S. HRG. 107–712

PROTECTING THE SOCIAL SECURITY NUMBER: AN ISSUE OF PRIVACY OR SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY AND FAMILY POLICY

OF THE

COMMITTEE ON FINANCE UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ON

S. 848

TO AMEND TITLE 18, UNITED STATES CODE, TO LIMIT THE MISUSE OF SOCIAL SECURITY NUMBERS, TO ESTABLISH CRIMINAL PENALTIES FOR SUCH MISUSE, AND FOR OTHER PURPOSES

JULY 11, 2002

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE

82–113—PDF WASHINGTON : 2002

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

COMMITTEE ON FINANCE

MAX BAUCUS, Montana, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	CHARLES E. GRASSLEY, Iowa
TOM DASCHLE, South Dakota	ORRIN G. HATCH, Utah
JOHN BREAUX, Louisiana	FRANK H. MURKOWSKI, Alaska
KENT CONRAD, North Dakota	DON NICKLES, Oklahoma
BOB GRAHAM, Florida	PHIL GRAMM, Texas
JAMES M. JEFFORDS (I), Vermont	TRENT LOTT, Mississippi
JEFF BINGAMAN, New Mexico	FRED THOMPSON, Tennessee
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
ROBERT G. TORRICELLI, New Jersey	JON KYL, Arizona
BLANCHE L. LINCOLN, Arkansas	CRAIG THOMAS, Wyoming

JOHN ANGELL, *Staff Director*
KOLAN DAVIS, *Republican Staff Director and Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY AND FAMILY POLICY

JOHN BREAUX, Louisiana, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	JON KYL, Arizona
JEFF BINGAMAN, New Mexico	DON NICKLES, Oklahoma
TOM DASCHLE, South Dakota	TRENT LOTT, Mississippi
JOHN F. KERRY, Massachusetts	PHIL GRAMM, Texas
JAMES M. JEFFORDS (I), Vermont	CRAIG THOMAS, Wyoming

CONTENTS

OPENING STATEMENTS

CONGRESSIONAL WITNESSES

AGENCY WITNESSES

PUBLIC WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATIONS

PROTECTING THE SOCIAL SECURITY NUMBER: AN ISSUE OF PRIVACY OR SECURITY

THURSDAY, JULY 11, 2002

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 2:25 p.m., in room 215, Dirksen Senate Office Building, Hon. John Breaux (chairman of the subcommittee) presiding.

Also present: Senators Lincoln and Kyl.

OPENING STATEMENT OF HON. JOHN BREAUX, A U.S. SENATOR FROM LOUISIANA, CHAIRMAN, SUBCOMMITTEE ON SOCIAL SECURITY AND FAMILY POLICY

Senator BREAUX. The subcommittee will please come to order.

Good afternoon, everyone. I would like to thank everyone for attending our hearing. I would like to thank our witnesses. Judd Gregg is with us and will be testifying, and also Senator Feinstein is on her way, having just completed the vote.

We are going to examine today a subject that many Americans know very little about. Identity theft is one of the most insidious forms of white color crime, in that its victims rarely even know that a crime has even been committed against them.

Identity theft is generally defined as theft or fraud that involves stealing another person's personal identifying information, such as a Social Security number, date of birth, or mother's maiden name in order to fraudulently establish credit or incur debt to take over financial accounts, or engage in other criminal endeavors. The prevalence of identity theft in our Nation is growing very rapidly and needs to be addressed.

At the heart of the identity theft is the theft and misuse of Social Security numbers. It is the theft and misuse of Social Security numbers that we are here to examine this afternoon. The general public needs to be more aware of this silent, and often unnoticed, crime.

My hope is that, through hearings such as this, the Congress will be able to show citizens how better to protect themselves and their personal information from identity thieves, while also developing real, concrete solutions to address the problem.

Any solutions that are developed to address the theft and misuse of Social Security numbers and the ensuing identity theft must be a collaborative effort between the Congress, government agencies, the federal, State, and local levels, and also private industry. I

think it is clear that we have much work to do, and I am looking forward to hearing from our witnesses.

We are delighted to have our colleague, Senator Judd Gregg.

