USE AND MISUSE OF SOCIAL SECURITY NUMBERS

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 9 AND 11, 2000

Serial 106–108

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

68–072 DTP WASHINGTON : 2001

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

PHILIP M. CRANE, Illinois
BILL THOMAS, California
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHILIP S. ENGLISH, Pennsylvania
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida
LLOYD DOGGETT, Texas

A.L. SINGLETON, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

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

SAM JOHNSON, Texas
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
JIM MCCRERY, Louisiana

ROBERT T. MATSUI, California
SANDER M. LEVIN, Michigan
JOHN S. TANNER, Tennessee
LLOYD DOGGETT, Texas
BENJAMIN L. CARDIN, Maryland

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

MAY 9, 2000

MAY 11, 2000

USE AND MISUSE OF SOCIAL SECURITY NUMBERS

TUESDAY, MAY 9, 2000

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

The Subcommittee met, pursuant to notice, at 10:00 a.m., in room 1100, Longworth House Office Building, Hon. E. Clay Shaw, Jr. (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
May 2, 2000
No. SS–17

Shaw Announces Hearing on Use and Misuse of Social Security Numbers

Congressman E. Clay Shaw, Jr., (R09FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing to examine the increasing use and misuse of Social Security numbers (SSNs). The hearing will begin on Tuesday, May 9, 2000, in the main Committee hearing room, 1100 Longworth House Office Building, beginning at 10:00 a.m. The hearing will be continued on Thursday, May 11, 2000, also in 1100 Longworth House Office Building, beginning at 2:00 p.m. The first day of the hearing will provide an overview of the issue and discuss current laws and proposals to protect SSNs from misuse. The second day will focus on the advantages and disadvantages of restricting the use of SSNs.

Oral testimony at this hearing will be from invited witnesses only. Witnesses will include representatives of the U.S. General Accounting Office, the Social Security Administration's Office of Inspector General, watchdog groups promoting privacy concerns, and affected industries. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

The SSN was created in 1936 solely for the purpose of tracking workers' Social Security earnings records. Today, approximately 277 million individuals have SSNs. Because of its near universal coverage as a unique identifier of individuals in the Social Security system, the SSN is commonly used as a personal identifier in other settings. For example, use of the SSN is required, by law, for the administration of several Federal programs, such as the income tax, Food Stamp program, and Medicaid. SSNs are also commonly used in the private sector for record-keeping and data exchange systems. Consequently, use of the SSN has expanded significantly beyond its original purpose. According to the Social Security Administration (SSA), the SSN is the single-most widely used personal identifier in the public and private sectors.

Some believe that the expanded use of the SSN benefits the public by improving access to financial and credit services in a timely manner, reducing administrative costs, and improving record-keeping so consumers can be contacted and identified accurately. Others argue that the pervasive use of SSNs makes them a primary target for fraud and misuse. Allegations of fraudulent SSN use increased from 10,915 in fiscal year 1998 to 30,115 in fiscal year 1999—a 175 percent increase. SSA and its Office of Inspector General have increased efforts to combat fraudulent use of SSNs through jointly-developed "zero tolerance for fraud" initiatives. In addition to concerns about SSN misuse, privacy concerns have also been raised as companies increasingly share and sell personal information without the customer's knowledge or consent.

There are two primary laws aimed at protecting privacy and reducing SSN misuse. The Privacy Act of 1974 prohibits Federal agencies from disclosing personal information, including the SSN, without the individual's consent. The Identity Theft Act, enacted in 1998, makes it a Federal crime to assume another person's means

of identification. However, no Federal law regulates the overall use of SSNs and Federal laws neither require nor prohibit other public and private uses of the SSN. As a result, several legislative proposals have been introduced that would restrict SSN use. These proposals are aimed at protecting consumer privacy and curbing fraudulent use of SSNs. Some believe that proposals to restrict the use of SSNs would negatively impact many businesses and State and local governments which rely on SSNs to administer transactions and provide services.

In announcing the hearing, Chairman Shaw stated: "This hearing will explore how Social Security numbers are used and sometimes misused. We will consider ways to better protect Americans' privacy and security, and what ramifications—both positive and negative—such changes may have. Given the importance of this issue and how interwoven SSNs have become in the fabric of our information society, it is critical that changes are assessed with great care."

FOCUS OF THE HEARING:

The hearing will focus on the widespread use of SSNs in the public and private sectors. The growing misuse of SSNs and associated costs will also be discussed. The hearing will examine current laws which restrict or regulate SSNs and the adequacy of these laws. The hearing will also examine legislative proposals aimed at combating SSN misuse and protecting privacy. The ramification of these proposals on businesses, governments, and consumers will also be examined.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should submit six (6) single-spaced copies of their statement, along with an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, with their name, address, and hearing date noted on a label, by the *close of business*, Thursday, May 25, 2000, to A.L. Singleton, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the Subcommittee on Social Security office, room B09316 Rayburn House Office Building, by close of business the day before the hearing.

FORMATTING REQUIREMENTS:

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

1. All statements and any accompanying exhibits for printing must be submitted on an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, typed in single space and may not exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

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

3. A witness appearing at a public hearing, or submitting a statement for the record of a public hearing, or submitting written comments in response to a published request for comments by the Committee, must include on his statement or submission a list of all clients, persons, or organizations on whose behalf the witness appears.

4. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers where the witness or the designated representative may be reached. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the

Members, the press, and the public during the course of a public hearing may be submitted in other forms.

Note: All Committee advisories and news releases are available on the World Wide Web at "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 20209225091721 or 20209226093411 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.

Chairman SHAW. Good morning. I apologize for being about ten minutes late starting this morning.

Welcome to the first day of our two-day hearing about a topic that is on many people's minds today. That is privacy and security of their personal information, starting with their Social Security number.

Just about everyone's privacy and financial security depend upon seeing these numbers used as originally intended, that is, to track our earnings so Social Security knows whether we qualify for benefits and what we should get.

Today, our interests go well beyond that. Social Security numbers have evolved into every corner of our lives from qualifying for other government benefits to collecting child support to obtaining instant credit. We value these expanded uses when we want to buy and drive home a car on the same day, on a Saturday afternoon. Yet many have started to wonder about the proliferating uses of Social Security numbers and the privacy and security implications of all of this.

Most telling are the rapidly rising allegations of fraud involving Social Security numbers. That is cause for great alarm. That is why we are holding these extended hearings. We need to carefully consider the causes and consequences of the expanded use and increasing misuse of Social Security numbers.

While we are committed to finding better ways to combat fraud, we need to carefully consider the consequences of any actions on this complicated issue.

With us today are two people who know too much about Social Security number fraud. John T. and Mary Elizabeth Stevens will tell us how their lives were turned upside down by someone who stole their Social Security numbers. They lost their credit rating, were refused loans, incurred large legal bills and spent three years fighting to get their good names back and their battle still isn't over.

Next, the General Accounting Office will provide an overview of the effect of limiting the use of these numbers for government and private businesses.

Then Social Security's Inspector General will provide specific recommendations for improving systems designed to protect the privacy and security of Social Security numbers.

Later this week, we will hear from privacy experts, consumer advocates and representatives of industries that use Social Security

numbers in the course of their business. We will also consider legislative recommendations of outside groups as well as members of Congress. Clearly, we won't suffer from the lack of ideas to better protect everyone who has a Social Security number.

To be sure, better protecting Social Security numbers is only one piece in the puzzle of combating identity theft. No one proposal will constitute a total solution. Since Social Security numbers often represent the entry point for ripoff artists and identity thieves, there is no better place that we should start. We will find that each proposal we consider comes with tradeoffs, often balancing privacy and security against commerce and efficiency.

Just because this is complicated and difficult doesn't mean we should not act. Indeed, we should. In the coming weeks, with the support of the Administration and our colleagues on this panel, we can approve legislation to better protect Social Security numbers from misuse. In my view, such legislation should increase fines and penalties for identity theft, give the Inspector General new powers to catch thieves and better protect the privacy and integrity of Social Security numbers.

As I mentioned, that will not solve all problems of identity theft, many of which stretch far beyond our subcommittee's reach. If we can take some common sense and bipartisan steps in the right direction, indeed we should.

I look forward to working with all of our witnesses and all of our members to do the right thing.

At this time, I yield to Mr. Matsui for any remarks he might want to make.

Mr. MATSUI. Thank you very much, Chairman Shaw.

I appreciate the fact you are holding these hearings. I think they are extremely important. Last year my staff advised me there were 19,000 reported cases of Social Security fraud and abuse and we suspect there were many more. With the increased use of the Internet, I suspect unless the Congress gets involved in this issue in a very substantive way, we will probably see more and more fraud and abuse. Certainly with both the Social Security number and a driver's license, a criminal can do almost anything he or she wants in terms of getting private information from our citizens.

I look forward to hearing from Colonel and Mrs. Stevens, the GAO and the Inspector General of the Social Security Administration.

I want to thank you, Chairman Shaw, for your leadership on this issue and certainly I look forward to working with you in a bipartisan fashion.

Thank you.

[The opening statement of Mr. Matsui follows:]

Opening Statement of Hon. Robert T. Matsui, a Representative in Congress from the State of California

I would like to thank the Chairman for holding this hearing. Our topic today is extremely important as it affects every American, young and old, whether or not they currently collect Social Security.

The Social Security number is almost as old as the program itself. Created in 1936 to keep track of workers' earning records, the uses of the Social Security number have extended far beyond its original intent, to the point where it is now commonly used as a personal identifier.

These days, it is quite common to give out one's Social Security number—for record keeping, on health forms, to obtain a drivers license or to sign up for a government program such as Medicaid.

Unfortunately, there is some risk associated with the expanded use of the Social Security number. Since the Social Security number can be linked with confidential information, there is the possibility that if it falls into the wrong hands, an individual's Social Security number and information could be mis-used as Lt. Col. John T. Stevens will testify to this morning.

Common areas for fraud and abuse of the Social Security number include counterfeiting Social Security cards for citizenship and fraudulently collecting government benefits. And it seems that the problem is growing worse. From FY 1998 to FY 1999, there was an increase of 19,200 allegations of fraudulent Social Security number use. That is a startling number.

Because of this potential, many people are concerned about their ability to protect their privacy. On Thursday we will be hearing from Members of Congress who will talk about their legislation to increase privacy protections and combat the mis-use of the Social Security number.

Today we will hear from Barbara Bovbjerg, Associate Director of the General Accounting Office, and James Huse, Inspector General of the Social Security Administration. Both of these witnesses will discuss their agencies' findings on the use and abuse of the Social Security number.

We will also hear from Lt. Colonel John Stevens and his wife Mary who had the unfortunate experience of discovering firsthand the horrors of having their lives turned upside down from identity theft.

I want to welcome all of our witnesses. I look forward to hearing your testimony and to working with my Republican colleagues to address this growing problem.

Thank you.

Chairman SHAW. Thank you.

Should any other member have an opening statement, we will make that a part of the record.

[This opening statement of Mr. Portman follows:]

Statement of Hon. Rob Portman, a Representative in Congress from the State of Ohio

Thank you, Mr. Chairman, for holding this hearing today on a critical issue.

As we're learning, one of the negative consequences of the digital economy is that what most of us consider to be private personal information is becoming neither private nor personal.

The Social Security Number is a perfect case in point. While there are some laws and regulations that require and restrict use of the Social Security Number within certain federal programs, these could be improved. I have real concerns about the lack of restrictions on the use and privacy protections on Social Security Numbers by state and local governments and the private sector.

Mr. Chairman, Americans are increasingly concerned that the benefits of the information age are coming at the expense of their personal privacy. I hope this hearing will help shed some additional light on this problem -and I hope that this Congress will consider taking appropriate action to protect the taxpayers of this country against unauthorized, unnecessary or fraudulent use of their Social Security Numbers.

At this time, I would like to recognize our first panel whom I mentioned in my opening statement, Lieutenant Colonel Stevens and Mrs. Stevens. You may proceed as you wish.

We have the text of your full statement and you may summarize as you see fit.

STATEMENT OF LIEUTENANT COLONEL (RETIRED) JOHN T. STEVENS, JR., UPPER MARLBORO, MARYLAND

Colonel STEVENS. I have summarized the full statement and this is what I will present today.

My wife and I are encouraged that this subcommittee is looking into the widespread use and misuse of the Social Security number. We have experienced this misuse for over three years now. We hope by testifying here today, we can alert others to the danger of this crime and the toll it takes on your life to fight it.

This horrible nightmare started in March 1997 with a phone call from Nations Bank, demanding payment on a 1997 Jeep Cherokee, which of course I don't have. We immediately requested our credit reports from the three major credit reporting agencies. The total damage was 33 fraud accounts with a value of $113,000.

We wrote letters to the credit reporting agencies listing the fraud accounts and requesting their removal. When this approach failed, we hired an attorney to write to them. This did not work either. I then used the Internet to locate the fraud accounts, identify a point of contact and have our attorney send them a sworn affidavit.

We cleared most of the fraud accounts and data in about a year. There were some creditors, however, who refused to accept our affidavits. The nightmare continues.

When some creditors delete an account, it is transferred to a third party collection agency. This returns the account to our credit report under their name and with the same account number. So far, we have had to deal with over 14 third party collection agencies. They are nasty people to deal with.

When we refused to pay even a reduced amount to close the account, it is transferred to another collection agency. My wife has had one account recycled six times to different collection agencies. I have had one recycled four times within the same collection agency. They are all from accounts that have been previously cleared.

We have received some copies of the applications that opened these accounts. Usually only a first and last name is listed. Sometimes a wrong middle initial is given, various spellings of the last name, different places of employment, birthdays, home addresses all are listed. Usually the only correct item is a Social Security number. The creditor approves these applications after the information is verified by the credit reporting agency. Although we have lived in Maryland for over 35 years, neither the creditor not the credit reporting agency, questioned a home address in Texas, the opening of numerous accounts in different States or any other significant changes to our personal data.

My wife currently has a default judgement against her in Texas. This is for furniture bought and delivered to an address there. It was repossessed from the same address when the loan defaulted. The furniture company obtained a default judgment against the name listed on the application. This is not my wife's name. The credit reporting agency then listed it in my wife's credit report.

Our attorney wrote to the furniture company to have the judgment vacated. The furniture company stated in a letter back to him, that they had used the items in the application to check our credit file with the Credit Bureau of North Texas. It was approved

even though the Social Security number was the only correct item in the application. The judge never responded.

The Social Security number is the primary and sometimes the only means of identification required to open an account. Any variation of a name, address and place of employment, age or spouse name is acceptable. When the account goes bad, the correct address is located and the harassment begins.

When you challenge a fraud account, a 30-day investigation is initiated. This investigation is usually a farce. The usual finding is that the information being recorded is correct. As long as there continues to be a lack of responsibility and accountability by the creditors and the credit reporting agencies and the Social Security number is considered a national personal identification number or PIN, we will have a problem of identity theft.

Our Social Security numbers are available on the network of DOD computers and through DEERS. We have to put our Social Security number, home address, telephone number and rank on a check to pay for purchases in the base exchange or the commissary on any military base. The Andrews Federal Credit Union uses a Social Security number for an account number. The last four digits in your Social Security number must be provided to have clothes cleaned or altered at Andrews Air Force Base. Civilian medical facilities, which we are now forced to use, demand our Social Security number and our driver's license number. Merchants ask for a Social Security number and a drivers' license number to write on your check or charge slip. Our greatest vulnerability to fraud, however, is on a military base where the Social Security number is openly used and not fully protected from unauthorized disclosure.

I believe that the creditors who accept fraudulent information from an imposter and the credit reporting agencies that ignore these obvious changes should be held equally responsible for the mental, physical and monetary damage caused by their negligence. They are just as guilty of fraud as the imposter who opens the account.

We do not want to spend the rest of our lives correcting the fraud accounts and false data that so easily becomes a part of our credit reports. We are prevented from buying a home, establishing a credit account, making purchases and leading a normal life. We are tired of the harassing phone calls and the threatening letters.

I am now 72 years old and my wife is three years younger than me. We have been married for over 45 years. We hope some day soon that we can get our lives back and begin to enjoy our retirement in the time we have left to be together in this world.

We do not consider ourselves victims. It doesn't fit. I prefer the designation targets. A target can take evasive action, Activate counter measures and fight back. Our warrior instinct drives us to keep going until we win this battle. We intend to fight this crime with every resource we can muster. We have been assisted by many people and we wish to express our thanks for their help and encouragement.

I would also like to thank this subcommittee for recognizing that there is a very severe identity theft problem in this country caused by the free access and widespread use of the Social Security number as a primary and sometimes the only means used to identify

a person. I hope that with your continued concern and support this national problem will be contained and solved. My wife and I thank all of you.

[The prepared statement follows:]

Statement of Lieutenant Colonel (Retired) John T. Stevens, Jr., and Mary Elizabeth H. Stevens, Upper Marlboro, Maryland

My wife and I are encouraged that this subcommittee is looking into the widespread use and misuse of the social security number. We have experienced its misuse now for over three years. We are sure that very few people realize the problems that this little 9-digit number can create. It has reached the point that names and other personal data don't matter anymore. This 9-digit number is the only correct identification you need to initiate major credit transactions and other purchases. We hope that by testifying here today, we can alert others of the danger of this crime and the toll it takes on your life to fight it.

Since March 1997 my wife and I have been going through hell. We have received harassing phone calls, been yelled at, insulted, humiliated and accused of not paying our bills and defaulting on loans. We have been denied credit and been forced to pay cash for major items that would normally be financed. Our Maryland home has been under surveillance and my 1990 Ford Bronco was almost towed by Nations Bank (now Bank of America) attempting to repossess a 1997 Jeep Cherokee.

I am a retired Air Force officer. While on active duty, a breach in fiscal responsibility or personal integrity would have ended my career. After an automobile accident forced me to retire in 1972, I was employed as a physicist at The Johns Hopkins University Applied Physics Laboratory. I was trusted by both government and industry to have the integrity, experience and knowledge to analyze, test and evaluate advanced and complex weapon systems. Any breech of fiscal or personal responsibility would have affected my security clearance and my employment. My wife and I had always paid our bills on time and never defaulted on any obligation. Since retiring from The Johns Hopkins University, we have been looking forward to moving to South Carolina to be with my 96-year-old mother and enjoy being closer to our grandchildren. All these plans ended very quickly when we discovered that our social security numbers and names had been used to open 33 fraud accounts with a total value of $113,000. Our credit had been destroyed.

We did not know this was happening until March 1997. I received a phone call from Nations Bank, demanding payment on a Jeep Cherokee purchased in Texas. This was our first realization that something was wrong. When we requested credit reports from the major credit-reporting agencies, we were shocked to learn the extent of the damage done to our credit and our lives. Our attempts to clear these accounts through the credit-reporting agencies failed. They would initiate a 30-day investigation and then tell us that the information being reported is correct. We hired an attorney to contact them. He was also ignored. I was forced to locate the address and phone numbers of these fraud accounts by using the Internet, as the credit reports did not provide this information at that time. After we verified the location of a fraud account by calling them and establishing a point of contact, our attorney would send them a sworn affidavit stating that we are not the persons who opened this account. It is ironic that we were being required to prove a negative. We have since learned to make the creditor prove their assumption that we opened an account with them by insisting that they send us a copy of the application, the delivery tickets, or charge receipts.

In less than a year we cleared the initial reports of the fraud data, and all of the fraud accounts we could identify and locate. When a fraud account is established, the new address, birthday, place of employment and other personal data, submitted in the application, all become a part of that credit record. We have had to continuously write or call the credit-reporting agencies to remove the same fraud data that keeps reappearing in our credit reports. This information should be used to identify or flag an application as being legitimate or false. For instance, the date of birth submitted on the applications that I have received indicated that the social security number was issued before the applicant was born. Although we have lived in Maryland for over 35 years, applications were readily approved for an address in Texas. The social security number was the only consistent item in the copies of the applications that we have received. It was the primary identification factor required by the creditors and the credit-reporting agencies.

Some of the creditors clear the fraud accounts at the credit-reporting agency and then assign them to a third party collection agency. The delinquent or charged off fraud accounts then reappears on our credit reports with a different name and the

process starts over. We have cleared our reports of all identifiable fraud data at least three times. These accounts seem to reappear on the credit report about every three to six months. Some collection agencies recycle the account within themselves or pass it over to another collection agency. This has occurred even after they have sent us a letter clearing the account or they have verbally cleared it through a telephone call. Dealing with credit-reporting agencies that keep reinserting fraud data and accounts in your report and collection agencies that keep recycling cleared fraud accounts is like the trick candle that keeps re-lighting itself every time you blow it out. To partially quote Forrest Gump, " Getting a credit report is like opening a box of chocolates, you never know what you are going to get."

Third party collection agencies are rude, nasty, and mean to deal with. We have dealt with more than 14 of them. We have dealt with one agency four times on the same account. One of the worst and meanest companies to deal with was Household Bank Credit Services. Their representative was demanding, nasty and rude to both my attorney and me. He refused to accept the sworn affidavit that we had previously sent to clear the account. He would only accept their forms. When we refused to resubmit in their format, the account was transferred to Gulf State Credit in Atlanta, Ga. So far Gulf States has recycled it four times since initially clearing it in July 1997. This account is for an Oreck vacuum cleaner bought over the phone and delivered to an address in Texas. It is still on my latest credit report. Norwest Bank in Lubbock, Texas closed a fraud account opened in their Wichita Falls branch after an affidavit was sent to them on May 29, 1997. The same account showed up again with Mountain States Adjustment in Golden, CO. Again the social security number was the primary means of identification used in opening these accounts and in locating and harassing us. It did not matter to them that we have never lived in Texas.

My wife has a cell phone charge that has been recycled through four different third party collection agencies. This account has had a resurfacing period of four to six months. It should reappear at any time now, as it has been dormant for six months. There is also a jewelry purchase of over $2000 that keeps showing up in her records. The initial purchase was made in Texas and has cycled through six different third party collection agencies. Even though it has been verbally cleared it just resurfaced again on April 10, 2000.

There is a new fraud account listed on my latest Trans Union report. It is charged off as a bad debt. The name is GECS CARE CR with an account number. There is no address or phone number. By using the account number listed I traced this account back to a fraud account with a company called Lew Magram Credit located in Tulsa, OK. They were sent a letter and affidavit in May 1997. The account was deleted from my credit report on July 7,1997. This account has now resurfaced through this third party collection agency and is now appearing on my credit report. Again my social security number was used to open the account and to reinstall it in my credit report. We have never lived in Oklahoma or opened any accounts there.

My wife currently has a default judgment against her in Texas. Greens Furniture Company opened an account using her social security number, her first and last name with a different middle initial. The application was not completely filled in. A desk was delivered to the address shown on the application in Wichita Falls, Texas. It was later picked up from the same address when the loan defaulted. A default judgment was issued when no one showed up in court. This judgment is now on my wife's credit report listing our address in Maryland. Our attorney called the store and the Judge to get the judgment vacated. Neither the Judge nor the furniture company has bothered to correct their error or notify us of any action taken. The furniture company stated, in a letter, that they had no reason to doubt the person's identity, as the social security number and other information was checked by the Credit Bureau of North Texas.

It is frustrating to know that a social security number is the primary identification required in opening an account. Any variation of a name, address, place of employment, age, or spouse name will be accepted without a challenge. When the account goes sour, the address and owner of the social security number is suddenly discovered and that person is now held responsible for the debt. When a fraud account is opened through the negligence and lack of attention of the creditor and the credit-reporting agency, there is little concern shown about correcting the damage done to the person whose name and the social security number was used. Their 30-day investigation is a farce, as it usually shows that the information provided (by the creditor) is correct. Even when the account is cleared, it may be assigned to a third party collection agency. Only one person in all of the 33-fraud accounts bothered to apologize to us. She was a loan officer at Nations Bank in Wichita Falls, Texas. She stated that she met and talked with John and Mary Stevens when they applied for a loan. When she described the couple as being in their late 30's, I point-

ed out to her that this meant my social security number had been issued before they were born. As long as there continues to be a lack of responsibility and accountability by creditors and credit-reporting agencies and the social security number is considered as a National Personal Identification Number (PIN), we will be faced with this problem of identity theft. Who would provide his or her ATM PIN to anyone requesting it?

When asked if I had filed a police report, I answered no. Identity theft was not a crime in the state of Maryland and in many other states when this started in 1997. Also, the creditors are considered the victims of fraud, not the person whose identity was stolen. Some states, including Maryland, have now passed laws making identity theft a crime. Since the Maryland bill amended so many other statutes, I have never seen a clean copy of the law so I am really not sure what it covers. Maryland just passed another law, to be signed this month, that limits the use of the social security number on identification cards or putting it on a driver's license. South Carolina is considering a bill that is one of the toughest in the nation. It includes the unauthorized sharing of personal information for business or promotional purposes without their written approval. Prince George's County in Maryland just recently passed a law making it a misdemeanor to assume someone's identity. The federal law, recently passed, may provide some help if it is properly funded. Since we had spent over $6000 in attorney fees plus other expenses such as long distance telephone calls, I requested help from my USAA homeowner's insurance policy under their credit card theft coverage. Their reply was " There has been no direct physical loss to personal property; and, no apparent actual credit card forgery on accounts established by you, or issued to you. Having your credit record questioned is not a loss that would be covered in our policy contract, even under the Additional Coverage provision of your policy." They weasel-worded themselves out of that one. Having your identity stolen is not an insurance covered crime.

My wife first had to use her own social security number on her Air Force dependents ID card in 1996. Social security numbers are available on the network of DOD computers and through DEERS. In addition, your social security number, home address, telephone number and rank must be placed on your check to make purchases in a Commissary or Base Exchange on any military base. The Andrews Federal Credit Union uses it as an account number. Even to have clothes altered or cleaned on a base requires the last four digits of your social security number. Civilian medical facilities, which we are now forced to use, want both your social security number and your driver's license number. Our Medicare number is the social security number with a letter suffix. Merchants ask for a social security number and driver's license number to write on your check or charge card slip. My wife and I have resisted giving them this information. We would state that they might look at any identification we have, but they do not have our permission to write down any numbers. If they insisted, we walk away and leave our intended purchases at the checkout counter. Our greatest vulnerability to fraud is on a military base where a social security number is openly used and not fully protected from unauthorized disclosure.

Treating a social security number with the same respect and handling as a classified document would alleviate some of the problems now being experienced. To receive a classified document, the recipient must have the proper clearance and a valid need-to-know for that information. It must be properly stored, protected and accounted for. Any loss or improper use is subject to severe penalties.

The creditors who accept the fraudulent information from an imposter and the credit-reporting agencies who do not recognize or warn of the obvious changes in names, addresses, age, and other personal data that might indicate fraud should be held equally responsible for the mental, physical and monetary damages caused by their negligence. They are just as guilty of fraud as the imposter who opens the account. A representative of a credit-reporting agency told me that all the information they collect on a person is their property to distribute and sell to their clients. If they accept and distribute false and damaging data about a person, it seems that the damaged person should be allowed to sue them for liable, defamation of character and mental stress as well as recover the expenses incurred in repairing the damage they caused. After all, they said they own the data.

We do not want to spend the rest of our lives correcting the false data and fraud accounts that are accepted into our credit reports. We are prevented from establishing credit accounts, making required purchases and leading a normal life. We are tired of the harassing phone calls and the threatening letters. I am now 72 years old and my wife is 3 years younger. We have been married for over 45 years. We hope someday soon that we can get our lives back and begin to enjoy our retirement and the time we have left to be together in this world.

I have cited just a few of the many problems and some of the numerous frustrations that we have encountered in trying to restore our lives from the wreckage that this crime causes. We do not consider ourselves victims. It doesn't fit. I prefer the designation "TARGETS." A target can take evasive action, activate countermeasures and fight back. Our warrior instinct drives us to keep going until we win this battle. We intend to fight this crime with every resource we can muster. We could not have made it this far without the help, advice and encouragement of people like Beth Givens, Ed Mierswinsky, Mari Frank and Cynthia Lamb. Without them we might still be fighting 33-(or more) fraud accounts, waiting on the credit-reporting agencies to complete their 30-day investigation, stating that the information being reported is correct, and being insulted and harassed by third party collection agencies. We want to thank them for helping us through some very rough times. They gave us the encouragement, the knowledge and the courage to keep fighting and in knocking down those stonewalls that keep getting in our way. I would also like to thank this subcommittee for recognizing that there is a very severe identity theft problem in this country, caused by the free access and wide spread use of the social security number as the primary and sometimes the only means to identify a person. I hope, that with your continued concern and support, this national problem will be contained and solved. My wife and I thank all of you.

Chairman SHAW. Mrs. Stevens, do you have a statement?

STATEMENT OF MARY ELIZABETH H. STEVENS, UPPER MARLBORO, MARYLAND

Mrs. STEVENS. I just wanted to say that we really do appreciate being able to share our what I would call "Stevens Soap Opera" at this point. It is not a very pleasant one.

We would like to see that others, as many as we can prevent, from going through this kind of nightmare by working together and with your help. We do appreciate you going into this problem.—I think we can ace it.

It has really been an interesting experience and one we could have done without.

May I leave you with a quick quotation. There is the saying, "A diamond is not polished without friction, nor man without adversity." My husband seems to think, and I do, too that we have had enough polishing, but I guess it is going to go on for a while longer until we can solve it.

Thank you so much, all of you, for your help.

Chairman SHAW. Thank you, both.

Mr. Johnson?

Mr. JOHNSON. Thank you, Mr. Chairman.

It is a pleasure to have you all with us.

Do you feel there is any connection between the military and your problems, the Social Security number in particular?

Colonel STEVENS. All I know is when my wife first had to put her Social Security on her own dependent's ID card, the fraud seemed to increase, it seemed to start at that point. We have no proof that was what did it or if it was just a coincidence.

Also, our Social Security numbers are listed in all the DOD computers which you can access at any base, anywhere they are located. We also used to come under the medical facility, DEERS, until they kicked us out. Our numbers were available there too.

Mr. JOHNSON. But those numbers are the military identification number as well. What do you want them to do?

You were probably in the service at the same time I was, I remember when we had different numbers. They went to the Social Security number because it was easier to collate. It is listed on your ID card just as a number; it doesn't say it is a Social Security number.

Colonel STEVENS. It is so easily identifiable, it is only a nine digit number. It is on everything we have to do. You cannot even get clothes drycleaned without leaving your last four. Whenever you make a purchase and use a check, you have to put all that information on it.

They may protect it themselves, say in the base exchange system, but it has to go through a lot of people before it gets back to you as a canceled check. Anyone along the way can pick off this information and use it, as we suspect probably happened.

Mr. JOHNSON. My experience has been that you don't have to put that number on a check.

Colonel STEVENS. No, sir. We just gave something an article that was in the Air Force Times that says it must be on your check and that there is a law that requires that.

Mr. JOHNSON. Wait a minute. I don't think there is any law that requires that.

Colonel STEVENS. On a military base, to use any of their facilities like a base exchange or a commissary, you have to put your Social Security number, home address, phone number, rank and all the other information on your check before they will cash it.

Mr. JOHNSON. It is called a military ID number too. I understand what you are saying but I don't think there is any Federal law that requires that.

Colonel STEVENS. This article is in the Air Force Times.

Mr. JOHNSON. It is probably a military regulation and they have done that to protect themselves at those stores.

Can you tell me if you believe there is any other reason other than Social Security number that your credit people got involved the way they did?

Colonel STEVENS. If you look at some of the applications, sir, you will see that the only correct item on many of them was the Social Security number. Different addresses, different spellings of our first and last names, different places of employment. In other words, it was so obvious it was not us that we wondered why it got through the credit reporting agency. The Social Security number has been the consistent piece of identification that has been used to identify us in all the fraud accounts.

Mr. JOHNSON. When you asked the credit companies for your credit rating and listing, they are supposed to give you that information. Do they do that?

Colonel STEVENS. Oh, yes, they will give it to you. In fact, in Maryland, thank goodness you can get them free but in other States they charge you. If you have been denied credit or have a problem, you can request them and they will send you one free.

Mr. JOHNSON. They are supposed to give you one free in any State. They do in Texas because I have done it.

Colonel STEVENS. That was not my understanding, sir, but it is only Maryland and several other States they don't charge you five or seven dollars for them.

Mr. JOHNSON. When you pursue it, do they then clear your records because my experience has been that they clear your records and your testimony indicates they did not?

Colonel STEVENS. Absolutely not. We would submit letters. I wrote stacks of letters to them listing all the fraud accounts. Some of them would be cleared but the majority of them would not. They had to go through a 30-day investigation period which I believe all they do is go back to the person who opened the account in the first place, the creditor, and say is this information correct. Of course it comes back that it is. We would get a reply that the information is correct as listed. I finally gave up on that approach.

Mr. JOHNSON. Let me ask you one more if I may. Do you feel we should investigate the military process of requiring Social Security numbers on all their documents?

Colonel STEVENS. I don't know whether investigate is the correct term but due to the fact that it is required everywhere and everyone wants it, is what makes us very vulnerable. The fact that the Social Security number can be used in other civilian aspects such as opening accounts rather than identifying you as a legitimate military person.

Mr. JOHNSON. Thank you so much.

Colonel STEVENS. I had a five-digit serial number before as a regular office and that was much more convenient.

Mr. JOHNSON. Yes, I did too.

Thank you for your testimony.

Chairman SHAW. When they say they want your name, rank and serial number, that means name, rank and Social Security number?

Colonel STEVENS. Yes. I guess that is what the enemy asks you for now.

Chairman SHAW. Mr. Matsui?

Mr. MATSUI. Thank you for your testimony, Colonel and Mrs. Stevens.

Do you know whether there as more than one person involved in this $113,000 consumer fraud?

Colonel STEVENS. It is fairly widespread, it could be more than one person. It seems to be consistently located around Sheppard Air Force Base at Wichita Falls, Texas. We really don't have any proof other than just looking at the applications that come back to us and the various information that shows up on our credit reports.

Mr. MATSUI. It is somewhat frightening, what you have testified because apparently this person purchased a 1997 Jeep Cherokee, right?

Colonel STEVENS. Yes, sir.

Mr. MATSUI. Do you know if whoever that person was had any other credit information on you or they used the Social Security number to get other information and then basically identified themselves as you?

Colonel STEVENS. The other information would generally be that was available through the fact that I am retired military but I have no proof of that.

Mr. MATSUI. Have they apprehended this individual?

Colonel STEVENS. The applications are there. If the people who granted them the credit wanted to, they could go after the people listed in the application but they don't do that, they come after us.

Mr. MATSUI. Obviously you have been to the law enforcement agencies and I am assuming they have opened a file. Have they at least identified the individual who has been using your good name?

Colonel STEVENS. Let me give you an example, sir. An account that was opened at Nations Bank in Wichita Falls. We got a call from the person who opened the account, the loan officer, and she said she had talked to John and Mary Stevens. They had come in and she had met them personally while they were opening an account. She called to apologize to us for the problems.

I asked her what was the age of these people. She said they were in their mid-to late-30s. Then I pointed out to her, it was so obvious but it wasn't obvious to her, I understand that, but what it amounted to is that my Social Security number was issued before they were born. A simple check like that would have eliminated quite a lot of problems.

Mr. MATSUI. To your knowledge—and I would not expect you to have this information but I would imagine you have done some research on this or maybe not, and there would not be any reason for you to have done any research on it—you don't know how this person actually made the transaction and what information the individual using your name used in order to drive out with a $30,000 automobile?

Colonel STEVENS. We don't know where they got it, if I am hearing you correctly, sir. All we know is they had the first and last name, Social Security number and in the same case as my wife, they just generally used her first and last name, plus her Social Security number.

Mr. MATSUI. You have no knowledge at this time about whether the individual that has used your name has been apprehended?

Colonel STEVENS. I don't know that they have been apprehended, however, they could have been. It seemed to me that the person who opened the account has enough information to go and get them. We are not considered the person experiencing the loss.

Mr. MATSUI. The bank is, I guess?

Colonel STEVENS. The banks are the ones who have the loss and they are the ones that really can bring the charges. Up until recently, there was no law against this, especially since we live in Maryland and they were in Texas.

Mr. MATSUI. If I can ask you this question, have finally the credit collection agencies stopped and has your record been cleared?

Colonel STEVENS. No.

Mr. MATSUI. Not at all?

Colonel STEVENS. I just got a recent report where they recycled another account for the fourth time, even though I have a letter clearing me of that account from that same third party collection agency. This was on an account that had been previously cleared back in 1997 with an affidavit. They just keep recycling these things.

My wife has one on a $2,000 diamond that she can tell you about.

Mrs. STEVENS. As of April 10th, this account seems to come around every four to six months. I explain to them that I am not the individual. Well, give us your last four and we will determine if you are the right individual. I will say, by what authority or what law are you asking for this information. All through the past up, to the time the Federal law that has now been passed I would get no help. They would say, All right, we will delete it.

Before they would agree to delete it, they would let it rest for a little while and in about two or three weeks or a month I would get a letter stating that, if you will pay this amount, maybe $800 or something, we will clear this for you. Of course I wouldn't pay them a dime. So, we would start around again. They give it back to the credit bureaus. It is deleted and later on it comes around again.

I have, in my briefcase, three sets right now and there are more. I travel with about ten boxes in my little station wagon up and down the coastline visiting grandchildren. I am always prepared to explain this issue.

It is really devastating because there seems to be no end to the recycling by the third parties. There now seems to be a new approach. In the past month, my husband has had two phone calls come in. The phone will ring and they leave an 800 number that we are to call back on a business call—My husband can explain more about this.

Colonel STEVENS. You call back on an 800 number and then they tell you about this account you owe money on and you can make arrangements to pay it. So it just continues. It is a neverending story. It is like when you blow out this trick candle and it keeps relighting itself.

Mr. MATSUI. Thank you for sharing your very sad story with us. We appreciate it very much.

Chairman SHAW. Mr. Portman?

Mr. PORTMAN. Colonel and Mrs. Stevens, thank you for being willing to stand up for the rights of others. As Mrs. Stevens said, you are here in part to tell us your story but what you are doing is helping others avoid what you went through.

When I looked at your testimony and hear what you had to say today, you spent the last three years living in a horror story.

Mrs. STEVENS. Absolutely.

Mr. PORTMAN. I am sorry for that. I wish that we had the power to wave a magic wand and make your problems go away and be able to keep others from having to go through that because I know how frustrating it is. I have not been through what you have but all of us have been through some of these issues with credit card companies and collection agencies and so on with misinformation and it is so frustrating to get through the bureaucracy.

I am concerned because my wife was born in Wichita Falls, Texas at an Air Force base and maybe I will get linked to that same source of your problem. Is it Sheppard Air Force Base?

Colonel STEVENS. Sheppard Air Force Base. It seems to center around that area.

Mr. PORTMAN. You talked about what creditor reporting agencies could do better and what creditors could do better. I cannot believe the spelling of your names wasn't even correct, and yet, based on

the Social Security number, they went ahead and processed things and did not even look at the application. That clearly is a major problem.

I do not know enough about the rules and regulations. I know this committee does not have jurisdiction over all that but it seems to me that is one area where we could do more. Do you agree? Shouldn't the reporting agencies, at the least, be responsible for looking at the application and have some liability if they go ahead and process something where the names are not spelled right?

Colonel STEVENS. Absolutely. The things are so obvious that it is a wonder they don't do it. One of the things I have run into is that one of the representatives of the credit reporting agency said they could not be concerned with changes of address because at least 15 percent of the people move every year and they would be inconvenienced when they applied for credit.

My answer to that was that means 85 percent of the people do not move, therefore why are you subjecting them to all this harassment based on trying not to inconvenience the 15 percent.

Mr. PORTMAN. What did they say with regard to not looking at the spelling of the name?

Colonel STEVENS. They really had no answer. That is one of the things we have to continuously do when we get our credit reports. We have to correct the misinformation that keeps recycling into it—the wrong address, the wrong employment, the wrong spelling of the name.

What infuriates my wife is when they use only her first name because that is now her fraud name. She likes to go by both of her names. The reports will come in and list my wife's name as Mary. Of course I have to sit there and listen to the explosion.

Mrs. STEVENS. Quickly, on this line of thought. I was just remembering, how much I had to use the Social Security number, during the first time frame my husband did the letter writing and I stayed on the phone with the credit bureaus for about three months every day giving my Social Security number to total strangers. In that process, I found I could cross reference numbers and identify the accounts.

They would then send us a new report. They even co-mingled our Social Security number at one point. In other words, they had part of my number and part of his number. Then another report came in from one of the bureaus with totally brand new number—000, 000, 000, a string of zeros and then a one. I could not figure that one out and the credit bureaus had no answer, it was just a mistake.

The one that really got to me was, I read a report and at the very end, it said, according to this Social Security number this individual has been deceased for 22 years. They are addressing this letter to me.

Mr. PORTMAN. That makes you feel kind of bad, doesn't it?

Mrs. STEVENS. My husband said he knew something was wrong.

Mr. PORTMAN. We do have jurisdiction over the Social Security Administration and that is something this subcommittee takes very seriously. We do a lot of oversight.

Have you contacted SSA and have they been helpful to you? Have you sought a new Social Security number, for instance, and

have they responded to that? What could the Social Security Administration do to help in these kind of problems?

Colonel STEVENS. We have not contacted them. Getting a new Social Security number, I don't think would be a good idea since it is my retired Air Force service number.

Mr. PORTMAN. It could lead to other problems.

Colonel STEVENS. It would really complicate things to change that because the VA would have to come into it and everything else since I am a disabled veteran.

The only thing I haven't run into is they don't seem to be using my Social Security number for employment because I have received no information that additional contributions have been made.

Mr. PORTMAN. That is where you want it to be used.

Colonel STEVENS. That would help offset some of the expenses we have gone through.

Mr. PORTMAN. Thank you.

Chairman SHAW. Mr. Weller?

Mr. WELLER. Thank you, Mr. Chairman. This is a very interesting hearing.

I very much want to thank Colonel and Mrs. Stevens for stepping forward and being a part of this. Reading your testimony and listening today, it is frightening what can happen to individuals.

In Congress we have some issues before us that are concerned with personal security and here is a case where your personal security was violated. I remember when I was in college we often joked that the only number we needed to remember was our Social Security number. People used to put it on the back of their T-shirts and jerseys as a joke because that was a number that identified us everywhere we went. Here is a case where someone took yours.

Also, with the advent of technology, particularly information technology and the Internet, we were looking at how we can protect the privacy of individuals. In this case, your privacy was violated as well as your personal security when someone absconded with your Social Security number.

When you discovered that someone was using your Social Security number, did you contact law enforcement?

Colonel STEVENS. No, sir, because at that time, it wasn't against the law. Again, we are not considered the victims so to speak, it is the credit card company or the bank, so making a police report would have been useless. We didn't try.

Mr. WELLER. So you did not even contact law enforcement in any way?

Colonel STEVENS. No because as I said, we are not considered the ones experiencing a loss—in other words, there was no law against it.

Mrs. STEVENS. The attorney was not even aware there was no Federal law. We weren't aware either. This began March 27, 1997. Until up recently, with the new law we weren't covered.

Mr. WELLER. Over what period of time did it take when you discovered someone was using your Social Security number before everything was cleared up and cleaned up, the mess that was created as it impacted you personally?

Colonel STEVENS. This candle keeps relighting itself. We actually cleared our records within a year. Then they started the recycling

of the third party collection agencies. The fraud data kept recycling and we would fight to clear that. Then it would lie dormant for maybe three to six months and then show up again. As I said, we have some that have been recycled six times. In my case, one collection agency has recycled the same account within their own organization four times for an account that was cleared.

Mr. WELLER. What do you feel was the biggest obstacle you faced as an individual when you tried to resolve this issue?

Colonel STEVENS. Getting people to believe that you are not the one that opened the account. We have been yelled and screamed at, cursed at, everything else, especially by collection agencies. There was one that was very, very nasty to us. They don't believe you. You have to prove a negative, you have to prove I am not the person that opened that account. We finally wised up on that one. We go after the creditor and say prove to us that we are the ones that opened the account, send us a copy of the application, send us a delivery slip, send us a charge card slip. A lot of them are reluctant to do that but that is the approach we have now taken.

Mr. WELLER. When you were looking for help in solving this, what was your best source of assistance? Who did you turn to that actually was helpful in solving your problem?

Colonel STEVENS. There were several people—Beth Givens, Privacy Rights; Ed Mierswinsky, USPIRG.

Mrs. STEVENS. One of our children found the address of the Privacy Rights Clearinghouse, Beth Givens, Director. I contacted her, I guess, over a year ago and that is how we became involved with this and then through her U.S. PIRG and Maryland PIRG. I was not aware of Mary PIRG at the time. Through them we met Mari Frank and obtained her material that we were using. She had suffered the same kind of crime as an attorney.

Colonel STEVENS. In the Federal Trade Commission, there was Cynthia Lamb who was most helpful.

Mr. WELLER. They can all serve as resources as we look for ways to help prevent this from happening.

If there was one suggestion you could make as individuals having suffered the consequences of identity theft through someone else using your Social Security number, what suggestion would you have for the Congress and how we could prevent this from happening to someone else?

Colonel STEVENS. The fact that the Social Security number is used as the primary means of identification that importance should somehow be diluted. People should not give out this information. The problem stems from the fact that everyone accepts this one nine-digit number as you, no matter who is bearing it or who is handing it out, that number is you. Nothing else matters. So, if you could degrade the importance of that number being used for identification it would help.

My original Social Security card had on the front of it "Not to be used for identification." They don't put that on there anymore, but if you could reduce the importance of it and have some other means of identification, that would help.

Chairman SHAW. Colonel Stevens, I want to go back to some of the questioning for a moment and then I will recognize Mr. Tanner—the colloquy you had back and forth with Mr. Johnson regard-

ing the commissary and how they require that, and your thought this was some type of Federal regulation.

As I understand, most if not all of these commissaries are private-owned or privately-run under contract with the Government. If I go into Safeway or Winn-Dixie back home and in the checkout line I want to give them a check, they don't require my Social Security number, so why should a commissary, which actually has a more select clientele than any store on the outside has in which you probably had to show an ID to get in the door, why should they require your Social Security number for you to give them a check?

I think we had better look into what the contracts are with these commissaries because to me, I would doubt that is a military regulation. I am pretty sure it is not statutory. In any event, it is something the Congress should look into.

Mrs. Stevens, you have a comment on that?

Mrs. STEVENS. Just last night, I discovered in the Air Force Times of May 15, 2000, "Is Social Security number still a must when you write a check?" I made a batch of copies of this last night because I was looking for some copies I have of December 17, 1999, Capital Flyer newspaper from Andrews Air Force Base. I happened to pick up a copy that particular afternoon—it comes out on Friday—and the story was there, that a military fraud ring had been discovered in Trenton, New Jersey. I did not get that copy together but I can secure that documentation for you. My husband can explain that better than I can.

Colonel STEVENS. When the major promotion list was approved by Congress, it listed all the ones that were promoted with their Social Security number in the Congressional Record. A ring around McGuire Air Force Base used that to open fraud accounts.

Chairman SHAW. Interestingly enough, I think many members of Congress don't realize on our congressional ID card is our Social Security number just as it is on your identification card.

Colonel STEVENS. It is a national PIN.

Chairman SHAW. I have a copy of the article you referred to and while Mr. Tanner is inquiring, I will read through it.

[The information follows:]

Social Security number still a must when you write check

By Karen Jowers
TIMES STAFF WRITER

Every time Lee and Walter Carroll pay for groceries at the commissary, they begrudgingly write Walter's Social Security number on the checks.

"This is kind of scary. We could lose everything if someone stole his Social Security number," said Lee Carroll, wife of the retired Navy gunner's mate technician. It's the only thing she dislikes about the commissary.

The Carrolls shop at the Fort Jackson, S.C., commissary. They've complained to store managers about having to write the Social Security number on checks, she said, and have written to the Defense Commissary Agency — to no avail.

"Complaints from shoppers about having to include SSNs on checks are very few," said Flo Dunn, spokeswoman for the commissary agency.

Still, most experts, including those at the Federal Trade Commission, advise consumers to protect their Social Security numbers.

"Give your SSN only when absolutely necessary," according to an FTC report on identity theft. "Ask to use other types of identifiers when possible."

Thieves who find out a Social Security number and can connect it with someone's name can get new credit cards, buy cars and make other financial transactions in the victim's name. When payments are not made, the delinquency is reported on the consumer's credit report.

In an age where identity theft is becoming more prevalent, privacy is becoming more of a concern to all Americans, including those in the military.

Army and Air Force Exchange Service officials are looking at alternative methods of identifying people that would eliminate the need for Social Security numbers on checks, said AAFES spokesman Fred Bluhm.

"However, until we are able to work through the various cost and administrative issues associated with implementation, we must continue to require the SSN when checks are presented for cash or purchase of merchandise," he said.

Both AAFES and the Navy Exchange Service Command also plan to increase security in credit-card transactions by not showing the complete credit-card number on customers' receipts.

Many customers, "including those who patronize AAFES exchanges," think that printing the entire number "is an open invitation to credit card fraud," Bluhm said.

AAFES hopes to implement the system, which will involve changes in checkout software, in all stores this summer. Navy Exchanges will begin the year-long process at the end of this year.

A widespread practice

The use of Social Security numbers for identification is far more widespread in the military than in the civilian world, where it's actually decreasing.

But the use of Social Security numbers is the standard procedure for government tracking, said Heather Jones, a spokeswoman for the Navy Exchange Service Command. "If someone bounces a check to the Navy Exchange, he is bouncing a check to the U.S. government. Through the Social Security number, we can initiate garnishment procedures, if necessary."

"Because checks are only in AAFES channels and the Federal Reserve and banking system, and based on our experience, we do not feel there is a significant threat posed by the use of the SSN on checks," Bluhm said. "The experience of our customers indicates this is not a problem."

Store officials said their Social Security number requirement is founded in law.

"The data disclosed, including the SSN, is used to identify the individual being served and to aid in the collection of unpaid checks returned to the commissary," commissary spokeswoman Dunn said.

People don't have to provide their Social Security numbers, but if they don't, they can't write a check, she said. They can still shop; they will just have to use cash, traveler's checks, or debit or credit cards, she added.

The Carrolls say they feel so strongly about their privacy, that they may start taking cash to the commissary instead of checks.

"You think you can trust people, but you never know. People are human," said Lee Carroll. □

Mr. TANNER. I too am impressed by your statement and the severity of what can happen to innocent people who have their identity stolen in the way that has happened to you. Is it still ongoing?

Mrs. STEVENS. Yes.

Mr. TANNER. With the use of your number, are there new charges being placed?

