and the private sector lose the ability to match data about individuals. Studying the potential impact of redaction or limits on collection of information is highly recommended before making any policy changes. Policymakers should solicit direct input from the custodians of the records and those that use them to determine how a proposed policy will affect the records themselves as well as the ability of custodians to perform their duties.
- Policymakers must identify, or provide, funding mechanisms to carry out the redaction of public records so as to avoid an unfunded mandate. In this regard, a “go forward” recording fee for creating electronic versions of all recorded documents could be used to carry out the redacting process as well.

Suggested Elements for Social Security Number Legislation

The PRIA has drafted model legislation, the Social Security number and Privacy Protection Act (SSNAPP Act), which is included in Appendix A and incorporates the elements below.

Legislation Relating to Public Records Should be on a “Day-Forward” Basis

Any legislation impacting a governmental agency’s acceptance, redaction, or truncation of documents which contain social security numbers should be effective on a “day-forward” basis only. This means that any legislation should not require redaction or expungement of records already filed or recorded.

In particular, recorders will be faced with a nightmarish task of redacting records that are already filed, or recorded, including those in other mediums such as microfilm or microfiche. Depending on the method used for redaction, the recorder may be faced with managing two databases or two sets of redacted documents. It is possible that mistakes or omissions could occur in the public record if recorders are required to manage and maintain two sets of databases, or redacted and unredacted images. Redaction of official records and updating archival and security copies could mean having to delve into technology or methods of preservation that are no longer available to the recorder or archiving facility.

Immunity of Recordors

Recordors are custodians, or stewards, of the information they are required by law to maintain. It should be the responsibility of document preparers and individual consumers, and not recordors, to make sure that documents presented to recordors for recording do not contain social security numbers if the inclusion of social security numbers is prohibited by law. Therefore, recordors should be immune from suits relating to documents filed or recorded that include social security numbers, and any liability should be imposed on the document preparers.

Authority to Redact Post Effective Date

Model legislation may grant recordors the authority to redact social security numbers from documents that are recorded after the effective date of that legislation. This authority should not affect the integrity of the original recorded document. This can be accomplished by masking the information available to the general public, for example, on the Internet, using redaction software that allows disclosure of the unredacted image on certified documents used for official purposes, such as probate.

This provision provides an important ministerial function—that of providing certified copies of records from government offices. Certification of public documents requires recordors and clerks to provide an exact copy of a recorded document. Recordors need to be explicitly empowered to redact the social security number after the

effective date of the legislation, without compromising the integrity of future certified copies.

Voluntary Redaction by Public Prior to Delivery for Recording

Legislation may grant members of the general public the opportunity to remove social security numbers and other private identifying information prior to the filing of their documents, such as provided in Texas (Texas Property Code Section 11.008). This provision removes discretionary issues from the government official and provides members of the general public with a self-help remedy if they are concerned about the privacy of their personally identifiable information. We recommend an individual be able to remove, or request removal of, a social security number or other personally identifiable information from the document before or after it is recorded.

Recorders Not to Redact Information from Documents to be Recorded

Legislation may provide that recorders not have the responsibility of redacting social security numbers or other personally identifiable information from documents prior to recording. Recorders would continue to record whatever they receive.

This provision continues the important ministerial, non-discretionary function—that of creating a public record of documents exactly as they were presented to the government offices. Certification of public documents then complies with the recorders' and clerks' responsibility to provide an exact copy of the document as it was when recorded.

CONCLUSION

Practical and informed policy making is a must to further solidify the integrity of our public records system and to achieve a meaningful balance between the public's concern about privacy and businesses' legitimate use of data. Enlightened policymakers have an opportunity to resolve these issues in a way that empowers consumers, enables business, and enhances our nation's economy.

Appendix A

SOCIAL SECURITY NUMBER AND PRIVACY PROTECTION ACT

1. Definitions

(a) "Personally Identifiable Information" means one or more of the following specific unique identifiers when combined with an individual's name:

- (1) Social security number.
- (2) Driver's license number or state identification card number.
- (3) Financial institution account number, credit, debit or charge card number.
- (4) Date of birth.

(b) "Preparer" means the person or entity who creates, drafts, edits, revises or last changes the documents that are recorded with the [Recorder].

2. Inclusion of Personally Identifiable Information

The Preparer of a document shall not include an individual's Personally Identifiable Information in a document that is prepared and presented for recording in the office of the [Recorder]. This Section shall not apply to documents that were executed by an individual prior to the effective date of this Act. All documents described by this Act are subject to inspection and copying by the public.

3. Reduction on Recorder's Publicly Available Internet Web site

If a document that includes an individual's Personally Identifiable Information was recorded with the [Recorder] and is available on the [Recorder's] public Internet website, the individual may request that the [Recorder] redact such information from the Internet record. The [Recorder] shall establish a procedure by which individuals may request that such Personally Identifiable Information be redacted from the Internet record available on the [Recorder's] public Internet website, at no fee to the requesting individual. The [Recorder] shall comply with an individual's request to redact Personally Identifiable Information.

4. Liability of Preparer

A Preparer who enters Personally Identifiable Information in a document that is prepared and presented for recording is liable to the individual whose Personally Identifiable Information appears in the recorded public document in violation of Section 2 of this Act for damages of up to five hundred dollars (\$500.00) for each act of recording.

5. Liability of Recorder

The [Recorder] shall not be liable for any claims arising from a violation of this act.

6. Applicability

(a) This Act shall not apply to state or federal tax liens, certified copies of death certificates or other documents required by law to contain Personally Identifiable Information that are filed or recorded in the office of the [Recorder].

7. Effective Date This Act shall be effective on _____.