Judd, if you would like to proceed, and we will take Senator Feinstein as soon as she returns.

STATEMENT OF HON. JUDD GREGG, A U.S. SENATOR FROM NEW HAMPSHIRE

Senator GREGG. Thank you, Mr. Chairman. I appreciate your holding this hearing on this issue which is very significant.

I see Senator Feinstein is arriving. I want to thank Senator Feinstein for her efforts in this area, and especially for including some of the language which I developed in her bill as she reported it out, and for having the opportunity to allow me to join with her in this effort on S. 848. I do have a statement which I will submit for the record. Unfortunately, I have to run. I apologize for that.

My interest in this arose because a young woman in my hometown named Amy Boyer was stalked by an individual, and later killed by the same individual, who obtained much of the information he needed to accomplish that off the Internet by paying $75 and getting her Social Security number.

Her Social Security number had been obtained by a company who sold it over the Internet. They did it under a pretext. They allegedly called her home and said they were insurance salesmen, or something like that, I think. I am not absolutely sure of that, but it was something in that area. They got her number, and as a result, that number was then sold. This individual, who had some sort of fixation on her, stalked her and killed her.

There are a lot of legitimate uses for Social Security numbers. We know that. The bill that Senator Feinstein has put together and I have participated in attempts to address those legitimate commercial uses. We do not want to create a situation where legitimate commercial uses are undermined.

But what we need to create is a situation where things like what happened to Amy Boyer do not happen, and lesser levels of activity such as your Social Security number being abused by somebody who gets their hands on it, as the Chairman referred to in his opening statement.

So I appreciate the committee holding this hearing. I do hope you can move the bill promptly, as I do think it is an important piece of legislation. Again, I want to thank Senator Feinstein for her efforts and leadership in this area, which I think has been extraordinary.

Senator BREAUX. Thank you, Judd. We look forward to working with you on this process.

[The prepared statement of Senator Gregg appears in the appendix.]

Senator BREAUX. Now we will hear from the principal author of the legislation that is before the committee, Senator Feinstein from California.

Dianne, welcome.

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM CALIFORNIA

Senator FEINSTEIN. Thanks very much, Mr. Chairman. I also would like to thank Senator Gregg. He has been great to work with and I very much appreciate it.

What are we talking about? We are talking about one of the largest-growing crimes in America, with literally hundreds of thousands of victims a year. It is called identity theft.

It is the ability of a thief to go to the Internet or anywhere else, get identity information about another individual, become that individual for the purposes of credit, and then rip off that individual for, sometimes, hundreds of thousands of dollars.

The average identity theft costs $17,000. The average length of time it takes an individual to recover their identity before they can go out, use their charge cards, et cetera, is a year and a half. It is a substantial and serious crime.

The Attorney General just held a press conference a while back in which I participated on aggravated identity theft, which we know that, for example, terrorists and people committing murders have used stolen identities. People that want to become another identity, generally for a criminal purpose, go out and steal documents.

Now, what is the most common personal identifier that is stolen? It is the Social Security number. Because with that and a driver's license, and you can buy a Social Security number on the Internet today for about $15, you can go out and assume another's identity and proceed to commit a felony crime.

Now, this bill is not a bill that has been easily put together. Senator Breaux, this is the culmination of 5 years of work. It has been done in conjunction with Senator Grassley, Senator Kyl, Senator Hatch, and the staffs of many Senate offices.

I have had countless meetings with industry groups, privacy groups, and even CEOs of major American companies to try to develop a fair and balanced proposal on Social Security numbers.

I have chaired a half-dozen hearings on identity theft issues in the Judiciary Committee on Technology and Terrorism. We have held hearings in California, where the largest city for identity theft in United States is Los Angeles. The second largest in the state is Oakland, California.

After sponsoring competing bills in the 106th Congress, Senator Gregg and I spent several months hammering out a compromise bill. The compromise has gone through multiple stages of drafting and redrafting, and again, hours of additional meetings and staff work.

The end result of this effort, I believe, is a bill that strengthens protections for Social Security numbers, while minimizing costs as much as we can to businesses and government entities.