Colonel STEVENS. We have not seen any new accounts. However, our latest credit report listed, one in my wife and one for me in each of our credit reports, an inquiry that was made, one to buy a car, and the other was for I don't know what, but it was to establish credit Someone had applied and was getting information, obviously, to open an account.

We immediately wrote letters to both of these organizations and told them that we had not made any application whatsoever. That is why I say it is probably still more attempts to continue opening these accounts but the primary thing we are concerned with now is the recycling of the ones we have closed and cleared.

Mr. TANNER. Which brings me to the question I really want to know. I was reading through your statement and your attorney has notified these people that you are not the ones who opened those accounts. Has he advised you that it seems to me after one is notified that this account is a fraud, it is not yours, you don't owe it, properly notified, if they continue to recycle it looks to me like there might be a legal remedy called defamation of character lawsuit or something against these credit card companies that refuse to accept and acknowledge the fact that it is not your account but yet keep recycling it. I think you described it as a candle that keeps reigniting itself. Could you enlighten me on where you are there? I don't know that is a possibility but your attorney I am sure would.

Colonel STEVENS. We have not explored that possibility. Our main focus was to just get our lives back and get rid of these things.

Mr. TANNER. I don't mean to suggest but I just say that once I know something is false and I continue to publish it, then it seems to me I have some responsibility there. You spent, I think you said in your statement, over $6,000 just on telephone calls and letters. Somebody owes you for that if they continue, it seems to me, to publish untrue, and they know it is untrue, allegations with respect to your credit and your payment performance. I hope you will explore that with your attorney because oftentimes market forces have a much more, may I say, dramatic effect in commerce than anything we might do here immediately. So I hope you will explore that, particularly when they know and continue to republish what they know to be false information is not, in my judgment, something the law will tolerate, civil law.

Colonel STEVENS. I agree, sir. We would like to pursue that. As I said, our main focus has been not to recoup as much as to clear.

Mr. TANNER. But if it is ongoing, how does one ever. You want relief.

Colonel STEVENS. It has kept us from moving. When I retired, I intended to move back to South Carolina because my 96-year-old mother is there as well as a lot of our grandchildren. We couldn't qualify for a loan to buy house. We would get the higher interest rates, being a high risk because we have all these things on our credit record. This has delayed us in moving. That is why our main focus so far as been to clear it the point where we could really retire and start to do some of the things we have been putting off for so many years.

Mrs. STEVENS. I think your idea of going this route of getting help is great. The situation has been that not too many lawyers know how to fight this crime. As we are learning more about it, the legal profession, I think is coming forward.

In reading the material from Mari Frank, an attorney that was a victim, she suggested that an individual keep perfect documentation so if it comes to a point, that one can go into the legal aspect of trying to correct all this, we would have something to go on. I think that is possibly the avenue we will have to go which will be burdensome.

Mr. TANNER. Of course libel and slander laws have been around for a long time and this seems to me to be something that would

be libelous to publish known false information about one's credit. I hope you will pursue that. I would like to know.

Thank you for being here. This has been enlightening.

Chairman SHAW. I have looked at this article and we are running it down, particularly the paragraph that says, "Store officials said their Social Security number requirement is founded in law." I think that is a misstatement and prior to the end of this hearing today, we will have the answer to that. If it is in law, Mr. Johnson and I intend to try to take it out of law. In any event, there has to be some clarification. I can't conceive of that particular requirement. We will have the answer and take the corrective action if corrective action is necessary.

Mr. McCrery?

Mr. MCCRERY. I don't have any further questions but I appreciate the Stevens coming forward today and sharing with us your story which really brings to light some of the problems that undoubtedly many across our Nation are having because of the widespread use these days of the Social Security number.

Thank you very much.

Chairman SHAW. Mr. Collins?

Mr. COLLINS. I don't know about South Carolina but in Georgia, and Mr. Portman and I were discussing Ohio, it is an option in each of our States as to whether or not you use your Social Security number for your driver's license number because when we go into a store in Georgia, the driver's license is what they ask for to verify the photo and that you are who you say you are, and they write down the driver's license number. Some States do have that option but according to this article, South Carolina does not. I encourage you to move to Georgia, it is not far from Columbia.

Mrs. STEVENS. We have grandchildren there, a great State.

Mr. COLLINS. Move to Augusta and play the Augusta National and commute up there to Columbia to see your mother.

Thank you very much for being here.

Chairman SHAW. I am looking at my Social Security card which was issued many years ago. In fact, I still have the original. I was just advised I should not be carrying it. I am looking at one of our younger staffer's card and his does not say anything about identification. My says, "For Social Security purposes, not for identification." Why that was taken off the card, I don't have any idea but I think we ought to look into that too because I think that should probably be reinstated on the card itself.

I, too, want to thank you for being here and being a part of this hearing. It is quite important to us that you would share your really bizarre tragedy with us. We certainly hope you can work out of it.

I see that C-Span is carrying this hearing so you might want to get a copy of it so that the next time you have a creditor who gives you problems, you can send them a tape of your appearance here before the subcommittee. You have done a real service and I can tell you that it concerns me greatly that name, rank and serial number has now been changed to name, rank and Social Security number. That is not a good thing and we need to take a close look at that. The fact that you have to constantly give your Social Secu-

rity number as your employment identification is a real problem and I can certainly recognize that. We will look further into that.

Thank you both.

Chairman SHAW. The next witness we have from the United States General Accounting Office is Barbara Bovbjerg, Associate Director, Education, Workforce and Income Security Issues, Health, Education and Human Services Division. Welcome back to this subcommittee and we look forward to your testimony. We have placed your full testimony in the record and you may summarize as you see fit.

STATEMENT OF BARBARA D. BOVBJERG, ASSOCIATE DIRECTOR, EDUCATION, WORKFORCE AND INCOME SECURITY ISSUES, HEALTH, EDUCATION, AND HUMAN SERVICES DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Ms. BOVBJERG. Mr. Chairman, members of the subcommittee, I am pleased to be here today to discuss the uses of the Social Security number.

Almost 277 million Americans have been assigned an SSN and because each is unique to the individual, the SSN is frequently used for a variety of purposes. Privacy concerns, coupled with mounting instances of identity theft, have raised public sensitivity to this issue.

I would like to focus my remarks on three aspects of this topic: Federal laws directing SSN use, the purposes for which the SSN is used and, finally, the possible impact of restricting its use. My testimony is based on a report we prepared for this subcommittee in 1998.

First, laws directing use. No single Federal law regulates the overall use of the SSN, but several require its use to help enforce the law, determine benefit eligibility, or both. For example, the Internal Revenue Code requires that the SSN serve as the taxpayer identification number. This means that the taxpayers must report their SSNs when they pay taxes and their SSNs must also be known to their employers and financial institutions from whom they receive income.

Federal law also requires individuals to provide their SSN when they apply for a means tested benefit such as Medicaid or food stamps. The numbers are used not only for recordkeeping but also to verify income that individuals report. States are also required to use SSNs in their child support enforcement programs and on a variety of documents such as marriage licenses and death certificates.

Federal law generally does not restrict SSN use except in a few instances. The Privacy Act of 1974 restricts Federal agencies in collecting and disclosing personal information including SSNs without the individual's consent. The Driver's Protection Policy Act, a more recent law, restricts State governments from disseminating the SSN with driver's license databases.

I would like to turn now to how the SSNs are actually used. In our work, we focused on those users who reached the largest number of people: State governments and, for the private sector, businesses that offer health services, financial services or personal information.

State officials say they use SSNs in both administering programs and enforcing the law. For example, State tax administrators routinely use the SSN as a primary identifier in their State tax systems and to cross-check taxpayer income. State driver licensing agencies must typically use SSNs to check an individual's driving record in other States. Law enforcement agencies use SSNs to check criminal records.

In the private sector, the health care industry generally uses SSNs as backup identifiers. Other numbers serve as primary identifiers for patient medical records but SSNs are needed to trace patients' medical care across providers or to integrate patient records when providers merge.

Credit bureaus also use SSNs. Such organizations build databases of consumer payments and credit transactions. Credit bureaus use the SSN as a principal identifier for retrieving credit histories on demand. Most customers—insurance companies, collection agencies, credit grantors—provide an SSN when requesting a credit history and can deny credit to individuals who refuse to provide them.

In contrast to these administrative uses, businesses that sell personal information collect SSNs for the sole purpose of selling them in a linkage with other information. Generally, these databases use SSNs to facilitate records searches when they are sold to customers like lawyers, debt collectors, employers or anyone who might want to carry out some form of background check on an individual.

Finally, I would like to summarize the possible effects of restricting use of the SSN. Users told us that without the SSN as the unique identifier, data exchanges would be at risk. Tax enforcement would be hampered by not being able to verify income reported, States could not readily identify drivers concealing out-of-state traffic violations, consumer credit histories could not be quickly updated and accurately retrieved.

Some users have voluntarily taken measures to restrict the disclosure of some personal information, including SSNs. Many of the businesses in the personal information industry have signed an agreement restricting SSN disclosure to only a limited range of customers such as law enforcement agencies.

In conclusion, the wide use of the SSN is permissible but its presence in databases creates privacy concerns and fosters the growing problem of identity theft. Restricting the use of SSNs in law could reduce dissemination of personal information but could also restrict commercial and public sector activities. Such effects could be only temporary, however, until users devise a new means of identifying personal records.

In an increasingly electronic world, protecting privacy will continue to be a public policy challenge.

That concludes my statement, Mr. Chairman. I would be happy to answer any questions you may have.

[The prepared statement follows:]

Statement of Barbara D. Bovbjerg, Associate Director, Education, Workforce and Income Security Issues, Health, Education, and Human Services Division, U.S. General Accounting Office

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today to discuss usage of the Social Security number (SSN) for purposes not related to Social Security. The SSN was created in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. Today over 277 million individuals have a unique SSN. For this reason it is used for myriad purposes not related to Social Security. Both private businesses and government agencies frequently ask individuals for their SSNs because in certain instances they are required to or because SSNs provide a convenient means to track and exchange information.

Perceived widespread sharing of personal information and occurrences of identity theft have raised public concern. To provide information about how the SSN is currently used, in my remarks today I will describe (1) federal laws and regulations directing the number's use, (2) the nonfederal purposes for which the number is used, and (3) what businesses and state governments believe the effect would be if federal laws limiting the use of SSNs were passed. My testimony is based on findings from a study [1] we conducted for this Subcommittee during 1998 and recent work conducted to update our information.

In summary, the federal government, states and local governments, and private businesses all widely use SSNs. In the case of the federal government, a number of laws and regulations require the use of SSNs for various programs, but they generally also impose limitations on how these SSNs may be used. However, no federal law imposes broad restrictions on businesses' and state and local governments' use of SSNs when that use is unrelated to a specific federal requirement. Currently, governments and businesses frequently use SSNs to identify and organize individuals' records. Some may also use SSNs to exchange information with other organizations to verify information on file, to coordinate benefits or services, or to ensure compliance with certain federal laws. For example, by sharing information about applicants for the Supplemental Security Income (SSI) program, the Social Security Administration (SSA) can identify individuals whose benefits should be reduced, such as those in prison. In addition, some information brokers use SSNs to retrieve the large amount of personal information on individuals that they collect and sell. Public concern over the availability of personal information has encouraged some to consider ways to limit using SSNs to disclose such information. However, officials from both private businesses and state governments have stated that if the federal government passed laws that limited their use of SSNs, their ability to reliably identify individuals' records would be limited, as would their subsequent ability to administer programs and conduct data exchanges with others. Nonetheless, some state agencies and businesses have voluntarily taken steps to limit their disclosure of SSNs.

Federal Laws and Regulations Require and Restrict Certain SSN Uses

Although SSA originally intended SSNs as a means to identify workers' earnings and eligibility for Social Security benefits, a number of federal laws and regulations now require the use of the SSN to track participation in a variety of federal programs. Use of SSNs facilitates automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both. The Internal Revenue Code and regulations that govern the administration of the federal personal income tax program require that individuals' SSNs serve as taxpayer identification numbers. Employers and others making payments to individuals must include the individual's SSN in reporting to the Internal Revenue Service (IRS) many of these payments. In addition, the Code and regulations require that individuals filing personal income tax returns include their SSN and those of any dependents or former spouses to whom they pay alimony. Similarly, the Social Security Act requires individuals to provide their SSNs in order to receive benefits under the SSI, food stamp, Temporary Assistance for Needy Families (TANF), and Medicaid programs—programs that provide benefits to people with limited income. Applicants give program administrators information about their income and resources, and program administrators use applicants' SSNs to match records with those of other organizations to verify the information. For example, we have recommended in previous reports that SSA match its records with other state and federal program records to reduce SSI payments to individuals whom agencies find residing in nursing homes and prisons. Similarly, the Commercial Motor Vehicle Safety Act of 1986 requires states to use individuals' SSNs to determine if an individual holds a commercial license issued by another state. Also, federal law requires that states use SSNs to maintain records of individuals who owe state-ordered child support or are owed

[1] Social Security: Government and Commercial Use of the Social Security Number Is Widespread (GAO/HEHS09990928, Feb. 16, 1999).

child support and to collect from employers reports of new hires identified by SSN. States then transmit this information to the Federal Parent Locator Service, an automated database searchable by SSNs. The use of SSNs in these instances ensures compliance with federal tax laws, enhances program payment controls, reduces the possibility of inappropriately licensing applicants, and facilitates enforcement of child support payments.

Federal laws that require the use of an SSN generally limit its use to the statutory purposes described in each of the laws. For example, the Internal Revenue Code, which requires the use of SSNs for tax purposes, also declares tax return information, including SSNs, to be confidential and prescribes both civil and criminal penalties for unauthorized disclosure. Similarly, the Social Security Act, which requires the use of SSNs for disbursement of benefits, declares that SSNs obtained or maintained by authorized individuals on or after October 1, 1990, are confidential and prohibits their disclosure. Finally, the Personal Responsibility and Work Opportunity Act, which expanded the Federal Parent Locator Service, explicitly restricts the use of SSNs to purposes set out in the act, such as locating absentee parents to enforce child support payments.

In addition to the restrictions contained in laws that require the use of SSNs, the Privacy Act of 1974 also restricts federal agencies in collecting and disclosing personal information, which includes SSNs. The act requires federal agencies that collect information from individuals to inform the individuals of the agencies' authority for requesting the information, whether providing the information is optional or mandatory, and how the agencies plan to use the information. The act, which also prohibits federal agencies from disclosing information without individuals' consent, does not apply to other levels of government or to private businesses.

Except as discussed above, federal law does not regulate the use of SSNs. Thus, nonfederal agencies and legitimate businesses have uses of SSNs not covered by federal law, which I will now discuss.

GOVERNMENTS AND BUSINESSES USE SSNS EXTENSIVELY

Because there are so many users of the SSN, I will focus on organizations that routinely use SSNs for activities that affect a large number of people. These include state government agencies as well as private businesses that sell health services, financial services, and personal information. In general, organizations may record SSNs in their databases for two purposes: to locate records for routine internal activities, such as maintaining and updating account information and, more frequently, to facilitate information exchanges with other organizations. Governments, health care organizations, and financial services businesses use SSNs, at least in part, to perform services for the person who owns the number. Information brokers, however, collect information that may include SSNs for the sole purpose of selling it.

State Agencies

States use SSNs to support state government operations and offer services to residents. The Social Security Act allows states to use SSNs to identify individuals who pay taxes, receive general public assistance, own a vehicle, or drive. My comments today will focus on two examples of how states use SSNs to administer programs: states' personal income tax programs and licensing of drivers.

All states that have personal income tax use SSNs to administer their programs, according to an official at an organization representing state tax administrators. States use SSNs as primary identifiers in their programs and for auditing purposes. Tax administrators from Maryland and Virginia told us that their states require individuals to provide their SSNs on state tax returns and that those who do not risk being considered nonfilers if tax administrators cannot otherwise identify them. In order to monitor taxpayer income reporting, states rely on SSNs to match data with IRS and state tax agencies. In addition, tax administrators said they use SSNs to cross-reference owners' or officers' business income tax returns with their personal income tax returns so that an audit of one triggers an audit of the other. They also use SSNs to identify residents who received income or tax credits in other states. Finally, when they assess liens against a taxpayer, tax administrators may also use SSNs to gather information from credit bureaus and information brokers about a taxpayer's assets.

State driver licensing agencies are more likely to use SSNs to exchange data with other organizations than to support internal activities. Information from the American Association of Motor Vehicle Administration (AAMVA) and other sources suggests that many states request, but may not require, applicants for noncommercial driver licenses to provide their SSNs. Most state driver licensing agencies that re-

quest SSNs include SSNs in driver records as a secondary identifier and devise their own license numbers. To monitor drivers' compliance with state laws, state officials said they use SSNs during the licensing process to search national databases maintained by AAMVA. This allows states to identify driver licenses an applicant may hold in other states and to determine whether the applicant has had a license suspended or revoked in another state. Licensing officials told us that courts and law enforcement agencies may request driver records by SSN when they do not know the driver's license number. In the past, some states have sold personal information collected from drivers and automobile owners, including SSNs, to individuals and businesses. However, the federal Drivers' Privacy Protection Act now prohibits states from disclosing this personal information for purposes such as surveys, marketing, and solicitation without the express consent of the individual.[2]

Having discussed how state governments use SSNs, I would like now to focus on how private businesses use these numbers. Specifically, I will discuss use of SSNs by health care service organizations, financial services businesses, and businesses that sell information.

Health Care Services Organizations

Officials representing hospitals, a health maintenance organization (HMO), and a health insurance trade association told us that their organizations always ask for an SSN, but they do not deny services if a patient refuses to provide the number.

Officials from a hospital and an HMO told us that although they ask patients for their SSNs, they assign patients other identifying numbers, which they use internally as the primary identifiers for patient medical records. If a patient either forgets or does not know the patient number he or she was assigned then the hospital or HMO uses SSNs as a backup to identify records. These officials also told us that hospitals and HMOs use SSNs to track patients' medical care across multiple providers because doing so helps establish a patient's medical history and avoid duplicate tests. Similarly, health care providers use SSNs to integrate patients' records when providers merge, a trend that is growing.

We also spoke with a representative from a health insurance trade association to understand how insurers use SSNs. He told us that some health insurers use the SSN or a variation of the number as the customer's insurance number. We were told that the BlueCross BlueShield health insurance plans and the Medicare program frequently use this method. This representative also said that insurers and providers frequently match records among themselves, using SSNs to determine whether individuals have other insurance. This allows insurers to coordinate payment of insurance benefits.

Officials in the health care industry expect their use of SSNs to increase. Because health care services are generally delivered through a coordinated system that includes health care providers and insurers, it is important for health care providers to be able to accurately identify information about patients. However, health care providers may also use SSNs to gather information that is not directly relevant to a patient's health care. For example, one hospital official said that her hospital plans to use SSNs during the admission process to obtain on-line verification of patients' addresses.

Financial Services Businesses

Three national credit bureaus serve as clearinghouses for consumer credit reports and receive information about consumers' credit card transactions and payments from businesses that grant consumer credit. Officials from a bank and a credit card company told us that banks and credit card companies voluntarily report customers' payments and credit card transactions, accompanied by SSNs, to credit bureaus. They do so because ensuring that credit bureaus have up-to-date consumer payment histories serves the interest of companies, like themselves, that provide credit. An official for a credit bureau trade association estimated that each national credit bureau has more than 180 million credit records. SSNs are one of the principal identifiers credit bureaus use to update individuals' credit records with the monthly reports of credit and payment activity creditors send them. In addition, credit bureaus use SSNs that are provided by customers to retrieve credit reports on individuals. Credit bureau officials told us that customers are not required to provide SSNs when requesting reports, but requests without SSNs need to include enough information to identify the individual.

Businesses such as insurance companies, collection agencies, and credit grantors use SSNs to request information about customers from credit bureaus. Banks and

[2] Until a 1999 amendment to the act, states were permitted to disclose this information if they provided drivers with the opportunity to prohibit disclosure and the driver opted not to do so.

credit card companies in particular want information on customers' histories of repaying debts and whether customers have filed for bankruptcy or have monetary judgments against them, such as tax liens. Officials representing credit grantors said most banks and credit card companies ask applicants to provide their SSNs, and these credit grantors may choose to deny services to individuals who refuse. These officials said that their organizations generally do not use SSNs as internal identifiers but instead assign an account number as a customer's primary identifier.

Businesses That Sell Personal Information

Continuing advances in computer technology and the ready availability of computerized data have spurred the growth of information brokers who amass and sell vast amounts of personal information, including SSNs, about members of the public. One official from a firm that sells information told us that his organization has more than 12,000 discrete databases with information about individuals. Federal law does not prohibit these businesses from disclosing SSNs.

Brokers buy and sell information from and to a variety of public and nonpublic sources. Examples of the information they buy include public records of bankruptcy, tax liens, civil judgments, real estate ownership, driving histories, voter registration, and professional licenses. The information broker's purchase may include SSNs. Some brokers sell information only to businesses that establish accounts with them; others sell it to anyone. Law firms, law enforcement agencies, research organizations, and individuals are among those who use brokers' services. For example, lawyers, debt collectors, and private investigators may request information about an individual's bank accounts and real estate holdings for use in divorce or other civil proceedings; automobile insurers may want information about whether insurance applicants have been involved in accidents or have been issued traffic citations; employers may want background checks on new hires; pension plan administrators may want information to locate pension beneficiaries; and individuals may ask for information to help locate their birth parents.

To meet the needs of the parties to whom they sell information, information brokers have databases that can be searched by identifiers that may include SSNs; brokers may also include SSNs along with the other information they provide to customers. When possible, information brokers retrieve data by SSN because it is more likely than other identifiers to produce records for a specific individual.

Business and State Officials Believe Federal Laws Restricting Uses of SSNs Would Have a Negative Effect on Their Activities and Programs

Officials from the businesses and agencies we contacted told us that federal restrictions on using SSNs could hamper their ability to conduct routine internal activities and their ability to exchange data. For each of these entities, correctly matching a specific individual to a corresponding record of information is an important concern. Consequently, these officials told us, federal limits on the use of SSNs could adversely affect their activities and programs. They told us that limits on the use of SSNs, for example, would lessen the certainty with which credit information could be matched to specific individuals and hinder health care service providers' ability to track patients' medical histories over time and among multiple providers. They also told us that such action could impede state tax agencies' ability to identify those who file taxes, make it difficult to associate tax return information received from other tax agencies with tax information reported by residents, and make it more difficult for states to link driver license applicants to traffic violations they may have acquired under other state licenses. Finally, officials from state agencies that license drivers told us that if they could not use SSNs to query their databases, it would increase the likelihood that government and law enforcement agencies would receive the records of multiple people with the same name when they requested information about a particular individual.

Because of privacy concerns raised by the disclosure of personal information, some businesses and states have voluntarily restricted their disclosure of such information, including SSNs. In December 1997, 14 of the self-identified industry leaders of those businesses that sell personal information voluntarily agreed to make the SSNs they obtain from nonpublic sources available only to a limited range of customers. They identified such customers as those having appropriate uses for this information, such as law enforcement. Although these brokers agreed to limit their disclosure of SSNs obtained from nonpublic sources, it should be noted that most of the SSNs they acquire come from public sources, according to an official from an information brokerage company. As part of their agreement regarding disclosure of SSNs, the 14 organizations also agreed to annual compliance reviews by independent contractors. If an organization fails to comply with the agreement, the Fed-

eral Trade Commission can cite the organization for unfair and deceptive business practices. The agreement became effective on December 31, 1998. Recent reports indicate that the first round of compliance reviews is complete and all of the companies have generally complied with the agreement.[3]

In addition to the voluntary efforts of businesses, some states are discontinuing practices that result in routine disclosure of SSNs. For example, since July 1, 1997, Georgia no longer automatically prints SSNs on licenses but rather assigns its own numbers for driver licenses and uses the SSN as a license number only if requested by the license holder to do so. Ohio, which before July 29, 1998, routinely printed SSNs along with state-assigned numbers on driver licenses, now allows drivers the option of not having SSNs printed on their licenses. Also, AAMVA officials believe most states in which driver records are public now exclude SSNs when responding to requests for driver records.

Finally, SSA has stated that the expanded use and misuse of SSNs poses an administrative burden for the agency. According to agency officials, widespread use of SSNs as identifiers requires SSA to meet more requests for SSN verification from employers and government agencies. In addition, the disclosure of SSNs increases those instances in which the agency must issue individuals new SSNs when theirs are being misused by another party.

CONCLUDING OBSERVATIONS

In conclusion, the widespread use of the SSN is permissible under existing laws and regulations, but because it provides a means to build and share databases of personal information, it creates privacy concerns and enables the growing problem of identity theft. Although restricting the use of SSNs may slow or reduce wide dissemination of personal information, such an action could also restrict commercial and public sector activities. However, such effects could be only temporary, until a new means of identifying unique personal records was devised. In our increasingly electronic world, protecting privacy will continue to be a public policy challenge.

Mr. Chairman, this concludes my prepared statement. At this time, I will be happy to answer any questions you or other Members of the Subcommittee may have.

GAO CONTACT AND STAFF ACKNOWLEDGMENTS

For information regarding this testimony, please contact Barbara Bovbjerg at (202) 512097215. Individuals who made key contributions to this testimony include Kay Brown, Jacquelyn Stewart, Roger Thomas, and Patrick di Battista.

Chairman SHAW. Mr. Johnson?

Mr. JOHNSON. None.

Chairman SHAW. Mr. Tanner?

Mr. TANNER. We just ironically or interestingly enough got a call last week from a constituent in Tennessee whose home had been broken into, lockbox violated and stolen from that were the birth certificates and Social Security numbers of herself and her children.

My question is, what should she do to alert whomever to the possible misuse of the Social Security number and the birth certificate?

Ms. BOVBJERG. With the cautionary note that I am not a law enforcement officer, I would tell her to contact legal authorities. One of the things I was thinking when I was listening to the Stevens family's very troubling story is that in work we did a couple of years ago for this subcommittee on identity theft, we were struck that no single Federal agency has law enforcement power in this area. It is difficult, partly for this reason, to get a sense of frequency and magnitude of identity theft crimes. It is difficult to

[3] One company no longer offers products that fall within the scope of the agreement.

know how much money is involved, what the costs are, it becomes difficult to know who exactly to talk to when something like this happens.

The Federal Trade Commission has been given more authority to provide public information, to work with the personal information industry on this voluntary disclosure agreement, I believe they have to contact appropriate enforcement officials to actually find the offender and carry out penalties.

Mr. TANNER. Is your answer the Federal Trade Commission then at the moment? Would that be a good place to start?

Ms. BOVBJERG. That would be a good place to start.

Mr. TANNER. In your analysis of this, you said there is no single agency where identity theft crimes are housed. Do you have a suggestion for the Congress on how we should address this area and if there is any legislation you think appropriate?

Ms. BOVBJERG. I don't have a suggestion for you. I am sorry. I think it is such an emerging area that all Federal agencies are struggling with this. You will hear from the Social Security Inspector General later some of the things they are doing to deal with identity theft but much of what SSA does will focus on the issuance of cards and making sure that only the appropriate people are receiving Social Security numbers. They cannot always make changes on the back end, they cannot always go after people once they have stolen someone's number.

I really think this is something that needs more Federal attention, more policy attention. It is worth considering how best the Federal Government can respond to it.

Mr. TANNER. I really appreciate you having this hearing, Mr. Chairman. This is more potentially disastrous and widespread than many had thought. I want to commend you for having this. It is something I think we have some room to do some good work on.

Thank you.

Chairman SHAW. I think you are right, John. I think what we are seeing is just a new and growing theft industry that we have to nip in the bud.

Mr. Portman?

Mr. PORTMAN. A couple of things. First, I appreciate your testimony and following the comment of my colleague from Tennessee, I really appreciate, Mr. Chairman, your having the hearing and taking some time on this, and your personal commitment to it.

I understand you walked into a video store somewhere down in Florida and they asked for your Social Security number and you walked out without the video. That is a frustration.

I have a couple of things I would like to raise with GAO. First, with regard to driver's license, I notice on page seven of your testimony you talk about how since 1998 Ohio no longer prints Social Security numbers along State-assigned numbers on the driver's license. It is optional. I notice it is on mine and I am not going to try to get it off, but it does say optional now. It didn't use to be that way. In fact, it was the identifier. Mr. Collins mentioned that is true with Georgia as well. You can move to Ohio instead of Georgia for those who heard his earlier comments.

I think this is a very important step in the direction to help ensure an individual's privacy not to require these numbers on driv-

er's licenses. I would like to put into the record if I could a letter I got from the Registrar of the Bureau of Motor Vehicles of Ohio with further comment on the situation in Ohio. I think it would be helpful with regard to this discussion and perhaps help other States move in this direction as well.

Chairman SHAW. Without objection.

[The information follows:]

BUREAU OF MOTOR VEHICLES
COLUMBUS, OH 43266
May 9, 2000

The Honorable Rob Portman
United States Representatives
House Office Building
Washington, DC 20515

Dear Congressman Portman:

Thank you for the opportunity to further comment on Ohio's use of SSN relative to our motor vehicle records. For purposes of clarification, motor vehicle records includes driver license records, state identification cards, motor vehicle title records and motor vehicle registration records (license plates).

Since the early 1990's, the Ohio Bureau of Motor Vehicles (Ohio BMV) has not released SSN information from our records unless the requestor provides that information as part of their record request. For instance, if an automobile insurance company requests a copy of a driver record, we will only provide the SSN as part of the record report if the SSN was originally provided to us as an identifier.

Since July, 1998, the Ohio BMV has provided an option to individuals to request the SSN be removed from the face of their license. While the Ohio BMV permits an individual to request the SSN not be printed on their license, we still require verification of the SSN to determine eligibility to obtain a driver's license. Like most states, Ohio verifies driving status. This is done for all classes of motor vehicles. Federal standards specifically require states verify eligibility of drivers applying for a commercial driver license. The primary purpose of this procedure to avoid instances where drivers, with suspended or revoked driving privileges, apply for a license in another state.

Law enforcement agencies and courts are able to receive SSN information from the Ohio Bureau of Motor Vehicles.

To date, SSN remains the most common and relied upon identifier, to match the various records of courts and law enforcement agencies with our own records. Names are unreliable because of common names and variations in spelling and usage.

The use of motor vehicle records, by government agencies, has also been expanded beyond the traditional motor vehicle related activities. For instance, Ohio has a law that permits the revocation of driving privileges of a person who is in arrears for child support; children with excessive truancy can loose their driving privileges or ability to apply for a license; etc.

In order to tie all of these different activities together, a reliable form of identification is required. Presently, SSN is that identifier for most government agencies.

The Ohio BMV recommends that the opinion of the American Association of Motor Vehicle Administrators (AAMVA) be considered in determining an appropriate policy. AAMVA has spent considerable time and effort in determining an appropriate policy on behalf of its members.

Sincerely,

FRANKLIN R. CALTRIDER
Registrar

Mr. PORTMAN. My question to GAO would be, do you have any feedback on how this is working, either in Ohio or other States?

Ms. BOVBJERG. It is really an emerging area. It is permissible for States to put Social Security numbers on a driver's license, but they may allow people an option not to have it on there. In the

meantime, there is a recent court decision that upheld the law saying States may not sell that information without the express permission of the individual. There has been a lot of turmoil in the States on driver's license information, and we haven't been able to determine to what extent things are working or not working at the State level.

Chairman SHAW. Would the gentleman yield on that?

Mr. PORTMAN. Absolutely.

Chairman SHAW. It is my understanding, and I could be wrong, but in the State of Virginia that they use the Social Security number as the driver's license number. Is that correct, do you know? I see a head bobbing yes.

Ms. BOVBJERG. I am not a Virginia driver so I cannot say from personal experience, but they can. It is permissible for a State to do that. I think more States are following the Ohio and Georgia lead though of retaining the Social Security number in their records because they need it to determine if somebody has been a scofflaw in another jurisdiction. Also, they need it to demonstrate that person has not been a scofflaw in their jurisdiction when someone else asks from another State, but they can no longer sell that information without individual permission.

Chairman SHAW. I have just been handed a Virginia driver's license and the gentleman's Social Security number appears prominently on it and it is identified as "customer number." There is no other number on the license, so I think it is clear the State of Virginia is using Social Security numbers as the driver's license number which is something we ought to look into.

Mr. PORTMAN. I guess one of the issues that we might want to look at is penalties at the Federal level. What are the penalties now for Social Security number fraud or for misuse under the Identified Theft Act?

Ms. BOVBJERG. I don't know the answer to that question. Perhaps the Social Security IG will know better. I know that the penalties have stepped up. I am looking in my notes to see which law it is. It is the Identity Theft Assumption and Deterrence Act that made identity theft a Federal crime. This was in 1998. The penalties became substantial criminal penalties. I don't know exactly what those are but I know the penalties have expanded in response to that law.

Mr. PORTMAN. That would be helpful for the subcommittee to have that research. Perhaps the IG can provide it today. If not, if GAO could provide that?

Ms. BOVBJERG. I will contact your office with that information.

Mr. PORTMAN. Thank you. One final question, which is a general one.

Let us say someone refuses to disclose their Social Security number to a private business. Again, I reference the Chairman had to watch TV rather than a video. Can that business, by law, decline to provide the service?

Ms. BOVBJERG. We are not aware of any law that requires a business to serve you if you don't provide information. It is also common in a place like Radio Shack. I had a similar experience to the Chairman's where they asked for my phone number and my Social

Security number to buy a CD player. I said no, and they said, oh, okay, and I still got the CD player.

In some cases, credit agencies, credit bureaus, lenders, will deny credit without the number.

Mr. PORTMAN. And a bank deny a loan if you refuse to provide your Social Security number. I assume a bank can at this point deny a loan if you do not provide your Social Security number?

Ms. BOVBJERG. Yes, they can.

Mr. PORTMAN. Thank you, Mr. Chairman.

Chairman SHAW. Mr. Collins, your State was mentioned in the gentleman from Ohio's questioning. Would you like to respond?

Mr. COLLINS. We have a lot of residents of Georgia who were former residents of Ohio and we are pleased to have them. We expect more. [Laughter.]

Mr. COLLINS. In your review of the misuse of Social Security numbers as it pertains to commercial or the marketplace, in any sort of way did you find the same misuse of Social Security numbers or identity in earned income tax credit areas?

Ms. BOVBJERG. In our work, we did not look at misuse of Social Security numbers. We focused entirely on what legally was permissible, what was legally restricted, how different entities were using the numbers, but we did not investigate misuse.

Mr. COLLINS. The same could be true then for those who would misuse a Social Security number in application for the refundable income tax credit.

Thank you, Mr. Chairman.

Chairman SHAW. Thank you for your testimony. We appreciate it. It helps round out our knowledge.

With regard to the comment that there is no restriction on asking but they don't have to continue to do it to give you the service, this goes back to the check cashing and the military bases which we are still researching.

Thank you. It is always nice to have you back before this committee.

Ms. BOVBJERG. Thank you, sir.

[Questions submitted by Chairman Shaw, and Ms. Bovbjerg's responses follow:]

GENERAL ACCOUNTING OFFICE
WASHINGTON, DC 20548
July 7, 2000

The Honorable E. Clay Shaw, Jr.
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Subject: *Social Security Numbers: Subcommittee Questions Concerning the Use of the Number for Purposes Not Related to Social Security*

Dear Mr. Chairman:

This letter responds to your request that we provide answers to questions relating to our May 9, 2000 testimony.[1] In that testimony we discussed the usage of the Social Security number (SSN) for purposes not related to social security and the implication of restricting such usage. Your questions, along with our responses, follow.

[1] Social Security: Use of the Social Security Number is Widespread (GAO/T09HEHS090009111, May 9, 2000).

1. The term "national identifier" has a very bad connotation to many people. In your opinion, has the Social Security number become a national identifier?

The SSN is widely used by governments and businesses to maintain and exchange information. The Office of the Inspector General of the Social Security Administration (SSA) has noted that, over time, the SSN has become a "de facto" identifier used by federal and state governments. Banks, credit bureaus, insurance companies, and health care providers also use the SSN for identification purposes. This widespread use of the SSN beyond its original purpose has raised privacy concerns. While privacy concerns should not be discounted, it is important to note that the use of SSNs to link individuals to information about them enhances the administration of federal and state programs, makes credit more accessible to consumers, and allows medical care to be integrated across providers and insurers.

2. In your testimony, you indicated that there is no federal law that regulates the overall use of SSNs. In your view, is such a law needed? Is it feasible to enact, administer, and enforce such a law?

Whether a law regulating the overall use of SSNs is needed depends on a number of factors. The first of these is the extent to which such a law could effectively curb identity theft and address privacy concerns. Secondly, these potential benefits would have to be weighed against how additional restrictions on the use of SSNs might hamper government and businesses' ability to conduct routine business. The feasibility of administering and enforcing such a law would depend on how restrictive it was and its scope—whether it was intended to change existing practices or limit uses of the SSN beyond those currently practiced. In addition, it would be necessary to decide what agency or agencies would be responsible for administration and enforcement and the resources those agencies would have to carry out those duties.

3. As you pointed out in your testimony, the Social Security number was created as a means of tracking workers' earnings and eligibility for Social Security benefits. It was never intended to serve as a personal identification document. Only certain information is maintained by SSA as a part of its Social Security number database. What information is available? What proof is required to obtain a Social Security number? How have the proof requirements changed over time?

SSA collects only certain information about applicants for SSNs, and the documentation required as proof of this information has changed over time. Originally, SSA assigned an SSN to applicants based solely on individuals' unverified statements regarding age, identity, and place of birth. However, since 1978, applicants for new SSNs must provide proof of age, identity, and U.S. citizenship or proof that they are lawfully residing in the U.S. In addition, applicants must provide other information such as their place of birth, mother's maiden name, and father's name. Those applicants who are not U.S. citizens must also provide Immigration and Naturalization Service documentation showing whether they are allowed to work or provide a valid non-work reason for needing an SSN.

4. Despite public concerns about sharing personal information in today's electronic world, does the public benefit from the widespread use of SSNs and the sharing of personal information? Can you provide some examples?

When consumers want to be uniquely identified, particularly in the health care and consumer credit service industries, the use of SSNs to share personal information accomplishes this purpose with one uniform number. Using SSNs to link individuals to their medical records allows doctors, hospitals, and HMO's to coordinate a person's health care among health providers and with insurers. Similarly, because up-to-date consumer payment histories linked to SSNs are available through national credit bureaus, the use of SSNs helps individuals instantly demonstrate their credit worthiness anywhere in the country when requesting credit.

5. If someone refused to disclose his or her SSN to a private business, can the business, by law, decline to provide the service? For example, if someone refuses to provide his or her SSN on a loan application, can the bank deny the loan?

No federal law imposes broad restrictions on businesses' use of SSNs; consequently, businesses that request SSNs as a condition for receiving services may deny such services to individuals who refuse. However, practices vary by industry. Health care providers generally request patients' SSNs, but we were told that they do not require them as a condition for treatment. In contrast, most credit card companies request clients' SSNs as a condition for extending credit and may refuse service to those who do not comply. States vary in whether they require an SSN as part

of the application for non-commercial driver licenses. Some require it for inclusion in a database, some do not, and in some states it is optional.

6. What are the possible effects on businesses of restricting their use of SSNs?

Federal restrictions on using SSNs could hamper businesses' ability to conduct routine internal activities and their ability to exchange data. Correctly matching a specific individual to a corresponding record of information is an important concern for health care providers, information brokers, and credit agencies. Limits on the use of SSNs could make it harder for health care service providers to track patients' medical histories, make it less easy for employers to do background checks, and lessen the certainty with which credit information could be matched to specific individuals.

7. You mentioned in your testimony that many businesses and agencies are voluntarily restricting the use of SSNs to help protect their customers' privacy and reduce SSN misuse. Can you please elaborate on some of these self-regulatory policies?

In 1997, 13 of the self-identified leaders in the information brokerage industry agreed to limit their disclosure of the SSNs they obtain from nonpublic sources to those customers who have legitimate uses for this information, such as law enforcement officials. In addition, they agreed to annual compliance reviews by an independent contractor. The Federal Trade Commission can cite them for unfair and deceptive business practices if they do not do as they have agreed. While recent reports indicate that the companies have generally complied with the agreement to limit their sale of SSNs that they obtain from nonpublic sources, it should be noted that the SSNs contained in the records they acquire are more likely to come from public sources, according to an information broker.

Some states have taken steps to protect individuals' privacy by changing whether they display SSNs on driver licenses. For example, according to driver license officials in Georgia and Massachusetts, these states no longer automatically use SSNs as driver license numbers. They give drivers the option of using a state generated license number, instead of their SSN. Similarly, driver license officials in Ohio told us that the state previously printed SSNs along with state-assigned numbers on driver licenses, but now allows drivers the option of not having SSNs printed on their licenses. According to an American Association of Motor Vehicle Administrators official, only Hawaii still requires that SSNs be used as a driver's license number, but the state plans to discontinue this requirement next year.

8. One area not discussed in your written testimony is e-commerce. How has the high-tech economy affected SSN use? In general, can people conduct business on the Internet without providing their SSNs? How would restricting the use of SSNs affect e-commerce?

Our work to date has not included assessing the uses of SSNs within the high-tech economy or the effects of their restricted usage on e-commerce. However, in visits to two of the existing e-commerce sites, we found that certain consumer purchases can currently be made via the Internet without requiring the use of an SSN. Instead, these sites typically required new and repeat customers to register for online services by providing an identifier such as the user's name, and by selecting a password. Additionally, they require a credit card number to cover purchases of goods or services. Certain other e-commerce sites that we observed, however, such as those that sell securities or insurance policies, did require SSNs for tax or identification purposes.

9. You indicated that "information brokers" collect SSNs for the sole purpose of selling them. What exactly is an information broker? How are consumers served by this industry? What is the downside of limiting their activities? Why do information brokers need people's SSNs?

Information brokers buy personal information, amass it in databases, and then resell it to clients. Brokers buy some of this information from private sources. However, some of the information they buy is already available to the public. Brokers offer customers convenient one-stop shopping for information that might otherwise by widely dispersed. For example, an employer can obtain information about a person's driving history and criminal history from an information broker, rather than attempt to locate and access public records containing the same information. Information brokers serve a variety of clients—a lawyer may request information needed for a civil proceeding; a pension plan administrator may request information to locate pension beneficiaries; or an individual may ask for information to help locate a birth parent. Information brokers may use SSNs to search databases. Limiting in-

formation brokers' use of SSNs might make it more difficult for them to conduct searches that produce records unique to a given individual.

10. According to your testimony, the Social Security Act declares that SSNs obtained by authorized individuals after October 1, 1990 are confidential and cannot be disclosed. If the Social Security Act prohibits the disclosure of SSNs why is their use so widespread and why are businesses allowed to ask for the SSN?

The Social Security Act provision to which you refer, section 205(c), protects against unauthorized disclosure of SSNs, but does not restrict the many legally authorized uses of the SSN. Businesses are allowed to ask for and use SSNs because section 205(c) generally only applies to governmental use of SSNs.

Section 205(c) generally does not apply to business transactions. It prohibits disclosure by "authorized persons," and it defines that term in part to mean those who gain access to SSNs "pursuant to any provision of law.. . ." Someone who comes into possession of an SSN as part of a business relationship—for example, the bank that requires it as part of a credit card application—has not gained access to it pursuant to a provision of law, and is therefore not subject to the section 205(c) restriction on disclosure.

11. If the use of the SSN were restricted by federal law, is it likely that another personal identifier would take its place?

Although privacy concerns should not be discounted, exchanges of computerized data are important to the functioning of governments and businesses, and these exchanges can benefit the public. Given the large amount of such data available, in general, accuracy in linking the correct individual with information about him or her is desirable in the administration of some programs and in cases where people want to be uniquely identified. The SSN provides a convenient and effective method for doing this. If the SSN were not available for this purpose, in all likelihood, some other mechanism for doing the same would eventually take its place.

We are sending copies of this letter to other interested parties. If you have any questions on matters discussed in this letter, please contact Kay Brown or me on 512097215. Key contributors to this assignment were Jacquelyn Stewart, Patrick di Battista, Valerie Melvin and Roger Thomas.

Sincerely,

BARBARA BOVBJERG
Associate Director, Education, Workforce, and Income Security Issues

---

Chairman SHAW. Our final witness this morning is from the Social Security Administration, the Honorable James Huse, Inspector General, Office of the Inspector General.

Mr. Huse, welcome back to the subcommittee. You may proceed as you wish. We have your full statement which will be made a part of the record.

STATEMENT OF HON. JAMES G. HUSE, JR., INSPECTOR GENERAL, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. HUSE. Good morning, Mr. Chairman and subcommittee members.

Thank you for the opportunity to testify on this critical issue which impacts greatly on the lives of American citizens. In my full statement for the record, I outline for you the ways in which the SSN has been transformed from a simple agency recordkeeping tool into a cornerstone of modern commerce. Although the SSN was never intended to be a national identifier, it has rapidly evolved into the de facto identifier, especially with the introduction of electronic commerce.

Our office is acutely aware that SSN misuse is on the rise because of the large number of SSN misuse allegation we receive and by the increasing number of requests for constituent assistance. In fiscal year 1999, our fraud hotline processed over 75,000 allegations, 80 percent of which involved the misuse of an SSN, with about 32,000 of these having an impact on Social Security's trust funds.

Our work has revealed that certain misuse occurs because of vulnerabilities in SSA's processes such as cases where individuals apply for benefits under erroneous or counterfeit SSNs or where individuals sell legitimate SSNs for hundreds of dollars. We have also seen examples where Social Security's vulnerabilities in its enumeration business process adds to the pool of SSNs available for criminal, fictitious identities.

Once an improperly issued Social Security number enters the stream of commerce, there is scant hope for preventing subsequent damage. In our audit work, we have made several recommendations to Social Security to improve its business processes which I have outlined in my full statement for the record.

Through our audit work, we have also determined that there is a direct correlation between Social Security number misuse and Social Security's responsibility to maintain accurate earnings records for individuals. When Social Security cannot reconcile Social Security numbers and identifying information provided by employers, Social Security sends notices to wage earners requesting pertinent information to resolve these discrepancies. Most of the responses are returned "undeliverable, address unknown."

Ideally, we would like to pursue the thousands of potential Social Security number misuse and identity theft referrals that we receive each month. However, we are presently lacking the investigative capacity to handle the entire volume. As a result, we are forced to focus on major cases that directly impact on Social Security's operations.

One of our toughest challenges is to find realistic strategies to fight this battle in an effective and efficient manner while remaining focused on Social Security's programs. Our current approach to Social Security number misuse only provides protection for what is Social Security's current area of responsibility. It will be little consolation to the thousands of identity theft victims and private industry whose cases are the responsibility of an array of Federal, State and local law enforcement agencies.

We have several suggestions for Social Security and Congress to consider in addition to our formal audit recommendations, including, first, regulating the sale of Social Security numbers; second prohibiting businesses from refusing services for nondisclosure of a Social Security number when not relevant to the services being provided; third, requiring photo identification when conducting business with Social Security Administration; fourth, urging the implementation of new technologies and databases to help employers, government and private industry verify that names and/or Social Security numbers are correct to improve the identification process; fifth, legislating statutory law enforcement authority for our OIG investigators and sixth, broadening our civil monetary

penalty authority for the sale or misuse of a Social Security number.

When SSN misuse compromises Social Security's business processes, and the Social Security Trust Funds, our involvement is necessary and vigorous. To focus on our mission, we make tough choices to ensure that we bring the most benefit to the Social Security Administration. Yet, we often become the court of last resort for victims of identity theft. Therefore, I would appreciate your views on how to fulfill that role that the public seems to expect from SSA and our OIG.

Thank you for the opportunity to speak this morning and I would be glad to answer your questions.

[The prepared statement follows:]

Statement of the Hon. James G. Huse, Jr., Inspector General, Office of the Inspector General, Social Security Administration

Mr. Chairman and Members of the Subcommittee:

Good morning Mr. Chairman and members of the Subcommittee. I want to thank the Subcommittee for holding this hearing on Social Security number (SSN) misuse. Your interest in this critical issue, which impacts on the lives of American citizens, is heartening.

Today, I would like to provide you with a brief overview of how the SSN has been transformed, from a simple Agency record-keeping tool into a cornerstone of modern commerce and what this transformation means for the Social Security Administration (SSA), this Office of the Inspector General (OIG), and the American public. I would also like to provide you with an overview of our efforts in this area. Finally, I offer several options for preventing SSN misuse from the perspective of what I believe to be the responsibility of SSA and by extension, this OIG. The more extensive problem of identity theft requires far more Government action than SSA and this office can provide. I would like to inform you about that, and elicit your views as our oversight committee.

EVOLUTION OF THE SSN

With the enactment of the Social Security Act in 1935, a system was developed to track the annual earnings of employed individuals. This system required a specific, unique identifier that could accurately maintain earnings records for decades to come. Thus, the SSN was born. The SSN was never intended to be a "national identifier," but over the years, the SSN became the "de facto" identifier for Federal and State Governments. For example, in 1967 the Department of Defense adopted the SSN in lieu of the military service number for identifying Armed Forces personnel. An SSN was required to enroll in schools, receive financial assistance, and to apply for State drivers' licenses. Over time, the SSN has also become a critical identifier for banks, credit bureaus, insurance companies, medical care providers, and innumerable other industries.

Not surprisingly, the introduction of the SSN into the stream of electronic commerce has been accompanied by a dramatic rise in SSN misuse. There is no end to the creativity and ingenuity employed by those with fraudulent intent. Our office is acutely aware of this problem due to the large number of SSN misuse allegations received by our Fraud Hotline and by the increasing number of requests for constituent assistance that we receive from Congressional offices. In FY 1999, our Fraud Hotline processed over 75,000 allegations. Over 80 percent of the allegations and referrals made to our office involve the misuse of an SSN. Specifically, 32,000 had SSN misuse implications involving SSA programs and an additional 30,000 represented SSN misuse allegations with no direct program implication. In the future, we expect this number to escalate as we begin to process investigative referrals from the Federal Trade Commission (FTC), which was designated as the Federal clearinghouse for identity theft complaints in the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act). Once the public is fully aware of the FTC's new role, we expect a considerable increase in the number of referrals of SSN misuse each month. These daunting numbers will seriously challenge our already strained resources.

As such, I would now like to describe how SSN misuse impacts SSA's programs and operations, the public, and offer some possible solutions.

SSN MISUSE AND SSA'S PROGRAMS AND OPERATIONS

Our work has revealed that certain misuse occurs because of vulnerabilities in SSA's processes. In many instances, SSN misuse strikes at the core of SSA's programs and operations and we have dedicated substantial resources to this area. For example, our office has investigated numerous cases where individuals apply for benefits under erroneous SSNs. Additionally, we have uncovered situations where individuals counterfeit SSN cards for sale on America's streets. From time to time, we have even encountered SSA employees who sell legitimate SSNs for hundreds of dollars. Finally, we have seen examples where SSA's vulnerabilities in its enumeration business process adds to the pool of SSNs available for criminal fictitious identities. Each of these scenarios has a direct and material impact on the integrity of SSA's programs and operations.

To that end, we have conducted numerous undercover operations regarding trafficking in SSA cards and numbers. We have prioritized SSN misuse cases where there is a material impact on the SSA's Trust Funds, such as benefit application cases. And we have been unyielding in our commitment to root out employee fraud and abuse in the SSN arena. I am pleased to report that SSA employee fraud cases in this area have been few and far between.

Preventing SSN misuse will provide the greatest cost benefit to the Agency. To this end, we have dedicated substantial audit resources to study SSA's business processes, as it relates to the issuance of SSNs. Once an improperly issued SSN enters the stream of commerce, there is scant hope for preventing subsequent damage. As such, we would like to share some of our suggested preventative measures with this Subcommittee.

In May 1999, we issued a Management Advisory Report entitled *Using Social Security Numbers to Commit Fraud.* This report detailed cases in which the Agency issued SSNs based on fraudulent documentation. Thereafter, the improperly issued SSNs were used to commit identity crimes. For example, one individual and his associates obtained 1,120 SSNs for nonexistent children using fraudulent birth certificates. During our investigation, we learned a number of the SSNs were linked to a larger criminal network being investigated by a Secret Service task force where credit card companies were defrauded out of approximately $30 million. We recommended that SSA incorporate preventative controls in its Modernized Enumeration System and as a result, SSA is developing automated edits within the system to identify transactions that have the greatest potential for fraud. This systems upgrade will alert employees to suspicious SSN applications, which they can then refer to the OIG for investigation. The efforts of SSA's work in this area will potentially result in thousands of cases being referred to our office for investigation over and above what we currently receive.

This month, we released a follow-up report that further examined SSA's procedures for examining evidentiary documents. This draft audit report, entitled *Review of the Social Security Administration's Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications,* traced the SSN issuance process for over 3,000 SSNs. We selected a judgmental sample of original SSN issuances from a universe of transactions where SSA sent 10 or more SSN cards to a single address within a six-month period. While our small sample was not statistically selected, making extrapolations to the entire SSN universe inappropriate, it was quite instructive in identifying specific vulnerabilities in the SSN issuance process. In our sample, 28 percent of the original SSNs reviewed, or 999 SSNs, were based on invalid evidentiary documents. While a substantial portion of these improperly issued numbers were used to obtain employment, the majority of these numbers were not. It is not implausible to believe that these SSNs were obtained for identity-related crimes. Our draft audit also uncovered the following instances where false identification documents were used to acquire SSNs:

- SSA sent 43 SSN cards to three post office boxes in a small southern town. At our request, Immigration and Naturalization Service (INS) reviewed the application documents and determined that 98 percent of the documents presented were invalid.
- SSA sent 56 SSNs to nonexistent children at seven different addresses. In support of their SSN applications, the "parents" or "guardians" of these purported children had presented invalid birth certificates.

Our draft report concludes that SSA needs stronger procedures and better tools to verify evidentiary documents. Specifically, we will be recommending that SSA employees obtain independent verification of alien evidentiary documents, prior to issuing SSNs. We are also recommending that SSA accelerate negotiations with INS and the State Department to implement an "Enumeration at Entry" program; that SSA not mail new SSNs to a post office box; and that SSA employees receive work

credit and recognition for fraud detection and development. Without such recognition, we see little hope for long-term improvements.

We have also determined that there is a direct correlation between SSN misuse and SSA's responsibility to maintain accurate earnings records for individuals. When SSA cannot reconcile SSNs and identifying information provided by employers, SSA sends notices to wage earners requesting pertinent information to resolve the discrepancy. Most of the responses are returned "undeliverable—addressee unknown" to SSA. Some individuals provide the necessary information so that the earnings records can be reconciled while others reply that they do not have a legal SSN.

Our office performed an audit in 1999, entitled *Patterns of Reporting Errors and Irregularities by 100 Employers with the Most Suspended Wage Items,* to determine which major employers had the most suspended wage items, and to examine why this was occurring. Ninety-six of the 100 employers reported over 109,000 SSNs that had never been assigned by SSA. Over 3,000 of these numbers were entirely comprised of zeroes. As for the others, employers admitted that many workers provide incorrect names and SSNs because they do not want to be identified. One of our recommendations to SSA was to develop and implement a corrective action plan for these 100 employers and continue its efforts to contact those employers who are responsible for large numbers of suspended wage items. It is important to take this action because it only costs SSA 50 cents to post a wage item when originally submitted, as compared to $300 to correct it later.

SSN Misuse and Its Impact on the Public

SSN theft also has a substantial impact on the lives of private citizens, as well as private industry. Theft of SSNs is also becoming more and more prevalent as a result of today's electronic environment, which has facilitated easy access to individuals' SSNs and other personal identifying information. This point was highlighted in great detail at the Administration's Identity Theft Summit in March of this year, where several victims explained how the theft of their SSN turned their lives upside down.

Since the passage of the *Identity Theft Act,* which provided the OIG with additional tools to fight SSN theft, the OIG has been in the forefront of the Federal Government's efforts to fight identity theft crimes. The OIG, in conjunction with the U.S. Attorneys' Office in Milwaukee, Wisconsin, was responsible for one of the first criminal prosecutions under this new law. This case exemplifies the extent to which SSN theft has an impact on both SSA's operations and the public.

In Milwaukee, Waverly Burns, a Supplemental Security Income recipient, had commandeered another person's SSN. This stolen SSN was used to secure employment as a cleaning crew supervisor. While on the job, Mr. Burns stole over $80,000 in computer equipment from the offices of the Wisconsin Supreme Court. The stolen SSN was used to obtain a State of Wisconsin identity card, to open bank accounts in the victim's name, and to file fraudulent tax returns. Meanwhile, Mr. Burns continued to falsely represent to SSA that he was disabled and unemployed; indeed no earnings had appeared under his true SSN. On May 5, 1999, OIG special agents arrested Mr. Burns after tracking him to Chicago. Ultimately, Mr. Burns was sentenced to 21 months in prison and ordered to pay over $62,000 in restitution.

We would like to pursue the thousands of potential identity theft cases that we receive each month. With less than 300 investigators nationwide, however, we lack the investigative capacity to handle the entire volume of identity theft referrals. As a result, we are forced to focus on major cases that directly impact on SSA's operations such as the Wisconsin case. Or, we work collectively through task forces with other law enforcement agencies to make the most efficient use of our resources. One of our toughest challenges is to find realistic strategies to fight this battle in an effective and efficient manner, while remaining focused on SSA's programs.

To that end, our Office of Investigations launched an SSN misuse pilot operation in five major American cities last summer. We partnered with Federal and State law enforcement agencies to target identity crimes and SSN misuse. This allowed us to "bundle" smaller SSN cases for prosecutions -cases that would not typically be prosecuted if presented independently. In less than one year, we have opened 125 investigations which have resulted in 30 convictions to date. U.S. Attorneys' Offices and outside law enforcement entities have enthusiastically welcomed such pilots and have thanked our office for taking the investigative lead.

To prepare for the future, we are developing for our fiscal year 2002 budget submission, an integrated model that combines the talents of our auditors, investigators, and attorneys. If authorized, this group will focus its efforts on developing patterns and trends to better target our audit work, refer cases for investigation, and

liaison with other relevant public and private sector entities. This appears to be the most effective way of using our resources.

Without any change to our current priorities, I believe we have a responsibility to focus our resources on the SSN's integrity as it relates to SSA core business practices. In particular, we need to focus our audit and investigative attention where there is:

1. an apparent failure of SSA's business processes for issuing SSNs;
2. an apparent failure in SSA's wage and reporting systems;
3. a suspicion that SSN cards are being counterfeited;
4. concealment of work activity using false identifications to obtain or maintain eligibility for Federal benefits.

However, this approach will only provide protection for what is SSA's area of responsibility. It will be little consolation to the thousands of identity theft victims, including private industry, whose cases are the responsibility of an array of Federal, State, and local law enforcement. We have a responsibility to participate in this effort as a major partner to whatever extent we are able.

POSSIBLE SOLUTIONS

We have several suggestions for SSA and Congress to consider, in addition to our formal audit recommendations that I have discussed previously:

1. Regulating the sale of SSNs;
2. Prohibiting businesses from refusing services for nondisclosure of an SSN when not relevant to the services being provided;
3. Requiring photo identification when conducting business with SSA;
4. Urging the implementation of new technologies and data bases to help employers, Government, and private industry verify that names and/or SSNs are correct to improve the identification process;
5. Legislating statutory law enforcement authority for our investigators; and
6. Broadening civil monetary penalty authority for the sale or misuse of an SSN.

As I close, I hope I have informed this Subcommittee that we presently cannot investigate every instance of identity theft, while fulfilling our mission to protect SSA's programs from fraud, waste, and abuse. When SSN misuse compromises SSA business processes and the Social Security Trust Funds, our involvement is necessary and vigorous. Even in this context, the magnitude of SSN misuse is vast, and our resources are limited. To focus on our mission, we make tough choices to ensure that we bring the most benefit to SSA. Yet, we often become the court of last resort for victims of identity theft. Therefore, I would appreciate your views on how to fulfill the role that the public seems to expect from SSA and this OIG.

Thank you for the opportunity to appear today to discuss this most important issue. I would be happy to answer any further questions from the Subcommittee.

Chairman SHAW. Thank you, Mr. Huse.

I have one question and then I will yield to Mr. Johnson.

In your six-point solution, you referred to regulating the sale of Social Security numbers. Can you think of any good reason that we should even allow the sale of Social Security numbers?

Mr. HUSE. Mr. Chairman, as the previous witness spoke, there is a great deal of commerce—

Chairman SHAW. I am talking about the sale of it; I am not talking about passing it on. I mean actually getting paid for a list of people with Social Security numbers. To me, there is nothing but mischief involved in such actions.

Mr. HUSE. It is kind of hard to divide between those two uses but I agree with you, the flat sale of our identities to me is deeply troubling, but it does go on. Much of the information we leave on the record as we transact our own personal commerce migrates to these databases that are maintained by businesses and it is a big business.

Chairman SHAW. Yes, sir, but my question is a very pointed one. If you would just answer yes or no and elaborate as you see fit—

can you think of any legitimate reason why somebody would be engaged in the purchase and sale of Social Security numbers?

Mr. HUSE. No, there is no reason.

Chairman SHAW. Thank you. That is a good answer and I agree with you.

Mr. Johnson?

Mr. JOHNSON. I agree with that too. I think it is atrocious.

I wonder if you could tell us, the Federal laws mandate Social Security numbers in food stamp, Medicaid, those kind of programs, what would happen if we said you cannot use them anymore?

Mr. HUSE. It would be very difficult for us to sort out the identity of our recipient and beneficiary population. By default, over time, beginning with when our serial numbers were changed in the military in the 1960s and I was one of those who had a serial number changed over in Vietnam, the Social Security number has migrated to a variety of uses in government. It is not only at the Federal level, it is at the State level, and at local government level too. It is really what sorts us out one from each other.

Mr. JOHNSON. But it was pointed out by the gentleman from Georgia to the gentleman from Ohio that in Texas as well, we use the driver's license number for ID. What is wrong with using that as opposed to the Social Security number?

Mr. HUSE. Nothing whatsoever. I think those are choices that businesses and government can make, but it represents some business cost. There is a convenience issue here that is also attached to this. Perhaps in the future, with new technology, there will be better ways to sort us out one from each other and to identify us as a unique person but we are kind of locked into this by habituation, I think.

Mr. JOHNSON. When you talk about fraud and abuse, with the advent of the Internet and fast communication, do you anticipate more abuse of the Social Security number and the way it is used? Have you seen any of that?

Mr. HUSE. Yes, we have. It is growing—I hesitate to use the word "exponentially" but it is increasing by significant numbers each year. Some of that may be caused by the fact that we are a new agency, only five years old, and our capacity to take these reports gets better each year but the fact of the matter is the numbers have increased. They have gone up in the tens of thousands each year, each of the five years we have been in existence.

Mr. JOHNSON. You do not submit any solutions for our consideration in that arena.

Mr. HUSE. In terms of asking for resources?

Mr. JOHNSON. No, trying to fix the problem. How do we slow it down, without saying you cannot use the Social Security number for any identification?

Mr. HUSE. I think the solutions that I can recommend, there are some huge choices here. No one readily says that the Social Security number is the national identifier. We all are very careful that we do not say that, but in effect, it is. It has become that.

Until something replaces that and facilitates all the rights and freedoms and ability to trade that we have, I don't know that you can suggest anything else responsibly. I don't know that I can. I

agree with you, there needs to be some focus on regulating the use of the Social Security number.

There also needs to be some aggressive deterrence. We need to make examples of the people. We have good laws, the Identity Theft and Assumption Deterrence Act of 1998 is a good law. Before that, we had other good laws that Congress passed in the area of identity fraud, but it is seeing that those laws are enforced that are critical. All of this falls on law enforcement agencies which are already manifestly committed to many things. We need to make this a priority. I think there is an answer in that. I really believe that is the most effective answer, if you make it costly for people to do this.

Mr. JOHNSON. Federal attorneys would probably tell you this is pretty low on the totem pole and they are not going to spend time with it, isn't that true?

Mr. HUSE. It is true because it is hard to get to the bottom of what things of value are lost here. We heard Colonel Stevens and his wife tell us that their reputation has been lost. How do we put a dollar value on someone's reputation?

We receive hundreds of constituent letters from all of the members of Congress with individual stories very much like the Stevens. We have become a court of last resort because they have tried local, State and Federal law and they have been turned aside because their cases did not reach thresholds for prosecution. Yet horrific things happen to these folks. I think that is an area we need to fix too, but again we need some teeth in that. That is why we have asked for the civil money penalties.

Maybe there isn't a case there for a criminal prosecution but we certainly can sanction the people that are causing some of the trouble for these folks.

Mr. JOHNSON. Thank you for your comments. I appreciate them.

Chairman SHAW. Mr. Huse, is there any case law or statutory law to the effect that the numbers issued are the property of the Federal Government? You can supply that to the record.

Mr. HUSE. We may have to check that for the record. I don't know of my own accord.

Chairman SHAW. That is a line of questioning that we have that I think is important to this hearing.

Mr. HUSE. It is regulated in statute but it doesn't say that it is the property of the United States Government.

Chairman SHAW. When somebody dies is their number recycled?

Mr. HUSE. No.

Chairman SHAW. Why aren't you out of numbers?

Mr. HUSE. Again, I would have to ask my actuarial expert. I think there is an infinite possibility still in the issuance of numbers.

Chairman SHAW. Pardon me?

Mr. HUSE. We still have several hundred million to issue yet, so we are not at the point where they need to recycle.

Chairman SHAW. I guess then you will go to using the alphabet or something of that nature.

Mr. Tanner?

Mr. TANNER. Thank you for being here, Mr. Huse.

Did you hear my comment to the lady that testified before you? How does your office interact with the FTC when the FTC gets a complaint or notice that there is a possible identity theft in progress?

Mr. HUSE. We have a great relationship with the FTC. When the Identity Theft and Assumption Deterrence Act was passed making the FTC the clearinghouse for victims reports, we established a very close relationship with FTC and they refer to us those cases they receive that fall under our general jurisdiction.

There are other Federal law enforcement agencies in this also, the Postal Inspection Service, the Secret Service, the FBI, but I would say our relationship with the FTC is probably the closest because we both get into a lot of victim reporting. Sometimes the victim reporting comes to us in our fraud hotline and then we refer that to the FTC. These are relatively new processes, so I hope over time they become more vigorous and abiding.

Mr. TANNER. What happens then to stop it? Where do you go? What happens? Do you go to the FBI, do you go to the State police? How do you try to stop it?

Mr. HUSE. We have our own investigative arm of the Office of the Inspector General, albeit small, they are still Federal agents just like all the others. We actively investigate and bring cases to the Justice Department for prosecution just like other Federal law enforcement agencies.

Mr. TANNER. So you are an investigative, law enforcement agency yourself to go and try to find the perpetrator of an identity theft in progress?

Mr. HUSE. We focus our efforts on those portions that deal with where Social Security's programs are being defrauded or other government benefit programs, or an area where the activity, like sale of SSNs, has an impact on Social Security's business processes, perhaps trying to corrupt the integrity of one of our employees to get these numbers or something. That keeps us pretty busy.

Mr. TANNER. In your unit, you investigate and refer for prosecution individual instances of this?

Mr. HUSE. We do. Also, we do participate in task forces. We have established a number of these as pilot projects around the country with our Federal, State partners, and local partners to try and aggregate the impact that we can have in this area. This is a new attempt too.

Mr. TANNER. I understand your administration hopes to process 97 percent of all Social Security number applications within five days. Do you have the manpower to do that with some level of degree of certainty as it relates to the fact that the person you are actually giving a Social Security number exists and two, it is not somebody else. I mean, 97 percent in five days is a laudable goal but it seems to me if we are going to really research the accuracy of this event in our lives, that is a pretty tall order. Do you have the resources to do that?

Mr. HUSE. In our recent audit work on this issue of the customer service goal Social Security has to issue numbers within five days, we have suggested and recommended in our audit work to SSA that this process is probably too fast. With today's technology and the ability to counterfeit almost anything so that it looks real, we

need to slow down this process to verify the actual breeder documents that go behind Social Security numbers, birth certificates or other documentation.

Mr. TANNER. That was the purpose of my question. Most people now getting Social Security numbers, I would guess are infants. It seems to me waiting 10, 15 even a month to give an infant a Social Security number because you are going to check in some manner that is going to give you a reasonable degree of certainty that this person exists and is the one you want, it seems to me that is not an unreasonable imposition on an infant that is two months old. If I am wrong in that, I stand corrected.

You heard what Colonel Stevens and his wife testified, I assume?

Mr. HUSE. I did.

Mr. TANNER. Do you have any suggestions for us to tell them? I was horrified. This man and his wife's life has literally been ruined through no fault of their own in terms of their plans for their children, grandchildren and so forth. This to me is an outrageous abuse of the system and the system, I think, ought to respond in some manner more than just saying we are really sorry about this, we are going to look into it.

I suggested to him that the people who continue to circulate knowingly false credit reports may be liable if they know and continue to recycle these, the candle being relit all the time I believe is the way he put it.

Do you have any suggestions for people in their circumstance? I would sure like to help them.

Mr. HUSE. It is my understanding that as the Federal Trade Commission's ability to take in these victims' reports, they then would have the civil authority to sanction these entities that improperly recycle bogus credit histories. I think that same power probably should be applied to some of our investigative agencies perhaps in the civil monetary penalty area at least where victims have no other recourse, there needs to be a way to make people pay for recirculating what basically is data garbage.

Mr. TANNER. Does the FTC have that authority, in your opinion, now?

Mr. HUSE. I don't know that for a fact. They regulate but they don't have any enforcement authority, civil enforcement authority.

Mr. TANNER. If they were going to be civilly fined for recirculating this, who would do that?

Mr. HUSE. I am suggesting perhaps in the civil monetary penalty area that we could do that.

Mr. TANNER. Do you have that authority now?

Mr. HUSE. We have some civil monetary penalty authority in some areas, but we are asking for that to be expanded to add that dimension to our array of tools that we could use to help victims.

Mr. TANNER. Have you submitted a suggestion along that line formally to the Chairman and the committee?

Mr. HUSE. I have forwarded it to the Chairman, yes.

Mr. TANNER. I apologize for taking so much time but this is important.

Thank you.

Chairman SHAW. Don't apologize, this is important.

Mr. Portman?

Mr. PORTMAN. If I might follow up on some of the recommendations you made in your testimony today and see if we can get at the next level as to how we would approach this. This story we heard at the beginning from Colonel and Mrs. Stevens has to focus everybody's attention. They are not the only ones, of course. There are people out there all over the place unfortunately having their Social Security numbers stolen and then end up in a living hell which is what they are going through right now.

One of the things you just responded to in Mr. Tanner's questioning was something you testified to, broadening civil monetary penalty authority for the misuse of a Social Security number or the sale of a Social Security number. You said you thought the Social Security Administration might be the place to expand on existing authority. Can you elaborate on that and perhaps provide some more information to the committee regarding that possibility?

Mr. HUSE. I would be glad to do that. I think perhaps it would be better if I refine that a little better in writing and I would be glad to do that.

Mr. PORTMAN. Why don't we do that. I would be interested in it personally but I am sure the subcommittee would like to hear what specifically you would recommend in that regard. Clearly there is not adequate recourse right now for people like the Stevens.

Another recommendation you had is to legislate statutory authority law enforcement authority for your investigators. How would this help to combat Social Security fraud? Is this a Social Security fraud issue or some other issue?

Mr. HUSE. It is Social Security fraud that is the driver for us but Social Security fraud as it rushes into what becomes identity fraud.

Mr. PORTMAN. It is a Social Security number issue?

Mr. HUSE. We have a responsibility as part of this array of Federal, State and local law enforcement because we are at the front end of most of this process, to be a cooperative piece of whatever they do and our ability to task force, to cross deputize local and State law enforcement to participate with us in different investigative endeavors to tackle some of these things and some of them are very complex conspiracies. We can't do that under the existing authorities that we have now. We are deputized United States Marshals; that is the way IG investigators are upholding to the Federal law enforcement family under current rules.

If we had our free-standing statutory authority, as some inspector, general do in the Department of Agriculture and the Department of Defense, we would then have the ability to deputize other sworn law enforcement to help us in these projects. That is the key reason we need it.

Mr. PORTMAN. That is the authority you are looking for?

Mr. HUSE. Yes.

Mr. PORTMAN. Let me go to your other recommendations. One is that people show a photo ID when they are conducting business with the Social Security Administration. This seems like a useful suggestion but I wonder what portion of the population doesn't have a photo ID? Is this a practical solution?

Mr. HUSE. I am not aware of many that don't but I do know it is not a common business practice in Social Security's field operations today.

Mr. PORTMAN. They do not require a photo ID?

Mr. HUSE. They don't. We had evidence a week or so ago before this committee where a woman obtained the ability to become a representative payee without ever showing any identification. She did it over the telephone. These practices in today's world, you can't take people on faith anymore. It is unfortunate but you really need to have more vetting of your identity in a lot of transactions today.

Mr. PORTMAN. This could cut down on fraud in a lot of areas of Social Security, not just in terms of the number. I think it is a useful suggestion.

I also note that Social Security is rightly so doing much more on-line now and you are looking to expand that, like applications for retirement benefits. At least with existing technology, require a photo ID in the context of an on-line service is going to be difficult. How do you reconcile this trend toward more on-line services with a photo ID requirement?

Mr. HUSE. I agree, until we get to the actual visual biometrics that may come in the future, and I think they will. I think our commerce will drive that, for electronic service we are going to need some aspects of public key infrastructure technology to enable us to do business over the Internet or transact business electronically.

Mr. PORTMAN. Both for privacy and fraud reasons?

Mr. HUSE. For both reasons. I think this, of necessity, will limit then the potential of electronic commerce because not everybody is going to be able to have their piece of the public key tradeoff in order to be able to identify themselves. You would have to have some way to do that.

We are going to end up with both tiers of service for a long, long time, person to person and electronic but the electronic will have to be public key infrastructure.

Mr. PORTMAN. I appreciate what you are doing with regard to fraud and also with regard to ensuring people's privacy which in our digital economy is an increasingly troublesome issue to a lot of us and something in the area of Social Security we can make an impact.

Chairman SHAW. Mr. Cardin?

Mr. CARDIN. I very much appreciate your testimony.

I want to concentrate on some of your recommendations. You have recommended that we regulate the sale of SSNs and I hope you are aware of H.R. 1450 by Representative Kleczka. I see that you are, that he has introduced legislation that would prohibit the sale or purchase of any information that includes one's Social Security number less there is a written consent from the individual.

You have also recommended prohibiting business from recusing services for nondisclosure of SSN numbers when not relevant to the services being provided. That provision is included in Congressman Kleczka's bill along with prohibiting merchants from requiring a Social Security number on a check that is used for the purchase of an entity or utility company from asking for SSN numbers on service applications.

You also have suggested broadening the civil monetary penalty authority for the sale or misuse of SSN numbers.

Have you had a chance to review Congressman Kleczka's legislation and do you have a view as to whether what is included in that legislation would help carry out the recommendations you are making to the committee?

Mr. HUSE. The very short answer is we have seen Congressman Kleczka's bill. I believe it is a good start. I think it pretty much addresses the issues I suggest in my recommendations.

Mr. CARDIN. I understand we will have a subsequent hearing and Congressman Kleczka will have a chance to present his bill to our committee. I think your views on pending legislation is very helpful to us. We appreciate the information you made available to us as we try to give the right tools to protect our constituents.

Thank you.

Chairman SHAW. Very quickly, in your testimony you mention 85 percent of the cases you did—if my math is correct, that is 60,000—in 1999 involved the misuse of Social Security numbers. Is that a growing problem and what would be your guess as to the percentage of misuse that ever gets to your attention?

Mr. HUSE. I didn't hear the last.

Chairman SHAW. My question is twofold. One, is this an increasing problem, is 99 more than 98 and the second part of that is what percentage of the cases would you estimate are brought to your attention?

Mr. HUSE. That is a very good question. We have one of the largest hotlines in government and yet we don't really get the whole universe of calls that come to us every day. Each year we have had this capacity increase on the hotline, we have gotten more and more allegations.

The constant, in terms of from the allegations we get, the pieces that involve SSN misuse—

Chairman SHAW. How would someone know to get to you? Has Colonel Stevens come to you or do you know? How would anybody really think to get in touch with your office on this?

Mr. HUSE. We have made the number public. A lot of newspapers have published it.

Chairman SHAW. If I were to call the Social Security Administration and say, someone is using my number, would they refer me to you?

Mr. HUSE. They would gate you over to the hotline.

Chairman SHAW. So that is how you get most of your referrals?

Mr. HUSE. We get a lot of it that way. Others, people just call the 800 number directly.

To answer your question, it is growing. What I cannot answer for you is what the universe is.

Chairman SHAW. Perhaps for the record, you could let us know what the first four or five months of this year, how that curve is looking. If you could supply that for the record, I think it is important we measure that.

Mr. HUSE. We will do that.

Chairman SHAW. This has been a very good hearing. We have called the Pentagon to try to find out the answer to the question I asked to Colonel Stevens. You don't know the answer to that, do you?

Mr. HUSE. We don't know if it is a military regulation but there is no Federal law that requires the use of the Social Security number in the transaction.

Chairman SHAW. I think some people are making some misstatements in that regard and I think we need to let the Congress weigh in on that.

Mr. HUSE. I also wanted to say another piece of the Stevens testimony where they were told there were no Federal laws that applied to the situation in 1997, in effect, there were. We have always had good statutes. What Senator Kyl's bill did was even make it better.

The criminal teeth are there; it is really in the implementation and the coordination of that implementation that we are getting lost.

Chairman SHAW. I would say your staff would be swamped by the numbers you have now so you do not have the personnel to adequately investigate all these cases. That is my guess. I think I am right on that.

Mr. HUSE. You are. We have 300 special agents across the United States. That is far too small a number.

Chairman SHAW. They do more than just this?

Mr. HUSE. Their principal mission is the program fraud that Social Security faces.

Chairman SHAW. So the 60,000 complaints really are not—you don't have the personnel to adequately investigate them all?

Mr. HUSE. We do not.

Chairman SHAW. We will have the response to my question from the Pentagon at the hearing on Thursday which will be a continuation of this hearing. I think this has been very helpful.

I appreciate your testimony Mr. Huse, and all of the witnesses we have had throughout the morning. Thank you.

[Questions submitted by Chairman Shaw, and Mr. Huse's reponses, follow:]

Office of the Inspector General Response to Social Security Number Use and Misuse

1. You mention that a good deal of SSN misuse creates a cost to the Social Security program because people fraudulently apply for benefits. Has anyone estimated the cost of SSN misuse to the Social Security Trust Funds? Has anyone estimated the cost of SSN misuse to private-sector businesses?

To our knowledge, no one has estimated the total cost of SSN misuse to the Social Security Trust Funds (Trust Funds). Additionally, we are not aware of any reliable estimates that reflect the total cost of SSN misuse to private sector businesses.

In its May 1998 report entitled *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited,* the U.S. General Accounting Office (GAO) concluded that identity fraud is very difficult to track. One of the reasons for this difficulty is that identity fraud cuts across many of the statistical categories tracked by law enforcement authorities. We echo GAO's conclusion. Additionally, even though over 80 percent of the allegations and referrals made to our office involve the misuse of an SSN, our limited resources only allow us to investigate a small percentage of these cases. Therefore, our data only illustrates the impact to the Trust Funds and/or private sector entities of those cases we investigated, not the universe of such occurrences.

Since the issuance of GAO's report and the passage of the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act), we have started to redesign our systems to capture SSN misuse referrals in a more defined structure that will delineate SSN misuse by type. Also in response to the Identity Theft Act, other Federal Agencies, such as the Federal Trade Commission, have initiated system en-

hancements that will capture SSN misuse data. Therefore, we would anticipate more thorough statistics in the near future.

2. What are the key vulnerabilities in SSA's business processes relating to the issuance of SSNs? What recommendations have you made and how has the agency responded?

Based on our audit and investigative work, we believe the key vulnerability in SSA's enumeration business process is the Agency's procedures for verifying evidentiary documents submitted with SSN applications. Testimony given at the May 19, 2000, Hearing on the Sale of False Identification Documents via the Internet before the Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, provided evidence of how easily official documents can be counterfeited with today's computer technology. Unfortunately, SSA employees are faced with determining the legitimacy of such expertly counterfeited documents every day. Certainly, we acknowledge that the preponderance of SSN applicants are law-abiding individuals who present valid documents in support of their SSN applications. Nevertheless, we believe this vulnerability is significant because (1) obtaining an SSN is often the first step in committing other identity fraud crimes and (2) once an SSN is issued, SSA has little ability to prevent the misuse of that SSN. As such, we believe it is essential that SSA incorporate more front-end controls in its enumeration process that would help identify counterfeit documents and prevent the improper issuance of SSNs.

Based on our audits and investigations, we identified the following reasons that fraudulent documents are "slipping through the system."

- SSA employees do not have adequate tools (for example, real-time on-line verification mechanisms) to verify the validity of evidentiary documents.
- SSA's emphasis on customer service discourages personnel from employing security measures that might detect fraudulent documents.

SSA has implemented and is planning several initiatives designed to address the use of fraudulent documents in obtaining SSNs. For example, SSA is negotiating the Enumeration at Entry program with the U.S. Immigration and Naturalization Service (INS) and the U.S. Department of State. Under this program, INS and the State Department will collect enumeration data from aliens entering the United States. Additionally, SSA is attempting to negotiate with State Bureaus of Vital Statistics to gain on-line access to verify birth and death records. We applaud these initiatives, however, we believe that they will take several more years to implement.

As such, we recommended that SSA make both policy and procedural changes to ensure the integrity of the enumeration function. We recognize that the recommendations may affect the amount of time necessary to process original SSN applications. However, we believe that if SSA intends to fully address the issues of fraudulent SSN attainment and use, we believe these are investments the Agency should make. Our specific recommendations to SSA include the following:

- Obtain independent verification from the issuing agency for all alien evidentiary documents before approving the respective SSN applications, until the Enumeration at Entry program is implemented.
- Accelerate negotiations with INS and the State Department to implement the Enumeration at Entry program. Once implemented, all non-citizens should be required to obtain their SSNs by applying at one of these Agencies.
- Give credit for fraud detection and development in measuring the performance of field offices and their employees.
- Continue efforts and establish an implementation date for planned system controls that will interrupt SSN assignment in certain suspect circumstances.
- Propose legislation that disqualifies individuals who improperly attain SSNs from receiving work credits for periods that they were not authorized to work or reside in the United States.

In its recent response to our recommendations, SSA agreed to accelerate negotiations with INS and the State Department to implement the Enumeration at Entry program. On June 16, 2000, SSA, INS, and the Office of Management and Budget met to resolve any remaining concerns INS has so that implementation may occur. In its response, SSA also agreed to continue efforts and establish an implementation date for planned system improvements that interrupt SSN assignment in certain suspect circumstances. Due to the extensive systems improvements that will be required, SSA expects to have these controls in place by April 2002.

Although we are certainly encouraged by these planned actions, we regret to report that SSA disagreed with our remaining recommendations, both of which we believe are very important in preventing SSN fraud. SSA declined to obtain independent verification from the issuing Agency for all alien evidentiary documents before approving the respective SSN applications. SSA stated that the Agency already

verifies with INS all documents for noncitizens applying for SSNs, except documents for those who have been in the country less than 30 days. The Agency also responded that, while it is committed to reducing fraud, SSA also has an obligation to provide SSNs to newly-arrived noncitizens who have legal authority to work. SSA believes that delaying approval of their SSN applications for 1 to 2 months until INS can verify their applications would result in a grave disservice to these individuals. Instead, SSA stated that the Agency would continue to work with INS to shorten the lag time needed to update the latter Agency's systems and to have INS collect enumeration data.

SSA also disagreed with our recommendation to propose legislation that disqualifies individuals who improperly attain SSNs from receiving work credits for periods that they were not authorized to work or reside in the United States. SSA stated that the legislative proposal we recommended would be extremely difficult to administer because SSA cannot on its own determine when or if an individual's immigration or work status has changed. SSA believed that these determinations could only be made by INS or a court.

Although we acknowledge SSA's concerns with these recommendations, we do not agree with the Agency's position. We continue to believe that the vulnerability within SSA's enumeration process regarding the possible acceptance of counterfeit alien documents is significant enough to warrant the verification of such documents. Additionally, we believe a delay in the receipt of SSNs for many noncitizens will be inevitable under the Enumeration at Entry program, unless INS makes extensive changes in its processes. We also disagree that the implementation of our legislative proposal would be extremely difficult to administer. It is our contention that it would be the responsibility of the number holder to amend the SSN record if he or she subsequently became eligible to reside and/or work in the United States. In summary, we believe that if the holder of a fraudulently attained SSN applies for SSA benefits, he or she should be required to prove that they have sufficient work credits as a legal worker in the United States before those benefits are approved.

We will continue to work with SSA to resolve these two issues.

3. GAO testified before you that there is no federal law that regulates the overall use of SSNs. Is such a law needed? Is it feasible to enact, administer, and enforce such a law?

There is no doubt that such a law is needed. The abuse of SSNs is possible only when the number is made available to those who would misuse it, and existing law fosters misuse. The most potent tool we have to combat misuse of an SSN at the criminal level is Section 208(a)(8) of the Social Security Act, 42 U.S.C. 408(a)(8), but that statute only prohibits misuse of an SSN in violation of the laws of the United States. In other words, misuse of the SSN becomes a crime only if another crime is committed in the process (i.e., bank fraud).

I am sympathetic, however, to the second half of your question with respect to feasibility. The use of SSNs, legitimate and illegitimate, is so prevalent at this point that regulation would almost certainly bring a hue and cry from many honest industries. However, both the legislative and regulatory processes permit the public to be heard. Indeed, in this instance, their voices would be critical to the process. The use of SSNs is not likely to decrease—as it increases, so will instances of misuse. Only by making the difficult determinations of which uses will be permitted and which will not, can we can cull out those uses which facilitate misuse and criminality.

Certainly before we may outlaw improper uses of the SSN on a significant scale, appropriate uses would have to be identified and regulated. In this respect, the Federal Trade Commission and the Social Security Administration would have to work in concert. Once these difficult determinations are made, and proper SSN uses regulated by one or both of those agencies, it would become a relatively simple matter to provide clear and enforceable criminal, civil, and administrative sanctions against those who misuse the SSN either by putting it to uses that are outside the scope of that regulatory scheme, or by violating that scheme. Any such legislative amendments to the Social Security Act would bring violators within the jurisdiction of this office and the Department of Justice.

While this is by no means an easy task, it becomes more and more daunting with each passing day and each new use (or misuse) to which SSNs are subjected. Therefore, immediate action as contemplated above is critical.

4. GAO testified that many private-sector businesses and government agencies have adopted voluntary policies aimed at protecting privacy and reducing SSN misuse. Can self-regulation be an effective way to reduce SSN misuse?

Although we applaud private-sector businesses and governments that have been instrumental in facilitating the recent reform effort of information privacy issues,

we do not believe self-regulation should be considered the definitive solution in reducing SSN misuse. Our concerns rest with the inability of self-regulated entities to ensure uniform implementation of privacy measures and subsequent compliance. Additionally, we believe it is unlikely that self-regulation by reputable companies or government organizations that already have a fiduciary responsibility to protect the public's interest will significantly curb the current identity fraud crisis.

5. You note that your office issues a list of the 100 employers with the most suspended wage items (i.e., wages that do not match up to an SSN.) What are the reasons why these reported wages don't match up to an SSN? One of your recommendations to the Social Security Administration was to implement a correction action plan for these employers. Has SSA acted on this recommendation?

Our office issued an audit report in which we discussed patterns of reporting errors and irregularities by 100 employers with the most suspended wage items. During this audit, we found that about 55 percent of the wage items in SSA's suspense file either don't have (1) a name; (2) a SSN; (3) a name and SSN; or (4) a valid SSN. About 41 percent have valid SSNs but the names show no relationship to the names on SSA's master file of issued SSNs. Three industries, bars and restaurants, services, and agriculture account for 47 percent of the suspense file. These industries rely on a low skilled, low wage, and highly transient workforce. Nine states account for 70 percent of the suspended items. California alone contributes 31 percent.

Many of the suspense items occur at the earliest point of the wage reporting process, the time of hiring. Some of the reasons for these occurrences are as follows:

- Employers cannot require new hires to show their Social Security cards as a condition of employment. Under present Immigration and Naturalization guidelines, new hires can choose from a total of 27 documents to prove their identity and work eligibility. Presently, SSA can only encourage employers to ask for the Social Security card.
- Many employees whose wages are suspended may be aliens who do not have work authorization from INS and may be providing fraudulent documents to employers. With 27 documents for the employee to choose from, it is virtually impossible for the employer to detect all counterfeit documents.
- Employers are not required by either INS or SSA to verify the validity of documents provided by new hires. Presently, INS and SSA can only encourage employers to enter joint SSA/INS pilot programs and SSA verification programs.
- Employers have no incentive to follow-up with employees to ascertain the correct name/SSN, after SSA has rejected their wage reports. In fact, in many cases it may be impossible to locate the employees because they are no longer employed and have left no forwarding address.
- SSA does not have authority to sanction employers who repeatedly submit incorrect wage reports. Only IRS has this authorization and, to date, the Agency has used this authority only on an extremely rare basis.

In response to our report, SSA agreed to develop a corrective action plan for the top 100 employers contributing to the suspense file. As a part of this plan, SSA has taken or is in the process of implementing the following actions:

- Negotiating with IRS so that 50 of the 100 employers on the OIG list will now be included in IRS' large case audit program and subject to potential incorrect filing penalties.
- Continuing its efforts, now in its third year, of contacting employers with large numbers of suspended wage reports (100 or more items).
- Sent notices to employers in February 2000 for tax year 1999 that included a section informing them about their responsibilities and employee rights.

6. You mention that it costs SSA 50 cents to post a wage item when it is originally submitted compared to $300 to correct it later. Why are the costs to correct wage items so high?

Correcting wage items is a labor-intensive and therefore, expensive process. For example, about 20 million individual wage records initially cannot be matched to SSA's name and SSN records. To resolve these discrepancies, the Agency uses about 27 editing routines in an attempt to properly record wages to the Master Earnings File (MEF), prevent wage items from ending up in the Earnings Suspense File (ESF) and reinstate wage items from the ESF to the MEF.

The Agency uses both manual and electronic validation routines that manipulate wage earners' Social Security numbers (SSN) and/or names in efforts to find record matches. When matches are questionable, researchers use additional wage earners' records to identify possible matches. Some annual routines review the current reporting year and specific tax years. Other routines use the latest system improve-

ments and validation rules to periodically review the entire ESF dating back to 1937. These routines find correct matches from incorrectly reported SSNs or names (or both) when it meets SSA's validation rules.

It is also costly to notify employees and employers of discrepancies. When wage items reach the ESF, the system generates letters, known as Decentralized Correspondence (DECOR.) The main purpose of DECOR is to query individuals in an attempt to resolve SSN and/or name discrepancies. SSA must review responses to these letters to remove items from the ESF for posting to the individual's MEF record. DECOR annually generates and mails about 6.5 million letters.

SSA receives about a 20 percent response rate to these letters and is able to use the information to reinstate suspended wages in about 40 percent of those cases (that is, about 8 percent of the overall DECOR mailing). Another 20 percent are returned to SSA unopened as undeliverable mail. For the remaining 60 percent, there is no recorded response although some may result from telephone calls or visits to SSA field offices.

In addition, SSA employees annually have thousands of contacts with employers to help them report wages correctly. For example, the Agency estimates it received over 200,000 calls from employers in FY 1999.

Despite the Agency's efforts, approximately 5 million wage items cannot be posted to individuals' earnings records for any given year.

7. You mention the Identity Theft Act in your testimony. Are there any other laws aimed at protecting privacy and preventing fraud? In your opinion, are existing laws enforced effectively or do we need new laws to help prevent identity theft and other types of SSN misuses?

Existing laws, and the Identity Theft Act in particular, provide some measure of protection. As a whole, however, SSN misuse represents a significant legislative gap. With some limited exceptions, the criminal and administrative authority in the Social Security Act is aimed at protecting against SSN misuse in terms of misusing the SSN against SSA programs, rather than misuse in a more global context. To that extent, legislation has not kept up with the criminal universe. Certainly in the past, one could argue that SSN misuse was primarily a crime against SSA programs; that is no longer the case. The misuse of the SSN in ways never contemplated has created a situation in which the greater threat is not to SSA programs, but to private citizens and to commerce. The crimes against them being committed through misuse of an SSN have become crimes in which SSA is an unwitting accomplice, in which the integrity of the SSN is systematically violated for criminal purposes. And, even when the SSN misuse is not aimed directly as SSA programs, the misuse still costs SSA in terms of erroneous record-keeping (such as wage reporting) and improperly-paid benefits, as well as by corrupting the SSN itself.

As stated above, it is critical that a universe of appropriate SSN uses be identified and regulated, and that legislation providing criminal, civil, and administrative sanctions for misuse be put in place.

8. Can you please elaborate about the Federal Trade Commission's specific role in SSN misuse?

The Identity Theft and Assumption Deterrence Act of 1998 designated the Federal Trade Commission (FTC) as the clearinghouse for identity theft complaints. In this capacity, FTC indirectly assists identity theft victims by managing information sharing among public and private entities. The specific goals of the FTC's information clearinghouse are to (1) support criminal law enforcement efforts by collecting data in one central database and making referrals as appropriate; (2) provide consumers with information to help them prevent or minimize their risk of identity theft; (3) streamline the resolution of credit and financial difficulties consumers may have when they become victims of identity theft; and (4) enable analysis of the extent of, and factors contributing to, identity theft in order to enrich policy discussion.

To meet these goals, FTC developed a plan that centers on three principal components:

- A *toll-free telephone number* that consumers can call to report incidents of identity theft. Hotline counselors enter information regarding the consumers' complaints into a centralized database—the Identity Theft Data Clearinghouse. In operation since November 1, 1999, the hotline has averaged over 400 calls per week. This information is used to guard against or resolve problems caused by identity theft, and to assist in streamlining the process for the consumer wherever possible.
- The *Identity Theft Complaint Database* is designed to become a comprehensive, government-wide repository of information collected from victims of identity theft. It will also incorporate complaints received by other government agencies, such as

SSA. Consumers can also enter their own complaint information via the public user complaint form at *www.consumer.gov/idtheft.* The clearinghouse will be available to law enforcement agencies at the Federal, State, and local level through a secure, web-based interface allowing them to more effectively track down identity thieves and assist consumers.

• *Consumer education* is provided through both print publications and a website located at *www.consumer.gov/idtheft.*

9. One of your recommendations to combat SSN fraud is to regulate the sale of SSN's. How can this be done? What exceptions would the law have to include? Would there be any downside for consumers?

Again, regulation of the sale of SSN's is one part of the scheme envisioned above, wherein appropriate uses (whether sale, recordkeeping, banking, etc.) are identified and regulated. It is not for this office to determine what uses (or what sales) of an SSN will be appropriate—that is a matter best left to the expertise of the Social Security Administration, the Federal Trade Commission, and the legislative and rulemaking processes. While there may be a downside for consumers, if the process is conducted properly, I am confident that any downside would be vastly outweighed by the greater degree of protection and security that such legislation would provide to the American public.

10. The widespread use of the SSN creates a lot of administrative headaches for SSA, such as reissuing SSNs for people who have been the victims of identity theft. To your knowledge, has SSA ever developed a proposal that addresses this issue, especially one that seeks to limit how the SSN is used by other government agencies and the private sector?

We are not aware of any SSA proposal that would limit how other government agencies and the private sector use the SSN.

11. One of your recommendations for reducing fraud is that people should show photo ID when conducting business with SSA. That seems like a useful suggestion. Still, are there any arguments that some might make against it? Do you know what portion of the population do not have a photo ID? Wouldn't this cut down on fraud in other areas of SSA programs as well?

In proposing this recommendation, we did not intend to infer that photo identification would be feasible in every circumstance. In fact, we acknowledge that a number of exceptions would need to be allowed if SSA adopted this policy. Specifically, although we are unsure what portion of the population does not have picture identification, the numbers could be significant. Those without picture identification may include children, homeless individuals, and refugees. Opponents of this proposal might also argue that counterfeit photo identification is very easily attained and therefore provides little deterrent value. Nevertheless, where available, we believe providing photo identification may prevent some forms of identity fraud.

12. At the same time, SSA is studying conducting certain services online, such as applications for retirement benefits. Obviously, at least for now, showing a picture ID won't work in that setting. How can the trend toward online applications be reconciled with your suggestion of showing a photo ID to receive services?

As stated previously, we do not believe that photo identification is feasible in every situation. Additionally, we do not believe this measure will be a cure-all for identity fraud issues. Certainly, as SSA shifts more of its services online, other identification technologies must be explored. In the interim, however, we believe requiring photo identification when available is a small step towards addressing SSN misuse in SSA programs.

13. One of your recommendations is to legislate statutory law enforcement authority for your investigators. How would this authority for your investigators assist in combating SSN fraud?

My office is, first and foremost, a law enforcement organization. Unfortunately, our authority is not commensurate with our responsibilities. With no independent law enforcement authority, we are limited to the terms of a revocable agreement with the Department of Justice—as a result, many of our policies and practices are less than they could be. For example, we are frequently unable to make the most of limited resources through cross-designation of other law enforcement personnel, because we have no such authority. We are similarly hindered in our cooperative enforcement efforts at the State level because of restrictions in the aforementioned agreement. Statutory law enforcement authority would enable us to maximize our resources to combat SSN misuse.

14. You also suggest broadening civil monetary penalty authority for the sale or misuse of an SSN. Would you provide more details about this recommendation?

The civil monetary penalty authorities provided by Sections 1129 and 1140 of the Social Security Act have proven invaluable tools for both deterring and punishing fraud. We are hopeful to expand that authority beyond false statements and misuse of SSA words and symbols into several additional areas, including the sale or misuse of an SSN. As you know, United States Attorneys are limited in the number of cases they can accept for either criminal prosecution or civil action. Frequently, in the context of Social Security crimes, such decisions are made on the basis of monetary loss to the government. The sale or misuse of an SSN often results in little or no monetary loss to the government, but it is certainly not a victimless crime, as it wreaks havoc with individuals' credit histories and financial well-being, affects commerce, and causes enormous financial losses in the private sector.

With civil monetary penalty authority, my office would have the ability to pursue those offenders that the Department of Justice does not have the resources to pursue and impose fines that would punish those who sell or misuse SSNs, deter similar conduct by others, and at the same time, replenish the Social Security trust fund to compensate for any monetary losses that do affect SSA. By delivering a clear message that the sale or misuse of SSNs is not a crime that goes unpunished, the civil monetary penalty authority would play a critical role in a coordinated assault on SSN misuse.

15. You recommend that new technologies and databases be fostered to help employers, government, and private industry verify that names and/or SSNs are correct to improve the identification process. From a practical standpoint, how would this work? Would opening such a database to employers and private industry create new opportunities for misuse of this information? Who would monitor this process?

SSA currently has a voluntary program, the Enumeration Verification System (EVS) that offers employers a mechanism to match employee names and SSNs with SSA's records. However, employers can only submit a request to SSA on magnetic media, paper, or by telephone. Furthermore, depending on the number of requests, it can take SSA up to 30 days to verify name and SSN requests from employers. Only about 3,000 of about 6.5 million employers nationwide have registered to use EVS and only between 200 and 500 use it in any given year.

To better assist employers in verifying employee names and SSNs, SSA plans to begin a pilot project in July 2000 to provide employers with an on-line employee verification service (OEVS). This service would give employers two options to assist them in verifying employees' names and SSNs through the internet: (1) key in verification requests for an instant response, and (2) transmit a file and receive it from SSA the next business day. SSA believes OEVS will provide employers with quicker name and SSN verification in a more cost-effective manner.

We do not believe that the current EVS or the planned OEVS creates new opportunities for misuse of names and SSNs. SSA currently monitors the process and has various security features, such as PIN and password features, to prevent misuse of the data.

We would also propose expanding the use of EVS or OEVS to permit access to Federal, State, and local law enforcement agencies. Under current law, such agencies cannot verify the names and SSNs of individuals under investigation for a crime except in certain narrow circumstances. We are currently negotiating with SSA to permit to some extent the ability of law enforcement to verify names and SSNs, but even this expanded ability will fall well short of what is permitted by the Privacy Act (5 U.S.C. 552a). Given the prevalence of SSN misuse as a factor in so many different crimes, we would support legislation that would require SSA to comply with the Privacy Act and provide this limited information upon request to law enforcement agencies.

16. For the record, please provide a breakdown of the statistics from the SSA/OIG Hotline for the first six months of this fiscal year. I would like the total number of allegations received by the Hotline; the total number of these allegations related to SSN misuse (of this figure, please break this down further into the number the related to the programs and operations of SSA and the number not so related.)