The Senate Judiciary Committee reported this bill out by voice vote on May 16. We understood that Finance felt it was their jurisdiction, so we agreed on a short-time referral to Finance in the hope that it will come out of the Finance Committee and we will be able to take it up on the floor this session. Let me give you one example.

A young woman, Michelle Brown of Los Angeles, had her Social Security number stolen. It was used to charge $50,000 worth of goods and services, including a $32,000 truck, a $5,000 liposuction operation, and a year-long residential lease. While assuming Michelle's name, the perpetrator also became the object of an arrest warrant for drug smuggling in Texas.

Identity thieves use these numbers to create additional false identification documents, such as a driver's license, as well.

Now, what does this bill do? This bill prohibits anyone from selling or displaying an individual's Social Security number to the general public without the individual's consent.

It does permit legitimate business-to-business and business-to-government uses of this number. We have worked this out with many companies that were concerned.

I do not think there is adequate justification for allowing the sale of someone's Social Security number to a member of the general public.

As a matter of fact, I wish I had it with me. One law enforcement officer, in our committee, testified that he became me and used my Social Security number, got a credit card and held it up at the hearing for me to see. So, it is very easy to do.

Let me give you another case. Christopher Jones of Pembroke, North Carolina allegedly offered thousands of Social Security numbers for sale on Ebay, with an opening bid of a dollar per number for a block of a thousand numbers. So, you can see what happens. He would just sell those numbers.

This legislation gives consumers the right to refuse to give out their Social Security numbers to companies that do not really need it. Companies can still require Social Security numbers for purposes under the Fair Credit Reporting Act, for background checks, if required by law, or if the number is necessary to verify identity or prevent fraud.

Third, this legislation curbs the public display of Social Security numbers on government documents. This has been very tricky to arrive at. Specifically, the bill removes Social Security numbers from government checks within 3 years, and drivers' licenses within 1 year.

Starting in the year 2005, the bill requires the redaction of Social Security numbers on 11 key public records before they are released to the public. It is not retroactive in this respect, it is prospective. The reason it is prospective is to reduce costs as much as possible.

Additionally, privacy groups wanted a very broad range of public documents, and some businesses wanted none. We tried to limit the public documents to the 11 documents that are the most widely used public documents, where people do get these numbers to exercise this fraud.

They are: death certificates, occupational licenses, property settlement documents, birth certificates, land ownership records, marriage licenses, bankruptcy case files, court judgment, child support documents, and tax liens.

So let us say you or I wanted to obtain one of those documents, and you go to your local recorder or health department, or wherever. They would pull that document out. They would simply redact the number before they turned it over to you.

It turns out that these government documents really constitute a major source of Social Security number for identity thieves. A recent survey by the GAO found that 119 of 250 counties—that is 47 percent—that maintained public records give out records with Social Security numbers to the public.

Of greater concern, 11 of the counties in the GAO study give the public access to records with Social Security numbers via the Internet. So, that is just kind of "open sesame." Anybody can punch it up, get somebody else's Social Security number and from that the driver's license, and then go out and practice identity theft.

I would hope that the Finance Committee would be willing to support this proposal because it strikes a balance between legitimate business uses and the need to prevent identity theft.

Now, some privacy groups think we are permitting too much commercial use of the Social Security numbers. Some business groups argue that we have come down too hard on legitimate use of the numbers.

When we had our last conversations with business entities, it was my understanding that they were in agreement with the bill the way we had finally drafted it.

I know they have been going out now and looking for greener pastures, but I think we have struck a fair balance here in trying to produce a bill that is going to protect the American public from what has become the number-one identifier of our Nation, and also, I am sorry to say, the number-one identifier that enables people to practice identity theft.

Senator BREAUX. Well, Senator Feinstein, thank you very much for your appearance and for your commitment to try and address this legislatively. It is a problem that is of immense proportions, and yet most Americans do not realize how serious it is.

I was coming over on the subway after the vote, and I was telling some of our colleagues that we were going over to chair a hearing on identity theft and the theft of your Social Security numbers.

One of our colleagues said, what does that get you, just getting somebody else's Social Security number? What help does that give them to do anything? Our staff started explaining all of the things that could occur and our colleague said, I had no idea that that was possible. I think that is probably true for a lot of Americans.