In the first six months of this fiscal year, the SSA/OIG Hotline received a total of 44,944 allegations. Of these, 37,008 (approximately 82%) involved SSN misuse as the primary or secondary allegation. In 22,408 of these 37,000 cases, SSN misuse was the sole basis of the allegation. The remaining 14,600 cases were program fraud allegations involving SSN misuse.

The hearing is adjourned.
[Whereupon, at 11:59 a.m., the hearing was adjourned.]

USE AND MISUSE OF SOCIAL SECURITY NUMBERS

THURSDAY, MAY 11, 2000

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

The Subcommittee met, pursuant to recess, at 2:09 p.m. in room 1100, Longworth House Office Building, Hon. E. Clay Shaw, Jr. (Chairman of the Subcommittee) presiding.

Chairman SHAW. Good afternoon, and welcome to the second day of our two days of hearings about the use and the misuse of Social Security numbers.

Just about everyone's privacy and financial security depends on seeing these numbers used as intended and not misused. As we learned on Tuesday, the Social Security number misuse is rising fast, with often devastating consequences for families like the Stevens, who testified before us on Tuesday. They have spent years trying to get their identities and good names back. Since Tuesday, people have been calling us from every corner of the country with similar stories about how their Social Security numbers were compromised.

Today, we will learn more about the pluses and minuses of restricting the use of Social Security numbers. First, we will hear from several Members who have proposals, themselves, that go to various lengths to restrict the use of Social Security numbers. After that, we will hear from groups interested in protecting personal privacy, as well as representatives of industry and government agencies that regularly use Social Security numbers in conducting their business.

As I mentioned on Tuesday at our hearing, with the support of the Administration and our colleagues on this panel, we can approve legislation to better protect Social Security numbers from misuse.

Social Security's Inspector General has already made several recommendations. Today we will learn more about these ideas and several others. But we also need to carefully consider the consequences of any actions on this complicated issue. As we look for ways to better protect privacy and security, we must be on the lookout for unintended consequences, which abound in this complex field.

Given the passion on all sides of this issue and the excellent testimony we will hear today, I trust that we will have lots of good advice on how to proceed.

We want to be extraordinarily careful that we do not overreact, but it seems to be very clear, from our hearing of Tuesday, that definitely something has got to be done. Mr. Kleczka's points that were in his bill were referred to by one of our witnesses on Tuesday. It was the Inspector General who set out several points that I think are in Mr. Kleczka's bill.

We will be very interested in hearing what you gentlemen have to say today.

Without objection, all Members will have the privilege of putting opening statements into the record, and at this time we will proceed as they appear on the agenda, with a member of this committee, Mr. McDermott of Washington.

STATEMENT OF HON. JIM MCDERMOTT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mr. MCDERMOTT. Thank you, Mr. Chairman.

I would ask unanimous consent to have my statement put in the record.

Chairman SHAW. Without objection.

Mr. MCDERMOTT. My interest in this started in 1995, when I read an article in the "New York Times" about a man whose son had a medical genetic disease called "Marie-Charcot Tooth Disease." It is a weakness of the upper limbs. The youngster was examined and the family was tested genetically.

Shortly thereafter, after all the medical things had been done, the father lost his auto insurance. No moving violations. No accidents. No nothing. And when he asked, they said, "Well, you have this disease, Marie-Charcot Disease." And he did not have it, but it had been gotten through, somehow, the system.

I began working on that and dropped in a privacy bill in 1995. I think that, as we progress down the way toward the human genome being completed and access to everybody's genetic information will be on the record, you will have enormous potential for abuse in terms of insurance and employment and a whole variety of other things, and the whole issue of privacy is going to come to a head as the human genome project actually gets out into the medical field.

Now, there is a second strand to my concern, and that is in 1996 I went to the democratic convention, and when it was over I came back, and my Secretary said to me, "How are you going to pay for this limousine that you used in Chicago?" And I said, "I did not rent any limousine." Somebody was impersonating me, had rented a limousine, had done all kinds of things all over the city using my name, and they had tried to get into my credit records. They had done all sorts of things.

The fact is that our information is very much open to the public if they want to look.

There was an article recently in the "New York Times" of a meeting that occurred in Seattle, and I would like to report on that in my remaining minutes. It was a meeting of a group called the "Agora." It was convened by a man who is the security person for Regions Blue Shield, which is the insurance company, the Blue Shield plan in Seattle. It includes all the security officers from all the insurance companies, from the police department, from the

sheriff's department, from the Federal Government. It was a room of probably 75 people.

Two months before, he had challenged them. He said, "Here's my name and my birth date. Do anything you can legally and find out everything you can between now and the next meeting."

Well, what happened was they demonstrated everything from the fact that he was in second grade in a particular school, and they showed a picture. They showed the fact that he owed $7.19 to the gas company. They showed his whole driving record. They showed his divorce decree. They showed some scrapes he had had as an adolescent with the law. All of this simply by giving the name and the birth date.

Now, how did they do that? Well, they sent somebody in to pick up a birth certificate. They sent somebody for a credit record. They sent something, and they gradually accumulated it all by using legal methods.

The common thread to most of it was getting his Social Security number. Once they had his Social Security number, they could tie into his bank account, they could tie into the gas company, they could tie into his automobile insurance, they could tie into everything.

The importance of this issue I think is not well understood by the average American. I think that the committee is right to be thinking about this issue. Mr. Kleczka has a bill specifically on that issue. My bill has more to do with medical privacy, which I think is an issue that needs to be dealt with.

I think that this whole question of use of Social Security numbers is central to what we do. My bill on medical privacy would have prevented the use by any medical establishment of your Social Security number as your identifier, so when you go into the hospital, when you go in to apply for your insurance coverage, or whatever, if you give your Social Security number you have opened up your whole life. Anybody who has that number can get into all the places. As the newspaper reported this morning, the voting card that we have from the House of Representatives has at the bottom of it our Social Security number. I mean, it never was intended to be an identification number, but there it is.

I think that whole issue is something that this committee ought to take within its purview, and I commend you for having these hearings. I hope that we can, on a bipartisan basis—because this is not a republican issue or a democratic issue. Everybody has a Social Security number.

Chairman SHAW. You are quite correct.

[The prepared statement follows:]

Statement of Hon. Jim McDermott, a Representative in Congress from the State of Washington

Chairman Shaw, Mr. Matsui, and members of the subcommittee thank you for allowing me to testify today on a topic that has long concerned me, the confidentiality of personal identifying information.

As a practicing psychiatrist for more than 20 years, I can tell you firsthand that a person's confidence that what he or she says will remain private is a crucial component of ensuring he or she fully discloses personal information.

The need to protect the confidentiality of personal information has become even more important given the many new technological advances, particularly in the medical and financial industries. Computers have revolutionized the way informa-

tion is collected, stored, and disseminated. Without adequate, enforceable controls, this information can easily be used to breach confidentiality and to allow discrimination.

With the passage of legislation like the Health Insurance Portability Act and the Financial Modernization Act the public has become increasingly worried that private businesses are building databases of personal information. Many businesses require customers to provide their Social Security number as a condition of doing business. Yet, congress has only imposed superficial walls around our most personal information with no more assurance of confidentiality than to say "trust us." I believe people are right to worry.

Over five years ago I began writing legislation to address the lack of strong national standards for confidentiality of medical records. One of the first issues I worked through is how to identify and de-identify patient information. It was clear that the Social Security number was not confidential. And, that using the Social Security number as an identifier was almost the same as using one's name. I concluded that a Social Security number, or a derivative of a Social Security account number, must not be used for any purpose relating to personal health information or the use or disclosure of such information.

As you know, Congress has grappled for years with when and how the Social Security number should be used. When Congress passed the Privacy Act of 1974 it first attempted to limit the disclosure and use of the Social Security number. Unfortunately, Congress' attempts have been largely unsuccessful.

We have all heard harrowing tales of the misuse of sensitive medial and financial information. The more we hear news reports about confidential personal information getting into the wrong hands the more people will lose confidence in the security of their personal information. This loss of confidence is causing people to think closely about the type and amount of information they disclose as well as how the information will be used.

I'm sure that you remember your constituents' uproar when Health and Human Services Secretary Shalala proposed using a unique health identifier to identify patients. This unsuccessful effort raised awareness of the issue unlike any other recent event. Yet, it was not enough to affect change.

Many states, without notification, list the Social Security number on drivers' licenses. Thus the information from a single piece of identification provides a criminal with the name, address, date of birth, and Social Security number of an individual. This information can easily be used to "steal" an individuals' identity.

Some of you may know, shortly after I visited Chicago for the Democratic Convention in 1996 a individual in Illinois began impersonating me. This individual left a trail of bad checks, scams, and attempts to obtain my credit card information.

I was informed in 1997 only because one of his victims recognized my name. Even though this individual did not obtain my credit information, it took me months to sort out. Luckily, my schedule is regimented so I had documentation of where I was and what I was doing on the days in question.

Place yourself in the shoes of your constituents. How would they learn someone was impersonating them? Most likely, when they are turned down for credit, contacted by a collection agency or the authorities. By which time months, if not years, had passed. Proving who they are, where they were, and what they bought to retailers, financial institutions, and credit bureaus would be an enormous undertaking.

The genie is out of the bottle, it is now our job to mitigate the damage. Clearly, at this point it is impossible to maintain the confidentiality of Social Security numbers. What Congress must do is pass strong laws to protect the confidentiality of medical and financial records.

Thank you.

Chairman SHAW. Mr. Kleczka?

STATEMENT OF HON. GERALD D. KLECZKA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN

Mr. KLECZKA. Thank you, Mr. Chairman.

Let me thank you for your interest in this subject matter, for having the hearing, and for permitting me to come before your subcommittee to share a few comments.

The committee, in yesterday's testimony, heard from the Stevens family and how their identification was stolen. Someone ran up a whole bunch of credit. I had a similar situation with a woman in my District.

The problem that occurs after that fact is the person has to clear their name, themselves. They have to, through whatever means, prove that the purchases on the card were not theirs, and this takes literally hours and years to clean up so finally their record is clear so they can again apply for credit.

What is the key to identity fraud? Well, as you have been told probably yesterday and by Mr. McDermott, the key to establishing fraud or identity in your name is, number one, your Social Security number. That flings open the door to do whatever the unsavory person wants to do.

The second bit of information, if he or she has it, is your mother's maiden name. At that point, not only the door is thrown open, but the windows are thrown open.

Mr. Chairman, I think that part of the problem in our society today is that people ask for this number, our Social Security number, by habit. It has been pointed out that our voting card has a Social Security number on it. For what reason, we do not know. But I discovered, along with my friend, Ron Paul, this was on the card one of the first days of session, so we wrote a letter to the chief clerk and said, "Wait a minute. Why are you putting our Social Security number on our voting card? The voting machine is not going to read it."

Well, his initial answer was, "You gave your okay when you signed up for the card." I said, "Well, I do not recall that." And so then he rechecked, and there was no box to check. It was put on there just by habit.

Checking out some toys—not for myself, but for my nieces and nephews—a Christmas or two ago, I was at the counter and I was giving a check, and the clerk insisted I give my Social Security number. For what reason? It links with nothing that she has at hand to verify that I am the person whose name is on the check. But, Mr. Chairman, this, I think, is being done by habit.

I went to a new dentist to have some dental work done. On the application, "Give us your Social Security number." Well, what I did at Toys 'R Us, I thought of the first ten numbers that came to mind, put it on the check. She smiled. I walked out with a purchase. I did not fill it in for the dentist. I still got the work done and a $2,400 bill.

Something has to be done. People will say, "The horse is out of the barn, Gerry. What are you going to do about it?" Well, Mr. Chairman, walking over here, talking with you, I think we agree that it has to start somewhere, and maybe, yes, these lists are out there, but we have to stop the dissemination and the abuse of these lists being sold, given away, or whatever reason.

For the last couple sessions, I have introduced the Personal Privacy Information Act, PPI Act, H.R. 1450, and it does a few things that I would ask the committee to look at when you draft your response to this problem.

Number one, credit bureaus sell header information in their files. Header information is the information that is most important to

you and I. It is our name, our address, phone number—listed or otherwise—mother's maiden name, Social Security number. And so firms come to the credit union and say, "Okay, I need all the people in California who buy Nike shoes, or who have a very good credit rating and a ZIP code," and they will sell that header information.

My bill prohibits selling that header information in its current form. Yes, if you want to sell a person's name, address, and listed phone number only, but the rest of the things that you have in your file on this person should not and cannot be sold without the authorized explicit consent of the person who is named.

The bill next goes to talk about the use of Social Security numbers for commercial purposes. It prohibits the sale of any list which contains your Social Security number. And the bill further goes on to talk specifically about motor vehicle departments, but they are the biggest abuser. Insurance firms, rating firms, all sorts of other commercial firms can purchase the motor vehicle list from your State motor vehicle department, and on there will be your Social Security number.

The bill I have introduced disallows that bit of information being on there. If they want to sell the name and address, fine, but not the Social Security number.

One of the other things the bill does, which I think is relatively important, if a person refuses to do business with an individual who refuses to give their Social Security number, that is against the law. That would be made a civil crime. Because I do not give Toys 'R Us my Social Security number or the dentist or whoever else, I should not be refused service.

Another good example of that is a constituent who called me saying she is applying for cable service in the city of Milwaukee, and on there was a request for the Social Security number. She refused. They denied cable service. Why does a cable company need your Social Security number?

So, Mr. Chairman, the time has come where, especially with the Internet and disseminating information much quicker, that Congress, I think, has a duty and a responsibility to look at that Social Security number again, restate what the purpose is, and start some legislation to stop the willy-nilly dissemination of our Social Security numbers.

Again, Mr. Chairman, thank you.

Chairman SHAW. I look forward to working with you.

[The prepared statement follows:]

Statement of the Hon. Gerald D. Kleczka, a Representative in Congress from the State of Wisconsin

- Amends the Fair Credit Reporting Act to prevent credit bureaus from giving out identifying information like Social Security numbers, unlisted phone numbers, past addresses, and mothers' maiden names.
- Prohibits the commercial use of a Social Security number without the owner's written consent.
- Prohibits the use of a Social Security number as an identifier by persons not already authorized to do so in current law.
- Businesses that refuse to do business with anyone who does not consent to the use of their Social Security number will be considered as committing an unfair or deceptive business practice.
- Prohibits a state department of motor vehicles from selling or transferring Social Security numbers and photographs.

• Prohibits the distribution of a consumer report for transactions not initiated by the consumer without the consumer's written authorization.
• Prohibits the sale or transfer of a consumer's transaction or experience information for marketing purposes without the express written consent of the consumer.
• Provides for civil and criminal prosecution for violations of the act.

SECTION BY SECTION ANALYSIS OF H.R. 1450, THE PERSONAL INFORMATION PRIVACY ACT

Section 1.Short Title.

The title of this Act is the "Personal Information Privacy Act of 1999."

Section 2. Confidential Treatment of Credit Header Information

Section 2 would add a sentence to § 603(d) of the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681a(d), which defines the term "consumer report" for purposes of the FCRA. The term currently means, essentially, any communication of information by a consumer reporting agency about a consumer that is used or expected to be used as a factor in establishing the consumer's eligibility for credit, insurance, employment, or for any other legitimate business purpose. Under § 604 of the FCRA, 15 U.S.C. § 1681b, a consumer reporting agency may not furnish a consumer report except for specified purposes. The new sentence that § 2 would add to the definition of "consumer report" provides: "The term also includes any other identifying information of the consumer, except the name, address, and telephone number of the consumer if listed in a residential telephone directory available in the locality of the consumer." If this new sentence becomes law, then consumer reporting agencies would be prohibited from disclosing such identifying information except for a purpose specified in § 604.

Section 3. Protecting Privacy by Prohibiting Use of the Social Security Number for Commercial Purposes Without Consent.

This section would add a new section to the general administrative provisions of Title 11 of the Social Security Act, 42 U.S.C. § 1301 et seq., prohibiting persons from buying or selling any information that includes an individual's social security account number ("SSN"), without the written consent of the individual. In addition, no person may use an individual's SSN for identification purposes without the written consent of the individual. In order for consent to be valid, the person desiring to use an individual's SSN must inform the individual of all the purposes for which the SSN will be utilized, the persons to whom the number will be known, and obtain the individual's consent in writing.

These new prohibitions would not affect any statutorily authorized uses of the SSN under § 205(c)(2) of the Social Security Act, 42 U.S.C. § 405(c)(2) (SSN used for Social Security wage records, and for various enumerated purposes by federal agencies and state and local governments), § 7(a)(2) of the Privacy Act of 1974 (5 U.S.C. 552a note) (authorizing state and local governments to require disclosure of an individual's SSN if required by federal law or if the required disclosure was pursuant to a system of records in effect prior to January 1, 1975), or 26 U.S.C. § 6109(d) (an individual's SSN is used for all identifying purposes specified in the Tax Code).

Individuals are authorized to bring a civil action seeking equitable relief and damages in a U.S. District Court for violations of this section. Damages may include the greater of actual damages or liquidated damages of $25,000, or, in case of a willful violation resulting in profit or monetary gain, $50,000. The court may assess, against the respondent, reasonable attorney's fees and other litigation costs in cases where an individual prevails. A statute of limitation of 3 years is provided. The remedies provided by this section are in addition to any other lawful remedies available to an individual.

The Commissioner of Social Security is authorized to assess a civil money penalty of not more than $25,000 for each violation of this section, or in the case of violations found to constitute a general business practice, not more than $500,000. The enforcement procedures for civil money penalties are the same as set forth in section 1128A of the Social Security Act, 42 U.S.C. § 1320a097a(d),(e),(g),(k),(l) and the first sentence of (c). These set forth the criteria for determining the amount of the civil penalty, the investigation and injunction authority of the Commissioner, and courts of appeals review of civil money penalty determinations. Also applicable are the provisions of section 205(d) and (e) of the Social Security Act, 42 U.S.C. § 405(d) and (e), which authorize the Commissioner of Social Security to issue subpoenas during investigations, and provide for judicial enforcement of such subpoenas.

The Commissioner of Social Security is directed to coordinate enforcement of the provisions of this section with the Justice Department's enforcement of criminal provisions relating to fraudulent identification documents, and with the Federal Trade Commission's jurisdiction relating to identity theft violations.

The provisions of this section do not preclude state laws relating to protection of privacy that are consistent with this section. The effective date of this section would be two years after enactment of this bill.

If a person refuses to do business with an individual because the individual will not consent to disclosure of his or her SSN, then such refusal will be considered an unfair or deceptive act or practice under section 5 of the Federal trade Commission Act (15 U.S.C. § 45). The Commission may issue a cease and desist order, violation of which is subject to civil money penalties of up to $10,000 per violation.

Section 4. Restriction on Use of Social Security Numbers by State Departments of Motor Vehicles.

18 U.S.C. § 2721(b) sets forth permissible uses of personal information obtained by a state department of motor vehicles. This section provides that, with respect to the SSN of an individual, such personal information may only be disclosed to a government agency, court or law enforcement agency in carrying out its functions to the extent permitted or required under section 205(c)(2) of the Social Security Act, 42 U.S.C. § 405(c)(2), section 7a(2) of the Privacy Act of 1974, 5 U.S.C. § 552a note, section 6109(d) of the Internal Revenue Code, or any other provision of law specifically identifying such use. This section would also prohibit the disclosure of SSNs by state departments of motor vehicles for bulk distributions for surveys, marketing or solicitations purposes.

Section 5. Restriction on Use of Photographs by State Departments of Motor Vehicles.

Section 5(a) would add a new subsection to 18 U.S.C. § 2721, which currently generally prohibits the release of certain personal information from state motor vehicle records. This new subsection would prohibit the release of an individual's photograph, in any form or format, by a state department of motor vehicles without the express written consent of the individual. An exception would be permitted for disclosure of an individual's photograph to a law enforcement agency of any government for a civil or criminal law enforcement activity if authorized by law and pursuant to a written request.

Section 5(b) would make technical amendments to 18 U.S.C. § 2721(a) and (b) to conform that section to the new provisions added by this section. It would also amend 18 U.S.C. § 2722(a) to reference the new subsection (e) added by this section.

Section 6. Repeal of Certain Provisions Relating to Distribution of Consumer Reports in Connection with Certain Transactions Not Initiated by the Consumer.

Section 6(a) would amend § 604(c) of the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681b(c), which governs prescreening to determine a consumer's eligibility for credit or insurance. Prescreening is a practice whereby a user of consumer reports, such as a lender or insurer, contacts a consumer reporting agency without having received an application for credit or insurance from a particular consumer. The user might submit a list of names and ask the agency to identify persons on the list who meet criteria that the user specifies. Or it might ask the consumer reporting agency to create its own list based on the user's criteria. Section 604(c) currently prohibits prescreening, except in two situations, to determine a consumer's eligibility for credit or insurance. It prohibits, in other words, except in two situations, a consumer reporting agency from furnishing a report on a consumer who has not applied for credit or insurance.

The two situations in which it permits prescreening are when: (1) the consumer authorizes the consumer reporting agency to provide the report, or (2) the lender or insurer will make a firm offer to the consumer if prescreening shows the consumer eligible for credit or insurance, and the consumer has not previously asked to be excluded from prescreening done by the consumer reporting agency. Section 6(a) would, in effect, prohibit prescreening in connection with credit and insurance except when authorized by the consumer. It would amend § 604(c)(1) to provide that a consumer reporting agency would be permitted to furnish a consumer report in connection with a "credit or insurance transaction that is not initiated by consumer only if the consumer provides express written authorization in accordance with paragraph (2) . . . ." "Paragraph (2)" refers to § 604(c)(2) of the FCRA, which would be rewritten by § 6(b) of the bill.

Section 6(b) would rewrite § 604(c)(2) to provide: "No authorization referred to in paragraph (1) [§ 604(c)(1)] with respect to any consumer shall be effective unless the consumer received a notice before such authorization is provided which fully and

fairly discloses, in accordance with regulations which the Federal Trade Commission and the Board of Governors of the Federal Reserve System shall jointly prescribe, what specifically is being authorized by the consumer and the potential positive and negative effects the provision of such authorization will have on the consumer." The regulations would have to require that the notice be prominently displayed on a separate document or, if the notice appears on a document with other information, that it be clear and conspicuous.

Section 6(c) would repeal the provision, mentioned above, that allows consumers to exclude themselves from prescreening lists. The provision would be unnecessary if prescreening were prohibited except when a consumer had authorized it.

Section 7. Sale or Transfer of Transaction or Experience Information Prohibited.

Section 7(a) would add a new § 626 to the FCRA. New § 626(a) would provide: "No person doing business with a consumer may sell, transfer, or otherwise provide to any other person, for the purpose of marketing such information to any other person, any transaction or experience information relating to the consumer, without the consumer's express written consent." A consumer's consent would not be required for the sale, transfer, or provision of transaction or experience information for a purpose other than marketing.

New § 626(b) would define "transaction or experience information" as "any information identifying the content or subject of 1 or more transactions between the consumer and a person doing business with a consumer . . . ." Section 626(c) would allow six exceptions, where a consumer's consent would not be required for the provision of transaction or experience information: (1) communications "solely among persons related by common ownership or affiliated by corporate control," (2) information provided pursuant to court order or federal grand jury subpoena, (3) "[i]nformation provided in connection with the licensing or registration by a government agency or department, or any transfer of such license or registration, of any personal property bought, sold, or transferred by the consumer," (4) "[i]nformation required to be provided in connection with any transaction in real estate," (5) "[i]nformation required to be provided in connection with perfecting a security interest in personal property," and (6) "[i]nformation relating to the amount of any transaction or any credit extended in connection with a transaction with a consumer."

Section 7(b) would make a technical amendment to § 603(d)(2)(A) of the FCRA to ensure that it does not conflict with new § 626, and § 7(c) would make a clerical amendment to add a reference to new § 626 to the table of sections for the FCRA.

Chairman SHAW. Mr. Markey?

STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. Thank you, Mr. Chairman, very much, and thank you for focusing upon this critically important issue.

Points that Mr. McDermott and Mr. Kleczka have already made are going to, obviously, be further embellished upon by the other Members of Congress who are going to testify before you today.

What I would like to do, though, is to just step back here for a second and look at why it is so important for us to have this conversation.

We are at the dawn of a new era. It is the Internet era. I think that is why so many people are so concerned.

But put it in context. In the last quarter of 1999, of the $875 billion worth of retail sales in the United States, only $5 billion of that was on line. So at this point it is only 7/10ths of 1 percent of all commerce in the United States, all retail commerce.

The concerns which ordinary Americans have are reflected by the fact that increasingly on line they are asked to put these identifying numbers into the computer, but without any guarantees that

that information—that Social Security number or any other information which they are providing—cannot be reused for other purposes. that is why it becomes so much of a concern to people.

Now, I happen to believe that one of the things which the online industry is going to have to do is recognize the fact that the reason they are only at 5 billion out of 875 billion in the last quarter of 1999 is that many Americans just do not want to give out all that information without some guarantee that it is not going to get compromised.

Yes, we want the new revolution, but we want the new economy with old values. We want the new technologies animated by the old values. It is a merger of the old with the new that ultimately is going to result in the production of this new economy.

Commerce with a conscience—that is what the American people want.

Now, if an ordinary American goes up to the ATM machine and they punch in their little secret number and then they push in the number for the $50 they are trying to extract, when out comes their receipt, they do not throw it in the bucket that is right there because they do not want anyone to know what their Social Security number might be or what their bank number might be or how much money they took out. But that very same person, as a condition of banking with a large financial institution, has to basically cede the right to have that information used for purposes that they would never have wanted it to be used—all the information that is on the check about the illnesses of your children or your parents or your wife or yourself, or any financial transaction that you might have engaged in. You might not even have told your spouse, much less everybody else in the neighborhood, about one of these transactions.

So most people are naturally quite protective of their privacy and they want rules put in place to ensure that the Social Security number does not become a universal identifier that allows data miners to be able to, with access of your Social Security number and your mother's maiden name or all the other clues that you are forced to give up, to be able to go and find everything that ever happened to you—in fact, a more-comprehensive compilation of your life than anyone else in your family might know about you, including a lot of stuff you might have forgotten, for them to then use this as a product that they market to hundreds of companies across the globe, in terms of their ability then to bring those products that are of interest to them into your home, but using your personal, private family secrets.

So, Mr. Chairman, you cannot have a more important hearing than this, because there is a Dickensian quality to this new technology. It is the best of wires and the worst of wires simultaneously. It has the ability to enable and to ennoble, but it also has the power to degrade and to debase.

I think what is going to happen is that the American public is going to demand that their family's privacy be allowed to be protected and that this is going to become the number one civil rights issue of the next 10 years in the United States, and the concern about the issue will rise concomitantly with the rise of retail commerce online in our country.

I think we have a chance to engage in a bit of anticipatory democracy, putting in place today the protections which the public is going to need in the years ahead to ensure that their family's most intimate secrets are not made a product that hundreds of marketers use, regardless of the impact it might have upon that family's psychological, physical, financial, or medical well-being.

I cannot compliment you enough, because ultimately the key to all of this is the Social Security number, because that has become the way in which the door is opened so all of the other clues to who we are are able to be found.

I just want to contrast it with the world in which we grew up in, very briefly, which is the world in which the nurse or the doctor that we went to when we were children had our medical record around their neck, and it was just between us, our mother and father, and the doctor and the nurse. Or we went into the bank, and all it was was the man behind the counter who showed us how the miracle of compound interest would help us if we kept putting money in each month from our paper route, or the money that we earned doing chores at home for our moms and our dads.

Well, today those doctors work for HMOs. Those bankers work for some large conglomerate. They do not protect your privacy any longer, in the absence of laws being put on the books that ensure that the privacy keepers are not replaced by the privacy peepers, the data mining reapers who see us all as just sources of profit for them rather than individuals with families who need the protection of their privacy.

I thank you, Mr. Chairman, very much, for holding this critically important hearing.

Chairman SHAW. Thank you for a very thoughtful presentation.

[The prepared statement follows:]

Statement of Hon. Edward J. Markey, a Representative in Congress from the State of Massachusetts

Mr. Chairman and Members of the Subcommittee, thank you for allowing me to testify before you this afternoon.

What I would like to do is try to put the matter of the privacy of a consumer's Social Security Number into the broader context of how consumer information is being used by businesses as we proceed into the e-commerce era.

We are told that e-commerce is qualitatively different, qualitatively better than bricks & mortar commerce. Right now, only $5 Billion of the $860 Billion in annual sales currently occur over the Internet. But that figure will continue to grow exponentially in the future. So, the question we must ask, is how are we going to adjust our laws to deal with that new reality? What are we going to do about the laws dealing with privacy, fraud, pornography, pharmaceuticals, alcohol, gambling, and sales taxes? How do we animate the new economy with the old values?

The problem that we face today isn't Big Brother; it's Big Browser. Right now, when it comes to your financial records, there are very few protections against a financial services firm from disclosing every check you've ever written, every credit card charge you've ever made, the medical exam you got before you received health insurance. And as you surf the Web, there are no rules in place to prevent various web sites from collecting information about what sites you are viewing and how long you are viewing them. If you buy anything over the Internet, that information can be linked up to other personal identifiers to create disturbingly detailed digital dossiers that can profile your lifestyle, your interests, your hobbies, or your habits.

Clearly, the Social Security number is an important identifier that many online and offline businesses wish to obtain about consumers. But consumers who value their privacy, have a strong interest in not allowing this number to become a ubiquitous personal identifier and allows companies to tie together bits and pieces of information in various databases into an integrated electronic profile of their interests and behavior that can be zapped around the world in a nanosecond.

There are even more sinister possibilities. 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, with social security numbers for other citizens, or to link 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 are offering these services obtaining these numbers? In all likelihood, they are accessing information held by credit bureaus, financial services or other commercial firms.

If someone actually obtains a Social Security number from one of these sites, they have an important piece of information that can be used to locate the individual or get access to information about the individual's personal finances. For example, if you have a social security number, and can also obtain access to certain other readily available information about an individual, such as the individual's mother's maiden name or their date of birth, you can sometimes get a bank to provide you with detailed information about the individual's personal finances over the phone. Now, that practice, known as pretexting, is already against the law. But that does not mean that it does not occur, or that unscrupulous individuals are not obtaining access to Social Security numbers and then using them to perpetrate identity thefts that can destroy the credit or reputation of innocent consumers.

Now, last year's banking bill gave consumers the right to "opt out" of having their personal, nonpublic financial information transferred to unaffiliated third parties. The term "personal, nonpublic financial information" would include a consumer's Social Security number. This means that a financial institution would not be able to provide a social security number to a nonaffiliated third party who had opted out. However, there are no limits on disclosures to affiliates. Furthermore, there's a "joint marketing agreement" provision that allows disclosures of a customer's information (including a Social Security number) to nonaffiliated third parties with which the institution has signed a contract. These two loopholes render the limited "opt out" requirements in the bill a pathetic joke. And this week, we have learned that the financial regulators have decided to delay full implementation of even these minimal privacy protections until July, 2001.

We need to do more. Right now, under current law, we have an "opt-in" for a tax preparer transferring your tax return to any other party. We have an opt-in before drivers license information can be transferred. We have an opt-in for information about videocassette rentals. We have an opt-in for cable TV viewing habits. We have an opt-in for telephone call records. We have an opt in for information about cell phone whereabouts. But we do not have an opt-in for sensitive financial information and for certain medical information.

In order to remedy this situation, Representative Joe Barton (R09TX) and I have introduced H.R. 3320, the "Consumer's Right to Financial Privacy Act," which would close the affiliate sharing and joint marketing loopholes and require an "opt in" before a financial institution could disclose sensitive financial information -including Social Security numbers. Our bill currently has 71 bipartisan cosponsors, and has been introduced in the Senate by Senators Richard Shelby (R09AL) and Richard Bryan. In addition, I have also joined with Representatives John LaFalce (D09NY) and John Dingell (D09MI) in introducing the Administration's privacy proposal, H.R. 4380, which would establish an "opt in" for medical information and sensitive information about a consumer's spending habits, and an "opt out" for the disclosure of other nonpublic personal information about the consumer.

I urge the Subcommittee to support these legislative reforms, and also the proposal by my colleague, the gentleman from Wisconsin (Mr. Kleczka) to prohibit commercial distribution or acquisition of Social Security numbers, or their use as a personal identifier.

Thank you, again, Mr. Chairman, for allowing me to testify today. I look forward to working with you and other Members of the Subcommittee to address the current risks to consumer privacy.

Chairman SHAW. Mr. Hostettler?

STATEMENT OF HON. JOHN N. HOSTETTLER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF INDIANA

Mr. HOSTETTLER. Mr. Chairman, thank you for this opportunity to share with you and members of the committee. I am pleased to come before you today in support of my bill, H.R. 2494, the Chil-

dren Tax ID Alternative Act. This bipartisan bill, which currently has 23 cosponsors, would provide a religious exemption for those who do not wish to obtain a Social Security number for their children. It would remove the barriers that exist to those who choose to exercise their religious beliefs by not attaching Social Security numbers to their children.

The Children Tax ID Alternative Act would simply provide an alternative way of claiming dependent tax credits and deductions for these families.

This subcommittee has been hearing testimony regarding expanding use of Social Security numbers and the associated use and abuse that accompanies such an expansion. There are, however, a significant group of American citizens who are resisting this progression because it violates their religious beliefs. These are honest, law-abiding citizens who pay their taxes and promote the laws and principles of our civil order. They are the public school teacher in Oregon, the minister in Washington, the professor of a State university, as well as State representatives, yet, because they choose to follow the dictates of their religion, they pay substantially more income tax than do their neighbors.

The history of the use of Social Security numbers indicates that this has not always been a problem and need not be a problem any more. It was not until the Tax Reform Act of 1986 that taxpayers who wished to claim exemptions for dependents were required to provide Social Security numbers for all dependents ages five and older. This age requirement was changed in 1995 to require that any claimed dependent have a taxpayer identification number, which, under section 6109 of the IRS code, is an individual's Social Security number.

Finally, in 1996, the IRS was authorized to reject a dependency exemption if no taxpayer identification number was supplied.

What are the implications of these laws? As a result of the changes made by the Tax Reform Act of 1986, the IRS reported that there were approximately 7.5 million fewer dependents claimed in 1987 than 1986. Instead of the estimated 77 million dependency exemptions, the IRS reported that only 69.7 million such exemptions were claimed. This translated into a revenue increase of $2.8 billion for the Federal Government in tax year 1987, alone.

The IRS has indicated that the significant drop in claimed exemptions is, in fact, due to the required use of Social Security numbers; however, they believe that the exemptions dropped because the use of the numbers eliminated the potential for fraud and abuse.

The IRS is unable to conclusively assert this finding because no study or report has been conducted to determine the actual reason for this significant drop. Rather, we have every indication that this drop was due, at least in some degree, to personal religious objections by parents who do not wish to attach Social Security numbers to their children.

While there may be disagreements and varying opinions about the levels of causation concerning these statistics, it cannot be denied that the drop is due, at some level, to religious objections. Simply put, families who hold to such religious beliefs are being forced to pay for their right to exercise their religion.

I understand that these laws were implemented in order to curb the use of improper dependency exemptions; however, I would also like to point out, Mr. Chairman, that my bill does not add to the potential for tax fraud and abuse. Under the provisions of this bill, parents seeking to receive a deduction or credit for children without Social Security numbers would be required to submit several forms of official documentation. Only by providing: one, an affidavit describing the religious belief; two, an affidavit from a knowledgeable third party; and, three, documentation such as birth records, medical records, school records, or insurance records to verify the relationship of the dependent to the taxpayer, would these families be able to claim the exemptions.

Such an exemption is not without precedent. There are currently a number of U.S. citizens who are permitted to be exempt from participation in Social Security based on their religious beliefs. There is also an allowance for certain ministers and members of religious orders to be exempt from self-employment taxes on income for those who are opposed to these insurance programs. However, there are no exemptions for those who fail to provide a taxpayer ID number when it is required on a tax return. This is precisely what my bill seeks to address.

As our laws stand, many families have voluntarily forfeited thousands of dollars worth of legitimate dependent deductions rather than violate their religious beliefs. I find it unjustifiable that our Government would force its citizens to make that choice, yet we persist in doing just that.

My bill, H.R. 2494, would restore fairness to our tax code by doing away with this injustice and protecting the religious beliefs of all American taxpayers.

Thank you, Mr. Chairman, once again for this opportunity.

Chairman SHAW. Thank you.

[The prepared statement follows:]

Statement of Hon. John Hostettler, a Representative in Congress from the State of Indiana

Mr. Chairman, I am pleased to come before you today in support of my bill HR 2494, the Children Tax ID Alternative Act. This bipartisan bill, which currently has 23 cosponsors, would provide a religious exemption for those who do not wish to obtain a Social Security number for their children. It would remove the barriers that exist to those who choose to exercise their religious beliefs by not attaching Social Security numbers to their children. The Children Tax ID Alternative Act would simply provide an alternative way of claiming dependent tax credits and deductions to these families.

This subcommittee has been hearing testimony regarding the expanding use of Social Security numbers and the associated use and abuse that accompanies such an expansion. There are, however, a significant group of United States citizens, who are resisting this progression because it violates their religious beliefs. These are honest, law-abiding citizens who pay their taxes and promote the laws and principles of our civil order. They are the public school teacher in Oregon, the minister in Washington, the professor of a state university as well as state representatives. Yet, because they choose to follow the dictates of their religion they pay substantially more income tax than their neighbors.

The history of the use of Social Security numbers indicates that this has not always been a problem and need not be a problem anymore. It was not until the Tax Reform Act of 1986 that taxpayers who wished to claim exemptions for dependents were required to provide Social Security numbers for all dependents age 5 and older. This age requirement was changed in 1995 to require that any claimed dependent have a taxpayer identification number, which under Section 6109 of the Internal Revenue Code, is an individual's Social Security number Finally, in 1996, the IRS

was authorized to reject a dependency exemption if no taxpayer identification number was supplied.

What are the implications of these laws? As a result of the changes made by the Tax Reform Act of 1986, the IRS reported that there were approximately 7.5 million fewer dependents claimed in 1987 than in 1986. Instead of the estimated 77 million dependency exemptions, the IRS reported that only 69.7 million such exemptions were claimed. This translated into a revenue increase of $2.8 billion for the federal government in tax year 1987 alone. The IRS has indicated that the significant drop in claimed exemptions is, in fact, due to the required use of Social Security numbers. However, they believe that the exemptions dropped because the use of the numbers eliminated the potential for fraud and abuse. The IRS is unable to conclusively assert this finding because no study or report has been conducted to determine the reason for this significant drop. Rather, we have every indication that this drop was due, at least in some degree, to personal religious objections by parents who do not wish to attach Social Security numbers to their children. While there may be disagreements and varying opinions about the levels of causation concerning these statistics, it can not be denied that the drop is due at some level to the religious objections. Simply put, families who hold to such religious beliefs are being forced to pay for their right to exercise their religion.

I understand that these laws were implemented in order to curb the use of improper dependency exemptions. However, I would also like to point out, Mr. Chairman, that my bill does not add to the potential for tax fraud and abuse. Under the provisions of this act, parents seeking to receive a deduction or credit for children without Social Security numbers would be required to submit several forms of official documentation. Only by providing 1). an affidavit describing their religious belief, 2). an affidavit from a knowledgeable third party and 3). documentation, such as birth records, medical records, school records or insurance records to verify the relationship of the dependent to the taxpayer, would these families be able to claim the exemptions.

Such an exemption is not without precedent. There are currently a number of U.S. citizens who are permitted to be exempt from participation in Social Security based on religious belief. There is also an allowance for certain ministers and members of religious orders to be exempt from self-employment taxes on income for those who are opposed to these insurance programs. However, there are no exemptions for those who fail to provide a taxpayer identification number when it is required on a tax return. This is precisely what my bill seeks to address.

As our laws stand, many families have voluntarily forfeited thousands of dollars worth of legitimate dependent deductions rather than violate their religious beliefs. I find it unjustifiable that our government would force its citizens to make that choice. Yet, we persist in doing just that. My bill, HR 2494 would restore fairness to our tax code by doing away with this injustice and protecting the religious beliefs of all American taxpayers.

Chairman SHAW. Mr. Paul?

STATEMENT OF HON. RON PAUL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. PAUL. Thank you, Mr. Chairman.

I would like permission to insert my printed statement in the record.

Chairman SHAW. Without objection, the full statement of all the witnesses will be inserted.

Mr. PAUL. Along with a statement from the Liberty Study Committee. Unanimous consent to put that in the record, as well.

Chairman SHAW. I, too, am grateful that you are holding these hearings, because I think privacy is a very important issue, and we are going to hear more and more of it.

I think it came to the attention of the public and to many in our regulatory bodies when "know your customer" regulations were proposed a year or so ago, and, with a little bit of encouragement, there were over 500,000 comments sent to the Federal Reserve and

the FDIC because these were regulations that were way over-stepping and ignoring the privacy of the individual.

I take a little different approach to the issue of privacy than others, but I think that there is a common thread among us that the solution is going to be found somewhere in dealing with the Social Security number, and for that reason I am encouraged.

In 1974 the Privacy Act was written to combat some of the things the Bank Secrecy Act did in 1970. The Privacy Act was designed to say you cannot use the Social Security number as an identifier. But then, like so often in our legislation, later on in the bill it said, "But Congress can make use of the Social Security number any time they want," and we certainly have been doing that since then. I think that is where the serious problem is.

But where I disagree with some of my friends who will write more legislation, I think there is a certain part of privacy that should be dealt with in the marketplace. For instance, I do not believe that Congress should write a law compelling the Sierra Club and the ACLU to deal with their memberships and have them fill out a form and get permission before they can rent lists or do anything, because the more information they collect the more likely it is that information will go to the Government and then abused by possibly their political enemies.

So I am not in favor of more regulations. For instance, the bank bill that we passed last year said that the bank would have to ask questions about privacy—again, accumulation of more material.

The real problem I see is the Social Security number, the universal identifier. It is true, in the old days medical privacy was taken care of much better, but now that we have government-mandated health care programs and health management, yes, it is convenient for government to be more efficient. But the question is, do we want to weigh the two? Can you always argue the case for efficient government and at the same time protect privacy? I think there is a conflict there. But our goal should be the privacy. The goal of privacy should override the efficiency of government, and I think that sometimes is where we slip on this.

Just providing new rules I think can be very, very damaging to us, and we should not just ask the government or ask these organizations to provide more forms to fill out, because that invites abuse.

My bill, H.R. 220, addresses this. This is where I am hoping more of us can come together. It does more or less state what the law in 1974 states, but it has the force of law, that you cannot use the Social Security number as a universal identifier. It was not intended. We never even used Social Security numbers on our tax forms until the early 1960s. There is no reason that we cannot pass something like this.

If we are concerned about identity theft, the best thing we can do for those who steal identities is to have all our information brought together by the universal identifier.

So the most important thing that we could do to stop identity theft is to make sure that there is a law on the books, that we live by it, and that we do not have a universal identifier. It will be and is the Social Security number. It is universal. I delivered babies in my professional life, and it is true, in the last several years we

were required—everybody was getting Social Security numbers before the baby left the hospital. Everybody wants to know everything about everything, and the most important way they accumulate this information and can find out information on us is the Social Security number.

So if it makes government a little less efficient, I think that might have to come about. I do not believe you can demand the efficiency that some people would like on government programs at the same time saying that we will protect our privacy. There will have to be a choice. Of course, my choice is for privacy and my choice, of course, would be to pass H.R. 220, and there could be no universal identifier for any of our programs.

I thank the chairman.

Chairman SHAW. Thank you, Mr. Paul.

[The prepared statement and an attachment follow:]

Statement of Hon. Ron Paul, a Representative in Congress from the State of Texas

Mr. Chairman, thank you for holding a hearing on the important issue of the misuse of the Social Security number as a uniform standard identifier. For all intents and purposes, the Social Security number has been transformed from an administrative device used to administer the Social Security program into a de facto national ID number. Today, most Americans cannot get a job, get married, open a bank account, or even get a fishing license without their Social Security number. Many hospitals require parents to obtain Social Security numbers for their newborns before the hospital will discharge the baby. Moreover, many jurisdictions will not issue a death certificate without obtaining the deceased's Social Security number.

The Congress that created the Social Security system in no way intended to create a national identifier. In fact, Congress never directly authorized the creation of the Social Security number—they simply authorized the creation of an "appropriate record keeping and identification scheme." The Social Security number was actually the creation of the Internal Revenue Service!

The Social Security Number did not become a popular identifier until the 1960s. In response to concerns about the use of the Social Security number, Congress passed the Privacy Act of 1974, because "The Congress finds the opportunities for an individual to secure employment, insurance and credit and his right to due process and other legal protections are endangered by the misuse of certain information systems."

The Privacy Act of 1974 states that "It shall be unlawful for any Federal, State or local government agency to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his Social Security number." This is a good and necessary step toward protecting individual liberty. Unfortunately, the language of the Privacy Act allows Congress to require the use of the Social Security number at will. In fact, just two years after the passage of the Privacy Act, Congress explicitly allowed state governments to use the Social Security number as an identifier for tax collection, motor vehicle registration and drivers' license identification.

Since the passage of the Privacy Act, Congress has been all too eager to expand the use of the Social Security number as a uniform identifier. For example, in 1996, Congress required employers to report the Social Security number of employees as part of the "new hires" database, while in 1998, 210 members of Congress voted to allow states to force citizens to produce a Social Security number before they could exercise their right to vote.

Mr. Chairman, my legislation, the Freedom and Privacy Restoration Act (HR 220) forbids Federal or State governments from using the Social Security number for purposes not directly related to administering the Social Security system.

Since I introduced this legislation on the first day of the 106th Congress, my office has received countless calls, letter, faxes, and e-mails from Americans around the country who are tired of having to divulge their national ID number in order to get a job, open bank account, or go fishing. The strong public outrage over the federal banking regulators' "know your customer" scheme, as well as the attempt to turn state drivers' licences into a national ID card, and the Clinton Administration's so-

called "medical privacy" proposals all reveal the extent to which the American people oppose the "surveillance state." These Americans believe that since Congress created this problem, Congress must fix it.

Certain well-meaning members of Congress are focusing on the use of the Social Security number by private businesses. However, this ignores the fact that the private sector was only following the lead of the federal government in using the Social Security number as an ID. In many cases, the use of the Social Security number by private business is directly mandated by the government, for example, banks use Social Security numbers as an identifier for their customers because the federal government required them to use the Social Security number for tax reporting purposes. Once the federal government stops using the Social Security number as an identifier, the majority of private businesses, whose livelihood depends on pleasing consumers, will respond to their customers demands and stop using the Social Security number and other standard identifiers

I hope that we in Congress would not once again allow a problem Congress created to become an excuse for disregarding the constitutional limitations of federal police powers or imposing new mandates on businesses in the name of "protecting privacy." Federal mandates on private businesses may harm consumers by preventing business from offering improved services such as the ability to bring new products that consumers would be interested in immediately to the consumers' attention. These mandates will also further interfere with matters that should be resolved by private contracts.

Furthermore, as we have seen with the administration's so-called "medical privacy protection" proposal, federal "privacy protection laws" can actually undermine privacy by granting certain state-favored interests access to one's personal information.

Finally, I would remind my colleagues that no private organization has the power to abuse personal liberty on as massive a scale as the federal government. After all, consumers have the right to refuse to do business with any private entity that asks for a Social Security number, whereas citizens cannot lawfully refuse to deal with government agencies. Furthermore, most of the major invasions of privacy, from the abuse of IRS files to the case of the Medicare clerk who sold the names of Medicare patients to an HMO, to the abuse of the FBI by administrations of both parties have occurred by government agents. Therefore Congress should focus on the threat to liberty caused by the federal government's use of uniform identifiers.

In conclusion, I once again thank the Subcommittee for holding this hearing on the uses and abuses on the Social Security number. I hope that this hearing is the first step toward Congressional action designed to stop the use of the Social Security number as a national ID number.

LIBERTY STUDY COMMITTEE
FALLS CHURCH, VA 22046
May 11, 2000

Ludwig von Mises, economist and true champion of liberty, concluded that with respect to political and economic systems, one can choose either totalitarianism or capitalism—there is no middle ground. Few issues demonstrate the justification for his conclusion so clearly as does that of privacy protection.

The premise of Mises' argument was that intervention is necessarily begets interventionism as the negative effects of government's initial intervention become the justification for each of the subsequent interventions. For example, when government establishes a minimum wage above the market wage, that class of employees whose marginal product is below the artificially established minimum wage become legally unemployable, and, hence in "need" of governmental support. Of course, government's response to then support every unemployed member of society at some subsistence level creates yet another incentive for more intervention when those actually working to achieve that level of subsistence realize it can be achieved without to achieve that level of subsistence realize it can be achieved without continuing their efforts. Of course, this privacy hearing is not exactly about the minimum wage but rather whether government should intervene yet again to remedy the negative consequences of its prior, privacy-destructive intervention or whether they should properly recognize themselves as the source of the malaise and repeal the prior intervention.

In *America's Great Depression*, economist Murray Rothbard explains how massive federal intervention into the monetary sphere (contrary to the usual tripe proffered regarding "unbridled capitalism" causing the depression) served as the intervention that sent this country into the throws of the great depression. Among the subsequent and numerous interventions to remedy the negative effects of governmental monetary mischief, was the Social Security Act, a bill which after nearly one hundred and fifty years of history to the contrary, "relieved" citizens of the individual responsibility for providing for their own financial futures and those of their family

members. Of course, as Mises understood and explained, these interventions were the natural result of the negative consequences triggered by interference in the monetary sphere.

Because individual and private accounts would no longer be the means by which most savers provided for their financial futures and as though money was actually being placed by government into individual accounts for those without the requisite self-discipline to provide for their own future financial well-being, every participant in the system was ultimately issued a Social Security "Account Number." Although the Congress that created the Social Security system in no way intended to create a national identifier, a subsequent executive order by President Roosevelt authorized the use of the Social Security number as a standard federal identifier.

In the name of "protecting" the taxpayer against government inefficiency and various forms of fraud, government took subsequent steps to further establish the SSN as a uniform identifier. For example, where military members once used their military serial number, this was replaced by the Social Security number as a standard identifier. Additionally, the Bank Secrecy Act of 1970 generated regulation requiring the collection of Social Security Numbers by banking institutions. When, at a minimum, banks were mandated by government to use at least that number and to preserve scarce data resources and avoid duplicity of records, financial institutions naturally adopted the social security number as their record number of choice.

In response to concerns about the widespread use of the SSN, Congress passed the Privacy Act of 1974, but, unfortunately, the language of the Privacy Act allow Congress to require the use of the Social Security number at will. In fact, just two years after the passage of the Privacy Act, Congress explicitly allowed state governments to use the Social Security number as an identifier for tax collection, motor vehicle registration and drivers' license identification. The federal government has also compelled extensive disclosure and use of the Social Security number in its labor, medical, and education databases.

Given that government, to accommodate its own prior interventions, has not only facilitated but compelled the creation of a massive tool for privacy invasion, government is now, of course, presented with the question of whether to undo at least some of the prior intervention or use the culmination of negative effects of all these prior interventions to, yet again, intervene further in the liberty and private dealings of individuals.

The Liberty Study Committee supports what is the only proper response to this question: eliminate the proliferation of the government-instilled, privacy-destroying tool—the Social Security Account Number. While it certainly does not return government to its proper role and restore responsibility for saving to individuals, The Freedom and Privacy Restoration Act, H.R. 220, introduced by Representative Ron Paul, would limit the use of the Social Security number to the Social Security system administration, and is an important step in the right direction of at least protecting the privacy of individuals. Without question, certain inefficiencies will necessarily result in limiting the use by government of this number but, first and foremost, we must not forget that government's primary role must be to preserve individual liberty rather than "efficiently" run government programs, many of which lack constitutionally legitimacy in any case.

Under no circumstances should the government use their very own government-created privacy crisis as a justification to restrict what private individuals do or don't do with their private information (even to include release of their own Social Security number). As much as free speech includes the right to be still, inherent to privacy is the right to share or not share private information with those of one's own choosing.

Government has, in essence, turned the notion of privacy protection on it's head with proposals to limit information sharing by private individuals while compelling disclosure to government by those very same individuals. I hope this Congress will recognize and, thus, not fall prey to the "intervention-begets-intervention" recognized by Mises and, as such, not move our nation yet another step further down the road to totalitarianism.

KENT SNYDER
Executive Director

Chairman SHAW. I just have a couple of questions that I would like to direct, one to Mr. Kleczka and one to Mr. Paul.

Some of the witnesses on the next panel will testify that restricting the commercial use of the Social Security numbers will seriously impede their ability to do business. They will testify that such restrictions will harm consumers, because Social Security number is often used for law enforcement, fraud prevention, and to provide services which consumers value.

How would you respond to these criticisms? And how does your bill ensure that consumers are not harmed by Social Security number restrictions?

Mr. KLECZKA. Well, Mr. Chairman, first of all, I do not believe there is any basis for indicating that this will impede anyone's ability to do business.

We found in a GAO report that credit bureaus make tens of million dollars annually by selling credit header information, which contains a Social Security number. What it is going to harm is their ability to increase the bottom line.

So my response to that argument would be you can still check a consumer or a credit file for accuracy—a name, address, phone number, and past addresses. If that matches with the request that has just come in for a credit rating, you will still sell that information and send it on down.

By virtue of the fact that you are using it as a national ID number, which it was never intended to do, and no one in this room or no Member of Congress will agree to that usage, I am saying is not something that we should try to maintain for their business purposes.

In fact, the big harm to the consumers, Mr. Chairman, will be if Congress fails to do anything.

Chairman SHAW. Thank you for that.

My next question is directed to Mr. Paul.

The American Association of Motor Vehicle Administrators will testify later on that your bill, H.R. 220, will negatively impact on the ability of States to combat fraud and ensure public safety.

Would you like to respond to that criticism?

Mr. PAUL. Well, I think the opposite would be true. If you are interested in stopping the fraud of identity theft, since the Social Security number being used as a universal identifier enhances the identity theft, I would say we would go a long way to stopping that.

I guess what they are referring to is the possibility of putting the Social Security number on our driver's licenses, and that has been started, and that, of course, is what the individuals who like the national ID card would like.

Even though I do not happen to believe it would impede the ability to combat fraud, because it would stop the identity theft, I would be quite willing to say, even if there was the slightest benefit, it is still so dangerous to use a universal identifier, that our freedoms and our liberties and our privacies—I mean, if we had armed guards every place, of course, there may be less fraud and less theft, but we would be living in a police state, so there is an extreme there.

So this is just the introduction of the heavy hand of government monitoring us, and therefore, even if there can be a slight justification, I do not think it should be accepted. I do not believe that is

the case, because I think it would be a tremendous benefit to stop the identity theft.

Chairman SHAW. Mr. Markey?

Mr. MARKEY. Can I very briefly just say that I do agree with Representative Paul that we have to be very concerned about government misuse of private information within our society, but the big problem today is not Big Brother, it is Big Browser. It is the ability, not only for the government, but for private sector companies, together all this information, which would never have been able to be compiled before.

While some industries say, "Well, you know, you are going to interfere with this revolution," I think that is the greatest fear which we all have. Who would want to be somebody that is given responsibility for ending the Internet revolution, as though, by animating this revolution with old values you are now going to ruin it. My god, just think if Internet stocks had to be valued on the same basis as the old economy stocks. They might go down a couple thousand points, you know. That would be terrible if they had to actually have profits and have a cash flow. "You cannot value stocks that way," they say. "You are foolish."

Are we going to prohibit fraud on line? Under their argument, no, that would actually interfere with their ability to get this thing going.

But right now we have rules that say that you cannot transfer, as a tax preparer, somebody's private tax information without their permission. You cannot transfer driver license information without their permission.

Because of Judge Bork, it is illegal to transfer any information about any video cassettes which you rent at a video store. It does not ruin their business, but it allows you to protect the information about the movies that you rented.

No cable company can sell the information about which channels you watch and for how long and what time in the middle of night you might have flipped to that station and been watching that movie while everybody was upstairs asleep. They cannot sell that information as to what you were watching to anybody.

People cannot sell your telephone numbers at the phone company, even though it would make a lot of money for them.

The cell phone industry cannot use their cell phone as a tracker to sell to people as to where you go. That is illegal.

Again, it limits these industries, but it gives us some additional sense of privacy.

All we are saying about the Social Security number is that it falls into a category which deserves special protection, not only from the government but also from any industry, as well, that sees us as nothing more than a product.

Chairman SHAW. If I am reading this panel right, I find Mr. Markey and Mr. Paul agreeing with each other.

Mr. MARKEY. When the liberal left and the libertarian right join up, it does not leave a lot of room in the middle. I think we are pretty much in agreement in terms of what has to happen in our country.

Chairman SHAW. Well, we will have to put this down as a red-letter day.

Mr. Tanner?

Mr. TANNER. Thank you, Mr. Chairman.

I want to thank you all, all of you, for being here. I really believe that this issue is a sleeping giant; that if people really stopped to think about the potential ramifications of this problem, they would be terrified. And it is our job—and I want to thank Chairman Shaw—to not only hold these hearings to educate, but also to try to find the answers, and you all are here to help us do that, and we very, very much appreciate it.

I think, in listening to you all and the other day, that the appeal of the Social Security number is that it tends to give absolute assurance that whomever has asked for it that you are who you say you are. It is ironic that this very attractive, appealing practice could be the very thing that gets us in trouble with that and you are not who you say you are, because we heard a couple of days ago from Colonel Stevens—I do not know if you all who are not on the committee—I know Gerry and Jim were here. This was a heart-wrenching story.

This retired lieutenant colonel and his wife have had their identity stolen. They were looking forward to retirement in South Carolina or Florida with their grandchildren and so on, and now they cannot leave this area because of recurrent credit problems and because, as far as they know, it may still be unfolding.

Now, their lives, if not being ruined physically by ravaging illness, have been altered to the extent that their lifetime dreams of their golden years have become unreachable for them.

Not having heard them, but knowing of the circumstances that they and others find themselves in, I would like to ask Mr. Kleczka and Dr. Paul: how does your bill help the situation that Colonel Stevens and his wife testified to? Gerry?

Mr. KLECZKA. Well, hopefully, Congressman Tanner, the bill would help the next Stevens case, where someone who is trying to steal someone's identity would not be permitted to do so because they will not have access to the Social Security number. So it would help people in that similar situation by making it almost impossible to get one's Social Security number. I think that is where we have to start with any bill that the Ways and Means Committee deals with.

Again, these numbers are disseminated not only through the websites, on the Internet, motor vehicle departments are selling them, the credit bureaus are selling them as part of the header information, and so a person who is out looking for John Tanner's Social Security number can probably, with relative ease, find it.

What we tried to do in my legislation is prohibit the sale, the commercial use of the Social Security number. If, in fact, your bank has it, fine, but they cannot sell the list, nor do they, but we know the lists are being sold by such concerns like the motor vehicle department.

Let me respond at a point to the response from Mr. Paul.

Mr. TANNER. Does your legislation apply to Eddie Bauer and L.L. Bean and those people, too?

Mr. KLECZKA. To who?

Mr. TANNER. L.L. Bean, Eddie Bauer—people I do business with?

Mr. KLECZKA. Right. But they are not the ones selling it. Usually, they might be buying information that could be contained on those lists.

But State legislators are also getting the same pressures and hearing the same problems that we are, and, as time goes by, less and less number of States are using the Social Security number as your driver's license number. In fact, if I am correct, I believe Virginia just passed legislation or stopped the use of that being on your driver's license. As time goes on, more and more States are going to be—

Mr. TANNER. If you will yield, does your bill restrict the usage of the Social Security number by the States and local jurisdictions?

Mr. KLECZKA. No, it does not. That is a State responsibility. My bill provides that they cannot sell that information. So if they sell a driver's license file, they cannot include on there or leave on there a Social Security number.

Mr. TANNER. Dr. Paul?

Mr. PAUL. And, of course, I think that is very important that States not use these numbers for the sale of State information.

But my bill I think would go a long way to stopping this kind of a problem, because it says that you cannot use the Social Security number for anything other than to identify your Social Security account. So it does not deal with the sale so much as it deals with trying to prevent the setup.

So when we talk about commercial interests, it is the fact that we have—just like our voting card, I mean, we are lackadaisical about it and we accept it. It is the same way with corporations. They use it as a convenience. It is convenient for corporations. It is convenient for everybody. My bill says you cannot use it in any other government agency. We cannot universalize it and require it.

Certainly, we would never be able to write the proposed law that says the States will use the Social Security number and have it universal as a universal ID card.

Mr. TANNER. Am I correct in then stating that your bill deals more with the gathering of the information and Gerry's bill deals more with the dissemination?

Mr. PAUL. I think that would be correct.

Mr. KLECZKA. I think so.

Mr. TANNER. Is there a way to bring those two together? It seems to me both have appeal.

Mr. PAUL. I think his problem would be lessened if my bill were passed, in that there would be no accumulation and it would be less likely to have information to sell.

Mr. TANNER. You have got nothing to disseminate. All right.

Mr. KLECZKA. The problem is that those lists and those numbers are out there. Today we need his bill, yesterday we need mine to stop it.

Chairman SHAW. Mr. Hayworth?

Mr. HAYWORTH. Thank you, Mr. Chairman.

As the bells have rung with votes, I just have a couple of very quick questions, in addition to thanking our colleagues for coming down and offering their opinions on this. I would concur with my colleagues here on the subcommittee: this is an issue of great concern, especially to the people of the 6th District of Arizona.

First, to our friend from Wisconsin, Mr. Kleczka, your bill has also been referred to the Committees on Banking and Financial Services, and also the Committee on the Judiciary. What has been their reaction to your legislation?

Mr. KLECZKA. I have not checked with the chairmen. Naturally, they have not had a hearing to date. Clearly, there is joint jurisdiction, because for banking we deal with credit bureaus. We do have penalties in my bill. So whatever product this committee comes up with will have to be meshed with those other committees, also.

Mr. HAYWORTH. Have you heard anything from either committee about the plan of any action?

Mr. KLECZKA. No, I have not. The last we heard Washington, on our financial modernization bill, that was the major, major issue this time around, but two years ago it was not even debated. that is how important this issue has become in a very short while.

Mr. HAYWORTH. Yes, indeed. I would concur. Thank you.

Now I turn to my friend, Dr. Paul, from Texas.

Talking about jurisdiction being shared, your bill has also been referred to the Committee on Government Reform, and I would ask the same question: have you gotten a reaction from the committee? And has there been any action planned or taken by the Committee on Government Reform?

Mr. PAUL. I think Government Reform, if I am not mistaken, has some hearings scheduled next week on it.

Mr. HAYWORTH. Good. All right. Very good.

I thank you, Mr. Chairman.

Chairman SHAW. At this point, since Mr. Tanner brought up the name of Colonel Stevens, we did ask and the representation had been made that this was, in some way, some requirement in law for the Social Security number at the base commissaries. We made an inquiry to the Pentagon, and I would like to read into the record the answer that we got.

The answers says, "The Department of Defense directives governing commissaries and exchange do not require that the Social Security numbers be used for check cashing purposes." Well, something has been misrepresented. "The commissary and exchange services have adopted operating procedures that use the Social Security number for check cashing verification, since it identifies the authorized patron. The military ID uses a Social Security number as a service number," and that we determined yesterday by just looking at Mr. Johnson's card. We may want to do some more inquiring into that particular area.

[The following was subsequently received.]

Statement from the Office of the Deputy Assistant Secretary of Defense

The DoD Directives governing commissary and exchanges do not require that the Social Security Number be used for check cashing purposes. The commissary and exchange services have adopted operating procedures that use the SSN for check cashing verification since it identifies the authorized patron. (The military ID card uses the SSN as the "Service Number"—according to Sheila Ford in DHRA)

In requesting the SSN, the resale activities must conform with DoD Directive 5400.11 and DoD 5400.11R (DoD Privacy Program) and E.O 9397 (dated November 23, 1943).

I have been advised that we have three votes on the floor. This panel will be dismissed, and I thank you. Each one of you gave some very fine testimony, and I find myself in agreement with just about everything that has been said.

We will recess until the conclusion of that vote, and then we will return to hear our second panel.

Thank you.

[Recess.]

Mr. HAYWORTH [assuming Chair]. The committee will come to order.

The second panel consists of: Stuart Pratt, vice president, government relations, Associated Credit Bureaus, Incorporated; Edmund Mierzwinski, consumer program director, United States Public Interest Research Group; Katherine Burke Moore, chair, international board of directors, American Association of Motor Vehicle administrators; Marc Rotenberg, executive director, Electronic Privacy Information Center; and Robert Meyer, senior counsel, American Council of Life Insurers.

We welcome each of you. You will each have your full statement entered into the record, and we will proceed.

We will start with you, Mr. Pratt.

STATEMENT OF STUART K. PRATT, VICE PRESIDENT, GOVERNMENT RELATIONS, ASSOCIATED CREDIT BUREAUS, INC.

Mr. PRATT. Thank you, Mr. Chairman and members of the subcommittee. My name is Stuart Pratt, and, for the record, I am vice president, government relations, for the Associated Credit Bureaus.

ACB, as we are commonly known, is an international trade association representing over 500 consumer information companies, and those companies provide fraud prevention and risk management products, credit mortgage reports, tenant and employment screening services, check fraud and verification services, as well as collection services.

Really, our members are an information infrastructure in our society here that contributes to the safety and soundness of our banking systems, and does, in fact, escalate the efficiencies of our secondary mortgage securities marketplace, which saves consumers as much s 200 basis points on the cost of mortgage, according to those agencies that administer those securities programs.

We help e-commerce and bricks-and-mortar businesses to authenticate applicant data, reducing incidents of fraud, and we help State and Federal agencies to reduce entitlement fraud of various types, amongst other products that we offer.

We thank all of you on the committee for choosing to hold this hearing on such an important subject, the Social Security number, how it is used in our society, and, in fact, to expand our understanding and share our thoughts on the circumstances surrounding misuses of this number.

Before I specifically address how we in our industry do use the Social Security number, I have always found it helpful in this type of testimony to review a little bit about the industry we represent, the types of businesses we have, the laws that govern us, and this

provides a bit of context, I think, for some of the testimony you have, in fact, heard up to this point.

Consumer reporting agencies do maintain information on individual consumer payment patterns associated with various types of credit obligations. Credit histories are derived from the voluntary provision of information about consumer payments on various types of credit accounts and other debts from thousands of data furnishers, such as credit granters, student loan guarantee and child support enforcement agencies. A consumer's file may also contain public record items, such as bankruptcy filings, judgments, or liens.

For purposes of data accuracy, our members also maintain information on a consumer's full name, current and previous addresses, Social Security number, and places of employment.

Perhaps as important as knowing what we have in our files is also to often clarify what we do not have in a consumer's file. We do not know what consumers have purchased using credit. We do not know where they have shopped. We do not know which bank cards they have used. We do not have a record of when consumers have been approved or when consumers have been declined. We do not maintain medical treatment information. No bank account information of that sort, such as a balance on a checking account, is available in a traditional consumer report.

The law that governs this, the Fair Credit Reporting Act, was enacted in 1970 and was most recently amended in the 104th Congress with the passage of the Credit Reporting Reform Act. In fact, here at the table with us are some of the folks who lived through the years and years of debate on that—Ed, in particular. We often spent a good amount of time talking about that law as we evolved it through the Congress, or I should say several Congresses, at this point.

We believe the FCRA is an effective privacy statute. It does protect consumers by narrowly limiting the appropriate uses of the consumer report.

Beyond protecting privacy, the FCRA also accomplishes another very elemental goal of good privacy policy, and that is to ensure rights of consumers with regard to access, the right to dispute, the right to have information corrected in their file, the right to have a baseline expectation of accuracy. In fact, one of the advances under the FCRA is the fact that accuracy is now a responsibility and it is a shared liability for both the consumer reporting agency and also for the various data furnishers with whom we share information.

Let me turn to the question of how we use Social Security numbers, which is more so the subject matter of our hearing today.

Under the FCRA, one of our liabilities, as I have just said, is to employ reasonable procedures to ensure the maximum possible accuracy of the consumer report. We must design these systems based on exactly the data that has been requested on a specific individual, and we must accomplish this dual mission of accuracy and data extraction in the context of a highly mobile society.

There are some facts that I think are very important for this committee to consider. For example, about 16 percent of our Nation's population moves each year, and that generally translates to

about 42 million consumers a year moving from one location to another, thus addresses are changing for principal residences.

About 2.4 million marriages and another 1.2 million divorces occur annually. This, too, results in not only addresses changing, but also the last names of individuals changing, in most cases.

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

In light of the mobility of our society, the Social Security number does, in fact, play a very significant role in ensuring data quality. Where a consumer, for example, has changed a last name due to marriage or divorce, has moved to a new address—which is also very common in those cases—the Social Security number is the most stable identifying element we would have in the file.

It helps us, first, to be able to identify the consumer's file with precision during this life transition where this consumer is very likely to be applying for new credit, perhaps for making new purchases, for this new home that they are moving into, seeking approval for utilities—even, in fact, seeking approval for the loan that is going to allow them to purchase the residence, itself. The consumer expects to have that consumer report available, even during this transitional period.

Secondly, the consumer expects his or her file to be accurate. The SSN helps us to accomplish this goal of file accuracy in the midst of these cycles of change occurring with identifying information.

Beyond the FCRA, we produce a range of other products that I think it is important for this committee to consider. The Social Security number is a critical element in locator services. Our members do produce these types of services, and they are used by, for example, child support enforcement agencies to locate non-custodial parents, pension funds to locate beneficiaries, law enforcement for locating criminals or witnesses, health care providers to locate individuals who have chosen not to pay their bills.

Most recently—and this is an advance in the area of privacy policy—our members have committed ourselves to another organization that they established voluntarily and negotiated with the Federal Trade Commission called "The Individual Reference Services Group," and this has placed limitations on who should have access and in what contexts. This, in fact, also applies to the Social Security number therein.

Yes, the Social Security number plays a role in fraud prevention for us, as well. Where a consumer makes application for a product or service, it helps businesses to ensure they are doing business with the right consumer. These authentication or verification tools are other products that we do make available.

I am looking to see if I am out of time. How am I doing?

Mr. HAYWORTH. If you could, Mr. Pratt, kind of wind it down so we can hear from the other panelists.

Mr. PRATT. Absolutely. Yes, sir.

Mr. HAYWORTH. Thank you. Your full statement will be entered into the record.

Mr. PRATT. Let me just suggest that, in the area of fraud prevention, we have taken one additional step that I hope the committee will consider, and that is that on March 14th of this year we added new voluntary initiatives to our own practices to help the very situ-

ation of the victims you heard in the last round of testimony. Those are in the record for you to review. In fact, we have launched new software systems and will bring those on line this year to monitor a consumer's files and make sure we stay in touch with consumers who have been victimized.

In conclusion, let me urge a message which I have seen in the press releases associated with this committee, and that is: it is a question of balance. It is a question of maintaining viably the kinds of valued programs that we have that are tied with information products, and, at the same time, ensuring the appropriate protections for the very sensitive Social Security number.

I thank you for giving us this opportunity to testify.

Mr. HAYWORTH. Thank you, sir.

[The prepared statement and attachment follow:]

Statement of Stuart K. Pratt, Vice President, Government Relations, Associated Credit Bureaus, Inc.

Mr. Chairmen and members of the Subcommittee, my name is Stuart Pratt and I am vice president, government relations for the Associated Credit Bureaus, headquartered here in Washington, D.C. ACB, as we are commonly known, is the international trade association representing over 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services.

Our members are the information infrastructure that contributes to the safety and soundness of our banking and retail credit systems; which:

- allows for the efficiencies of a secondary mortgage securities market place that saves consumers an average of 200 basis points on the cost of a mortgage.
- helps e-commerce and bricks-and-mortar businesses to authenticate applicant data thus reducing the incidence of fraud.
- gives child support enforcement agencies the information tools necessary to meet their mission.
- allows states to reduce many forms of entitlement fraud.

We want to commend you for choosing to hold this hearing on the importance of the Social Security Account Number in our society and to expand our understanding of the circumstances surrounding misuses of this number.

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

Consumer Reporting Agencies and Consumer Reports

Consumer reporting agencies maintain information on individual consumer payment patterns associated with various types of credit obligations.[1] The data compiled by these agencies is used by creditors and others permitted under the strict prescription of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to review the consumer's file.

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

For purposes of data accuracy and proper identification, generally our members maintain information such as a consumer's full name, current and previous addresses, Social Security Number (when voluntarily provided by consumers) and places of employment. This data is loaded into the system on a regular basis to ensure the completeness and accuracy of data.[2]

---

[1] Our members estimate that there are approximately 180 million credit active consumers. Since our members operate in competition with each other, these consumers are likely to have more than one credit history maintained.

[2] Note that there are in fact a number of major credit reporting systems in this country. Within ACB's membership the three most often recognized systems would be Equifax, Atlanta, GA;

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

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

The Fair Credit Reporting Act (FCRA)

In addition to our general discussion of the industry, we believe it is important for your Subcommittee to have a baseline understanding of the law which regulates our industry. Enacted in 1970, the Fair Credit Reporting Act was significantly amended in the 104th Congress with the passage of the Credit Reporting Reform Act.[3]

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

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

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

Beyond protecting the privacy of the information contained in consumer reports, the FCRA also provides consumers with certain rights such as the right of access; the right to dispute any inaccurate information and have it corrected or removed; and the right to prosecute any person who accesses their information for an impermissible purpose. The law also includes a shared liability for data accuracy between consumer reporting agencies and furnishers of information to the system.

Social Security Number Uses

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

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

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

• Approximately 16% of the nation's population moves each year according to the U.S. Census Bureau, which means many addresses change each year. (This equates to approximately 42 million Americans)

• Based on National Center for Health Statistics, it is estimated that there are 2.4 million marriages and 1.2 million divorces annually. This event frequently triggers changes in addresses as well as last names.

• In 1998 there were 6 million homes in the U.S. that are considered vacation or second homes. Consumers often switch billing addresses if they stay at such residences for long periods of time and in some cases maintain billing addresses for both residences with various creditors. (Source: U.S. Census Bureau House Vacancy Survey as extrapolated by the National Association of Realtors)

Experian, Orange, CA; and Trans Union, Chicago, IL. These systems not only manage their own data, but provide data processing services for the over 400 local independently-owned automated credit bureaus in the Association's membership.

[3] Public Law 10409208, Subtitle D, Chapter 1.

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

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

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

The SSN is also a critical element in producing information products, which are commonly called locator services. Our members limit access to these products via voluntary initiatives established by our largest members and others under an organization called the Individual Reference Services Group. These services are made available, for example, to child support enforcement agencies for purposes of locating non-custodial parents; to pension funds which must locate beneficiaries; to law enforcement for locating criminals or witnesses; to healthcare providers that must locate individuals who have chosen not to pay their bills and for other similar uses.

Further, the SSN plays a role in fraud prevention products. Where a consumer makes application for a product or service, information products that help the business to ensure that they are doing business with the right consumer use information products to authenticate or verify the application information. This is true in both for bricks-and-mortar business and in e-Commerce. If applicant data doesn't match, then the business can take additional steps to verify the consumer's identity and thus prevent fraud.

Fraud Prevention and Identity Theft

In your press release announcing this hearing, you mention the potential for misuse of the SSN. Our industry has a history of bringing forward initiatives to address fraud. These efforts focus on use of new technologies, and better procedures and education.

Consider the following efforts undertaken during this decade:

- ACB formed a Fraud and Security Task Force in 1993
- A "membership alert form" was developed to be used in notifying other ACB credit bureau members of a customer, which was committing fraud through the misuse of data. Implemented in 1994.
- A "Universal Fraud Information Form" was developed for use by creditors when communicating the incidence of fraud to national consumer reporting systems.
- A generic credit reporting industry presentation on ACB fraud and security initiatives was developed and presented to customer segments during 1995.
- Minimum standards for data access equipment and software were announced to industry suppliers in March 1995.
- ACB members implement company-specific limitations on the availability of account numbers, and truncation of Social Security Numbers on consumer reports sold to certain customer segments.
- Experian, Equifax and Trans Union voluntarily formed special fraud units with 800 number service and consumer relations personnel specially trained to work with fraud victims.
- A hardware and software certification program is created by the industry and administered by a third-party certification authority for those access products, which have implemented minimum industry security standards.
- Over 150,000 copies of a new customer educational brochure entitled "We Need Everyone's Help to Protect Consumer Privacy and Reduce Fraud" have been distributed since its first printing in the last Q.1997. An education program was also developed for use by ACB members in presenting the information found in the brochure. 2nd Q. 1998.
- On March 14, 2000, the ACB announced new voluntary initiatives to assist consumers who have been victimized by identity theft. Following is a description of each initiative and also attached is our press release.
- Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.

• Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
• Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
• Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.
• Launch new software systems that will monitor the victim's corrected file for three months, notify the consumer of any activity, and provide fraud unit contact information.
• Fund, through ACB, the development of a series of consumer education initiatives through ACB to help consumers understand how to prevent identity theft and also what steps to take if they are victims.

Conclusion

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

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

Thank you for this opportunity to testify.

3 Public Law 10409208, Subtitle D, Chapter 1.

NEWS RELEASE

Contact: Norm Magnuson
Vice President of Public Affairs
202/408097406
For Immediate Release
March 14, 2000

Credit Reporting Industry Announces Identity Theft Initiatives

Associated Credit Bureaus, the international trade association for the consumer reporting industry, announced today a commitment on behalf of the nation's leading credit reporting agencies to voluntarily implement a comprehensive series of initiatives to assist victims of identity theft in a more timely and effective manner.

"While there is no evidence to show that the credit report is a source for identity theft, our industry has always taken an active role in assisting consumers who are fraud victims. Our members have taken this responsibility seriously, and we're very proud of these initiatives that help consumers who are victims of identity theft or fraud," noted D. Barry Connelly, president of Associated Credit Bureaus. "Designing and implementing these initiatives is a significant milestone in the ongoing efforts of our industry to help address the problem of identity theft. As long as there are criminals who prey on innocent consumers, we will continue to seek even better ways to serve consumers and work with law enforcement and our industry's customers to address this threat."

Connelly outlined the industry's six-point program to improve identity theft victim assistance:

• Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.
• Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
• Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
• Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.

• Launch new software systems that will monitor the victim's corrected file for three months, notify the consumer of any activity, and provide fraud unit contact information.

• Fund, through ACB, the development of a series of consumer education initiatives through ACB to help consumers understand how to prevent identity theft and also what steps to take if they are victims.

ACB's initiatives, to be fully implemented within seven months of this announcement, resulted from a task force comprising senior executives from the ACB Board of Directors and former state Attorney General, M. Jerome Diamond. Diamond interviewed consumer victims and law enforcement officials, made on-site visits to credit reporting agency fraud units, and obtained input from privacy advocates. His counsel was an integral part of the decision-making process and influenced the final content of the initiatives.

Connelly said: "Identity theft is a crime that is deeply unsettling for the victims. Our initiatives will make it easier for victims to put their financial lives back together." Connelly stressed, though, that the crime extends beyond individuals to creditors and ACB members and added, "We must all work together in the areas of prevention and victim assistance. We supported the enactment of the Identity Theft Assumption and Deterrence Act of 1998 and have worked with more than half of the state legislatures on similar laws. We urge law enforcement to vigorously investigate and prosecute the criminals."

Associated Credit Bureaus, Inc. is an international trade association representing 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services.

Source: Associated Credit Bureaus, Inc. Web site: www.acb-credit.com

Mr. HAYWORTH. Mr. Mierzwinski?

STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, UNITED STATES PUBLIC INTEREST RESEARCH GROUP

Mr. MIERZWINSKI. Thank you.

Mr. Chairman, members of the committee, I am Ed Mierzwinski. I am consumer program director with the Public Interest Research Groups. The State PIRGs are consumer and environmental and good government reform groups active around the country. US PIRG serves as their national lobbying office.

I am pleased to be here today to talk about the critical issues of misuse of the Social Security number and how that contributes to identity theft. Just last week, the California Public Interest Research Group and another organization, the Privacy Rights Clearinghouse, two of the leading organizations that work with identity theft victims, such as Colonel and Mary Elizabeth Stevens, the witnesses from Tuesday's hearing, our organizations released a new report based on a survey of identity theft victims and the problems they go through.

We found that the average victim has a basic number of losses. I think the Stevens were up over $100,000. The average victim is around $18,000 or so and spends 175 hours trying to solve their problem, so we think identity theft is a very serious problem that the committee and the Congress need to continue to work with, and the report, "Nowhere to Turn," documents a strong platform for identity theft solutions.

One of the most important parts of that platform is to close something that we called a "credit header loophole." Both Con-

gressman Kleczka's bill and a similar piece of legislation by Representative Hooley of Oregon would close that loophole.

Who wants access to your credit header, which is a product sold by the credit bureaus outside of the protection of the Fair Credit Reporting Act?

First, identity thieves want your credit header, and it is easy for them to get it. Just this week, I appeared on a Fox TV News broadcast where I assisted the reporter, who actually found it was quite easy to do himself, in obtaining the Social Security number of his boss, with his boss' permission. He was then able to apply for credit in his boss' name. And, by the way, he has received credit from at least one bank.

One person spent about $49 to use a locator service on the Internet. He obtained a Social Security number of someone that he knew, and he was then able to get credit in their name. That is how easy it is. That is how scary it is.

The other kind of person who wants to get access to you through these locator services, through these credit headers—that include, by the way, your Social Security number and other sensitive information—are stalkers. And it has been widely reported recently about the tragic death of Amy Boyer in New Hampshire. Her stalker, a jilted grammar school acquaintance, tracked her down through a locator service on the Internet.

We believe that in 1993, when the Federal Trade Commission said that credit headers which contain your name, address, Social Security number, telephone number, and other pieces of information that are not actually associated with your credit lines, are not part of the credit report, and therefore exempt from the protection of the act, that the Federal Trade Commission made a serious mistake. That is one of the easiest ways for identity thieves to obtain information on the Internet about your Social Security number is to use a pretext to obtain your credit header.

So we would urge the committee to take a hard look at Mr. Kleczka's bill, which includes, by the way, several other important provisions to prevent the misuse of Social Security numbers, but I think the most important one is to clear up the problem caused when the Federal Trade Commission said that your Social Security number, your name, and your address are not part of your credit report; therefore, the credit bureaus can sell them.

Now, they sell them to these companies. Many of the companies are part of this Industry Self-Regulatory Association called the IRSG, as Mr. Pratt described. In our view, the IRSG principles do not meet what we call "fair information practices" designed to protect the uses of information. Even the Federal Trade Commission, when it agreed to the IRSG experiment, said the IRSG needed to go further than it has.

The IRSG has not made public its assessments or audits of its members' uses of information, and I believe that was one of the principles that they promised the Federal Trade Commission back when they were founded, so I would encourage the committee to look into the IRSG.

What other actions would protect Social Security numbers from misuse? I think there are a number, and I will associate myself

with the remarks of Mr. Rotenberg, who will go into some other details on how to protect the Social Security number.

In conclusion, I would like to thank the committee for the opportunity to talk about this very important problem of the misuse of Social Security numbers and again urge you to take action to protect identity thieves. It is one of the fastest-growing crimes out there. There are 500,000 to 700,000 complaints a year. Probably the most significant step we could take is to limit access to Social Security numbers indiscriminately.

Thank you.

Mr. HAYWORTH. Thank you.

[The prepared statement follows:]

Statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group

May 11, 2000 Chairman Shaw and members of the committee: We are pleased to present the views of the U.S. Public Interest Research Group on the misuses of Social Security numbers. As you know, U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups, which are non-profit and non-partisan consumer and environmental advocacy groups active around the country.

Summary

U.S. PIRG believes that the widespread availability of the social security number contributes to identity theft, which is well-documented as one of the nation's fastest growing white-collar crimes. The 1999 Shelby amendment to the Drivers Privacy Protection Act is an excellent start toward protecting Social Security Numbers, but more needs to be done.[1] We recommend that the Congress also enact one of several bills that would close the so-called "credit header" loophole in the Fair Credit Reporting Act. The credit header loophole has led to the proliferation of information broker websites on the Internet that make it easy for identity thieves to obtain Social Security Numbers and other bits and pieces of a consumer's identity that are used to build a fraudulent identity in the victim's name.

(1) What Does It Mean To Be An Identity Theft Victim?

Earlier this week the committee heard passionate pleas for help from Colonel and Mary Elizabeth Stevens, just two of many victims of identity theft. They are not alone. Current statistics show that credit bureaus and federal agencies are receiving as many as 50009700,000 identity theft complaints annually.

Last week, California PIRG and the Privacy Rights Clearinghouse released a report[2] summarizing the results of a survey of victims. We found that identity theft victims had labored 2094 years or more to rid themselves of an average of $18,000 in fraudulent accounts. However, worse than cleaning up the financial mess is the enormous time commitment victims spend cleaning up their lives:

Respondents spent an average of 175 hours actively trying to resolve problems caused by the theft of their identity. The victims reported missing several days or weeks of work to put their lives back together, and two people even reported losing their jobs due to the time devoted to identity theft resolution. A victim from California felt that resolving her problem was "nearly a full-time job." Robin, a victim from Los Angeles, explains, "One bill—just ONE BILL—can take 6098 hours to clear up after calling the 800 numbers, waiting on hold, and dealing with ignorant customer representatives." She concludes, "The current system is not created for actual assistance, it is created to perpetuate the illusion of assistance."[3]

(2) Who Wants Your Social Security Number?

---

[1] The Shelby amendment expanding consumer privacy rights in information held by state motor vehicle departments is scheduled to be implemented on 1 June 2000 and would subject social security numbers, photographs and health and medical information held by motor vehicle departments to more stringent consumer protection.

[2] "Nowhere To Turn," Benner, Givens and Mierzwinski, CALPIRG and Privacy Rights Clearinghouse, 1 May 2000. See <http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>. We have released two previous reports on identity theft "Theft of Identity: The Consumer X-Files," CALPIRG and US PIRG, 1996 and "Theft of Identity II: Return to the Consumer X-Files," CALPIRG and US PIRG, 1997, as well as four reports on errors by credit reporting agencies since 1991, most recently "Mistakes Do Happen," 1998.

[3] See "Nowhere To Turn," <http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>

Identity Thieves: Earlier this week, I appeared on Fox TV News in a story on identity theft. The piece was designed to demonstrate how easy it is easy to use a pretext to obtain Social Security Numbers from on-line information broker websites, despite supposed limitations on disclosure to unauthorized persons claimed by the sites. With the permission of his editor, the TV reporter logged onto the Internet and, for a fee, was able to obtain his editor's social security number. He then applied for, and obtained, at least one credit card in the editor's name. To its credit, at least one bank suspected fraud and denied the card. He is waiting to hear from other banks. While identity thieves can also obtain social security numbers from other sources, such as drivers' licenses in some states, student IDs, and medical records, why go to the trouble when you can log onto the Internet? As the Christian Science Monitor and Nando News explained this week:

So you think your private information is relatively safe? Think again. For a mere $49, someone can hop on the Internet, give a company your name, wait a few days, and bingo: up pops your Social Security number. Want someone's bank account balance? That costs $45. An unpublished telephone number? $59.[4]

Stalkers: The reporter in that story wasn't writing about the "white-collar" crime of identity theft, however. Actually, the story was about the brutal stalker murder of Amy Boyer in New Hampshire. As the story explains:

Her killer, a man obsessed with her since 10th grade, left evidence that he tracked her down through the online personal-data service Docusearch.com.

On his own Web site, Liam Youens detailed his plans for killing Boyer, including how he found her: "I found an internet site to do that, and to my surprize everything else under the Sun. Most importantly: her current employment. It's accually obsene what you can find out about a person on the internet." After shooting Boyer, Youens turned the gun on himself.

Stunned that such information could be purchased by anyone, Boyer's parents, Tim and Helen Remsburg, recently filed a suit against Docusearch.com. They also testified before a Senate subcommittee about the killing.[5]

(3) What Is The Credit Header Loophole That Allows Easy Availability Of Social Security Numbers?

As part of a 1994 consent decree with TRW (now Experian) that properly prohibited target marketing[6] from credit reports, the Federal Trade Commission (FTC) made a serious mistake. It defined certain sensitive personal information contained in consumer credit reports as exempt from the definition of credit report and therefore exempt from regulation under the Fair Credit Reporting Act. Under this loophole, the credit bureaus now traffic widely in "credit headers," which include the demographic information found in a credit report that is not associated with a specific credit trade line or public record.

Credit headers may include names, addresses, dates of birth, previous addresses, telephone numbers (including unlisted numbers) and Social Security numbers. Credit header databases are re-sold by the Big Three credit bureaus in bulk and used for a variety of people-finder and related products. Many information brokers operate websites that sell credit headers, along with other public record information.

In 1997, the credit bureaus and several of the firms that traffic in the credit headers that the credit bureaus sell formed a so-called "self-regulatory" association known as the Individual References Services Group. The organization says its "principles impose significant restrictions on the access and distribution of non-public information, such as non-financial identifying information in a credit report. For example, Social Security numbers obtained from non-public sources may not be displayed to the general public on the Internet by IRSG companies.[7]

Despite this assertion, U.S. PIRG, the Privacy Rights Clearinghouse, other advocates, reporters, and identity thieves and stalkers have found that SSNs can still be purchased from websites. We strongly support closing the credit header loophole because, even if the IRSG's voluntary rules were effective in halting the sale of

---

[4] "Suit alleges online privacy breach had deadly consequences" By KRIS AXTMAN, The Christian Science Monitor (May 9, 2000 1:34 a.m. EDT http://www.nandotimes.com)

[5] ibid.

[6] At the time, Equifax voluntarily agreed to stop target marketing from credit reports. Trans Union, on the other hand, refused, and has since led the FTC through eight years of litigation, while it continues to use credit reports to generate target marketing lists in defiance of the FTC. Most recently, on 1 March 2000, the FTC again ordered Trans Union to stop, although it then (30 March 2000) agreed to stay the ruling while Trans Union appeals yet again. <http://www.ftc.gov/opa/2000/03/transunion.htm> The Act should also be clarified to ban target marketing explicitly to end Trans Union's lawsuit.

[7] See *http://www.irsg.org*

SSNs to the general public, it is easy to use a "pretext" to obtain SSNs from one of the many sites on the Internet that purports to only sell it to qualified requestors.

We also support Congressional review of the adequacy of the IRSG's self-regulatory system. While the FTC encouraged the formation of the IRSG in 1997, it said at the time that the IRSG Principles did not meet all Fair Information Practices (see below for discussion of the need for these Practices). The FTC also said that the IRSG must make public a "Summary" of the results of "third-party assessments," or audits, of its members. To our knowledge, while the IRSG provided the FTC in 1999 with what we believe to be a highly unsatisfactory letter[8] stating that the assessments were completed, no summaries have ever been made public.

(4) How Should We Close The Credit Header Loophole?

Several federal proposals would close the credit header loophole. Among the proposals that we support are the following, although there may be others. U.S. Senators Dianne Feinstein (D09CA), Charles Grassley (R09IA) and Jon Kyl (R09AZ) have proposed'S 2328. Similar companion legislation, HR 4311, has been proposed by Rep. Darlene Hooley (D09OR). Rep. Jerry Kleczka (D09WI) has a broader proposal, HR 1450, to close the credit header loophole and further restrict the use of Social Security numbers in other ways.

Most of the bills re-define the header exception from the FCRA so that sensitive information including Social Security Numbers is protected by the Act rather than exempt from it. For example, HR 1450 would re-define all information held in credit files to be protected by the act "except the name, address, and telephone number of the consumer if listed in a residential telephone directory available in the locality of the consumer."

(5) What Are Fair Information Practices?

In our view, the credit header loophole is a gross violation of Fair Information Practices. Collecting information for one purpose and using it for another without the individual data subject's consent violates the Fair Information Practices originally proposed in 1973 and incorporated in the Privacy Act of 1974. As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices that provide for the following consumer rights: notice, consent, access, correction, liability for violations.[9]

(6) What Other Actions Would Protect Social Security Numbers From Misuse?

Using the Social Security Number as a medical ID or college student ID or motor vehicle ID leads to identity theft or other problems. In our strong view, in addition to closing the credit header loophole, the other most important thing Congress should do to protect Social Security Numbers is not to repeal or weaken the 199 Shelby amendment to the Driver's Privacy Protection Act. Last year, Congress enacted the Shelby amendment expanding consumer privacy rights in information held by state motor vehicle departments. It takes effect on 1 June 2000, as enacted by Congress. Direct marketers are currently campaigning to delay or weaken this amendment, which substantially strengthens protection of Social Security Numbers,

---

[8] See Letter from IRSG's Ron Plesser to FTC, 28 April 1999, <http://www.irsg.org/html/letter—to—the—ftc.htm>

[9] Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. <http://www.privacyrights.org/AR/fairinfo.html> The document cites the version of FIPs in the original HEW guidelines, as well as other versions: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973 [From The Law of Privacy in a Nutshell by Robert Ellis Smith, Privacy Journal, 1993, pp. 500951.]

1.Collection limitation. There must be no personal data record keeping systems whose very existence is secret.

2.Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.

3.Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4.Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

5.Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

driver's license photographs and health and medical information held by motor vehicle departments. Their efforts should be rejected.

(7) Additional Recommendations To Protect Privacy

While the U.S. has a strong history of privacy protection, our statutory privacy protections are a patchwork—what industry prefers to call a "sector-by-sector" approach. Yet, whatever the merits, if there ever were any, of the industry-prescribed sector-by-sector approach, it is rapidly obsolescing as industry sectors converge. The names of the videos you rent are better protected than your not-so-confidential bank account balances, credit card records and medical history. U.S. PIRG strongly supports enactment of over-arching privacy legislation that requires all businesses to protect consumer and customer information under laws based on Fair Information Practices and gives consumers enforceable rights if their personal information is misused. The first step should be enactment of the Shelby (S. 1903)-Markey (HR 3320) proposals to protect financial privacy by requiring opt-in consent. U.S. PIRG's new identity theft report, Nowhere To Turn, makes additional recommendations to improve both the accuracy and privacy of credit reports.[10]

Conclusion

We want to thank you, Mr. Chairman, for the opportunity to present our views on the need for strong privacy protections to protect Social Security Numbers from misuse. We look forward to working with you on this and other matters to guarantee the privacy of American citizens. Restricting the widespread availability of Social Security Numbers is one of the most important solutions to the identity theft epidemic.

Mr. HAYWORTH. Ms. Moore?

STATEMENT OF KATHERINE BURKE MOORE, INTERNATIONAL CHAIR, BOARD OF DIRECTORS, AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

Ms. MOORE. Good afternoon, Mr. Chairman and members of the subcommittee. My name is Katherine Burke Moore. I serve as the chair of the American Association of Motor Vehicle Administrators, and as the deputy director in the Department of Public Safety for the State of Minnesota.

AAMVA is a voluntary association representing the motor vehicle administrators and chief law enforcement officials in North America. Our members administer the laws that govern motor vehicle operations, the driver credentialling process, and highway safety enforcement.

I appreciate the opportunity to brief the subcommittee on the use of the SSN by our members. The use of the SSN for drivers license issuance and motor vehicle registration was authorized in 1976 in section 405 of title 42, U.S. Code. This authorization was specifically for the purpose of establishing the identification of individuals. Congress has consistently used this authority to mandate State DMVs to carry out a whole host of Federal objectives.

As you may know, H.R. 220, introduced early in the 106th Congress, seeks to repeal this authority. Passage of H.R. 220, as currently written, would severely impact the motor vehicle and law enforcement communities' ability to combat fraud and ensure public safety.

The other Federal mandates that DMVs currently work under would be in direct conflict with H.R. 220. Some of those mandates

[10] See "Nowhere to Turn." <http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>

include: the Welfare Reform Act, the Illegal Immigration Reform Act, and the Commercial Motor Vehicle Safety Act of 1986, or CMVSA. Details of these mandates are included in our written testimony.

When the SSN is obtained in conjunction with name, date of birth, and gender, DMVs can positively identify a person on an agency's driving record. This helps to minimize the possibility that erroneous information, such as accident or convictions, would be placed on the wrong person's driving record, or that a license will be issued to someone who is not qualified to obtain one.

Today, DMVs maintain the driver history of more than 200 million vehicle operators in the U.S., alone. AAMVA believes that the use of the SSN as a unique identifier is necessary to maintain accurate records and to prevent harm to individuals and businesses as a result of misuse of official credentials.

These credentials include not only documents such as driver's licenses that are widely used by everyone for personal identification, but documents that evidence ownership in other property interests in motor vehicles such as registration and titles.

The SSN also is used as a common identifier to facilitate electronic data exchange among DMVs and other authorized users. Without an effective way to ensure data is correctly applied to the right driving record, useful data exchange will be compromised.

The tendency today, particularly with driving record information, is to institute an even greater exchange of driver history data to enhance public safety.

The recently-passed Motor Carrier Safety Improvement Act of 1999 mandates that the courts share commercial driver convictions with DMV, regardless of whether the violation occurred in a commercial vehicle or passenger vehicle. The CMVSA mandated the creation of the commercial driver's license information system, or CDLIS, to provide the electronic means to share commercial driver histories among States and other authorized users.

The CMVSA also mandates that the SSN be used as a unique identifier for commercial driving records in CDLIS. All 51 U.S. jurisdictions operate CDLIS. All collect the SSN for commercial drivers, as the Federal law requires.

AAMVA has long supported the one driver/one license concept. We encourage Congress to support the establishment of the driver record information verification system. This system will enable DMVs to verify that a driver does not have more than one license.

Until we are able to query such a system prior to initial issuance and renewal of a license, the deceptive practice of obtaining multiple licenses to unlawfully distribute citations and violations will continue. Without a standardized, unique identifier, the ability to electronically transfer driver record information will fail.

To assist States in the ID verification process, AAMVA's subsidiary, AAMVAnet, provides an electronic data exchange application through the Social Security Online Verification system SSOLV. This online support allows a DMV to instantly verify an individual's SSN during the driver's license issuance or renewal process.

In recent years, the public's concern about privacy of personal information on their driving record has caused many jurisdictions to

change their policies about displaying the SSN on the license. Today, 49 States either do not display the SSN or give the public the option of using a State-issued identifier; however, the SSN remains an important identifier for record-holder verification.

The Driver Privacy Protection Act also forbids and prohibits the sale and disclosure of the SSN that is collected by the DMVs.

In closing, I want to reiterate the importance of using the SSN for driver's licensing. The public safety benefits of SSN use are numerous and far outweigh any potential disadvantages. We urge the Congress to consider these public safety uses and not restrict the motor vehicle and law enforcement community from utilizing the SSN as a unique identifier for the millions of driver records we administer.

I appreciate the opportunity to testify and will answer questions at the appropriate time.

Mr. HAYWORTH. Thank you, Ms. Moore.

[The prepared statement follows:]

Statement of Katherine Burke Moore, International Chair, Board of Directors, American Association of Motor Vehicle Administrators

Good morning Mr. Chairman and esteemed members of the Subcommittee. My name is Katherine Burke Moore. I serve as Chair of the International Board of Directors of the American Association of Motor Vehicle Administrators, and as Deputy Director of the Office of Traffic Safety, under the Department of Public Safety for the State of Minnesota.

The American Association of Motor Vehicle Administrators (AAMVA) is a voluntary association representing the motor vehicle administrators and chief law enforcement officials in North America. Our members administer the laws that govern motor vehicle operation, the driver credentialing process and highway safety enforcement. We appreciate the opportunity to brief the Subcommittee on use of the Social Security Number by our members.

The use of the social security account number (SSN) for driver's license issuance or motor vehicle registration was authorized in 1976, in Section 405(c)(2)(C)(i) of title 42, United States Code. This authorization was specifically for the purpose of establishing the identification of individuals. Congress has consistently used this authority to mandate state motor vehicle agencies carry out a whole host of federal objectives. At the same time, some members of Congress have introduced legislation to prohibit this authority. These conflicting congressional objectives have wreaked havoc at the state level.

As you may know, H.R. 220, which was introduced early in the 106th Congress and seeks to repeal motor vehicle agencies' authority to use the SSN is one of the best examples of this congressional conflict.

Passage of H.R. 220 would severely impact the motor vehicle and law enforcement community's ability to combat fraud and to ensure public safety. The other federal mandates that DMVs currently work under would be in direct conflict with H.R. 220.

Of particular note, Public Law 10409193, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 requires state motor vehicle agencies to collect the SSN for all drivers to help facilitate the collection of child support payments. This requirement takes effect on October 1, 2000 and mandates states to share this data with their state Office of Child Support Enforcement.

States were also required to collect the SSN under Section 656(b) of Public Law 10409208, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. AAMVA supported that provision because it would have gone a long way in helping to enhance the security of the credentials our members issue. The Act required the collection of the SSN but did not require states to display the SSN on the license.