Until it actually happens to them and they find out, you do not think that just having someone's Social Security number can lead to such great problems. I think what you have done is provide the leadership to alert an awful lot of Americans to the potential, and now we have got to find a way to correct it. Your legislation is one of those suggestions, and we will take a very serious look at it. Time is a'wasting. We do not have a lot of time to do it.

Senator Kyl, any comments?

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM ARIZONA

Senator KYL. Mr. Chairman, thank you very much for holding this hearing. I have a statement which I would like to put in the record.

Just to expand one bit on what Senator Feinstein said, we started working on this when I was chairman of the Terrorism and

Technology Subcommittee and Senator Feinstein was Ranking. Now our positions are reversed. This is our third time now.

We have had two other bills actually pass and they have made significant strides in helping people with identity theft. But it is apparent to us that we have to go further. The legislation that Senator Feinstein drafted is designed to do that.

Now, we recognize the concurrent jurisdiction of Finance and Judiciary, and it happens that I am on both committees so it is easy for me to say. But I have been trying to assure Senator Feinstein that, while there are some industry concerns about costs and difficulties in implementing the bill and we are all very interested in hearing what those concerns are and trying to meet them, we very much hope that our friends in industry will work with us to craft a bill that we can get through this committee.

Now that we are finished in the Judiciary Committee we hope to get the bill to the floor, because you are correct, time is wasting. Every day that passes, there is more crime that affects our citizens and opportunities for terrorists.

So I look forward to the testimony of the others here today and commend Senator Feinstein, as always, for the pioneering work that she has done in this area.

Senator BREAUX. Well, thank you, Senator Kyl.

Senator FEINSTEIN. I might just mention one thing to Senator Breaux. Senator Kyl, the other day when we had a hearing, Mr. Lormel from the FBI testified. He is head of the Financial Fraud Division of the FBI that is analyzing the finances of terrorism.

What they found out that was very interesting, is six of the hijackers that came earlier went into banks, made up Social Security numbers, and got loans, which is very interesting.

Senator BREAUX. People have no understanding of the concept of how easily this can be done until you are faced with it.

Well, Dianne, thank you very much for appearing.

Senator FEINSTEIN. Thank you. I appreciate it.

Senator BREAUX. We will do our very best.

We would like to welcome up a panel that we have next and that will consist of Hon. James Lockhart, who is Deputy Commissioner of the Social Security Administration, and Mr. John Arterberry, who is Deputy Chief of the Fraud Section, Criminal Division of the Department of Justice, who will be answering questions, as I understand it. We thank you, gentlemen, for being with us.

I will tell you what I am going to do. I am going to bring all of our witnesses up, because I think we have enough chairs. We are all talking about the same subject, so we are not going to fool with panel numbers.

We are also going to invite Mr. James Huse, who is Inspector General of the Social Security Administration; and Norm Willox, who is Chief Officer for Privacy, Industry, and Regulatory Affairs with LexisNexis; and Mr. Don Evans, Director of Industry Marketing with NCR Corporation.

Gentlemen, we will have you all here and we will start in the order that I first read off our witnesses. That would mean that, Mr. Lockhart, James, you are on.

STATEMENT OF HON. JAMES B. LOCKHART III, DEPUTY COMMISSIONER OF SOCIAL SECURITY, WASHINGTON, DC

Mr. LOCKHART. Thank you very much, Chairman Breaux and Senator Kyl. Thank you for asking me here today to discuss protecting the Social Security number, commonly called the SSN.

It is a key stewardship issue that I highlighted at my confirmation hearing before this committee. I am pleased to report that Commissioner Barnhart has taken significant steps to better protect the SSN since then.

As legitimate uses for Social Security numbers increase, so does the potential for misuse. Social Security number misuse can lead directly to identity theft, with serious personal and economic consequences, as we have already heard.

But it also can have even more far-reaching consequences. The tragic events of September 11th and reports that some terrorists used fraudulent Social Security numbers have brought home the need to strengthen and safeguard against SSN misuse.

As you know, the original purpose of the Social Security number was solely for tracking the earnings of people who worked in jobs covered under the new SSN program. But use of the SSN as a convenient way to identify people in record systems has mushroomed over the years.