The public safety and identity protection benefits were ignored as DMVs were accused of creating a national identification card. The reality is that because of the increased fraudulent use of current security features on falsified documents, states thought it important to upgrade the minimum security standards of these documents.

Support for Section 656(b) disappeared because of privacy concerns surrounding the use of the SSN, but the AAMVA membership has continued the effort to enhance the security of driver license credentials. It is unfortunate that the benefits of Section 656(b) were lost because of the SSN component.

When obtained in conjunction with the name, date of birth and gender, the SSN enables DMVs to positively identify a person on the agency's driving record files. This helps to minimize the possibility that erroneous information such as accidents or convictions will be placed on the wrong person's driving record.

Today, motor vehicle agencies maintain the driver history records of more than 200 million vehicle operators in the United States alone. AAMVA believes that the use of the SSN as a unique identifier is necessary to maintain accurate records and to prevent harm to individuals and businesses as a result of misuse of official credentials. These credentials include not only documents such as the driver's license that are widely used and accepted for personal identification, but documents that evidence ownership and other property interests in motor vehicles such as registrations and titles.

The SSN also is used as a common identifier to facilitate electronic data exchange among motor vehicle agencies and other authorized users. Omitting the social security number as an identifier could result in inaccuracies in driver information retained and exchanged among states. Without an effective way to ensure data is correctly applied to the right driver record, useful data exchange will be compromised. The tendency today, particularly with driver record information, is to institute an even greater exchange of driver history data.

Case in point, the recently passed Motor Carrier Safety Improvement Act of 1999 mandates that the courts begin sharing commercial operator conviction data with state motor vehicle agencies—regardless of whether the violation occurred in a commercial motor vehicle or a passenger vehicle.

The Commercial Motor Vehicle Safety Act of 1986 (CMVSA) mandated the creation of the Commercial Drivers License Information System (CDLIS). CDLIS provides the electronic means to share commercial driver histories among the states and other authorized users. The CMVSA also mandates that the SSN be used as the unique identifier for commercial drivers' records on the system. All 51 U.S. jurisdictions operate CDLIS. All collect the SSN for commercial drivers as the federal law requires.

AAMVA has long supported the "one driver—one license" concept. We encourage Congress to support the establishment of the Driver Record Information Verification System (DRIVerS) that will enable motor vehicle agencies to ensure that a driver does not have more than one driver license and to accurately post conviction data to the record associated with that license. Until we are able to query such a system prior to the initial issuance of a driving credential or upon renewal, the deceptive practice of obtaining multiple licenses to unlawfully distribute traffic citations and violations among them will continue.

Congress provided funding in TEA0921 to undertake an assessment of available electronic technologies to improve access to and exchange of motor vehicle driving records. One of the elements of the assessment is the review of alternative unique motor vehicle driver identifiers that would facilitate accurate matching of drivers and their records. Some unique identifier is necessary for the states to carry out their safety mission. The SSN has proved itself to be an effective tool in uniquely identifying drivers that pose a safety risk.

Without a standardized unique identifier, the ability to electronically transfer driver record information will fail.

To assist states in the identification verification process for a driver license credential, AAMVA, through its subsidiary organization AAMVAnet, provides an electronic data exchange application through the Social Security Online Verification system (SSOLV). This system allows DMVs to send an individual's name, date of birth and SSN to the Social Security Administration (SSA) and the SSA, in turn, verifies that information against its Master File and reports back to the requesting DMV whether or not the DMV information did or did not match.

This on-line support allows a jurisdiction to instantaneously verify an individual's SSN during the driver license issuance or renewal process while the driver is still at the counter. Currently eight jurisdictions are in production at this time through a Memorandum of Understanding with the SSA.

In recent years, the public's concern about privacy of the personal information stored in their driver's license records has caused many motor vehicle agencies to change their policies about displaying the SSN on the driver's license. Today, 49 states either do not display the SSN or give the public the option of using a state issued alpha-numeric identifier. However, the SSN remains an important identifier for electronic driver record exchange and record-holder verification.

The Driver Privacy Protection Act also forbids and prohibits the sale and disclosure of the SSN that is collected by the DMVs.

In closing, I want to reiterate the importance of using the SSN for issuance of driver license credentials and other property documents. The public safety benefits of SSN use are numerous and far outweigh any potential disadvantages.

We urge the Congress to consider these invaluable uses and not restrict the motor vehicle and law enforcement community from utilizing the SSN as the unique identifier for the millions of driver records we administer.

I appreciate the opportunity to testify and will respond to questions at the appropriate time.

Mr. HAYWORTH. Mr. Rotenberg?

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, AND ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Mr. ROTENBERG. Mr. Chairman, Mr. Tanner, members of the committee, thank you very much for the opportunity to testify this afternoon. I am the director of the Electronic Privacy Information Center. I am also an adjunct professor at Georgetown. I have taught privacy law for 10 years and was involved in two of the leading privacy cases involving the use of the Social Security number.

I want to thank you for holding the hearings this week. I think this is an issue, obviously, of great concern to many Americans.

I am here mostly to tell you that I think efforts to establish privacy safeguards for the collection and use of the Social Security number are completely consistent with the tradition of U.S. law, both in Congress and also in the courts.

As you know, in 1936, when the nine-digit number was created, it was solely for the purpose of administering Social Security benefits. Now, that purpose was expanded in 1961, when the SSN became a taxpayer identification number. But when the Government looked closely at the issue of Social Security number use in the early 1970s and issued this very important report called, "Records, Computers, and the Rights of Citizens"—this was from the Department of Health, Education, and Welfare—many of the concerns that you are hearing today were described and addressed in that report more than 25 years ago—the risk of profiling, of identity theft, the dangers of building these big computer databases tied to the Social Security number.

That report specifically recommended a prohibition on the use of the Social Security number for promotional or commercial purposes.

Now, Congress, the following year, did not go quite so far as to prohibit the use of the SSN for these other purposes, but it did establish a very important privacy provision in the 1974 Privacy Act, and it said that any Federal or State agency that was collecting this number had to make clear whether that collection was mandatory or voluntary, how the SSN would be used, and what the statutory authority was for the collection of the Social Security number.

Congress also said that no person should be denied the right or privilege for their decision not to provide a Social Security number,

and I think it was clearly the intent to do everything short of prohibition to limit the use of the SSN as much as possible.

Now, it is certainly the case that, since 1974, there has been an expanded use of the Social Security number, both in the public sector and in the private sector, and some of those benefits have been described for you today. But I would also like to describe for you the views of at least two of the courts that have looked recently at the Social Security number and concluded, as Congress did back in 1974, that this is a very important privacy matter.

For example, Mark Allen Greidinger, who went to register to vote in the State of Virginia back in 1992, refused to provide his Social Security number when he learned that that number would be published in the State voting rolls. Even though the district court said that the State had the right to collect the SSN and use it in this fashion, the Federal appeals court eventually concluded that it was an unreasonable burden on the right to vote to collect the Social Security number for that purpose, and Mr. Greidinger was free to vote in the State of Virginia. The State was required to change its practices because of the important privacy issues associated with the SSN.

The Ohio supreme court, even more recently, said that, even where you have an open record statute, you cannot compel the disclosure of the SSNs of State employees. The benefit is too small and the risk to privacy would be too great.

So I believe there is plenty of support, both on the legislative side and the judicial side, to support the proposals that were put before the committee today.

I would also like to suggest to you that, while legislation limiting the use of the Social Security number will not solve all of the identification problems we face today, I think it would certainly put us on the right track going forward, particularly with this new technology and with the Internet, because, as you may be aware, people using the Internet today, both the technical experts and the consumers, are very much concerned about the protection of their privacy. And when Intel, the world's largest manufacturer of computer chips, proposed to put a unique processor serial number in their new chips—this number would be just like a Social Security number, but literally burned into the microchip—there was such a protest that Intel had to back off that plan and announced just recently that their new chips would not contain these Social-Security-number-like numbers for computers.

So this is a good development, but, at the same time, we are going to face new challenges, new forms of identification, and new threats to privacy. And so for that reason I think it is very important that Congress take this opportunity, when there is this public support in place, this clear legislative tradition and this clear judicial tradition, to support those important safeguards that protect the privacy interests of American citizens.

I thank you again for the chance to testify and would be pleased to answer your questions.

Mr. HAYWORTH. Thank you.

[The prepared statement follows:]

Statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, and Adjunct Professor, Georgetown University Law Center

My name is Marc Rotenberg and I am the executive director of the Electronic Privacy Information, a public interest research organization based here in Washington. I am also on the faculty of the Georgetown University Law Center where I have taught the Law of Information Privacy for ten years. I wrote briefs in two of the leading cases involving the privacy of the Social Security Number, I helped organize the campaign against the Intel unique Processor Serial Number, and I have worked with many technical experts to encourage the development of identification systems that avoid the flaws of the Social Security Numbers and other types of Universal Identifiers.

I appreciate the opportunity to testify this morning. I will briefly review the legal status of efforts to regulate the use of the SSN, discuss some of the recent problems with universal unique identifiers, such as the SSN, and make a few brief recommendations. I believe that legislation to limit the collection and use of the SSN is appropriate, necessary, and fully consistent with US law. I also believe that if Congress fails to act, the problems that consumers will face in the next few years are likely to increase significantly.

History of the SSN and the Efforts to Regulate

The Social Security Number (SSN) was created in 1936 as a nine-digit account number assigned by the Secretary of Health and Human Services for the purpose of administering the Social Security laws. SSNs were first intended for use exclusively by the federal government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Over time, however, SSNs were permitted to be used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.[1]

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 that witnesses have outlined this week. 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.[2]

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

In addition, Section 7 of the Privacy Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it.[3] At the time of its enactment, Congress rec-

---

[1] Pub. L. No. 8709397, 75 Stat. 828 (codified as amended at 26 U.S.C. §§ 6113, 6676) cited in Greidinger at 270928.

[2] Records, Computers and the Rights of Citizens at 135.

[3] (a)(1) It shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. (2) the provisions of paragraph (1) of this subsection shall not apply with respect to -(A) any disclosure which is required by Federal statute, or (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure

Continued

ognized the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of this provision, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation."[4] Short of prohibiting the use of the SSN outright, the provision in the Privacy Act attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed where the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

It is certainly true that the use of the SSN has expanded significantly since the provision was adopted in 1974. This is particularly clear in the financial services sector. In an effort to learn and share financial information about Americans, companies trading in financial information are the largest private-sector users of SSNs, and it is these companies that are among the strongest opponents of SSN restrictions. For example, credit bureaus maintain over 400 million files, with information on almost ninety percent of the American adult population. These credit bureau records are keyed to the individual SSN. Such information is freely sold and traded, virtually without legal limitations.[5]

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

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

The Court said that:

The statutes at issue compel a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote. As illustrated by the examples of the potential harm that the dissemination of an individual's SSN can inflict, Greidinger's decision not to provide his SSN is eminently reasonable. In other words, Greidinger's fundamental right to vote is substantially burdened to the extent the statutes at issue permit the public disclosure of his SSN.[7]

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

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

We find today that the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs. Our holding is not intended to interfere with meritorious investigations conducted by the press, but instead is intended to preserve one of the fundamental principles of American constitutional law—ours is a government of limited power. We conclude that the United

---

is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

See Pub. L. No. 9309579, 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A 552a (West 1996).

[4] S.Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943, cited in Greidinger at 29.

[5] Komuves at 557.

[6] Greidinger at 300931.

[7] Greidinger at 320933.

[8] Greidinger at 36.

States Constitution forbids disclosure under the circumstances of this case. Therefore, reconciling federal constitutional law with Ohio's Public Records Act, we conclude that [the provision] does not mandate that the city of Akron discloses the SSNs of all of its employees upon demand.[9]

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

Problems Beyond the SSN

Efforts to regulate the collection and use of the SSN will not stop all the problems associated with the use of identifiers but they will address the most pressing current problem and could contribute also to future schemes that are less privacy intrusive.

Internet users are particularly concerned about the development of "GUIDs" or Global Universal Identifiers. Last year Internet users launched a campaign against Intel, the largest maker of computer chips in the world, when it proposed to create a Processor Serial Number, unique for each machine, that would make it easier to track and monitor the activities of Internet users. Eventually, under heavy pressure, Intel agreed to withdraw its plan, and more recently Intel announced that it would not include the unique identifier in its next generation of computer chips. This is clearly good news.

But there are also indications that in the absence of strong privacy laws and strong limitations on the use of new ID systems, new problems will arise. Experian, the large credit reporting agency, announced recently a new identification scheme that will enable tracking on a global scale. According to Helen McMillan, vice president of technology for Experian, "Names and addresses are very poor data elements for building search and match algorithms or for maintaining data integrity and hygiene on customer databases. Our industry leading PIN technology delivers the most reliable and accurate consumer identifier on the market." This may be welcome news for marketers who are trying to uniquely track customers and potential customers, but I suspect most consumers and users of the Internet would object strongly to the assignment of such permanent identification numbers.

Microsoft has raised concerns with the recent news that it plans to integrate a biometric identification scheme in the next version of the Windows operating system. A biometric identifier, such as a fingerprint, can be an effective and highly accurate way to establish the identity of an individual, but it can also facilitate a much higher degree of tracking and profiling than would be appropriate for many transactions. Should people who enter federal office buildings, for example, be required to provide biometric identifier, such as a fingerprint scan? It is not hard to imagine that such a practice could develop in the next three to five years. Of course, the problems that will arise when biometric identifiers are compromised are severe. What will happen at the point that your biometric identifiers no longer identify you?

These are issues that the Congress might also consider as it goes forward with legislation to limit the use of the Social Security Number. Perhaps the National Research Council or a fully formed privacy agency could be asked to look in more detail at how best to develop identification schemes that enable online commerce and promote security, while at the same time reducing threats to privacy and the loss of control over identity.

Conclusions

In conclusion, there is clear authority in both legislation and judicial opinion that supports the enactment of further laws to limit the collection and use of the Social Security Number. It is particularly important that such legislation not force consumers to make unfair or unreasonable "choices" that essentially require trading the privacy interest in the SSN for some benefit or opportunity.

Legislation in this area will not solve all of the problems with identity theft or invasive profiling but it will address the most pressing problem and it could encourage the development of better techniques in the future.

---

[9] Beacon Journal at 17.

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

References

Electronic Privacy Information Center, "Social Security Numbers" [http://www.epic.org/privacy/ssn/]

Flavio L. Komuves, "A Perspective on Privacy, Information Technology an the Internet: We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," 16 J. Marshall J. Computer & Info. L. 529 (1998)

Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991)

Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993) and brief amicus curiae for CPSR (Marc Rotenberg and David Sobel) (SSN requirement for voter registration) (lead case on privacy of Social Security number)

Beacon Journal v. City of Akron, 70 Ohio St. 3d 605 (Ohio 1994) and brief amicus curiae for CPSR (Marc Rotenberg and David Sobel) (SSN disclosure of city employees)

Marc Rotenberg, Privacy Law Sourcebook: United States Law, International Law, and Recent Developments (EPIC 1999)

Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens 1080935 (MIT 1973) (Social Security Number as a Standard Universal Identifier and Recommendations Regarding Use of Social Security Number)

STATEMENT OF ROBERTA MEYER, SENIOR COUNSEL, AMERICAN COUNCIL OF LIFE INSURERS

Ms. MEYER. Thank you, Mr. Chairman. I am Robbie Meyer, and I am pleased to be here today on behalf of the American Council of Life Insurers, the ACLI, to testify about the way in which life, disability income, and long-term care insurers use consumers' personal information, including their Social Security numbers, and to tell you about our position relative to the maintenance of the confidentiality of that information.

ACLI member companies are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information.

However, our member companies recognize that consumers do have special concerns about the confidentiality of medical information, so the ACLI board of directors has developed two separate policies dealing with confidentiality, one in relation to the confidentiality of medical information and the other with respect to the confidentiality of non-public personal information. Social Security numbers would fall into the category of non-public personal information.

In developing our policy principles in relation to non-public personal information, which would include Social Security numbers, we sought to balance consumers' desire and legitimate privacy concerns with their concerns for efficient and prompt service and innovative products. Consequently, our principles reflect our support for requirements that financial institutions, including insurers, develop privacy policies and procedures designed to protect the confidentiality, as well as the security of consumers' non-public, personal information, but at the same time our principles reflect our fundamental need to use consumers' personal information, including their Social Security numbers, in order to effect, administer,

and carry out our obligations under our insurance contracts with our customers.

The ACLI strongly supports the privacy protections in title five of the recently-enacted financial services modernization bill, the Gramm-Leach-Bliley Act. Title five subjects financial institutions—again, including all insurers—to one of the most extensive laws relating to privacy regulation that has ever been enacted in the United States.

As a result of this law, consumers doing business with financial institutions will now have clear, comprehensive, and rigorous privacy protections with respect to non-public, personal information, again including Social Security numbers.

This new law also is carefully constructed again to balance consumers' needs to have their privacy protected with the benefits that they obtain from certain uses of that information by financial institutions.

Insurance companies must use and share customers' personal financial information, including, again, their Social Security numbers, in order to perform legitimate, essential insurance business functions. In other words, they have to use this information in order to underwrite applications for coverage, to administer and service our existing contracts, and to perform related product or service functions.

I would like to give you a few examples of how insurance companies actually use Social Security numbers now. They are used by insurers to find missing or lost policy holders so that they can pay them death benefits that they are obligated to pay under existing contracts. Social Security numbers are used to identify policies for policy-holders who may have lost their account numbers. Insurers use Social Security numbers in their call centers in order to authenticate the individuals who call in for information. Social Security numbers are used by insurers to help make it possible to transfer assets from one financial institution to another upon the request of our customers. We use Social Security numbers as PIN numbers so that our customers can do business on line. We use them in connection with our employee group insurance so that individuals can use payroll deduction plans to pay for their coverage.

We are also required to make a number of disclosures to State insurance departments for their regulatory oversight of insurers, and, as required by the Federal Government, such as to the Internal Revenue Service, in order to report certain payments to our customers.

Mr. Chairman, the ACLI would like to thank you for this opportunity to testify; thank you for calling this hearing. Life, disability, and long-term care insurers have a long history of dealing with highly-sensitive, very personal information. We are very proud of our history in dealing with this information. We, again, recognize, however, that consumers have a very legitimate interest in the way in which we handle this information, and that we have an obligation to them to ensure them of the confidentiality of that information.

Thank you.

Chairman SHAW [RESUMING CHAIR]. Thank you.

[The prepared statement follows:]

Statement of Roberta Meyer, Senior Counsel, American Council of Life Insurers

INTRODUCTION

The American Council of Life Insurers (ACLI) is pleased to be here today to testify regarding the ways in which life, disability income, and long term care insurers use consumers' personal information, including their Social Security Numbers, and our position on protection of the confidentiality of that information. The ACLI is a national trade association whose 435 member companies represent approximately 73 percent of the life insurance and 87 percent of the long term care insurance in force in the United States. They also represent 71 percent of the companies that provide disability income insurance.

LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURANCE POLICIES

The fundamental purpose of life, disability income and long term care insurance is to provide financial security for individuals and families. Life insurance provides financial protection to beneficiaries in the event of the insured's death. Proceeds from a life insurance policy may help a surviving spouse pay a mortgage or send children to daycare or college. Disability income insurance replaces lost income when a person is unable to work due to injury or illness. Long term care insurance helps protect individuals and families from the financial hardships associated with the costs of services required for continuing care, for example, when someone suffers a catastrophic or disabling illness.

ACLI POLICY POSITION

ACLI member companies are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information. We also recognize that consumers have special confidentiality concerns in relation to medical information. Therefore, the ACLI Board has adopted separate policies regarding first, the confidentiality of medical information; and second, the confidentiality of other nonpublic personal information. Social Security Numbers would fall within the second category -nonpublic personal information.

ACLI's *Confidentiality of Medical Information Principles of Support* and *Confidentiality of Nonpublic Personal Information Principles Support* are grounded in the industry's long history of dealing with highly sensitive information in a professional and appropriate manner. These principles also acknowledge the changing horizon of the financial marketplace resulting from financial services modernization. Copies of the ACLI "Principles of Support" are attached.

The ACLI supports strict protections for medical record confidentiality, including a prohibition on an insurer sharing medical records with a financial company, such as a bank, for use in determining eligibility for a loan or other credit -even if the insurance company and the financial company are commonly owned. We also support a prohibition on the sharing of medical information by an insurer for marketing purposes.

Our principles on nonpublic personal information reflect our attempt to balance consumers' legitimate privacy concerns with their demands for prompt, efficient service and innovative products. Among other things, we support a requirement that financial institutions, including insurers, establish and maintain policies and practices designed to protect the confidentiality and security of nonpublic personal information against anticipated hazards and unauthorized access to or use of such information. We support a requirement that financial institutions provide notice to consumers and customers describing these policies and practices. We also support a requirement that financial institutions, upon request, provide customers with access and correction rights regarding nonpublic personal information collected about them in connection with applications for life, disability income or long term care insurance.

At the same time, our principles reflect the fact that in order for insurers to serve their prospective and existing customers, they must use and share nonpublic personal information, including Social Security Numbers, in connection with the origination, administration, and servicing of insurance products and services. For example, an insurer may need to use Social Security Numbers to obtain medical information, essential to underwriting, from a particular doctor or hospital, to authenticate consumer callers using a call center, to locate missing policyholders to whom it owes death benefits, to investigate fraud, or to report certain information to the Internal Revenue Service.

THE GRAMM-LEACH-BLILEY ACT

In line with these principles, the ACLI strongly supports the privacy provisions set forth in Title V of the recently-enacted financial services modernization legislation, the Gramm-Leach-Bliley Act (the Act). Title V of the Act subjects financial institutions, including insurers, to one of the most extensive regimes of privacy regulation that has ever been imposed in the United States. As a result of the Act and other federal privacy statutes, including the Fair Credit Reporting Act, consumers doing business with financial institutions now have clear, comprehensive, and rigorous privacy protections, which extend to Social Security Numbers, among many other forms of nonpublic personal information.

Unlike virtually any other types of consumers, financial institution consumers must receive detailed annual disclosures regarding a financial institution's policies for collecting and disclosing their personal information. They must also receive prior notice and the opportunity to "opt-out" of the institution's transfer of their nonpublic personal information to nonaffiliated third parties except under certain limited circumstances. The confidentiality and security of their personal information will be subject to extensive new standards that financial regulators are required to impose on financial institutions.

At the same time, these comprehensive new privacy protections expressly recognize that consumers benefit from financial institutions using consumer information for certain purposes. In short, the new federal privacy law is a carefully constructed balance between the need to protect the privacy of a consumer's nonpublic personal information, which would include Social Security Numbers, and the need to protect the consumer benefits that result from certain uses of that information.

The very nature of life, disability income and long term care insurance involves personal and confidential relationships. These insurers must be able to obtain, use, and share their customers' personal health and nonpublic personal information, including their Social Security Numbers, to perform legitimate insurance business functions. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers. ACLI member companies also believe that the use and responsible sharing of information generally increases efficiency, reduces costs, and makes it possible to offer economies and innovative products and services to consumers that otherwise would not be available.

INDUSTRY FUNDAMENTALS: USE OF PERSONAL HEALTH AND NONPUBLIC PERSONAL INFORMATION BY LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURERS

Once a life, disability income, or long term care insurer has an individual's personal health and nonpublic personal information, the insurer limits who sees it. However, the insurer must use and share that information to perform legitimate, essential insurance business functions -to underwrite the applications of prospective customers, to administer and service contracts with existing customers, and to perform related product or service functions. Life, disability income, and long term care insurers must use and disclose personal information in order to comply with various regulatory/legal mandates and in furtherance of certain public policy goals (such as the detection and deterrence of fraud). Activities in connection with ordinary proposed and consummated business transactions, such as reinsurance treaties and mergers and acquisitions, also necessitate insurers' use and responsible sharing of personal information.

Underwriting the Policy

The price of life, disability income, or long term care insurance is generally based on the proposed insured's gender, age, present and past state of health, possibly his or her job or hobby, and the type and amount of coverage sought. Life, disability income, and long term care insurers gather this information during the underwriting process. Based on this information, the insurer groups insureds into pools in order to share the financial risks presented by dying prematurely, becoming disabled or needing long term care.

This system of classifying proposed insureds by level of risk is called risk classification. It enables insurers to group together people with similar characteristics and to calculate a premium based on that group's level of risk. Those with similar risks pay the same premiums. The process of risk classification provides the fundamental framework for the current private insurance system in the United States. It is essential to insurers' ability to determine premiums which are adequate to pay future claims and fair relative to the risk posed by the proposed insured.

Insurers must be able to obtain, use, and sometimes share both medical and nonpublic personal information, including Social Security Numbers, in order to underwrite applications for coverage. Social Security Numbers are used in a number of

different ways in connection with this process. Insurers sometimes must use proposed insureds' Social Security Numbers in order to obtain medical information about them from doctors and hospitals which use Social Security Numbers as identification numbers. Insurers sometimes use motor vehicle record information in underwriting. In some states, insurers are required to use Social Security Numbers to obtain this information from the motor vehicle department. Insurers sometimes use information from credit reporting agencies in underwriting. Social Security Numbers are sometimes required to obtain information from consumer reporting agencies.

Performance of Essential Insurance Business Functions

Once an insurance policy is issued, insurers use their customers' personal information to perform essential, core functions associated with an insurance contract, such as claims evaluations and policy administration. In addition, insurers also use this information to perform important business functions, not necessarily directly related to a particular insurance contract, but essential to the administration or servicing of insurance policies generally, such as, for example, development and maintenance of computer systems. The ability to use this information for these purposes is crucial to insurers' ability to meet their contractual obligations to their customers and to perform important related service and administrative functions.

Many insurers use affiliates or third parties to perform these business functions which are necessary to effect, administer, or enforce insurance policies or the related product or service business of which these policies are a part. Often these arrangements with affiliates or unaffiliated third parties provide the most efficient and economical way for an insurer to serve prospective and existing customers. The economies and efficiencies devolving from these relationships inure to the benefit of the insurer's customers.

If an insurer were to be prohibited from using this information, or if an individual were to be permitted to withhold consent or to "opt out" of a life, disability income, or long term care insurer's right to use or share his or her personal information for purposes of performing insurance business functions, it would be extremely difficult, if not impossible in some cases, for the insurer to provide that consumer with the coverage, service, benefits, or economies that otherwise would be available. Insurers need to use Social Security Numbers to perform a number of these functions. Insurers view Social Security Numbers as unique identifiers and use them in a number of ways which enable them to better and more efficiently serve their customers and to protect their interests.

For example, Social Security Numbers are used by insurers to find missing or lost policyholders to inform them that they are entitled to life insurance proceeds. Social Security Numbers are used to identify policies owned by an individual who does not have the account or policy number available when a service request is made. Insurer call centers use Social Security Numbers as part of the data requested to authenticate customers who call in with requests for service or for product or account information or status. Social Security Numbers are often needed to transfer assets from one financial institution to another, for example, for purposes of transfers between mutual funds or annuities and life insurance. (Since one financial institution generally does not know the individual's account number at the other financial institution, the Social Security Number is needed to identify the client's identity for the two institutions. This reduces delay, error, and misplaced assets in such transfers.) Insurers also use Social Security Numbers in connection with the administration of pension plans, as identification numbers. They use them as PIN numbers for customers' use of on-line services. They use them in reporting to employer policyholders under employee group insurance plans and in connection with payroll deductions under these plans. These activities inure to the benefit of insurers' customers.

Disclosures pursuant to Regulatory/Legal Mandates or to Achieve Certain Public Policy Goals

Life, disability income, and long term care insurers must regularly disclose personal health and nonpublic personal information to: (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers; (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers' conduct in the marketplace; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information.

Any limitation on these disclosures would seem likely to operate counter to the underlying public policy reasons for which they were originally mandated -to protect consumers.

Life, disability income, and long term care insurers are required to make certain disclosures of information by the federal government. They also need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies, state insurance departments, or the Medical Information Bureau (MIB), the primary purpose of which is to reduce the cost of insurance by helping insurers detect (and deter) attempts by insurance applicants to conceal or misrepresent facts. Any limitation on insurers' right to make these disclosures would seem likely to undermine the public policy goal of reducing fraud, the costs of which are ultimately borne by consumers.

Social Security Numbers are used or disclosed by insurers for a number of these purposes. Life insurers are required to use Social Security Numbers to report to the IRS a variety of payments including, but not limited to, interest payments, certain dividends, and policy withdrawals and surrenders. Social Security Numbers are often integral to insurers' fraud investigations. Social Security Numbers are sometimes used verify identity in connection with inquiries to the MIB. At least one state, Rhode Island, requires that insurers match "deadbeat" parents data before making payments on claims. Social Security Numbers are required for that matching.

Ordinary Business Transactions

In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer be able to disclose company files. Naturally, these files can contain personal information, including customers' Social Security Numbers. Such disclosures are often necessary to the due diligence process which takes place prior to consummation of the deal and are clearly necessary once the deal is completed when the newly created entity often must use policyholder files in order to conduct business.

Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the amount and volume of coverage they can provide. These arrangements often necessitate the disclosure of personal information, which may include Social Security Numbers, by the primary insurer to the reinsurer.

CONCLUSION

Again, the ACLI would like to thank Chairman Shaw for calling this hearing and giving us an opportunity to testify. Life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information. The industry is proud of its record of protecting the confidentiality of medical information and nonpublic personal information; the industry is also committed to the principles that individuals have a legitimate interest in the proper collection and use of individually identifiable information and that insurers must continue to handle such information in a confidential manner.

CONFIDENTIALITY OF MEDICAL INFORMATION

Principles of Support

Life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. The life insurance industry is proud of its record of protecting the confidentiality of this information. The industry believes that individuals have a legitimate interest in the proper collection and use of individually identifiable medical information about them and that insurers must continue to handle such medical information in a confidential manner. The industry supports the following principles:

1. Medical information to be collected from third parties for underwriting life, disability income and long-term care insurance coverages should be collected only with the authorization of the individual.
2. In general, any redisclosure of medical information to third parties should only be made with the authorization of the individual.
3. Any redisclosure of medical information made without the individual's authorization should only be made in limited circumstances, such as when required by law.
4. Medical information will not be shared for marketing purposes.
5. Under no circumstances will an insurance company share an individual's medical information with a financial company, such as a bank, in determining eligibility

for a loan or other credit -even if the insurance company and the financial company are commonly owned.

6. Upon request, individuals should be entitled to learn of any redisclosures of medical information pertaining to them which may have been made to third parties.

7. All permissible redisclosures should contain only such medical information as was authorized by the individual to be disclosed or which was otherwise permitted or required by law to be disclosed. Similarly, the recipient of the medical information should generally be prohibited from making further redisclosures without the authorization of the individual.

8. Upon request, individuals should be entitled to have access and correction rights regarding medical information collected about them from third parties in connection with any application they make for life, disability income or long-term care insurance coverage.

9. Individuals should be entitled to receive, upon request, a notice which describes the insurer's medical information confidentiality practices.

10. Insurance companies providing life, disability income and long-term care coverages should document their medical information confidentiality policies and adopt internal operating procedures to restrict access to medical information to only those who are aware of these internal policies and who have a legitimate business reason to have access to such information.

11. If an insurer improperly discloses medical information about an individual, it could be subject to a civil action for actual damages in a court of law.

12. State legislation seeking to implement these principles should be uniform. Any federal legislation to implement the foregoing principles should preempt all other state requirements.

CONFIDENTIALITY OF NONPUBLIC PERSONAL INFORMATION OTHER THAN MEDICAL INFORMATION PRINCIPLES OF SUPPORT

Life, disability income, and long term care insurers have a long and established history of handling their customers' nonpublic personal information in a professional and confidential manner. Insurers recognize their affirmative and continuing obligation to respect their customers' privacy and to protect the confidentiality and security of their customers' nonpublic personal information.

Insurers support principles in relation to medical information which are described in a separate document. This document sets forth principles which insurers support in relation to nonpublic personal information other than medical information.

1) Requirements with respect to the confidentiality and security of nonpublic personal information should be addressed separately from those in relation to medical information in order to more fully address the different concerns that arise in connection with each type of information.

2) An insurer shall establish and maintain policies and practices designed to protect the confidentiality of nonpublic personal information and to protect against unauthorized access to or use of such information which could result in substantial harm or inconvenience to any customer.

3) An insurer shall establish and maintain policies and practices designed to protect the security of nonpublic personal information against anticipated threats or hazards or unauthorized access to or use of such information which could result in substantial harm or inconvenience to any customer.

4) An insurer shall provide its customers with a notice of the policies it maintains to protect the confidentiality and security of nonpublic personal information. This notice shall be provided at the time the insurer enters into an insurance contract and at least annually thereafter for as long as the contract is in force.

5) In order to serve its prospective and existing customers, an insurer may share its customers' nonpublic personal information in connection with the origination, administration, or servicing of its products or services or to engage in other non-marketing business operations. For example, an insurer may share nonpublic personal information to provide consolidated statements of an individual's different accounts, to prevent fraud, or to comply with the law or a civil or criminal subpoena or summons.

6) An insurer shall not share a customer's nonpublic personal information within its corporate family for marketing products or services unless the insurer's notice says that this information may be shared within its corporate family for this purpose. An insurer shall not share a customer's nonpublic personal information outside its corporate family for marketing unless: (a) the insurer's notice says that nonpublic personal information may be shared by the insurer outside its corporate family for this purpose; and either (b) the customer is given the opportunity to direct

that it not be shared; or (c) the products or services to be marketed are: ((1)) products or services of the insurer; or ((2)) offered by the insurer and another financial institution (or institutions) pursuant to a joint agreement.

8) An insurer shall not share a customer's nonpublic personal information with another person or entity unless such party is subject to the same restrictions on disclosure of nonpublic personal information to which the insurer is subject.

9) Upon request, a customer of an insurer is entitled to have access and correction rights regarding nonpublic personal information about the customer collected from third parties in connection with an application for life, disability income, or long term care insurance.

10) In order to provide insurers' customers protection that is as uniform as possible, any legislation or regulation seeking to impose requirements with respect to the confidentiality and security of nonpublic personal information shall be applicable in the same manner to all entities which collect and maintain such information.

11) State legislation seeking to implement these principles should be uniform. Any federal legislation implementing these principles should preempt any state law imposing requirements with respect to the confidentiality and security of nonpublic personal information.

Chairman SHAW. I have a couple of questions that I would like to ask the entire panel.

We just heard some legislative proposals—and I believe all of you were here—that would restrict the use of a Social Security number. Some proposals, such as Dr. Paul's bill, would restrict the use of Social Security numbers by government agencies. Others, like Mr. Kleczka's proposal, would restrict commercial use, sale, and exchange of Social Security numbers unless the entity has the customer's written consent to support these proposals.

For those of you who oppose the proposals, can you tell us specifically what provisions you propose and what improvements can be made?

Mr. Pratt?

Mr. PRATT. Our concern is a general concern, and let me respond in two ways. With Congressman Paul's proposal, if it were to remove the use of the Social Security number from, say, public records, this means that we would have a more difficult time putting a tax lien into a consumer report that would be used by credit grantors for safety and soundness or in noting a bankruptcy, so I think part of the question is the devil of the details. Does this mean the Social Security number is completely removed from many different public domains, or is it just more controlled or more limited? I have not actually read the entirety of the Congressman's proposal to respond more specifically than that.

But Congressman Kleczka's proposal in removing the Social Security number from the commercial domain—and he has mentioned credit headers several times—one point I would like to bring up is that we have mentioned already that, outside of the Fair Credit Reporting Act, which certainly governs and limits otherwise our use of information, including the Social Security number, we have established ourselves through the individual reference services group to further limit the disclosure of that information called "header information." It is identifying information, and that's a way that we have attempted to respond to the policy, and to try and restrain and balance the benefits that we think are out there societally for this type of data, and, at the same time, to acknowledge I think what has been said by a number of my co-panelists,

and that is this is not a number that should be out there in the general marketplace for all purposes.

Chairman SHAW. You, sir?

Mr. MIERZWINSKI. Mr. Chairman, US PIRG supports the credit header loophole bill, Mr. Kleczka's bill. We also have an official position on Mr. Markey's bill on financial privacy to close the loopholes in title five of the Gramm-Leach-Bliley Act.

The other three bills, the three specific bills before the committee, we support in principle, but our board has not yet taken a formal position on them.

Chairman SHAW. Ms. Moore? If any of you all want me to repeat the question, I will be glad to do it.

Ms. MOORE. I think I have it.

Chairman SHAW. Okay. Go ahead.

Ms. MOORE. H.R. 1450, Congressman Kleczka's bill, does not really affect the DMVs, because the Driver Privacy Protection Act forbids sale and distribution of the Social Security number by DMV, so that makes that issue moot for DMVs.

H.R. 220 does impact the motor vehicle agencies and we have our concerns as far as the SSN has become a unique identifier for exchanging information into the CDLIS system, the nine million commercial drivers that we track through there.

The primary concerns would be the inability to electronically transfer driver history records between jurisdictions, the cost States would have to incur to modify the computer systems, and utmost, the increase in fraud or the inability to verify our drivers.

Chairman SHAW. Thank you.

Mr. ROTENBERG. Mr. Chairman, let me say, just as a matter of U.S. privacy law, I think it is very consistent with the original purpose of the Social Security number, which is that it would be used solely to administer the benefits of the program, as well as the language in the 1974 privacy act, to support the proposals that have been put forward today.

I should also point out, in a very recent opinion from the U.S. Supreme Court, an opinion upholding the Drivers Privacy Protection Act, even after it had been challenged in several of the States, the court made quite clear that, to the extent that personal information has been sold in interstate commerce, then it clearly could be regulated by the Congress, so I do not think there is any question, particularly where you have services that are literally selling a person's Social Security number and enabling identity theft and other problems, that that would be appropriate legislation and that it would be upheld by the courts.

Chairman SHAW. I believe we had information last Tuesday about who owns those numbers, and I think that the testimony that we have says that the numbers are, indeed, the property of the Federal Government. We have not researched that, ourselves—at least I do not believe we have—but those numbers are the property of the United States Government and the Social Security Administration, and we certainly would have the right to regulate how they are used or how they are distributed.

Ms. Meyer, I think you answered the question—you mentioned in your testimony that the Social Security numbers are useful in the administration of service of the account. I have great doubt

about that, except when you got to the point of reporting earnings to the Internal Revenue Service. Then that does become a point that I think that would be well taken in that area.

But the other areas that you mention, I have some—I doubt that that is actually needed. I mean, we go through the policy number and everything else. But I am particularly curious, in your situation, if I were to want to buy a life insurance policy and I said, "No, I do not want to give you my Social Security number," would it be then the salesman would say, "Then you are not going to get this life insurance policy?"

Ms. MEYER. That's a—

Chairman SHAW. Is that a truthful statement? Can you buy life insurance without divulging your Social Security number?

Ms. MEYER. To my knowledge, Social Security numbers—and I would have to check this and see—that information is not required information. But I will confirm that. I think the concern is that it is so integral, because of the list of services or different things that we use it for, it is so integral to our ability to provide products and services to our customers, that it would be very difficult for us to do lots of things for that individual—

Chairman SHAW. Why?

Ms. MEYER.—that we could not do otherwise.

Chairman SHAW. Why?

Ms. MEYER. Well, for example, I am told by our member companies that, in underwriting an application for a life insurance policy, for example, it is often very important that we obtain medical information in order to determine the rate at which we should insure the individual.

Often, we have to get information from doctors and hospitals relative to the individual's medical condition. We are told that in some circumstances doctors and hospitals will not release that information to us unless we have the individual's Social Security number.

Chairman SHAW. Well, you have to get a consent form signed by that individual, anyway, do you not?

Ms. MEYER. Absolutely. We do get a consent form to get that information for purposes of underwriting; however, as I said before, there are a number of other purposes that we use the Social Security number for in order to administer the contract.

One problem we have is that there are literally millions of contracts out there with Social Security numbers that are part of the file, so if individuals revoke our ability to use Social Security numbers, then we would literally have to go through millions of files to delete the Social Security numbers out of the files; so we have problems, both from a practice standpoint and for getting information. I understand that there are still some States that require use of Social Security numbers to get motor vehicle information that we would need to investigate applications for coverage, as well. So we would have problems getting information, plus I am told that we use these Social Security numbers in our call service centers to make sure that we are giving out information to the correct individual, you know, to help them locate policies that they may have lost.

So we might need it to get information, as well as to perform service functions. Also, I am told that State insurance departments use Social Security numbers to help people identify coverage that they may not be aware of.

So I think the use of the numbers as identifiers, to be sure that we are getting information to the correct individuals and also to help consumers, is built into the system right now.

Chairman SHAW. Is your industry in any way prohibited from selling that information or sharing it with other agencies?

Ms. MEYER. Right now our industry is now subject to the rules of title five of the Gramm-Leach-Bliley Act. That would include, in our view, non-public personal information. It would include Social Security numbers within the definition of non-public personal information, which would mean that we could not share, which would include selling information with a non-affiliated third party, without giving the individual the opportunity of telling them, giving them notice of what we are doing, and also the opportunity to opt out, except if the sharing fell within one of the stated exceptions of the Gramm-Leach-Bliley Act.

Chairman SHAW. Speaking of that act, you have the ability to share, sell, transfer personal information to third parties who are not regulated by these laws. How is this information protected once it is sold or transferred to third parties?

Ms. MEYER. Actually, title five does place restrictions on third parties who receive information from us. Those third parties would be subject to the provisions of title five that say that a third party recipient of the information cannot use the information in any way in which the financial institution could not use it. So a third party recipient would be subject to the same constraints as the financial institution, as I understand the law.

Chairman SHAW. Mr. Tanner?

Mr. TANNER. Thank you very much, Mr. Chairman. I wish we had more time. This is a fascinating discussion. In the interest of time, I am going to read all of your statements, but I want to ask Mr. Pratt—a couple of days ago Colonel Stevens testified that, notwithstanding his best efforts to notify various credit bureaus that this was fraudulent activity going on on his Social Security number, he testified that every four to six months it was recycled and reappeared.

What, if anything, is your organization doing to stop that? And do not you feel that there is some obligation to verify the information and this repeated publication, knowing it to be false, or someone knowing it to be false may be legally actionable?

Mr. PRATT. Congressman, I think part of the response is found in the—we agree with you that we need to be doing more in the area of helping victims of identity theft, and I think that is thematically something you will hear across the board.

The initiatives that we announced in March were really also then announced at the Identity Theft Summit, where we presented those, and that was the summit sponsored by the Treasury Department, along with other agencies—Secret Service and so on.

One of the areas of response is to acknowledge that very problem of information showing back up in the file.

Part of the answer is found in the Fair Credit Reporting Act. Under the 1996 amendments, if data goes back into the file, we are obligated to send a letter to the consumer asking them to confirm the information if it does go back in, and that's part of the accuracy standard that we have to live by.

Part of the step is a new software product that we are going to launch this year, because it is true that when you hear a consumer who says, "I have been a victim of identity theft," it appears to go on and on and on.

The way the FCRA is structured, at a point in time we have to reinvestigated and take care of the problems on the file, and there is a limited time frame in which to do that, but the question is: what do you do after that file has been brought whole? Is that it? Is the crime over or does it go on?

In our estimation, we have another responsibility, and that's a responsibility we have put into our voluntary initiatives. We are going to keep track of that file. We are going to look at file activity. We are going to notify consumers of unusual activity in that file to make sure that we stay in touch with that consumer to keep the information from, if you will, polluting the consumer's credit history on a long-term basis.

So we think we are tracking in the right direction to try to build the right technologies in place and to create a better linkage between us and the consumer, not just between us and the credit grantor, so that is part of our response.

Mr. MIERZWINSKI. Congressman, could I add very briefly to that?

Chairman SHAW. Yes.

Mr. MIERZWINSKI. US PIRG believes that some of the steps that the credit bureaus are taking are good first steps, but I just want to point out that some of the problems are not the credit bureaus' fault, and I am not totally agreeing that the credit bureaus should not be blamed for part of this, of course.

Mr. PRATT. But I am writing this down that you said that.

Mr. MIERZWINSKI. But he is writing this down.

We feel and other privacy groups feel that part of the blame has to be laid at the feet of the banks, department stores, and other creditors that, in fact, issue credit without adequately verifying that the consumer is the actual consumer, and they will often, even though there is perhaps a fraud flag on a report, issue credit.

We think that that is part of the problem that Congress needs to look into in strengthening the Identity Theft Deterrence Act of 1998.

So it is the credit bureaus and the creditors who we think are both part of the problem.

Mr. PRATT. Part of our effort, Congressman, was to, in fact, launch a better program to make sure our customers, in partnership with us, understand the security alert—this alert that Mr. Mierzwinski is referencing—and to make sure they know where to look for it in the, if you will, data transmission, and then how to then respond to it.

We also have products that have been brought on line which notify our customers where there's differences in incoming applicant data and the data we have on file.

As I said in the testimony, there are 42 million consumers who move every year. Clearly, some of the address change activity on the files is legitimate.

One of the products we have informs our customers, though, that, in fact, there is a difference between what you have sent us, to some extent, and what we have on file, and this is another way for us to partner with our customers and to cue them that something is different about the data, giving them that opportunity to investigate it further.

Mr. TANNER. I have some more questions, but, in the interest of time, Mr. Chairman, I have got to go. Thank you. I thank all of you.

Chairman SHAW. I would like to just raise one more question with you, Mr. Pratt, and that is the question of what good is it or what usefulness is it to have your Social Security number put on the back of a check when you are cashing a check? You heard Mr. Kleczka say that he gave one to Toys 'R Us and he made up a Social Security number because he did not want to put it on there. What good is it?

Mr. PRATT. Well, I can answer that in part because our trade association does represent some companies that produce a specific type of FCRA governed database generically called a "check services database." Check fraud is an enormous problem in this country. It always has been, for many, many years, and it continues to be a problem.

One way for us to cross check and provide products for a retailer or grocery store to make sure that they minimize check fraud is to use that number, at least in this case, for a matching purpose, to make sure that we are matching back into this check database to determine whether or not we have had fraudulent—

Chairman SHAW. At what point is the match made?

Mr. PRATT. Well, for us the match would be made between the point of sale terminal, which is the register, as we used to call it, and the system that we have in place, which could be anywhere in the country and just a resident database.

Why it is written on the check versus just simply entered in, if you will, to use as a match, I really cannot deal with that element of it. I do not know if that is more of a retail question that might have to be addressed. But for us it is a matching question.

Chairman SHAW. Well, you mean this matching is done while the customer is still standing there at the register?

Mr. PRATT. Yes, sir.

Chairman SHAW. And they need the Social Security number in order to do that?

Mr. PRATT. That would be one element of how we are able to make sure that we are not, first of all, falsely registering and saying this consumer's check should not be processed, if you will, so it is a more precise way for us to achieve the match, make sure that we deliver accurately.

One of the standards under the Fair Credit Reporting Act is to make sure that we match the request for information with the correct record internally. In most cases with a check database of this type, the records is going to come back "no record found," meaning the majority of citizens are not bouncing checks or having a prob-

lem with check fraud. So that's one of the ways that we reduce the problem of consumers being inconvenienced.

Chairman SHAW. What does a cashier do? How do they transmit that number while they are in the checkout line?

Mr. PRATT. That number is entered in at the register, I believe.

Chairman SHAW. They enter the Social Security number instead of the name and bank?

Mr. PRATT. Well, that might be one way for us to check, but there might be other fraudulent accounts that are not listed under that bank name, so these databases cross check name and information against other accounts to make sure we are not opening up or processing an additional check against an account which has already been registered as opened fraudulently.

I do not think I made sense.

Chairman SHAW. Well, it did not sink in at this end. Go ahead.

Mr. PRATT. In other words, if I were the criminal and I was perpetrating bank fraud, if you will, by opening up falsified checking accounts, there might be more than one checking account in play, and so, as one checking account becomes designated as fraudulent and is registered, I might want to try to flip, if you will, to the next checking account I have opened up in order to perpetrate the crime all over again.

So, in order to reduce the incidence of that type of check fraud, these databases can cross check and say—

Chairman SHAW. Well, when I open a checking account, they will get my Social Security number. But they just ask me to give it to them. They do not ask to see a Social Security card or any type of identification that has a Social Security number on it. So if I wanted to get involved in that, just borrow somebody else's Social Security number and put it in there.

Mr. PRATT. In terms of what the security procedures are with the lending institutions, it is harder for me to answer that part of the question.

Chairman SHAW. Do they verify that they got the right Social Security number?

Mr. PRATT. I believe they do, but, again, I think there are others who might be better able to respond to that part of the question.

Chairman SHAW. How do they do that? Can I get in touch with the Social Security Administration and say, "Is John Dokes' number such and such"?

Mr. PRATT. I do not think the Social Security Administration allows private industry to do that.

Chairman SHAW. I hope not. So how do they verify that they have the right number?

Mr. PRATT. One way is to access a consumer report to determine whether or not it matches against a consumer report.

Chairman SHAW. So the consumer report has the Social Security number on it. Where did the consumer report get the number?

Mr. PRATT. These numbers are added into the system based on applicant data coming in and the regular cycle of data reporting into the consumer reporting Social Security. Social Security number is often an element of the information we receive from what are called "data furnishers."

Chairman SHAW. But if that name and Social Security number is not in your database, then they put it in the database, and all of the sudden they are in there with that number that is fraudulent.

Mr. PRATT. Well, it is certainly one of the problems of identity theft is that it can result in inaccurate, fraudulent information being loaded into the system. In this case, we do not keep checking account information, so that would not be in the system.

It is true—one of our challenges is to keep the fraudulent data out and to keep the accurate and correct information in.

Chairman SHAW. Okay. Well, thank you all for being here. We have got our work cut out for us, that's for sure.

I have two things I am told for the record, two inserts, the opening statement of Mr. Matsui, which I had already said for all of the Members who have an opening statement, and a letter from the Social Security Administration Inspector General supporting the Kleczka bill.

[The information follows:]

JAMES G. HUSE, JR.

The Honorable Jerry Kleczka
House of Representatives
Washington, D.C. 20515

Dear Mr. Kleczka:

Social Security number (SSN) misuse is a critical issue that impacts greatly on the lives of American citizens. From the beginning, our office has taken a proactive stance to work with other Federal organizations to reduce the incidents and impact of SSN misuse. However, given the current proliferation of the SSN in both governmental and private transactions, our task appears to be increasing with each passing day.

As I stated in my May 9, 2000, testimony before the Social Security Subcommittee's hearing on SSN misuse, I believe H.R. 1450 is an excellent start at legislatively protecting the integrity of the SSN and restoring the confidence of the American people in the security of their personal identifying information.

I appreciate your support for the IG community. If I can be of further assistance to you or your staff, please do not hesitate to contact me at 41009966098385.

Sincerely,

JAMES G. HUSE, JR.
Inspector General of Social Security

Chairman SHAW. Thank you again. We appreciate your attendance and your testimony.

[Questions submitted by Chairman Shaw to Mr. Rotenburg, Mr. Huse, Ms. Burke Moore, Mr. Pratt, Ms. Bovbjerg, Mrs. Meyer and Mr. Mierzwinski, and their respective answers, follow:]

May 31, 2000

The Honorable James G. Huse, Jr.
Inspector General
Social Security Administration
6401 Security Boulevard
Suite 300
Baltimore, MD 21235

Dear Mr. Huse:

Thank you for testifying before our Subcommittee regarding the use and misuse of the Social Security number (SSN). In order to complete our hearing record, I would appreciate your answering the following questions:

1.You mention that a good deal of SSN misuse creates a cost to the Social Security program because people fraudulently apply for benefits. Has anyone estimated the cost of SSN misuse to the Social Security Trust Funds? Has anyone estimated the cost of SSN misuse to private-sector businesses?

2. What are the key vulnerabilities in SSA's business processes relating to the issuance of SSNs? What recommendations have you made and how has the agency responded?

3. GAO testified before you that there is no federal law that regulates the overall use of SSNs. Is such a law needed? Is it feasible to enact, administer, and enforce such a law?

4. GAO testified that many private-sector businesses and government agencies have adopted voluntary policies aimed at protecting privacy and reducing SSN misuse. Can self-regulation be an effective way to reduce SSN misuse?

5. You note that your office issues a list of the 100 employers with the most suspended wage items (i.e., wages that do not match up to an SSN.) What are the reasons why these reported wages don't match up to an SSN? One of your recommendations to the Social Security Administration was to implement a correction action plan for these employers. Has SSA acted on this recommendation?

6. You mention that it costs SSA 50 cents to post a wage item when it is originally submitted compared to $300 to correct it later. Why are the costs to correct wage items so high?

7. You mention the Identity Theft Act in your testimony. Are there any other laws aimed at protecting privacy and preventing fraud? In your opinion, are existing laws enforced effectively or do we need new laws to help prevent identity theft and other types of SSN misuses?

8. Can you please elaborate about the Federal Trade Commission's specific role in SSN misuse?

9. One of your recommendations to combat SSN fraud is to regulate the sale of SSNs. How can this be done? What exceptions would the law have to include? Would there be any downside for consumers?

10. The widespread use of the SSN creates a lot of administrative headaches for SSA, such as reissuing SSNs for people who have been the victims of identity theft. To your knowledge, has SSA ever developed a proposal that addresses this issue, especially one that seeks to limit how the SSN is used by other government agencies and the private sector?

11. One of your recommendations for reducing fraud is that people should show photo ID when conducting business with SSA. That seems like a useful suggestion. Still, are there any arguments that some might make against it? Do you know what portion of the population do not have a photo ID? Wouldn't this cut down on fraud in other areas of SSA programs as well?

12. At the same time, SSA is studying conducting certain services online, such as applications for retirement benefits. Obviously, at least for now, showing a picture ID won't work in that setting. How can the trend toward online applications be reconciled with your suggestion of showing a photo ID to receive services?

13. One of your recommendations is to legislate statutory law enforcement authority for your investigators. How would this authority for your investigators assist in combating SSN fraud?

14. You also suggest broadening civil monetary penalty authority for the sale or misuse of an SSN. Would you provide more details about this recommendation?

15. You recommend that new technologies and databases be fostered to help employers, government, and private industry verify that names and/or SSNs are correct to improve the identification process. From a practical standpoint, how would this work? Would opening such a database to employers and private industry create new opportunities for misuse of this information? Who would monitor this process?

16. For the record, please provide a breakdown of the statistics from the SSA/OIG Hotline for the first six months of this fiscal year. I would like the total number of allegations received by the Hotline; the total number of these allegations related to SSN misuse (of this figure, please break this down further into the number related to the programs and operations of SSA and the number not so related).

I thank you for taking the time to answer these questions for the record and would appreciate your response by no later than June 23, 2000. In addition to a hard copy of your response, please submit your response on an IBM compatible 3.5-inch diskette in WordPerfect or Microsoft Word format. If you have any questions concerning this request, please feel free to contact Kim Hildred, Staff Director, Subcommittee on Social Security at (202) 225099263.

Sincerely,

E. CLAY SHAW, JR.
Chairman

May 31, 2000

Ms. Katherine Burke Moore
Chair, International Board of Directors
American Association of Motor Vehicle Administrators
c/o Linda Lewis
4301 Wilson Blvd.
Suite 400
Arlington, VA 22203

Dear Ms. Burke Moore:

Thank you for testifying before our Subcommittee regarding the use and misuse of the Social Security number (SSN). In order to complete our hearing record, I would appreciate your answering the following questions:

1. Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel about a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?

2. The fact that SSNs are so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place?

3. In the next 10 or 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics? Will the debate over the privacy and security of SSNs eventually be overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments?

5. Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples? If SSN use were restricted, what would be the downside for consumers? If the use of SSNs was restricted by Federal law, what impact would it have on your members? M

6. Most states give people the option of displaying their SSN on their driver's license or using a different number issued by the DMV. Has this option created administrative difficulties for States? Has it reduced accuracy or the ability to correctly identify people?

7. Your testimony indicated that States need to collect SSNs for a variety of law enforcement and public safety reasons. What are States doing to protect this information once it is collected? How do States ensure that the information is correct and not fraudulent? Do States collect SSN information solely for law enforcement and public safety reasons? Are SSNs used by the States for any other purposes?

8. Do States transfer, sell, or share SSN data to third parties under any circumstances? How many pieces of identifying information do States collect (for example, name, gender, age, address, etc.) With so many pieces of identifying information, why is the SSN needed to positively identify an individual?

9. You indicated that your members have continued their efforts to enhance the security of driver license credentials. Could you describe these efforts?

10. In your testimony you indicated that 49 states allow individuals to have a number on their drivers license other than the SSN. However, SSNs are used for checking information across state lines and with SSA. If you stopped using the

SSNs for that purpose, wouldn't the DMV-issued numbers that actually appears on the license become in effect a new national identifier, putting us back in the same place we started? Why do some States (Hawaii and Washington, DC) still require the SSN to be displayed on driver's licenses? Why don't they use their own internal identifying numbers?

I thank you for taking the time to answer these questions for the record and would appreciate your response by no later than June 23, 2000. In addition to a hard copy of your response, please submit your response on an IBM compatible 3.5-inch diskette in WordPerfect or Microsoft Word format. If you have any questions concerning this request, please feel free to contact Kim Hildred, Staff Director, Subcommittee on Social Security at (202) 225099263.

Sincerely,

E. CLAY SHAW, JR.
Chairman

May 31, 2000

Mr. Stuart K. Pratt
Vice President, Government Relations
Associated Credit Bureaus, Inc.
1090 Vermont Avenue, N.W.
Suite 200
Washington, DC 20005

Dear Mr. Pratt:

Thank you for testifying before our Subcommittee regarding the use and misuse of the Social Security number (SSN). In order to complete our hearing record, I would appreciate your answering the following questions:

1. Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel about a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?

2. The fact that SSNs are so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place?

3. In the next 10 or 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics?

4. Will the debate over the privacy and security of SSNs eventually be overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments?

5. Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples? If SSN use were restricted, what would be the downside for consumers?

6. If the use of SSNs was restricted by Federal law, what impact would it have on your operations?

7. On May 9, we heard testimony from a couple (Lt. Col. Stevens and Mrs. Stevens) who have had their identities stolen. Their story raised several troubling issues.

First, the Stevens told us that fraudulent accounts were opened using their SSNs even though all of the information on the applications was incorrect, including their names, addresses and birth dates. The SSN was the only piece of information that was correct on the applications.

A second troubling issue is that credit-reporting agencies verified this incorrect information. Variations of a name, address, place of employment, age, or spouse's name were not questioned -if the SSN matched up, the information was verified and the fraudulent application was approved.

—Can you explain how these fraudulent applications could have been verified and approved?

—Why did the credit-reporting system fail in this case?

—Under current law, are creditors and credit-reporting agencies accountable when their negligence contributes to identity theft and other SSN misuses? Do you think that creditors and credit-reporting agencies should share responsibility in such cases?

8. One of the disturbing items from the testimony by the Stevens was their statement that the collection agencies did not believe them. They had to prove they were victims of identity theft. What would you say to the Stevens? Should the burden of proof fall on the victims of identity theft?

9. The Stevens explained that they have been prevented from buying a home, establishing credit accounts, or making normal purchases because their credit was ruined by no fault of their own. How do credit reporting agencies assist identity theft victims today?

10. When someone's credit is ruined because of the identity theft, how long does it take to clear the bad credit from the victim's credit report? The Stevens complained that bad accounts are recycled through the same collection agency or they are turned over to other collection agencies so that the same bad debt keeps reappearing on the credit report. Can you explain to us how the process works?

11. You noted in your written testimony that your members collect SSNs *only when they are voluntarily provided by consumers.* But isn't it true that in many cases, consumers *must* provide their SSNs to receive credit? For example, can a customer be approved for a mortgage without giving his or her SSN? If consumers must provide SSNs to receive services, how voluntary is this disclosure?

12. Your members' use of the SSN is governed by the Fair Credit Reporting Act. In addition, you have a long list of voluntary initiatives your members have undertaken to combat identity theft and SSN misuse. Do all of your members follow these initiatives? What happens to them if they don't? Despite these efforts, fraudulent uses of SSNs is on the rise. Does this indicate that existing laws are not being enforced effectively or perhaps self-regulation is not working? What recommendations do you have to reduce SSN misuse?

13. How does a consumer reporting agency get its information? How does it determine what information to place in a record and what information not exclude? How is the authenticity of the information verified to ensure that incorrect information is not being posted?

I thank you for taking the time to answer these questions for the record and would appreciate your response by no later than June 23, 2000. In addition to a hard copy of your response, please submit your response on an IBM compatible 3.5-inch diskette in WordPerfect or Microsoft Word format. If you have any questions concerning this request, please feel free to contact Kim Hildred, Staff Director, Subcommittee on Social Security at (202) 225099263.

Sincerely,

E. CLAY SHAW, JR.
Chairman

May 31, 2000

Ms. Barbara D. Bovbjerg
Associate Director
Education, Workforce and Income Security Issues
Health, Education and Human Services Division
U.S. General Accounting Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Bovbjerg:

Thank you for testifying before our Subcommittee regarding the use and misuse of the Social Security number (SSN). In order to complete our hearing record, I would appreciate your answering the following questions:

1. The term "national identifier" has a very bad connotation for many people. In your opinion, has the Social Security number become a national identifier?

2. In your testimony, you indicated that there is no federal law that regulates the overall use of SSNs. In your view, is such a law needed? Is it feasible to enact, administer, and enforce such a law?

3. As you pointed out in your testimony, the Social Security number was created as a means of tracking workers' earnings and eligibility for Social Security benefits. It was never intended to serve as a personal identification document. Only certain information is maintained by SSA as part of its Social Security number database. What information is available? What proof is required to obtain a Social Security number? How have these proof requirements changed over time?

4. Despite public concerns about sharing personal information in today's electronic world, does the public benefit from the widespread use of SSNs and the sharing of personal information? Can you provide some examples?

5. If someone refuses to disclose their SSN to a private business, can the business, by law, decline to provide the service? For example, if someone refuses to provide their SSN on a loan application, can the bank deny the loan?

6. What are the possible effects on businesses of restricting their use of SSNs?

7. You mentioned in your testimony that many businesses and agencies are voluntarily restricting the use of SSNs to help protect their customers' privacy and reduce SSN misuse. Can you please elaborate on some of these self-regulatory policies?

8. One area not discussed in your written testimony is e-commerce. How has the high-tech economy affected SSN use? In general, can people conduct business on the internet without providing their SSNs? How would restricting the use of SSNs affect e-commerce?

9. You indicated that "information brokers" collect SSNs for the sole purpose of selling them. What exactly is an information broker? How are consumers served by this industry? What is the downside of limiting their activities? Why do information brokers need peoples' SSNs?

10. According to your testimony, the Social Security Act declares that SSNs obtained by authorized individuals afer October 1, 1990 are confidential and cannot be disclosed. If the Social Security Act prohibits the disclosure of SSNs, why is their use so widespread and why are businesses allowed to ask for the SSN?

11. If the use of the SSN were restricted by federal law, is it likely that another personal identifier would take its place?

I thank you for taking the time to answer these questions for the record and would appreciate your response by no later than June 23, 2000. In addition to a hard copy of your response, please submit your response on an IBM compatible 3.5-inch diskette in WordPerfect or Microsoft Word format. If you have any questions concerning this request, please feel free to contact Kim Hildred, Staff Director, Subcommittee on Social Security at (202) 225099263.

Sincerely,

E. CLAY SHAW, JR.
Chairman

May 31, 2000

Mrs. Roberta Meyer
Senior Counsel
American Council of Life Insurers
1001 Pennsylvania Avenue, NW
Washington, DC 20004

Dear Mrs. Meyer:

Thank you for testifying before our Subcommittee regarding the use and misuse of the Social Security number (SSN). In order to complete our hearing record, I would appreciate your answering the following questions:

1. Are there any legitimate uses of the SSN that you think should be allowed (such as law enforcement)?

2.Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel about a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?

3. The fact that SSNs are so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place?

4. In the next 10 or 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics? Will the debate over the privacy and security of SSNs eventually be overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments?

5. Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples?

6. If SSN use were restricted, what would be the downside for consumers? If the use of SSNs was restricted by Federal law, what impact would it have on your operations?

7. Your testimony indicates that you often share personal information with third parties who administer, serve, or enforce insurance policies. Do these third parties, in turn, share or sell the information to others? Do you know how these third parties protect the information which you give them?

8. If sharing personal information is necessary in the insurance business, do you disclose to your customers who the information is shared with and how it is used?

9. You note that the privacy provisions in the recently enacted Gramm-Leach-Bliley Act subject insurers to the most stringent privacy regulations ever imposed in the United States. When you share personal information with third parties, are these third parties subject to the same privacy provisions or do you lose control of what happens to the information once it is given to a third party?

10. You note that prohibiting the use or sharing of SSNs would make it almost impossible to provide consumers with certain services. How were these services provided before the widespread use of SSNs? Has the SSN always been the primary identifier in the insurance industry?

I thank you for taking the time to answer these questions for the record and would appreciate your response by no later than June 23, 2000. In addition to a hard copy of your response, please submit your response on an IBM compatible 3.5-inch diskette in WordPerfect or Microsoft Word format. If you have any questions concerning this request, please feel free to contact Kim Hildred, Staff Director, Subcommittee on Social Security at (202) 225099263.

Sincerely,

E. CLAY SHAW, JR.
Chairman

May 31, 2000

Mr. Edmund Mierzwinski
Consumer Program Director
U.S. Public Interest Research Group
218 D Street SE
Washington, DC 20003

Dear Mr. Mierzwinski:

Thank you for testifying before our Subcommittee regarding the use and misuse of the Social Security number (SSN). In order to complete our hearing record, I would appreciate your answering the following questions:

1. Are there any legitimate uses of the SSN that you think should be allowed (such as law enforcement)?

2. Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel about a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?

3. The fact that SSNs are so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place?

4. In the next 10 or 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics? Will the debate over the privacy and security of SSNs eventually be overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments?

5. Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples? If SSN use were restricted, what would be the downside for consumers?

6. Your testimony mentioned the fact that anyone can purchase someone else's personal information, including SSNs. Can you tell us more about the sale of SSNs? Who is allowed to sell SSN's? Who is allowed to buy them? Why is this information sold and bought? Are there any laws which currently regulate the sale of SSNs?

7. The widespread use of SSNs definitely contributes to identity theft. However, it can also protect consumers by improving the accuracy of record keeping. For ex-

ample, if John Smith is wanted for child support payments, having his SSN may make it easier to find the right John Smith. Are you concerned that restricting the use of SSNs may make it more difficult to track down the right person for legitimate reasons?

8. If I understood your testimony correctly, credit bureaus often collect personal information about consumers. Some of that information is then sold to third parties for various reasons. In your opinion, the practice of collecting information for one reason and then using it for another without the consumer's consent is unfair. Are you proposing that credit bureaus obtain the customer's consent before selling personal data, or are you opposed to the practice of selling personal information altogether?

9. We all agree that stories of identity theft, such as the Stevens' story, are atrocious. However, would you agree that unique identifiers do serve a purpose within the business community?

I thank you for taking the time to answer these questions for the record and would appreciate your response by no later than June 23, 2000. In addition to a hard copy of your response, please submit your response on an IBM compatible 3.5-inch diskette in WordPerfect or Microsoft Word format. If you have any questions concerning this request, please feel free to contact Kim Hildred, Staff Director, Subcommittee on Social Security at (202) 225099263.

Sincerely,

E. CLAY SHAW, JR.
Chairman

Statement of American Association of Motor Vehicle Administrators

1. Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel a bout a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?

AAMVA believes that the collection and use of the SSN has become widespread and, perhaps, over-used for business transactions. However, there are some business transactions that require unique identification of individuals with whom they do business, i.e., financial services, mortgage lending, health care services, law enforcement and motor vehicle licensing to name a few. In all of these cases, there is a bonafide reason for requiring the collection of this unique identifier.

The driver's license is the primary form of identification in the United States. Federal, state, and local governments as well as every business establishment in this country rely on their motor vehicle agency to conduct the necessary identity verification of the individual holding that drivers license prior to its receipt.

Once the license is received, its validity is rarely questioned when used as an identification document. It is presumed to be a valid, authentic official document, authorized by the administering agency.

If motor vehicle agencies were not permitted to collect the Social Security Number for identification purposes, the consequence of fraud or identity theft would be more far-reaching in this country.

2. The fact that SSNs are so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place?

Yes, if the use of the SSN is restricted, another unique identifier will take its place. AAMVA supports the concept of a national driver license number as it would increase the ability to track repeat DUI offenders and at-risk drivers. It will give states greater flexibility when drivers relocate to another state, particularly during the time of license renewal. Today, the Social Security Number has proven to be the most effective unique identifier for enhancing the effectiveness of driver control records. Were another identifier established, it would have to be national in scope and administered by one congressionally authorized body.

The Association believes it would take between 50910 years for states to be able to use such an identifier effectively. Requisite computer changes and varied license/registration renewal cycles among the states, would result in a lengthy and costly implementation period.

In a sense, it would create a driver's license identification number that would remain with the individual for a lifetime, regardless of where the individual lived in

the United States. This process would be similar to the one used to identify vehicles through the one-time issuance of a vehicle identification number or VIN.

3. In the next 10 to 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics? Will the debate over the privacy and security of SSNs be eventually overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments?

AAMVA and a majority of states support the concept of using biometric technology for identification purposes. Biometric technology may replace the SSN as a means of identification for most business transactions. The private sector is taking the lead in this initiative and is continually offering new technology. As the public grows more accustomed to credit card companies and banks requiring biometric identifiers for their transactions, we believe the public will be more likely to support government agencies using them as well.

Unfortunately, we do believe that the underlying privacy debate will probably remain the same regardless of how accurate, personalized or secure that new technology is.

4. Paragraph missing in original letter.

5. Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples? If SSN use were restricted, what would be the downside for consumers?

Yes, the widespread use of the SSN does benefit consumers in certain ways. The use of the SSN as an identifier can help reduce identity fraud, ensure that driver control records are accurate, and helps the law enforcement officer on the road to more accurately identifier the driver behind the wheel.

Many people have the same name and date of birth, but only one SSN, according to the federal government. Because of this, the SSN, when used as a primary or secondary identifier, benefits citizens by restricting the number of licenses issued to any one individual. Eliminating the use of the SSN by motor vehicle agencies would make it much easier for imposters, identity thieves, and scofflaws to obtain fraudulent documents and spread motor vehicle violations out among multiple licenses.

Consumers also benefit from the use of the SSN in the area of reciprocity. Were states unable to use the SSN to positively identify people, traffic violations and/or convictions from a nonresident jurisdiction could be misapplied to a driver's record.

The State of Delaware provided an excellent example as well. A few years ago, a driver attempted to renew his Delaware driver's license. The law enforcement network showed the applicant was an escaped prisoner and potentially dangerous. The name, date of birth and other identifying features of the driver license applicant exactly matched the person who escaped from jail. The social security data was not on file. The police arrested him. The gentleman spent the next six hours trying to clear his name.

If the SSN were available, the entire matter would not have occurred. Unfortunately, similar problems occur daily at motor vehicle agencies.

6. Is the use of SSNs was restricted by Federal law, what impact would it have on your members?

As we have mentioned previously, restriction on the use of the SSN by motor vehicle agencies would have a profound effect on the way our members do business. The SSN is the only cross-jurisdictional number that allows states to transfer accurate data to one another. Without the SSN, multiple matches for license holders will occur and make it much more difficult to transfer violations and convictions to the correct record holder or to get dangerous drivers off the road. This restriction would diminish DMVs' ability to fulfill their mission as public safety agencies. Without the use of the SSN as a primary or secondary unique identifier, the customer wait times at DMV counters or other service centers would increase dramatically due to the review of additional documentation for identification verification purposes.

7. Most states give people the option of displaying their SSN on their driver's license or using a different number issued by the DMV. Has this option created administrative difficulties for States? Has it reduced accuracy or the ability to correctly identify people?

Many states give their residents the option of choosing whether to display their SSN on the face of the license or an alternate number. It is important to note that

the SSN is used as a primary or a secondary unique identifier. Even though jurisdictions allow individuals to conceal their SSN, the number is retained on file to uniquely identify individuals when matches arise. Without it, DMV error rates would increase dramatically.

Under federal law, states must use the SSN as the license number for all commercial drivers. Congress mandated the use of the SSN as a means to enhance oversight of the commercial driving public. Prior to use of the SSN, it was easy for commercial drivers to get multiple licenses in a number of states to spread violations and convictions among them to avoid losing driving privileges. AAMVA supports the "one driver—one driver control record" concept. Using the SSN has proved to be very effective in limiting the number of commercial licenses issued, thereby ensuring that bad drivers do not continue to jeopardize highway safety.

8. Your testimony indicated that states need to collect SSNs for a variety of law enforcement and public safety reasons. What are states doing to protect this information once it is collected? How do states ensure that the information is correct and not fraudulent?

Under the federal Driver's Privacy Protection Act (18 U.S.C. § 2721092725), states are prohibited from releasing SSNs from their records with the exception of law enforcement, the courts, CDL employers (also required by federal law), and insurance companies for purposes of rate setting. In addition, this information is released to the Office of Child Support Enforcement, and other state agencies.

A significant amount of time is spent training document examiners in state DMVs with experts from the FBI and Immigration and Naturalization Service on document and identity fraud. AAMVA has developed a Fraudulent Identification Prevention Program (FIPP) in conjunction with the National Highway Traffic Safety Administration (NHTSA) aimed at training motor vehicle employees on fraud, document examination, forgeries, and correct identification of documents presented to establish identity. It is important for us to point out that motor vehicle agencies stop customers every day for fraudulent documents and prosecute offenders to the fullest extent of their state laws. AAMVA members are also frequently called to serve as expert witnesses at fraud trials based on their significant expertise in document examination and fraud detection.

9. Do States collect SSN information solely for law enforcement and public safety reasons? Are SSNs used by the States for any other purposes? Do states transfer, sell, or share SSN data to third partied under any circumstances?

As we mentioned in our answer to the previous question, the federal Driver's Privacy Protection Act bars state motor vehicle agencies from disclosing, releasing, or selling SSNs to anyone. It is permissible to release this data to law enforcement agencies, courts, insurance companies, and companies seeking to employ commercial drivers. Within the state, SSNs are shared with other state agencies, but only for the purposes of law enforcement, public safety, and child support.

10. How many pieces of identifying information do states collect (for example, name, gender, age, address, etc.). With so many pieces of identifying information, why is the SSN needed to positively identify an individual?

The number of pieces of identifying information required by states varies according to state law. AAMVA has developed a policy statement (DLC Policy 05.10, copy attached) that outlines acceptable identification documents as a guideline for the states, and this policy statement has been adopted by the AAMVA membership. This policy statement recommends that at least one primary and one secondary document be required from the applicant for identity verification. Aside from the identifying information you mention, states also collect telephone numbers, addresses, height, weight, vision restrictions, gender, eye color, hair color, SSN, and photograph, etc.

The SSN is a cross-jurisdictional number that uniquely identifies the holder of the number and is used behind the scenes to break ties between multiple matches. The image and signature have limited usefulness. Signatures and even pictures can sometimes uniquely identify individuals, but not those who have a close resemblance or similar handwriting. Without the ability to use an SSN to uniquely identify an individual, DMV databases will retrieve multiple matches on common names and it will not be possible to guarantee that the correct record will be queried or updated. Commonality in names, particularly in the Latino community, makes this problem particularly troublesome in states with large populations.

11. You indicated that your members have continued their efforts to enhance the security of driver license credentials. Could you describe these efforts?

In addition to the acceptable identification documents policy, AAMVA has also developed a policy statement (DLC Policy 02.7) that defines acceptable physical security features to be incorporated on the license or identification card and encourages jurisdictions to use at least one overt and covert security feature in the design of their license to reduce fraud and counterfeiting. A copy of this policy statement is also attached.

The initiative to create driver license standards has been underway within the AAMVA community for decades. Since early 1997, AAMVA has worked with the American National Standards Institute (ANSI) to publish a standard for the driver license and identification card.

Due to the overwhelming need for immediate direction in this area, effective June 30, AAMVA will electronically publish the first AAMVA National Standard for the driver license/identification card (DL/ID). The Association continues to pursue American National Standards Institute approval. The standard contains detailed specifications on what a DL/ID should contain and how the information would be encoded in various machine readable technologies. In addition, the Standard also gives guidance in the area of security: physical (features like holographics), data (encryption), and personal (biometrics like finger imaging).

12. In your testimony you indicated that 49 states allow individuals to have a number on their driver's license other than the SSN. However, SSNs are used for checking information across state lines and with SSA. If you stopped using the SSNs for that purpose, wouldn't the DMV-issued number that actually appears on the license become in effect a new national identifier, putting us back in the same place we started?

That would be the case only if the drivers license number is nationally administered in conjunction with federally authorized standards. Currently, each state issues a different unique identifier and since there is no uniformity at the state level, it would be impossible to consider the state issued alternate identifier as a "national" identifier. The non-uniform alternative would create havoc for the many data exchange systems such as the Commercial Drivers License Information System (CDLIS) or the Problem Driver Pointer System (PDPS) mandated by Congress and utilized by DMVs to ensure that drivers only hold one license, that bad drivers are taken off the road, and that violations and convictions are recorded on the correct driving record. The ability to uniquely identify individuals is of paramount importance to DMVs and law enforcement officers as well. Without a standardized approach, AAMVA believes the incidence of identity theft and fraud would increase greatly.

13. Why do some states (Hawaii and Washington, D.C.) still require the SSN to be displayed on driver's licenses? Why don't they use their own internal identifying numbers?

Following the recent hearing, we updated our information on which jurisdictions offer their residents the option to display their SSN or an alternate number on the license. We learned that the District of Columbia does provide residents with an option. So currently, 50 jurisdictions allow citizens to use another number as the driver license number. We have also learned that the State of Hawaii will plan to make the use of the SSN optional as of January 1, 2001, bringing every state on board as either prohibiting the SSN from being displayed or giving consumers the option. The use of the SSN behind the scenes will continue to be an important tool for our members to fulfill their missions and to enhance public safety. Our next step is to determine what percentage of citizens have opted to not use the SSN.

10. ACCEPTABLE IDENTIFICATION DOCUMENTS

Any applicant for an original or initial driver license or identification card shall be required to submit at least one primary document and one secondary document as approved by the Driver Licensing and Control Committee. A primary document must contain the applicant's full name and date of birth and must be verifiable.

Additional documentation may be required by the licensing agency if the documentation provided is questionable.

Licensing agencies shall publish information which contains identification procedures and lists acceptable documents.

PRIMARY DOCUMENTS

- U.S. Canadian photo driver license
- U.S. or Canadian photo ID card
- Microfilm / copy of a driver license or ID card certified by the issuing agency

• Certificate of birth (U.S. or Canadian issued). Must be original or certified copy, have a seal and be issued by an authorized government agency such as the Bureau of Vital Statistics or State Board of Health. Hospital issued certificates and baptismal certificates are not acceptable.
• INS documents (must be a valid unexpired document) as follows:
—Certificate of Naturalization (N09550, N09570, or N09578)
—Certificate of Citizenship (N09560, N09561 or N09645)
—Northern Mariana Card
—American Indian Card
—U.S. Citizen Identification Card (I09179 or I09197)
—Resident Alien Card (I09551)
—Temporary Resident Identification Card (I09688)
—Record of Arrival and Departure (in a valid Foreign Passport) (I0994)
—Valid foreign Passport containing an I09551 stamp
—U.S. Re-entry Permit (I09327)
—Refugee Travel Document (I09571)
—Employment Authorization card (I09688A, I09688B, I09766)
—Record of Arrival and Departure, stamped "Refugee" (I0994) (*Refugee I'94's will likely not be in a foreign passport*)
• Canadian Immigration Record and Visa or Record of Landing (IMM 100)
• Active Duty, Retiree or Reservist military ID card
• Valid Passport, U.S. or Canadian. *If foreign passport, appropriate INS document is also required.*
• U.S. or Canadian issued learner's permit. An out-of-state or province issued permit is acceptable only if it contains a photo.
• Canadian Department of Indian Affairs issued ID card. *Tribal issued card is not acceptable. U.S. issued Department of Indian Affairs card is not acceptable.*

SECONDARY DOCUMENTS

• All primary documents
• Court order. Must contain full name, date of birth and court seal. *Examples include adoption document, name change document, gender change document, etc. Does not include abstract of criminal or civil conviction.*
• INS documents listed above, under Primary Documents, which are expired one year or less
• Bureau of Indian Affairs Card/Indian Treaty Card. Tribal ID card is NOT acceptable. NOTE: *Some Tribal ID Cards are actually more reliable than the BIA card. Motor vehicle agencies should make a determination on whether to accept the card based on their own research of what is acceptable.*
• Employer photo ID card
• Foreign birth certificate. *Must be translated by approved translator.*
• Health insurance card, i.e., Blue Cross/Blue Shield, Kaiser, HMO.
• IRS/state tax form. W092 NOT acceptable.
• Marriage certificate/license
• Medical records from doctor/hospital
• Military dependent ID card
• Military discharge/separation papers
• Parent/guardian affidavit. Parent/guardian must appear in person, prove his/her identity and submit a certified/notarized affidavit regarding the child's identity. *Applies only to minors.*
• Gun permit
• Pilots license
• School record/transcript. Must be certified.
• Social security card. Metal card is NOT acceptable.
• Social insurance card (for Canadian residents only).
• Student ID card. Must contain photo.
• Vehicle title. Vehicle registration NOT acceptable.
• Photo public assistance card
• Prison release document.

Additional documentation may be required at the jurisdiction's discretion if documentation submitted is questionable or if the issuing agency has reason to believe the person is not who s/he claims to be.

In exceptional circumstances where a primary/secondary document contained on this list is not available, personnel authorized by the licensing agency may accept alternative documents to verify a person's identity. [Amended 1997]

July 7, 2000

The Honorable E. Clay Shaw, Jr., Chairman
Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
Washington, DC 20515

Re: Questions in relation to Social Security Numbers

Dear Chairman Shaw:

I am writing on behalf of the American Council of Life Insurers (ACLI) in response to your letter of May 31, 2000, posing several questions in relation to the use and misuse of Social Security numbers (SSNs). The ACLI is pleased to have the opportunity to elaborate on our testimony of May 11, 2000. The questions and our responses are as follows:

1. *Are there any legitimate uses of the SSN that you think should be allowed (such as law enforcement)?*

Yes, in fact , the ACLI strongly believes that there are a number of legitimate uses of SSN that greatly benefit American insurance consumers. As indicated in our testimony before your subcommittee, the very nature of life, disability income and long term care insurance involves personal and confidential relationships. However, insurers which sell these products must be able to obtain, use, and share their customers' health and nonpublic personal information, including their social security numbers, to perform legitimate insurance business functions. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers.

Insurers sometimes must use proposed insureds' SSNs in order to obtain medical information, essential to underwriting, from doctors and hospitals which use SSNs as identification numbers. Insurers may also use SSNs to obtain motor vehicle record information relevant to an application for coverage. (Motor vehicle information is sometimes used by insurers as one factor in assessing risk.)

Once an insurance policy is issued, insurers use their customers' personal information, including SSNs, to perform essential, core functions associated with an insurance contract, such as claims evaluations and policy administration. In addition, insurers also use this information to perform important business functions, not necessarily directly related to a particular insurance contract, but essential to the administration or servicing of insurance policies generally, such as, for example, development and maintenance of computer systems. The ability to use this information for these purposes is crucial. Service and administration are fundamental parts of insurers' relationship with their customers.

Insurers use SSNs to verify the identity of policyholders. They use them to authenticate the identity of individuals who call into call centers in order to get information about a particular policy or policies. SSNs are also used to help a customer locate lost policies or verify all of the policies they may have with a particular insurer. SSNs are used by insurers to locate missing policyholders to whom they may owe money. Insurers use SSNs in connection with the administration of pension plans, as identification numbers. They use them as PIN numbers for customers' use of on-line services. They use them in connection with payroll deduction under group insurance coverage provided by an employer to its employees.

Life, disability income, and long term care insurers must regularly disclose personal health and financial information, which is likely to include SSNs, to: (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers; (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers' conduct in the marketplace; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information.

Life, disability income, and long term care insurers need to (and, in fact, in some states are required to) disclose personal information, including SSNs, in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies, state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators, which work for the insurer.

Insurers are required to use SSNs to report to the IRS a variety of payments including, but not limited to, interest payments, certain dividends, and policy investigations. At least one state, Rhode Island, requires that insurers match "deadbeat" parents data before making payments on claims. SSNs are required for that matching.

In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer be able to disclose company files. Naturally, these files can contain personal information, including SSNs. Such disclosures are often necessary to the due diligence process which takes place prior to consummation of the deal and are clearly necessary once the deal is completed when the newly created entity often must use policyholder files in order to conduct business. Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the amount and volume of coverage they can provide. These arrangements, too, necessitate the disclosure of personal information, including SSNs, by the primary insurer to the reinsurer.

2. *Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel about a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?*

ACLI member companies would be strongly opposed to a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs. As indicated above, insurers must be able to use consumers' personal information, including their SSNs in order to perform essential business functions, as described above. If consumers were to be permitted to withhold SSNs, it would be extremely difficult, if not impossible, for insurers to provide consumers with the coverage, service, benefits, and economies that otherwise would be available. As also noted above, there are a number of disclosures of SSNs which insurers are required to make by law, such as disclosures to the IRS and law enforcement agencies.

3. *The fact that SSNs are so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place?*

The ACLI has no policy with respect to use of personal identifiers other than SSNs.

4. *In the next 10 or 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics? Will the debate over the privacy and security of SSNs eventually be overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments?*

The ACLI is not in a position to anticipate what types of personal identifiers will be used in the future and has no policy regarding future development of alternative personal identifiers.

5. *Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples? If SSN use were restricted, what would be the downside for consumer?*

As stated in our response to question #1, insurers use SSNs in a multitude of ways to benefit consumers. If insurers' use of SSNs were to be restricted, the downside to consumers would include the following, among other things: (1) fraud investigations would be impaired, the ultimate cost of which would be borne by consumers; (2) if insurers were to be prohibited from using SSNs to obtain medical information necessary to underwriting, the risk classification process would be jeopardized, which, in a nut shell, could jeopardize insurers' ability to pay consumer customers' future claims and insurers' ability to keep their products widely available at affordable prices, as they are now in this country; (3) it would make it difficult, if not impossible, for insurers to authenticate and quickly serve customers who phone into call-in centers and to locate missing customers to whom they may owe monies; (4) it would make it more difficult for insurers to administer employee benefit plans, likely to result in increased administrative costs which, again, ultimately are likely to be borne by consumers; (5) it would jeopardize market oversight activities by state insurance departments and insurance self-regulatory organizations, jeopardizing the consumer protections devolving from these activities; and (6) it would make more difficult the operation of state guaranty funds which seek to pay consumer claims in the event of an insurer's insolvency or impairment.

6. *If the use of SSNs was restricted by Federal law, what impact would it have on your operations?*

Our responses to questions #'s 1 and 5 address the importance of insurers' use of SSNs to insurers' day to day operations and their ability to serve their existing and prospective customers. In general, restrictions on insurers' ability to use SSNs would make it much more difficult for them to issue new insurance policies, to service and fulfill their contractual obligations under existing insurance contracts, and to engage in other ordinary business transactions. It would make it virtually impossible for insurers to make required reports to the IRS and other government agencies, including law enforcement agencies and state insurance departments.

7. *Your testimony indicates that you often share personal information with third parties who administer, serve, or enforce insurance policies. Do these third parties, in turn, share or sell the information to others? Do you know how these third parties protect the information which you give them?*

Third parties to whom insurer financial institutions disclose nonpublic personal information, including SSNs, are bound by the Gramm-Leach-Bliley Act (GLBA)

Title V privacy provisions. Under Section 502(c) of the GLBA, third parties recipients of information from financial institutions may only disclose nonpublic personal information to a nonaffiliate of the financial institution or the receiving third party the same extent to which the GLBA permits the financial institution to disclose the information.

Section 502 of the GLBA provides that, subject to specific, limited exceptions, a financial institution may not disclose nonpublic personal information, including SSNs, to a nonaffiliated third party unless: (a) the financial institution has clearly and conspicuously disclosed to the consumer that such information may be disclosed; (b) the consumer is given the opportunity, before the information is disclosed, to direct that the information not be disclosed; and (c) the consumer is given an explanation of how the consumer can exercise that nondisclosure (or "opt-out") option. (Attachment A -copy of Title V of the GLBA)

8. *If sharing personal information is necessary in the insurance business, do you disclose to your customers who the information is shared with and how it is used?*

Insurer financial institutions are subject to the extensive GLBA notice requirements. Section 503(a) of the GLBA requires that at the time of establishing a customer relationship and not less than annually during the continuation of such relationship, a financial institution shall provide clear and conspicuous disclosure to such consumer of such financial institution's policies and practices with respect to: (a) disclosing nonpublic personal information, including SSNs, to affiliates and nonaffiliated third parties, including the categories of information that may be disclosed; (b) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and (c) protecting the nonpublic personal information of consumers.

Section 503(b) elaborates on the information that must be included in these notices and requires that they also include descriptions of: (a) the categories of persons to whom the information is or may be disclosed; (b) the categories of nonpublic personal information collected by the financial institution; (c) the policies that the institution maintains to protect the confidentiality and security of the information; and (d) the disclosures required, if any, under the Fair Credit Reporting Act.

9. *You note that the privacy provisions in the recently enacted Gramm-Leach-Bliley Act subject insurers to the most stringent privacy regulations ever imposed in the United States. When you share personal information with third parties, are these third parties subject to the same privacy provisions or do you lose control of what happens to the information once it is given to a third party?*

Our response to question #7 also addresses this question.

10. *You note that prohibiting the use or sharing of SSNs would make it almost impossible to provide consumers with certain services. How were these services provided before the widespread use of SSNs? Has the SSN always been the primary identifier in the insurance industry?*

Given the length of time SSNs have been used by insurers and the multitude of ways in which insurers now use them, a prohibition or restriction on the use of SSNs would make it almost impossible to provide consumers with many of the services currently available. Moreover, the many changes in the insurance industry and technology over the last few years, make it questionable whether practices that worked successfully twenty five or thirty years will work today. Many of the pur-

poses for which SSNs are now used did not exist years ago. Moreover, a requirement that insurers return to their previous practices, whatever they were, would involve extensive and expensive changes in current practices.

We appreciate your continued consideration of our views and would be glad to respond to any additional questions that you may have in relation to this very important issue.

Sincerely,

ROBERTA B. MEYER

ASSOCIATED CREDIT BUREAUS, INC.
1090 VERMONT AVENUE, N.W.
SUITE 200
WASHINGTON, DC 20005094905
November 17, 2000

The Honorable Clay Shaw
Committee on Ways and Means
Subcommittee on Social Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Shaw:

I was contacted by George Penn on your staff regarding a letter you submitted to the Associated Credit Bureaus in May of this year which outlined a series of questions in follow up to our testimony before your Committee. Below are answers to your questions.

Q.1 Many people are annoyed by the fact that they have to give up their SSN for practically any business transaction. How would you feel about a proposal that would prohibit businesses from denying services to customers who refuse to disclose their SSNs?

A.1 Consistent with our testimony, the SSN plays a vital role in both the consumer reporting agency's ability to build accurate data bases and to extract data from these data bases.

Where, as a result of this proposal, data furnishers such as creditors are providing data to consumer reporting agencies without an SSN, our members will likely not load data with the same 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. The absence of an SSN will diminish the ability of the agency to meet this requirement of current law.

Another likely unintended consequence of this proposal would be diminished ability to identify the proper file of the consumer where he/she has applied for credit. 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.

As we stated in our testimony, according to the U.S. Census Bureau, 42 million consumers move every year. Added to this are millions of marriages and divorces. Other traditional items of identifying information are not always stable and thus the SSN is extremely important to our industry's ability to comply with current law.

Q.2 The fact that the SSN is so widely used indicates that there is a need for a unique personal identifier. If the use of SSNs is restricted, do you think another personal identifier will take its place.

A.2 Clearly the market would have to attempt to find alternative methods of identification.

If unique identifiers are not consistent across various systems, however, then child support enforcement efforts, for example, will diminish. In fact, all systems of location, which are used today to locate heirs to estates, stock holders for proxy votes, debtors who haven't paid their bills, organ or blood donors, and for other purposes, would be greatly diminished in effectiveness. Further, fraud prevention sys-

tems that are used to reduce the incidence of identity theft, or to authenticate consumers in an e-commerce or bricks-and-mortar context will be rendered less effective, as well.

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.

Q.3 In the next 10 or 20 years, what do you think will be used to identify people who apply for credit or other commercial services? Will it be the SSN? Some other number? Biometrics? Will the debate over the privacy and security of SSNs eventually be overtaken by new technologies that are more accurate, more personalized, and more secure from abuse? Does your industry anticipate and support such developments.

A.3 Our industry clearly supports and expects the continued evolution of technologies that allow for crime-free consumer-to-business and even business-to-business transactions. It is difficult for us to hypothesize about which technologies will be effective and acceptable to consumers. Consistent with our answer to question 2, there will continue to be a need for systems of identification that cut across industries and data bases to assure fraud prevention, location and more.

Q.4 Stories of identity theft and SSN misuse highlight the negative consequences of widespread SSN use. However, does the widespread use of SSNs benefit consumers in certain ways? Can you give us examples? If SSN use were restricted, what would be the downside for consumers?

A.4 The SSN allows for consistency across various systems and data bases. The benefits are manifold for consumers and society in general.

Child Support—For example, child support enforcement efforts are far more effective in accomplishing their mission where the SSN is used. One agency reports that they are able to locate fully 80% more delinquent non-custodial parents when the SSN is available.

Locator Services—The SSN increases the effectiveness of all locator/skip tracing systems, which are used today to locate heirs to estates, stock holders for proxy votes, debtors who haven't paid their bills, organ or blood donors, and for other purposes, would be greatly diminished in effectiveness. Further a number of states report that use of SSNs to match across data bases has greatly reduced entitlement fraud.

Fraud Prevention—The SSN also 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.

Q.5 If the use of SSNs was restricted by Federal law, what impact would it have on your operations.

A.5 In part our answer would have to be predicated on the restrictions imposed. In general our answers to the questions above provide a good overview of the consequences of a very broad restriction.

Q.6 On May 9, we heard testimony from a couple (Lt. Col. Stevens and Mrs. Stevens) who have had their identities stolen. Their story raised several troubling issues.

First, the Stevens told us that fraudulent accounts were opened using their SSNs even though all of the information on the applications was incorrect, including their names, addresses and birth dates. The SSN was the only piece of information that was correct on the applications.

A second troubling issue is that credit reporting agencies verified this incorrect information. Variations of a name, address, place of employment, age, or spouse's name were not questioned -if the SSN matched up, the information was verified and the fraudulent application was approved.

a. Can you explain how these fraudulent applications could have been verified and approved?

A.a This question is best answered by the business that approved the application.

b. Why did the credit reporting system fail in this case?

A.b Since ACB does not have access to the Stevens' file, nor to the particulars of the situation, we cannot provide any answer other than to say that our systems are designed to accurately identify a consumer's record when correct identifying information is submitted.

c. Under current law, are creditors and credit reporting agencies accountable when their negligence contributes to identity theft and other SSN misuses? Do you think that creditors and credit reporting agencies should share responsibility in such cases.

A.c Identity theft is a crime that affects consumers, credits and consumer reporting agencies. The consumer reporting industry has voluntarily established initiatives to help victims of identity theft. Further, the industry is already regulated by extensive law (15 U.S.C. 1681 et seq.) which creates duties for consumer reporting agencies to build accurate files, limit the uses of such data and ensure files are properly identified. Criminals who perpetrate this crime should be punished and ensure that there is a deterrent for others who might otherwise consider perpetrating identity theft.

Q.7 One of the disturbing items from the testimony by the Stevens was their statement that the collection agencies did not believe them. They had to prove they were victims of identity theft. What would you say to the Stevens? Should the burden of proof fall on the victims of identity theft?

A.7 Under the Fair Debt Collection Practices Act a consumer has the right to request that the debt collector validate the account in question. We encourage the committee to review the duties and consumer protections in this law as you evaluate the Stevens' situation.

Q.8 The Stevens explained that they have been prevented from buying a home, establishing credit accounts, or making normal purchases because their credit was ruined by no fault of their own. How do credit reporting agencies assist identity theft victims today?

A.8 In addition to the duties a consumer reporting agency has under the Fair Credit Reporting Act, see the attached initiatives which the industry announced in March of this year.

Q.9 When someone's credit is ruined because of the identity theft, how long does it take to clear the bad credit from the victim's credit report? The Stevens complained that bad accounts are recycled through the same collection agency or they are turned over to the other collection agencies so that the same bad debt keeps reappearing on the credit report. Can you explain to us how the process works?

A.9 It is difficult to make a general statement about the time frame for clearing a file. The Fair Credit Reporting Act requires that a reinvestigation of disputed data be resolved within 30 days. The extent of the crime is the key factor in clearing a consumer's record. We cannot comment on the practices of other industry segments with regard to an account being transferred to multiple collection agencies.

Q.10 You note in your written testimony that your members collect SSNs *only when they are voluntarily provided by consumers.* But isn't it true that in many cases, consumers *must* provide their SSNs to receive credit? For example, can a customer be approved for a mortgage without giving his or her SSN? If consumers must provide SSNs to receive services, how voluntary is this disclosure?

A.10 It is likely true that many creditors, in order to properly identify the consumer, prevent fraud and ultimately approve credit, do need the SSN. It would be best to explore this question further with the creditor community.

Q.11 Your members' use of the SSN is governed by the Fair Credit Reporting Act. In addition, you have a long list of voluntary initiatives your members have undertaken to combat identity theft and SSN misuse. Do all of your members follow these initiatives? What happens to them if they don't? Despite these efforts, fraudulent uses of SSNs is on the rise. Does this indicate that existing laws are not being enforced effectively or perhaps self-regulation is not working? What recommendations do you have to reduce SSN misues?

A.11 Our largest members, which operate nationwide consumer reporting systems, are implementing the initiatives discussed in our testimony. Due to the nature of our industry, the implementation of the initiatives by the nationwide systems will effectively extend them to our other members as well. We do believe that self-regulatory programs are an essential component of the solution to the problem of identity theft. We also agree that the laws that are on the books must be enforced and in particular the newly enacted Identity Theft Assumption and Deterrence Act of 1998 as well as Title V, Subtitle (b) of Gramm-Leach-Bliley, which prohibits the practice of pretext calling. Regarding SSN misuse, we believe consumer education can be an essential component of the solution. ACB is working towards consumer education efforts that should help consumers make better decisions about protecting sensitive information.

Q.12 How does a consumer reporting agency get its information? How does it determine what information to place in a record and what information not exclude [sic]? How is the authenticity of the information verified to ensure that incorrect information is not being posted?

A.12 Our testimony generally addresses the types of information we gather and the sources from which we receive it. Creditors, collection agencies and other data sources including the Department of Education report data on regular cycles. The market place generally determines what information is of value and thus what data

is included in a consumer report. The definition of a "consumer report" under the FCRA is purposely broad to ensure that a wide range of information sources are in fact governed by the Act and thus consumers are protected in terms of rights and an expectation that duties will be fulfilled. In terms of authenticity, data furnishers must first be evaluated to ensure that they are legitimate businesses, and that they can provide accurate information for data is accepted.

We look forward to working with you to ensure that consumer's Social Security Numbers are used responsibly and appreciate the efforts of your staff to understand our industry's practices and concerns.

Sincerely,

STUART K. PRATT
Vice President
Government Relations

This hearing is adjourned.
[Whereupon, at 4:52 p.m., the hearing was adjourned.]
[Submissions for the record follow:]

AMERICAN TARGET ADVERTISING, INC.
MANASSAS, VIRGINIA 20110
May 10, 2000

The Honorable E. Clay Shaw
Chairman
Subcommittee on Social Security
2408 Rayburn HOB
Washington, D.C. 20515

Re: Hearings on Social Security Number Misuse

Dear Chairman Shaw:

I became aware of your hearings on social security number misuse only last evening when watching C-Span, so I apologize for not getting these comments to you earlier.

I am President of Operations and General Counsel for American Target Advertising, Inc. ("ATA"). ATA is a direct marketing agency whose only office is in Manassas, Virginia. ATA's marketing services include a variety of fundraising-related activities, including advising and counseling clients about the use of direct mail and preparing direct mail letters for its clients. ATA's clients include political campaigns as well as nonprofit organizations under Internal Revenue Code sections 501(c)(3) and 501(c)(4). Recently, ATA began to expand its fundraising activities for its various political clients by providing a small telemarketing operation to both supplement the direct mail fundraising messages and to raise additional funds from active supporters.