The SSN has become the identity number for Federal employees, taxpayers, non-citizens authorized to work in this country and beneficiaries of federally-funded programs.

By 1974, Congress had become concerned about the widespread use of SSNs and passed the Privacy Act. It provides that, except when required by Federal law, no government agency could withhold benefits from a person simply because of a refusal to give his or her Social Security number.

But legislation shortly thereafter began to expand SSN use again, including State public assistance programs, motor vehicle registration laws, jury selection, and stronger child support enforcement, to name just a few.

Federal law does not restrict SSN use by private businesses or organizations. People may be asked for an SSN when they rent a video, apply for credit, go to a medical center, or apply for public utility service. People can refuse to give it, but in turn a business may refuse to furnish the product or service.

As you can see, the SSN has become the personal identifier through a gradual build-up over time. Unfortunately, the Social Security number has also become the identifier of choice for criminals, including terrorists.

After September 11th, Social Security formed a high-level response team to better prevent those with criminal intent from using Social Security numbers.

We put a new emphasis on training on enumeration rules. Enumeration is granting a Social Security number. We emphasized in the training, the enumeration of non-citizens. We actually issue 1.5 million Social Security numbers to non-citizens each year.

On March 1, we stopped assigning Social Security numbers to non-citizens for the purpose of applying for a driver's license. Non-citizens can now only get an SSN if they are authorized to work or if they need it for a public assistance benefit.

On June 1, we began verifying birth records of U.S.-born citizens older than age one who applied for a Social Security number, and we are piloting an on-line system that lets employers verify the names and Social Security numbers of newly-hired employees.

We have increased "no-match" letters which are sent to employers and employees with wage reports where the name and the Social Security number do not match our records. There are 8.5 million of those mismatches every year.

Also, we are beginning new data sharing projects with the Immigration and Naturalization Service and the State Department. As we have in the past, Social Security will proceed with the data matching initiative in a manner consistent with the requirements set forth in the Privacy Act.

Starting next week, we will begin to roll out a program to verify all INS documents with them before we issue a Social Security number. By the end of the year, under our Enumeration At Entry project, we will assign SSNs to new arrivals based on information that the State Department and the INS collect as they authorize non-citizen entry into the country. Also, we have already—and are, in some cases, planning to remove SSNs from much of our correspondence and all of our checks.

Now turning to S. 848. It would limit private and public sector use, display, and sale of the Social Security number and increase penalties for number misuse. Current law provides criminal penalties for SSN misuse, and adding civil monetary penalties as proposed in the bill would provide another level of deterrence.

We believe it would strengthen our ability to deal with the cases of misuse that are declined for prosecution by the Justice Department. We also support the bill's provision that would prohibit access to SSNs by prisoners.

In closing, I would like to emphasize that the Social Security Administration is committing to doing all it can to protect the Social Security number. In a larger view, however, our agency can only be part of the solution. Most identity theft results, not from any action or failure by the Social Security Administration, but from the widespread availability of personal information in today's society.

That is why, Mr. Chairman, we look forward to working with this committee and with the Senate on this vital national issue.

I would be happy to answer any questions.

Senator BREAUX. Thank you very much, Mr. Lockhart, for your statement.

[The prepared statement of Mr. Lockhart appears in the appendix.]

Senator BREAUX. I understand, Mr. Arterberry, you do not have a prepared statement, but will be answering questions.

Mr. ARTERBERRY. That is correct, Mr. Chairman.

Senator BREAUX. Thank you.

Mr. Huse, we have you up next. Inspector General of Social Security. Welcome back to the committee.

STATEMENT OF HON. JAMES G. HUSE, JR., INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, WASHINGTON, DC

Mr. HUSE. Thank you, Mr. Chairman. Good afternoon, sir. Senator Kyl.

It is a pleasure to have the opportunity to discuss with this subcommittee the need for legislation to protect the keystone of this Nation's Social Security programs, the Social Security number.

That need, though certainly not new, has never been more acute than it is today. The Social Security number has grown in statute to where it is no longer merely a social insurance number, but a tool for financial crimes and a significant homeland security vulnerability.

Our audit and investigative work has identified three distinct areas in which legislation is needed. The first is in the area of the Social Security Administration's enumeration processes.

In calendar year 2000, SSA issued over 5.5 million original Social Security numbers. Of these, 1.2 million were issued to non-citizens. Preliminary results of a study conducted by my office estimates that more than 100,000 were issued on the basis of fraudulent identity and/or immigration documents.

The laws and regulations which govern the issuance of Social Security numbers were designed for a social insurance number, not a de facto national identification number. As a result, the Social Security number is not afforded the security measures one might expect.

To give credit where credit is due, SSA has made great strides to improve the integrity of the enumeration process on its own. But SSA can only do so much without a clear Congressional mandate.

While SSNs are no longer used for the sole purpose of obtaining a driver's license, they are still issued to non-citizens where needed to obtain government benefits.

Most disturbing, in light of the events of September 11th last year, is the continued inability of SSA to verify the authenticity of identification documents presented by non-citizens who apply for SSNs.

The Immigration and Naturalization Service and SSA should find a way to authenticate immigration documents before an SSN is issued.

We must ensure that no SSN is issued based on INS documents that a simple, interagency check could have revealed to be fraudulent. The lack of adequate controls over this process creates a national security risk that both the Commissioner and I find unacceptable.

The second area in which legislation is overdue is in limiting the use and display of the SSN in the public and private sectors. Difficult decisions over appropriate uses remain subject to debate, but one easy decision can be made now. The public display of SSNs on identification cards, motor vehicle records, court documents and the like must be curtailed immediately. Those who use the SSN must share the responsibility for ensuring its integrity.

While we cannot return the SSN to its simple status of a half a century ago, we can ensure that identity thieves and other crimi-

nals cannot walk into a municipal courthouse and walk out again with the means of committing State-facilitated identity theft.

The cost to the victims of identity theft and to all of us is too great and the potential for these numbers to be used to commit crimes of violence and terrorism is unthinkable.

Finally, while no legislation can eradicate SSN misuse and identity theft altogether, the present panoply of criminal penalties is clearly insufficient to deter and/or punish identity thieves.

The felony provisions of the Social Security Act have no civil or administrative counterparts. Federal prosecutors cannot pursue every SSN violation criminally, or even civilly.

Our SSA Office of the Inspector General Civil Monetary Penalty Program has been a success in the area of program fraud and could have a similar impact in the area of SSN misuse if Congress would grant us that authority.

We have asked before, and I ask again, vest in us the authority to impose penalties against those who misuse SSNs. We can make a difference.

Various members of both Houses of Congress have introduced legislation over the past several years to deal with the national dilemma presented by SSN misuse and identity theft.

Very little has actually been enacted, and I urge this subcommittee to bring its influence to bear so that we might at least take the first legislative steps necessary to turn the tide in the war against SSN misuse and identity theft.

Thank you, and I would be happy to answer questions.

Senator BREAUX. Thank you very much, sir.

[The prepared statement of Mr. Huse appears in the appendix.]

Senator BREAUX. Next, is Mr. Willox.

STATEMENT OF NORM WILLOX, CHIEF OFFICER FOR PRIVACY, INDUSTRY, AND REGULATORY AFFAIRS, LEXISNEXIS, WASHINGTON, DC

Mr. WILLOX. Mr. Chairman and Senator Kyl, good afternoon. Thank you for this opportunity to address the committee.

My name is Norm Willox and I am chief privacy officer for LexisNexis. Our company is committed to the responsible use of Social Security numbers and other personally identifiable information. We commend Chairman Breaux and the subcommittee for their important work on this issue.

We share your concerns regarding the potential misuse of data for identity theft and fraud, and other harmful purposes. We are here today to discuss the importance of preserving access to SSNs by responsible businesses like LexisNexis, and to share our concerns with the subcommittee on the potential unintended consequence of Senate bill 848.

LexisNexis leads the information industry with the largest online information service, providing critical information to legal, business, and government professionals. LexisNexis maintains a database four times the size of the Internet and has nearly three million customers in 60 countries worldwide.

The LexisNexis database is an important tool in the fight against identity theft and has become a critical weapon in the global battle against terrorism. Information provided by LexisNexis was instru-

mental in locating suspects wanted in connection with the September 11th attacks.