When acting in a capacity for its nonprofit clients' direct mail, ATA must register as a fundraising counsel (or consultant, as it is also called) in a number of states that have what are known as charitable solicitation laws. ATA is obligated to register in many states before its nonprofit clients may mail letters into those states even though ATA does not conduct business in those states.[1] A growing number of counties and cities are enacting similar laws. Pinellas County, Florida is one of those counties. As part of its licensing application, Pinellas County requires the drivers license number of various employees of the applicants for a professional fundraising consultant's license. See Attachment A.

I notified the appropriate officials in Pinellas County that the Virginia drivers license number is actually the same as one's social security number. I informed those officials that under the Federal Privacy Act, it is unlawful to require the submission of one's social security number as a condition for the issuance of a separate state license. I was informed by those officials that they would not heed the Federal Privacy Act. ATA refused to provide those numbers in its application for a fundraising counsel license, and Pinellas County rejected ATA's license application.[2]

---

[1] ATA has challenged the constitutionality of such laws under First Amendment, Commerce Clause and Due Process grounds, and has recently filed a petition with the United States Supreme Court to ask the Court to determine whether such licensing laws are constitutional.

[2] The state of Utah's licensing application also required the listing of the social security number of the registered agent of a fundraising counsel. However, such part of the application was

On May 19, 1999, I wrote to the General Counsel of the Social Security Administration, noting that Pinellas County required the drivers license numbers of employees (and thus their social security numbers) on licensing application forms in violation of the Federal Privacy Act. I asked for the assistance of the Social Security Administration in enforcing the protection of social security numbers in light of the Pinellas County application form. See Attachment B. I received a reply dated October 18, 1999 from Associate General Counsel Michael Hoover noting that the SSA has no authority to enforce the Federal Privacy Act. See Attachment C.

Since then, ATA has reviewed the applications required to register to conduct telephone solicitations into various states under various charitable solicitation laws. In its review thus far, ATA has found that a number of states require either the drivers license numbers or social security numbers of ATA's employees as a condition to obtain a license to make solicitation calls on behalf of ATA's nonprofit clients. Some of those states, their statutes, and the corresponding license application forms are as follows: Alabama (Alabama Code section 13A0990971), Attachment D at item 13; Illinois (Illinois Charitable Organization Laws Ch. 23, par. 5108), Attachment E at item 6; Mississippi (Regulation of Charitable Solicitations section 79091109517), Attachment F at item 2; New York (Article 7-A of the Executive Law Solicitation and Collection of Funds for Charitable Purposes section 173-b), Attachment G at Item 7; South Carolina (Solicitations of Charitable Funds Act section 33095609110), Attachment H item 3; Tennessee (Tennessee Charitable Solicitations Act section 480910109507), Attachment I item 5.

With the concerns that the Subcommittee has with regard to the misuse of social security number, I ask that the Subcommittee consider the deplorable fact that states and their principal law enforcement officials (typically the attorneys general) require the public disclosure of individuals' social security number. These license applications are made available to the public. See, e.g., South Carolina's statute, section 3309560980, which reads in relevant part, "Registration statements and applications . . . and information required to be filed under this chapter . . . are public records in the Office of the Secretary of state and are open to the general public for inspection at such time and under such conditions as the Secretary of State may prescribe."

In other words, states, counties and cities, and their highest ranking law enforcement officials are inviting the misuse of social security numbers under laws and/or licensing application forms that already violate the Federal Privacy Act. This is doubly troubling, and in my opinion even more egregious than any misuse of social security numbers by private firms that may not be aware of such misuse of social security numbers. The ironic part about this whole situation is that the states claim that they need these licensing laws to prevent fraud. In fact, they open the doors to consumer fraud by requiring these numbers for public inspection.

It is incumbent on government officials to apply the laws correctly. As with Pinellas County, which was warned that their licensing application form violates the Federal Privacy Act and increases the chances of misuse of social security laws, many of the state officials to whom I have addressed these facts have not been merely complacent, but have been defiant.

I hope that the Subcommittee will look into this matter. While I am aware of these laws as they affect agencies like ATA, which is an admittedly small segment of businesses, this is a problem the nature of which I am relatively certain is more expansive than just within my particular industry.

I thank you for the opportunity to submit these comments. I apologize for their haste in the making, but I would be willing to answer more questions at the Subcommittee's request.

Very truly yours,

MARK J. FITZGIBBONS
President of Operations and
General Counsel

Enclosures

[Attachments are being retained in the Committee files.]

---

added at the discretion of the Director of the Division of Consumer Affairs. The portion of the Utah Charitable Solicitations Act which gave the Director such discretion was declared unconstitutional on its face in *American Target Advertising, Inc. v. Giani,* 199 F.3d 1241 (10th Cir. 2000).

Mineral, Virginia
May 11, 2000

Committee On Ways and Means
Subcommittee On Social Security
Hearings of May 9, 2000 and May 11, 2000

The following is a prepared written testimony to be recorded with the hearings on Tuesday May 9 and Thursday May 11, 2000 regarding " Use and Misuse of Social Security Numbers." This written testimony is submitted by Robert J. Anderson of Mineral Virginia, a private citizen.

WHAT SOCIAL SECURITY MEANS TO ME

I am a victim of Social Security number misuse. Last year, it was my privilege to testify before the Joint Commerce Committee's on April 22, 1999 (Serial 1060916 Cong. Record) regarding the issue of the new criminal law HR 4151 (18 U.S.C. 1028) and Identity Theft. I deeply regret that I was out of town when your office called me to testify in person, but nonetheless, want to submit this written update to my previous Congressional Record testimony.

In prior testimony, Identity Theft: Is There Another You? (April 22, 1999 1060916 Cong. Record pg. 140915) I submitted an account of what has occurred over the past several years of my life dating back to 1995 regarding SSAN misuse and erroneous enumeration, to others, by the Social Security Administration. SSA advised me by letter on Dec. 7, 1995 that SSA had issued my SSAN five different times to a person in California. That person than used the number for credit fraud. I was in constant contact with the Social Security Administration Office of Inspector General from February 1996 until last year. I got no results until I contacted the United States Congress with a complaint.

Following my Congressional testimony on April 22, 1999, I received the attached letter from the Social Security Administration OIG. I understand that Congressman Shaw was also sent a copy of the letter dated April 28, 1999. (Attach. A)

Basically, SSA/OIG Baltimore, Md. took the position that administrative error took place on the part of their SSA District Offices in California, and this had caused the severe problems I experienced, and that there was no finding of criminal wrongdoing on the part of the person in California. Of course, this negated any legal or law enforcement action under the new Criminal law. Since Civil action is nearly impossible, this left the person in California off the hook.

Subsequently, following a meeting with the local District Office here in Virginia, I received a kind letter apologizing for the multiple errors of the Administration, and offering to issue a new Social Security Number to myself. After checking with a number of financial institutions, including a major CRA, I found that in today's information world, changing the SSAN would not accomplish anything since there are too many cross references and they would certainly cross reference the credit file to the new SSAN. Pervasive use of the SSAN has resulted in a very tangled web. Thus I remain victimized by misfeasance on the part of several SSA California District Offices.

REVIEW OF SOCIAL SECURITY EARNINGS REPORTS

When credit fraud and other misuse of my SSAN began, strange things showed up on my SSA earnings record. During my years as a Federal Employee there was no record of SSA tax, being paid, rather I paid about 10 % of earnings into the Civil Service Retirement Fund. Thus, erroneous SSA earnings reported would have been obvious on my SSA earnings record. There were no errors. However, from 1988 thru 1992 after leaving Civil Service, I posted earnings in excess of the SSA taxable limits, and thus, small amounts posted to my account did not show. It is impossible for me to tell if the California person had been avoiding tax, or reporting on my SSAN. When I finally retired from private industry, it became obvious that small earnings were being reported to my SSA earnings account by the person in California.

As I previously testified, all of this activity occurred in a small area of California and seemingly should have been easy for the Social Security Administration to fix, given the amount of well documented evidence I provided, to the SSA/OIG. It is incomprehensible that the Federal Government could not fix the problem. Earnings report errors still occur. As recently as April, 10, 2000 there are still erroneous earnings for 1998 showing up on my report. My local SSA Office has quickly and kindly

corrected the intrusion, but I still must wait for a formal correction from Office of Central Records, (OCRO) in Baltimore to verify the error. I have no idea what happened in 1999 as earnings are not yes posted. My local SSA office tells me, nothing yet.

As a retired Civil Service Federal Employee devoting a career to the Federal Government,

I will never see Social Security benefits under current law, even though I am a widower (Survivors) and have paid into Social Security (Taxable earnings) for 17 years. This is due to the Windfall Elimination Provision (WEP)-AND the Government Pension Offset (GPO) laws.

The major questions in my mind are: how could this happen five times if the Privacy Act protected systems of records held by Social Security are secure ? Why didn't the SSA Offices in California positively identify the person ? The name and date of birth were different. I don't need apologies for mistakes. I would just like to see the system work, even If I shall never benefit. If all this happened thru walk in, accidents/mistakes, I shudder to think what would occur with increased access and online access.

Something seems to be broken, and I submit that tightening issuance controls, and restricting access to Social Security numbers would go a long ways towards fixing the problem.

You have my sincere thanks for inviting me to submit testimony in this hearing and I look forward to reviewing the Record.

Robert J. Anderson

[The attachment is being retained in the Committee files.]

Statement of Christopher J. Klicka, Esq., The Home School Legal Defense Association, Purcellville, Virginia

My name is Christopher J. Klicka, and I presently serve as Senior Counsel of the Home School Legal Defense Association and Executive Director of the National Center for Home Education. For the last 15 years, I have worked in the area of constitutional and education law—in the courts, state legislatures, and Congress. I have litigated many cases involving the Free Exercise of religion of parents. I have drafted state legislation and testified before state legislative committees regarding registration, religious freedom, and tax issues. I have worked with dozens of state boards and departments of education and thousands of local school districts to resolve problems over educational issues involving the religious convictions of home school families. I also assisted in drafting H.R. 2494.

The Home School Legal Defense Association is a nonprofit legal advocacy organization dedicated to protecting religious and parental freedom generally and promoting home schooling specifically. We have almost 70,000 member families in all 50 states at present.

One of the Home School Legal Defense Association's goals is to protect the religious freedom and privacy of home schoolers throughout the country. Since 1996, innocent families with sincerely-held religious convictions against getting a social security number for their children are being forced to pay for the exercise of those religious convictions. These families are being assessed thousands of dollars in taxes even though they have dependent children legitimately qualifying them for various tax deductions.

1996 AMENDMENT TO IRS CODE PUNISHES PARENTS WITH SINCERELY-HELD RELIGIOUS CONVICTIONS

Due to a change in federal law in 1996, a parent is required to submit a taxpayer identification number (TIN) for each minor being claimed for a deduction or a tax credit on his federal income taxes. Because the TIN for an individual is a social security number (SSN), this law essentially requires all parents to obtain a SSN for their newborn children if they want to receive the dependent deduction, the child tax credit, or other credits.

Some families have religious convictions against obtaining such a government-issued number (TIN) for a dependent.

Section 1615 (a)(1) of The Small Business Job Protection Act of 1996 amended 26 U.S.C. § 151 authorizing the IRS to completely deny the dependency exemption if the dependent's TIN is not included on the tax return. The relevant language states:

(e) Identifying information required. No exemption shall be allowed under this section with respect to any individual unless the TIN of such individual is included on the return claiming the exemption. [26 U.S.C. § 151 (e) (1998)].

Before the addition of this section, a taxpayer who failed to supply a dependent's TIN was served a deficiency notice, which could be appealed. Now, however, a failure to provide a correct TIN is treated like a mathematical or clerical error, which cannot be appealed. The taxpayer is simply assessed the tax and required to pay without appeal.

Many innocent families are suffering severe financial hardship as a result.

WHY CONGRESS SHOULD ENACT THE RELIGIOUS EXEMPTION CREATED BY H.R. 2494

There are several compelling reasons to support congressional action to create a religious exemption from providing identifying numbers for dependents. These include the following:

1. A minority of law-abiding families with sincerely held religious beliefs that make them opposed to obtaining a government issued number for their minor children, are suffering severe financial hardship.

Many families have voluntarily forfeited thousands of dollars worth of legitimate dependent deductions, rather than violate their religious beliefs. These families, who have children, are not taking the deductions they are entitled to in order to be true to their religious convictions. Other families are listing their children on their federal income tax form but not obtaining social security numbers for them. These families are claiming their legitimate deductions but are being assessed thousands of dollars as the IRS disallows their deductions.

Taxpayers with these sincerely-held religious beliefs are being forced to pay for their right to exercise their religious beliefs. Thus, the current federal law prohibits these families from freely exercising their religion—a fundamental right protected by the First Amendment.

One family with sincerely-held religious convictions was forced to take out a second mortgage on their home to pay for the taxes assessed against them for the last three years simply because the IRS has disallowed their deductions and credits for their children. See their personal testimony attached in Appendix I). Many innocent families are experiencing nightmares has as they are hounded by the IRS for not obtaining social security numbers. Other families are not listing their children on their income tax and forfeiting their legitimate tax deductions and credits.

We have record of over 150 families being penalized by the IRS simply because they have sincerely-held religious convictions making it impossible for them to get social security numbers for their children.

Here are excerpts from some of their testimonies collected by HSLDA in the last few weeks:

"Because of no social security numbers for our eight dependent children, the IRS assessed additional tax of $3100."

—NATHAN AND LISA BACH
Marshall, TX

"We live in fear continually that the IRS will send us a notice at any time that they will be seizing our hard-earned property, or that we will end up in a tax court dominated by one-sided legal procedures. . . . We expect that our total liability claimed by the IRS will shortly be approaching $3500, which would be nearly 20% of our total annual familial income. . . . We remain committed to following the Lord rather than the dictates of man."

—STEPHEN MARTIN NORTH
Amity, Maine."

"We are deeply troubled that our religious beliefs concerning our children receiving Social Security Numbers are being violated by the government. We are being forced to compromise our beliefs or pay an exorbitant tax bill which amounts to over $7,000 a year for our family. We have paid an additional $30,000 in taxes thus far to avoid getting Social Security numbers for our children. This is certainly an added hardship for our family of seven.

"We feel strongly that the requirement demanding we obtain numbers for our minor children is both unconstitutional and discriminatory in a country which has an heritage of religious and personal freedoms. We believe, as Christians, our children have been entrusted into our care and that God holds us personally responsible for their well-being. It is our belief that to number our children marks them as government property and forces us to register them in a tracking system as minors. We, as parents, believe we have a God-given role to oversee our children and pro-

vide for them. This is not the role nor function of government. Our religious freedoms and personal freedoms have been disregarded and violated in this coercion.

"We would welcome the opportunity to prove the legitimacy of our claim for child exemptions by presentation of birth certificates or other means. This is clearly not an issue of fraud, but rather deeply held convictions which have been overlooked by government policies."

—GARY AND DRENDA KEESEE
Mt Vernon, OH

"We have two adopted children. They were claimed without exception in 1994 and 1995 successfully. However, in 1996 and 1997 our income tax refund was withheld because they did not have social security numbers.

"The financial hardship we have suffered from this is over since we had to relinquish our beliefs and submit to having our children receive numbers. Due to an illness that incapacitated my husband we had to get numbers for our kids in order to get the necessary funds being withheld by the IRS. This was to assist us financially due to his inability to work.

"At the time of our compromise the IRS was holding $3,040.38 and we received it once we submitted to having numbers issued to our children.(We don't understand how these numbers prove dependency since the other documents we presented were of greater proof)."

—JOE AND SHARON TADLOCK
Las Vegas, NV

"Close to $3500 is at stake for 1998, and we still don't know what is going to happen for 1999."

—EFRAIN & GAIL RIVERA
Bronx, NY

"My wife and I have been married 21 years and have been blessed by the hand of God with 7 children. . . . Over the past four years, it has cost our family over $16,000 in additional taxes, not to mention the additional insult of interest penalties. For 1999 alone the increased tax impact was nearly $6,400 with the projection for year 2000 being even greater. We are not independently wealthy and could use this money as we raise the children the Lord has given us."

—SCOTT WEURDING
Conklin, MI

"Because of our religious convictions, we have not applied for social security numbers for our eight children. . . . Without the deductions, the IRS requires us to pay $15,200 in taxes plus $1,400 in penalties and interest. In addition, at the end of March, the IRS levied our checking and savings accounts for the entire $16,600 they calculate that we owe. We did not have nearly that much. The entire balance of our checking and savings accounts were seized, leaving us nothing with which to pay our mortgage, groceries, and utility bills. We have struggled these past two months to rebuild our credit and catch up on our bills, pay all our 'non-sufficient funds' fees, and repay those checks that bounced."

—ANDREW AND LYNNE SPEAR
Mesa, AZ

"We are pleased to be the parents of ten children. Our children have been given to us as blessings from God. We have willingly accepted these blessings and the responsibilities that come with raising them. We have chosen not to get social security numbers for our children because this would seem to be taking a precious gift given to us by God and transferring it to the government.

"Although we have experienced various difficulties related to our decision to avoid social security numbers, probably the harshest punishment is being taxed as if we were childless. Since we believe God expects parents, not baby-sitters or day-care, to raise children, we live on only one income. Fortunately we are able to be quite frugal, but the extra taxes we must pay are a definite financial liability.

"We calculated the amount of money we have lost since 1996 and found it to be approximately $21,640. This figure does not include the extra taxes we have paid on the state level since our state bases exemptions solely on the number claimed on our federal return. Such a large amount of money would easily replace our aging, rusting family van. Or it could go toward the college expenses that are rapidly approaching. We would appreciate the passage of-H.R. 2494 as that would allow us to obey God and also relieve some of our heavy tax burden as we seek to provide for our family."

—MR. AND MRS. RICHARD DERBY
Flint, MI

As Roman Catholics we are morally opposed to obtaining a universal identification number for our children. Because the IRS has denied the dependency exemption for our children we have paid in excess of $22,000.00 in additional tax over the past four years.

—DAVID AND CLAUDIA DREW
York, PA

We agonized as a family over this issue for years. The filing of our taxes each year brought stress, wondering at the repercussions of again challenging the state system. Our 1996 tax return was changed by the IRS to indicate that we owed an additional $2,292.96, because our children were disallowed as deductions, simply because they were not numbered. We were put in anguish over what to do to resolve our struggle. Some anonymous friends left money for us that was used to pay the balance.

—MARK AND PAM HOLDEN
Wampsville, NY

"Due to the fact that we are taking a faith stand, it has cost us approximately $ 3000.00 per year in lost refunds owed to us. Over the last 4 years that adds up to $ 12,000.00 lost revenue. . . . The government will count our children for census purposes, but will not count our children for our refunds just because they don't have social security numbers."

—CRAIG AND MARY PRENA
Attica, MI

Our additional tax burden amounts to $2000 per year that we cannot claim because we have chosen to not have SS numbers and have been unable to obtain any alternative form of identification.

—MICHAEL AND EVELYN WILLIAMS
Akron, OH

2. Courts already allow similar religious exemptions for federal aid programs.

Some federal aid programs require recipients to submit the social security numbers of dependents in order to receive the aid. However, courts have ruled that individuals who otherwise qualify for these benefits could not be denied funds solely because they were religiously opposed to obtaining social security numbers for their children. See Stevens v. Berger, 428 F.Supp. 896 (E.D.N.Y., 1977), and Callahan v. Woods, 736 F.2d 1269 (9th Cir., 1984). Congress should all the more allow a religious exemption for families filing their income tax returns to keep money that they rightfully earned.

3. A religious exemption would not revoke the current fraud protection mechanism.

The religious exemption proposed in H.R. 2494 would not revoke the fraud protection mechanism established in 26 U.S.C. § 151 (e). Any taxpayer seeking the religious exemption would be required to include birth certificates and medical records to prove the existence of his children. In addition, he would be required to submit a sworn affidavit with his tax return, explaining his sincerely held religious beliefs.

Here is one religious family's description of their desire to prove the identity of their children and abide by the law.

"We have always filed our taxes as accurately, honestly and quickly as possible (usually by the first week of February). When we discovered that the I.R.S. was no longer considering our children dependents for tax purposes we tried everything to satisfy them that we were not trying to deceive the government about the number of dependents in our home. We sent notarized, certified copies of the children's birth certificates to the IRS, only to have them mailed back to us. We offered to meet with IRS agents anywhere anytime with our complete family so that they could interview us and see that our four children truly do exist and that they truly have lived with us for each of the 12-month periods in question. The IRS has not responded to this offer. . . . Despite all our fear and frustration, we believe that the 'system' can still work."

—STEPHEN MARTIN NORTH
Amity, Maine

THE SOLUTION: THE CHILDREN TAX ID ALTERNATIVE ACT (H.R. 2494)

HSLDA helped draft a bill to correct this problem, the Children Tax ID Alternative Act, H.R. 2494 which is sponsored by Congressmen John Hostettler (R09IN) and Bill Goodling (R09PA). Under this legislation, families with a religious objection

will no longer be required to obtain a SSN for their children in order to claim them as dependents.

In lieu of a government-issued number, this bill requires a religious objector to produce several items:

1. A sworn affidavit from the parents describing their own religious belief;
2. An affidavit from a non-relative vouching that the children being claimed as dependents are indeed the parent's children;
3. Two other articles showing the relationship of the dependent to the taxpayer. The article choices include a birth certificate, medical records, insurance records or school records.

OTHER REASONS THIS AMENDMENT (H.R. 2494) SHOULD BE ENACTED

1. The religious objector retains the burden of proof.
2. Granting this religious exemption will not cause the loss of legitimate government revenue. These families have children and are entitled to money that is rightfully theirs—not the government's.

CONCLUSION

Families who qualify for a dependent deduction should be allowed to take this deduction even though they have an objection to the assignment of SSNs to their minor children. The policy of the United States should be to grant tax deductions on the basis of physical children in a family—not on the basis of identifying numbers in a family. The IRS is always able to challenge the truthfulness of any deduction. Should fraud be found, stiff penalties should be assessed.

Supporting H.R. 2494 will advance religious freedom and provide a minority of families the legitimate tax relief to which they are entitled. We need to stop making families pay to protect their religious beliefs.

APPENDIX A

It is my conviction that children are the God-given responsibility of their parents; that they do not have an independent status in relationship to the state; and that an identification number assigns control over our children in a way that compromises the separation of secular and parental authority, causing us to relinquish part of our accountability to answer to God for our children. The identification number foreshadows intrusive government action, and also echoes the horrible history of political regimes of totalitarianism. God expects us to protect our children and interpose ourselves for them, for example, by mediating the role of government in their lives as minor children.

The hardship of consistency to these convictions is extreme. It is very difficult to try to live up to both our responsibility of paying taxes in obeying the law, and our responsibility to what conscience decrees toward the children. The stress that we endure financially is troubling, as well.

Here is the pertinent financial situation:

1997	Calculated tax refund	$161.00
	Adjusted tax bill owed	$2,340.56
1998	Calculated tax refund	$511.00
	Adjusted bill	$7,872.49
1999	Calculated tax	$720.00
	Adjusted bill (estimated)	$7,000.00
Total additional tax	(excluding the refunds, interest, etc.)	$17,213.05

Last November, we took a second mortgage on our home; one of the main reasons was to become current and pay in full our 1997 and 1998 taxes. Please help us by passing this legislation.

RINNIE LIND

Respectfully Submitted

CHRISTOPHER J. KLICKA
Senior Counsel
Home School Legal Defense Association
PO Box 3000
Purcellville, VA 20134

Statement of Gil Hyatt, Las Vegas, Nevada

Thank you for this opportunity to present a written statement for the record of hearings before the House Ways and Means Subcommittee on Social Security on the "use and misuse of social security numbers." While there are many aspects to this issue and many examples of violations of safeguards to protect social security numbers, I would like to highlight for the subcommittee a growing and potentially out of control problem dealing with State taxing agencies. Across the country there is a growing problem with inappropriate disclosure and misuse of social security numbers, as well as other private information, by State taxing agencies, like the California Franchise Tax Board ("FTB").

I. STATE TAXING AGENCIES ARE INDISCRIMNATELY DISCLOSING AND MISUSING TAXPAYER'S SOCIAL SECURITY NUMBERS

The task of keeping one's social security number private is much more difficult in today's world where the number is used for a myriad of purposes. As a universal identification number, the social security number has taken on a role much greater than that for which it was ever intended. While individuals can choose whether or not to disclose their social security numbers to businesses or other individuals, these same individuals cannot control a state taxing agency's use and disclosure of their social security number as well as any other Federal tax information. In the past, Congress has passed legislation intended to ensure that steps be taken to ensure that a taxpayer's Federal tax information (most relevantly, a taxpayer's social security number) is kept confidential by all who receive such information. Under existing law, the IRS can share its taxpayer information with state tax agencies and others so long as those agencies abide by certain rules that protect confidential taxpayer information.

Even though Congress reformed the IRS with the Internal Revenue Service Restructuring and Reform Act of 1998 to protect taxpayers' rights and confidentiality, state taxing agencies, guilty of similar types of abuses that provoked Congressional reform of the IRS, have nevertheless resisted such reform measures. Many states use the same type of abusive tactics for which their federal counterpart—the IRS—was reprimanded by Congress. The state taxing agencies, however, have gone even further than the IRS ever dared to go by exacting revenue from non-residents using tax assessments that are significantly increased by ill-supported penalties. In making such assessments, state taxing agencies use Federal tax return information (including a taxpayer's social security number) without regard for its confidentiality. In a recently published study, the Joint Committee on Taxation highlighted the growing problem of breaches of confidentiality of Federal tax returns and return information by state tax agencies.[1]

As the Joint Committee on Taxation report clearly shows, state and local tax agencies have little if any respect for the safeguards put into place by Congress to protect the confidentiality of a taxpayer's social security number. No state taxing agency is more guilty of wrongful disclosure of a taxpayers' social security numbers than the California Franchise Tax Board ("FTB").[2] Set forth below is a description of personal experiences evidencing the misuse of social security numbers by the FTB.

---

[1] *See* Joint Committee on Taxation "Study of Present-Law Taxpayer Confidentiality and Disclosure Provisions as required by Section 3802 of the Internal Revenue Service Restructuring and Reform Act of 1998," January 28, 2000.

[2] The FTB is the agency that collects income taxes for the state of California.

II. Examples of Misuse of Confidential Taxpayer information (including Social Security Numbers) by the FTB

An independent observation of personal experiences with the FTB would suggest that no information, including social security numbers, is confidential to the FTB. As an example, during the course of a typical state tax residency audit, the FTB will promise that the confidentiality of a taxpayer's information is protected by California law in order to induce taxpayers to disclose such confidential information. Then, the FTB later creates reasons why the confidential information is no longer confidential. As part of this pattern, the FTB then unilaterally declassifies and, without even notifying the taxpayer, publicly discloses the confidential information, which includes a taxpayer's social security number.

In one particular case, the FTB was performing a residency audit on a wealthy Nevada resident who is well-known for his innovations in computer technology. The Nevada resident is justly protective of the location of his office and research lab in view of the industrial espionage that is rampant in the industry marketplace and in view of the established danger from stalkers and other predators. He has taken great care to keep the address of his home, office, and research lab secret to protect against industrial espionage and stalking, including purchasing the property through a trust and taking other precautions so that his name was not connected with the property. He gave the private address to the FTB only after the FTB provided assurances that it would keep it strictly confidential and that California law made it a crime for the FTB to disclose such information.

Then, without notice to the Nevada resident and with total disregard for his privacy, safety, and confidentiality, the FTB, within weeks, began indiscriminately broadcasting the private address along with the taxpayer's social security number to the very entities from whom the Nevada resident sought to keep the private address confidential. The FTB sent out formal Demands for Information (quasi-subpoenas) to newspapers and to other public entities that keep large databases of information on citizens which contained the individual's private social security number. See attached copy of the FTB's Demand for Information (with the confidential taxpayer information having been redacted for this copy, but which was not redacted in the original).

These quasi-subpoenas disclosed the Nevada resident's name, social security number, and his non-public residence address to the very entities from which he sought to be protected. This without even noticing, servicing, or informing the Nevada resident or his attorney that such quasi-subpoenas were being sent out, thereby depriving him of his legal right to take legal action to quash these fraudulent quasi-subpoenas. After unilaterally declassifying and indiscriminately disclosing to the public the Nevada resident's confidential information, including his social security number and private residence address, the FTB defended its disclosure by stating that it needed to disclose the confidential information (even though the FTB could have obtained the information it sought from the Nevada resident himself).

When challenged about this disclosure of confidential information, the FTB attempted to justify its disclosure of the Nevada resident's confidential taxpayer information by alleging that the confidential information was not confidential because it could be found in the public domain (even though the FTB never found the information publicly). The FTB asserts that because the Nevada resident's social security number could be found in an obscure public court filing, it need not be kept confidential. Such a position not only represents a "crass legal fiction"[3], but is also contrary to federal ase law—"a clear privacy interest exists with respect to such information as names, addresses, and other identifying information even if such information is already available on publicly recorded filings."[4] The court cited for support the Supreme Court's notation in *United States Dept of Defense v. Federal Labor Relations Auth.* that "an individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may [already] be available to the public in some form"[5]. The court also cited the Supreme Court's conclusion in *U.S. Dept of Justice v. Reporters Comm. for Freedom of the Press* that "the fact that 'an event is not wholly private does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[6]

---

[3] *Briscoe v. Reader's Digest Association, Inc.,* 4 Cal. 3d 529, 539 (Cal. 1971) ("It would be a crass legal fiction to assert that a matter once public never become private again.")

[4] *Abraham & Rose v. U.S.,* 138 F.3d 1075, 1083 (6th Cir. 1998) (footnote omitted).

[5] *Id.* (quoting 510 U.S. 487, 500, 127 L. Ed. 2d 325, 114 S. Ct. 1006 (1994) (alteration in original)).

[6] *Id.* (quoting 489 U.S. 749, 770, 103 L. Ed. 2d 774, 109 S. Ct. 1468 (1989).

In the case of the attached Demand for Information form letter, the FTB clearly lists the taxpayer's social security number in the upper-right hand corner of this form, which indicates that the FTB always sends out this form letter with the social security number disclosed. There is absolutely no reason why the Las Vegas Sun—a widely distributed public newspaper—needs to see the taxpayer's social security number in order to answer the FTB's queries. If the FTB needs some method of keeping track of cases, the agency can easily assign each taxpayer under audit a case identification number—this would accomplish the FTB's goal of keeping track of a taxpayer without unlawfully disclosing the taxpayer's confidential social security number to the public.

In the case of the Nevada resident, the FTB had also made specific promises that it would not disclose the taxpayer's private address. Nevertheless, the attached Demand for Information clearly equates the Nevada resident with the address—in direct violation of the FTB's promises of confidentiality toward the Nevada resident. The FTB could have easily divided its demand letters into two—the first one sent to the Las Vegas Sun asking for any and all records regarding the taxpayer (without any mentioning of a social security number, without stating that it was for an investigation into the taxpayer, and without stating a specific address) and the second one sent to the Las Vegas Sun asking for any and all records regarding newspaper subscriptions at XXX address (without any mentioning of a social security number, without mentioning the taxpayer's name, and without stating that it was for an investigation into the taxpayer). This would accomplish the FTB's goal of getting the information it wants (even though it could have just as easily received such information from the Nevada resident himself) and would also keep the Nevada resident's identity as a subject of investigation, his social security number, and his address confidential (as the FTB is required to do anyway and explicitly agreed to do in the case of the Nevada resident).

The FTB does not just disclose this confidential information accidentally or discretely. While the FTB asserts that these quasi-subpoenas are intended only to demand information from uncooperative third parties, the FTB has adopted another use for them—as tools for embarrassing and intimidating the taxpayer and disclosing the taxpayer's confidential information by indiscriminately sending them out in mailings. In fact, the FTB is very direct in using the aforementioned intimidating Demands for Information form to indiscriminately disclose a taxpayer's confidential information and at the same time cast the taxpayer in a bad light and getting the recipient's attention due to its formal, criminal-investigation type format. The Demand clearly states that it is "In the Matter of: <insert name here>" and that the information "will be used by this department for investigation, audit or collection purposes pertaining to the above-named taxpayer for the years indicated." The FTB could have easily requested information from the Las Vegas Sun without plastering the taxpayer's name all over the Demand. As suggested above, cases can be assigned case numbers for reference purposes and need not place taxpayers under such obvious suspicion by putting their name at the top of the Demand. The form would still accomplish its objectives were the name not on the Demand. The only purpose served by putting the subject's name on the Demand is to raise suspicion in the recipient's mind regarding the subject taxpayer.

Because first requesting information directly from the taxpayer (as required by California Civil Code § 1798) would not be intimidating or embarrassing enough to accomplish its purpose, the FTB instead prefers to break the law and go directly to third parties in the most intimidating way for the taxpayer. In the case of the Nevada resident, the FTB located a check made out to a Dr. Shapiro; but instead of asking the Nevada resident for information on this Dr. Shapiro, the FTB located six Dr. Shapiros in the telephone book and sent out the aforementioned quasi-subpoenas to all of them, thereby informing a group of professionals that the Nevada resident was under investigation, focusing more attention on him, and causing him even greater exposure and embarrassment. This in addition to the quasi-subpoenas sent by the FTB to several newspapers on a "fishing expedition" calculated to cause the victim even more exposure and embarrassment while disclosing his confidential information. Both of theses examples show how the FTB uses confidential taxpayer information (including social security numbers) to intimidate taxpayers in order to exact improper tax assessments.

The FTB's official position is that a taxpayer's confidential information is protected under California law but that the FTB can disclose the confidential information (including commingled Federal tax information and social security numbers) at its sole discretion without even notifying the taxpayer or giving the taxpayer an opportunity to challenge the declassification. Hence, confidentiality is all at the self-serving discretion of the FTB and the FTB is bent on public disclosure of taxpayer information to intimidate taxpayers to settle. In the case of the aforementioned Ne-

vada resident, the FTB assessed millions of dollars in false penalties and made millions of dollars worth of intentional errors in income calculations consistent with the FTB's established practice of significantly increasing assessments in preparation for settlement negotiations. Then, when the Nevada resident refused to submit to this practice, the FTB threatened that his confidential personal information would become public if he didn't settle like other citizens do—taxpayers usually settle at the protest stage to keep their private information from becoming public. The FTB has been accused of extortion and fraud as a result of this methodology.

The FTB is guilty of regularly revealing confidential Federal tax information (and social security numbers) in a public forum. In court papers submitted by the FTB to the SBE[7], the FTB routinely attaches its NPAs (Notice of Proposed Assessments) to the briefs without redacting the taxpayer's social security number (which is predominantly displayed on each of the NPAs sent out by the FTB). See the 52 pages of Federal tax return information that were attached to the FTB's Supplemental Brief.[8]

The FTB is so blatant in its disregard for the taxpayer's confidential Federal tax information that it, without hesitation, discussed specific monetary figures on the taxpayer's tax return: "As a result, appellants [sic] asserted that only $127,113 of their total federal adjusted gross income of $772,850 for 1990 was California income subject to tax in this state."[9] "Reported on the federal return is Schedule C income in the amount of $164,435.00. . . . Also reported on the federal return is partnership income in the amount of $567,446.00."[10] This material was supplied by the FTB to the SBE without any confidentiality statement or motion to seal the Federal tax information records and this Federal tax information is now available to the public.[11]

III. Social Security Numbers are the Least of the FTB'S Unscrupulous Actions

The FTB is one of many state taxing agencies which relies upon IRS information for its taxing activities. But California tax law has not been conformed with the Internal Revenue Service Restructuring and Reform Act of 1998. Thus, while the IRS collects taxes from taxpayers now protected under the reformed provisions, the FTB continues to reek havoc on unsuspecting taxpayers, held only to its own un-reformed, self-serving standards. Even worse, the FTB does not even follow its own un-reformed standards, blatantly violating California laws with impunity.

The FTB has been violating both Federal law and even California law for so long under the guise of assessing and collecting taxes that it cannot be expected to comply with the new more stringent Federal laws on confidentiality of Federal tax information (and social security numbers).[12]

Also, the FTB is so submerged in a culture of bad faith and fraudulent behavior that it cannot be expected to comply with laws that are based on good faith relationships with taxpayers. Hence, regardless of the lip-service paid by the FTB concerning the confidentiality of a taxpayer's information, the FTB is incapable of providing the safeguards necessary to protect not only shared IRS tax return information (including social security numbers) but also the FTB's own taxpayer information that it is legally required by statute to keep confidential.

An agency whose actions are based upon bad faith taints all who cooperate with it in its deeds. The FTB's record of bad faith is reason alone for it to be excluded from receiving IRS information and social security numbers. This kind of state tax agency cannot be trusted with confidential Federal tax information and social security numbers. Before the IRS shares information with such a state agency, the law should require that the Federal tax information be used only in cases where the state agency is acting in good faith and in compliance with its own state laws as well as Federal laws. Any evidence that a state tax agency is using Federal tax information and social security numbers in conjunction with any kind of improper and/or illegal state tax activities should be grounds for immediate suspension of any sharing by the IRS with that state tax agency.

---

[7] The SBE is the California State Board of Equalization, the agency that hears the administrative appeals from the decisions of the FTB.

[8] *See, e.g., In the Appeal of Paine/Norton,* 98A090741, Case No. 89002467180, California State Board of Equalization decision at 4 (October 7, 1999) (emphasis added).

[9] *See, e.g., Id.* (emphasis added).

[10] *See, e.g., Id.* in the letter from the FTB to Mr. Paine dated January 20, 1994 and included as part of the public record available to the public from the SBE (emphasis added).

[11] The file of the Appeal of Paine/Norton was ordered from the SBE and was supplied by the SBE without any form of confidentiality notation.

[12] Federal tax returns and return information (FTI). *See* OMB No. 1545090962 at 1.

The improper acts of the FTB involve both Federal tax information as well as state tax information. The FTB auditors are untrained, inexperienced, and unsupervised and do not distinguish between different types of information. They intermingle tax information and social security numbers of different citizens in the same audit file and produce it to citizens who do not have a right to access the other taxpayer's tax information.

The FTB auditors indiscriminately disclose confidential tax and social security information to associates that do not have a need to know. For example, one FTB auditor seeking peer approval and attention distributed her narrative, which described the confidential issues and details of the Nevada resident's audit (the largest in residency-audit history at the time) to her associates. This type of disclosure is prohibited by both the Taxpayer Browsing Protection Act and by common sense.

This same auditor visited that Nevada resident's private residence with her friend out of curiosity, to take "trophy" photographs of the private residence, to improperly rummage through garbage, and to trespass and investigate the private property. The auditor was no longer involved in the audit at the time, she had no right to continued activities thereon, and her friend had not been involved in the audit or had no right to be involved.

The FTB indiscriminately discloses or at times threatens to disclose confidential information publicly as a tool in forcing taxpayers to give up on or settle tax controversies. In one case, knowing of a particularly need for privacy, the FTB made a promise to keep information confidential and then, immediately after this promise, the FTB disclosed such confidential information in order to intimidate the Nevada resident to extort him of multi-millions of dollars in taxes, interest, and penalties. The FTB was convinced that he was very concerned about his privacy and that such public disclosure would force him to settle an unjust assessment. The common name for this type of tactic is extortion.

The FTB sends out letters to Federal officials, postmasters, to find out the taxpayer's forwarding address. But these letters, which were signed by the head of the FTB, made false certifications to the Federal officials. These letters certified that the FTB had exhausted all other avenues to obtain the taxpayer's address information. But the FTB had already received this information—from the taxpayer himself. More relevant here is the fact that this address that the FTB was investigating was the same address that was on the IRS tax return information shared with the FTB. The issue is that the FTB got information from the IRS that the IRS considers to be confidential, yet the FTB comes up with reasons that they should not keep it confidential. Accepting taxpayer address information (and social security number information) from the IRS requires the FTB to comply with Federal laws regarding the treatment of such information, otherwise the FTB's hair-splitting will extend to even more blatant violations of the IRS tax return sharing laws.

In one particular case, the FTB continued to refuse to disclose the Nevada resident's tax records to him (which he has a right to see under California law) but the FTB indiscriminately disclosed other citizens' tax records to the taxpayer that he did not at the time have a right to see and the FTB indiscriminately discloses the Nevada resident's tax records to others that do not have a right to see. The FTB habitually uses private and detailed taxpayer information for training materials that the FTB makes available to the public. The FTB changes the last names to something seemingly innocuous (such as to James H. Taxpayer), but the audit information provided by the FTB is so specific and so detailed that the real name and address of James H. Taxpayer was found within 15 minutes—it was as simple as ordering and looking through a phone book.

A state tax agency that would is involved with any of the aforementioned illegal acts cannot be trusted with confidential Federal tax information and social security numbers. Although the Federal statutes and guidelines do not expressly require any state tax agency to act in good faith on taxpayer matters, a state tax agency that acts in bad faith cannot be relied on to protect the confidentiality of Federal tax information and social security numbers. In fact, the Federal statutes and guidelines require competence and imply good faith, but the FTB shows neither when it is focused on exacting large assessments from former California residents.

California requires taxpayers to disclose to the FTB the Federal tax information (and social security numbers) from their Federal income tax return. The FTB then uses this information in its audits and publicly discloses it (such as in appeals to the SBE). Therefore, regardless of the protections that the IRS provides for Federal tax information in order to encourage taxpayers to provide the IRS with all tax information, taxpayers will be reluctant to provide the IRS with such information because states like California require taxpayers to provide them that Federal tax information (and social security numbers), but do not protect its confidentiality as the IRS is required to do. Because the IRS promises taxpayers that Federal tax informa-

tion will be kept confidential, it is improper for the FTB to require taxpayers to disclose this confidential information without proper legal process. State taxing agencies should not be permitted to require taxpayers to disclose Federal income tax information without legal process, and even then such information should be treated with the same respect to confidentiality as does the IRS.

IV. Congress' Role in Reforming Abusive State Tax Agencies

The FTB has been abusive and aggressive in its state taxing activities and the IRS is being made an unwitting party to the abuse. An agency that indiscriminately and intentionally uses and misuses social security numbers and undertakes other such illegal tactics as described above should not be trusted with Federal tax information and social security information until it has been reformed.

Instead of acknowledging the abuses and instituting reforms after being alerted to them, the FTB continues with the illegal activities. These include continuing illegal disclosure of confidential information (and social security numbers), falsification of official tax records, illegal destruction of important litigation-related documents, improper disclosure of other taxpayer's information, and much much more. The FTB practices the most abusive and often illegal tax collecting methods imaginable. Clearly, the FTB cannot be trusted to protect the confidentiality of Federal tax information and social security numbers.

Congress has a strong interest in the policies and procedures of the state tax agencies because the IRS shares its Federal tax information with the state tax agencies. Internal Revenue Code § 6103(a) makes it clear that state employees with access to Federal tax return information shall keep such information confidential and may not disclose it to anyone except for those properly authorized to view such information. Because Federal tax information is what is being shared, Congress must insure that the shared tax information (including social security numbers) is protected to the same degree called for by Federal law and state tax agencies must be held to the same standard to which the IRS is held regarding Federal tax information. Congress should also insure that the IRS reforms are not tainted by abusive state tax agencies misusing Federal tax information and social security numbers. Furthermore, Congress should also insure that the IRS is not tainted by associations with abusive state tax agencies acting in bad faith in exacting improper taxes.

State tax agency reform can be easily accomplished by Congress. All state tax agencies receiving IRS information should be required to adopt and abide by the taxpayer protection reforms present in the Internal Revenue Service Restructuring and Reform Act of 1998 as a prerequisite for obtaining Federal tax information from the IRS. Because most state tax agencies are dependent on Federal tax information obtained from the IRS for administering their own tax programs, they will most likely agree to conform to the Federal statutes in order to continue to obtain Federal tax information and social security number information if mandated by Congress.

V. Conclusion

State taxing agencies (including California's FTB) have a record of misusing confidential taxpayer information (including social security numbers) and have been found to violate well-intended safeguards to protect such information by a study of the Joint Committee on Taxation. Accordingly, Congress should take action to prevent such abuse, including directing the IRS to cease sharing tax return information (and social security numbers) with any state tax agency, such as the FTB, that abuses such information or violates such safeguards. These actions should be mandated until the abuses have been rectified, the agencies have taken appropriate measures to prevent future abuses, and the state statutes have been conformed with the Federal IRS statutes regarding taxpayer's rights. Furthermore, a Treasury Department investigation and a Congressional investigation by the GAO should be conducted to ascertain the scope of the egregious and illegal conduct of state agencies, including the FTB, and to determine the degree to which confidential Federal tax information and social security numbers have been inappropriately and illegally misused.

STATE OF CALIFORNIA
FRANCHISE TAX BOARD
333 N. GLENOAKS BLVD., SUITE 200
BURBANK, CA 91502-1170

DEMAND TO FURNISH INFORMATION
Authorized by
California Revenue & Taxation Code
Section 19504 (formerly 19254 (a) and 26423 (a)*)

The People of the State of California to:

Las Vegas Sun
800 S. Valley View Blvd.
Las Vegas, nevada 89153

In the Matter of: [redacted]

Social Security No. : [redacted]
or Corporation No. :
For the years :

This Demand requires you to furnish the Franchise Tax Board with information specified below from records in your possession, under your control, or from your personal knowledge. The information will be used by this department for investigation, audit or collection purposes pertaining to the above-named taxpayer for the years indicated.

1. Indicate if the above individual has subscribed to the Las Vegas Sun during the period from 1991 to the present. If yes, please indicate the start and stop dates of service and the address that the subscription was sent to.

2. Indicate if there were any subscriptions to the Las Vegas Sun at [redacted] during 1991-1992 and at [redacted] from 1992 to the present. If so, indicate the start and stop dates of service and the name(s) of the person(s) on whose account it was billed.

FRANCHISE TAX BOARD

By: S. Cox
Authorized Representative

Dated: 8/4/95

Telephone: (818) 556-2942

* Legislation effective January 1, 1994 (S.B. 3, Stats. 1993, Ch. No. 31) consolidated certain provisions of the California Revenue & Taxation Code which caused some sections to be revised and renumbered.

[redacted]

Statement of Kent Snyder, Executive Director, Liberty Study, Falls Church, Virginia

Ludwig von Mises, economist and true champion of liberty, concluded that with respect to political and economic systems, one can choose either totalitarianism or capitalism—there is no middle ground. Few issues demonstrate the justification for his conclusion so clearly as does that of privacy protection.

The premise of Mises' argument was that interventionism necessarily begets interventionism as the negative effects of government's initial intervention become the justification for each of the subsequent interventions. For example, when government establishes a minimum wage above the market wage, that class of employees whose marginal product is below the artificially established minimum wage become legally unemployable, and, hence in "need" of governmental support. Of course, government's subsequent response to then support every unemployed member of society at some subsistence level creates yet another incentive for more intervention when those actually working to achieve that level of subsistence realize it can be achieved without continuing their efforts. Of course, this privacy hearing is not exactly about the minimum wage but rather whether government should inter-

vene yet again to remedy the negative consequences of its prior, privacy-destructive intervention or whether they should properly recognize themselves as the source of the malaise and repeal the prior intervention.

In *America's Great Depression,* economist Murray Rothbard explains how massive federal intervention into the monetary sphere (contrary to the usual tripe proffered regarding "unbridled capitalism" causing the depression) served as the intervention that sent this country into the throws of the great depression. Among the subsequent and numerous interventions to remedy the negative effects of governmental monetary mischief, was the Social Security Act, a bill which after nearly one hundred and fifty years of history to the contrary, "relieved" citizens of the individual responsibility for providing for their own financial futures and those of their family members. Of course, as Mises understood and explained, these interventions were the natural result of the negative consequences triggered by interference in the monetary sphere.

Because individual and private accounts would no longer be the means by which most savers provided for their financial futures and as though money was actually being placed by government into individual accounts for those without the requisite self-discipline to provide for their own future financial well-being, every participant in the system was ultimately issued a Social Security "Account Number." Although the Congress that created the Social Security system in no way intended to create a national identifier, a subsequent executive order by President Roosevelt authorized the use of the Social Security number as a standard federal identifier.

In the name of "protecting" the taxpayer against government inefficiency and various forms of fraud, government took subsequent steps to further establish the SSN as a uniform identifier. For example, where military members once used their military serial number, this was replaced by the Social Security number as a standard identifier. Additionally, the Bank Secrecy Act of 1970 generated regulation requiring the collection of Social Security Numbers by banking institutions. When, at a minimum, banks were mandated by government to use at least that number and to preserve scarce data resources and avoid duplicity of records, financial institutions naturally adopted the social security number as their record number of choice.

In response to concerns about the widespread use of the SSN, Congress passed the Privacy Act of 1974, but, unfortunately, the language of the Privacy Act allows Congress to require the use of the Social Security number at will. In fact, just two years after the passage of the Privacy Act, Congress explicitly allowed state governments to use the Social Security number as an identifier for tax collection, motor vehicle registration and drivers' license identification. The federal government has also compelled extensive disclosure and use of the Social Security number in its labor, medical, and education databases.

Given that government, to accommodate its own prior interventions, has not only facilitated but compelled the creation of a massive tool for privacy invasion, government is now, of course, presented with the question of whether to undo at least some of the prior intervention or use the culmination of negative effects of all these prior interventions to, yet again, intervene further in the liberty and private dealings of individuals.

The Liberty Study Committee supports what is the only proper response to this question: eliminate the proliferation of the government-instilled, privacy-destroying tool—the Social Security Account Number. While it certainly does not return government to its proper role and restore responsibility for saving to individuals, The Freedom and Privacy Restoration Act, H.R. 220, introduced by Representative Ron Paul, would limit the use of the Social Security number to the Social Security system administration, and is an important step in the right direction of at least protecting the privacy of individuals. Without question, certain inefficiencies will necessarily result in limiting the use by government of this number but, first and foremost, we must not forget that government's primary role must be to preserve individual liberty rather than "efficiently" run government programs, many of which lack constitutionally legitimacy in any case.

Under no circumstances should the government use their very own government-created privacy crisis as a justification to restrict what private individuals do or don't do with their private information (even to include release of their own Social Security number). As much as free speech includes the right to be still, inherent to privacy is the right to share or not share private information with those of one's own choosing.

Government has, in essence, turned the notion of privacy protection on it's head with proposals to limit information sharing by private individuals while compelling disclosure to government by those very same individuals. I hope this Congress will recognize and, thus, not fall prey to the "intervention-begets-intervention" recog-

nized by Mises and, as such, not move our nation yet another step further down the road to totalitarianism.

○