LexisNexis has supported the Federal law enforcement community and other agencies for more than 30 years, including the Department of Justice, the Department of Defense, and the Treasury Department.

LexisNexis depends on Social Security numbers in public records and other information sources for important indexing, matching, and verification purposes to ensure the accuracy of the information we provide to our clients and customers.

Social Security numbers allow persons to be identified accurately and assure that records from different individuals do not get commingled. There are more than 43,000 Robert Joneses in the U.S. today. The use of a unique identifying number like a Social Security number is the only way to ensure that the information collected from multiple sources is accurately matched with other information and is associated with the correct individual.

Government agencies, businesses, researchers, and others rely on information contained in the LexisNexis database to do their jobs. In my written statement, I have outlined numerous examples of how our customers rely on LexisNexis databases and SSNs for a wide range of beneficial uses.

These include locating and recovering missing and abducted children, identifying and preventing fraud, helping to locate pension fund beneficiaries, performing anti-money laundering efforts in support of the U.S. Patriot Act, identify verification and authentication, and enforcing child support obligations.

These are just a few of the examples of how critical the use of SSNs are to LexisNexis and our customers. I would like to focus the remainder of my remarks on Senate bill 848, and I applaud the outstanding work by Senator Feinstein and the committee for recognizing the legitimate business use and government uses for SSNs, including important business-to-business and business-to-government exemptions in the bill.

We look forward to continuing to work with them to help ensure that the bill prevents the misuse of SSNs, while putting in place a workable system to allow continued access to SSNs by business and government agencies.

Although the bill contains the important exemptions I just mentioned, we are concerned that several provisions included in the bill would negate the benefit of these exemptions.

First, we believe that the public records provision in S. 848 are unworkable and should be dropped from the bill. The bill would effectively construct a two-tiered system for public records and would require State and local governments to maintain two sets of books, one copy of the records for public disclosure in which SSNs are redacted and the other for other purposes in which SSNs are included.

This two-tiered system of recordkeeping would be highly burdensome and costly to the State and local officials and would result in confusion concerning who could have access to the non-redacted records.

Faced with such problems, we believe that many State and local officials would simply eliminate all SSNs from their records. The

result would be that we would be cut off from the critical public record information at the source. The important exemptions in the bill for legitimate business and government uses are of little value if the SSNs are no longer available at that source.

In a General Accounting Office report issued in May of this year, the GAO concluded that redacting SSNs from public records would be an expensive and extraordinarily difficult and challenging process.

The complexity of this issue is underscored by the fact that the GAO itself did not provide a recommended approach. We believe that, until a viable approach is developed, public records should be exempted from the bill.

Second, we are concerned that the proposed rulemaking provisions are overly broad and could result in excessive restrictions, restricting access to SSNs by responsible businesses. The bill should clarify the scope of the Attorney General's rulemaking authority and ensure that the Attorney General's rule will implement the business-to-business and business-to-government exemptions.

Finally, we are concerned that the bill does not contain Federal preemption. Preemption is critical, given the current state of piecemeal legislative efforts in numerous States to restrict the use of SSNs by businesses. Given the uniquely Federal nature of SSNs and their importance to businesses engaged in interstate commerce, the bill should preempt State laws.

I appreciate the opportunity to provide the subcommittee with our view on this important issue and we look forward to working with the members of this subcommittee, and others, to develop a workable approach to this very, very complex issue.

Senator BREAUX. Thank you very much, Mr. Willox.

[The prepared statement of Mr. Willox appears in the appendix.]

Senator BREAUX. Next, is Mr. Evans.

STATEMENT OF DONALD EVANS, DIRECTOR OF INDUSTRY MARKETING, NCR CORP., DAYTON, OH

Mr. EVANS. Chairman Breaux and members of the subcommittee, my name is Rob Evans and I am the director of Financial Industry Marketing for the NCR Corporation. I would like to thank you very much for the invitation to offer testimony today before the subcommittee.

The company I represent, which is the NCR Corporation in Dayton, Ohio, is presently the world's leading manufacturer of ATMs. We also design, manufacture, and integrate a variety of specific-purpose financial terminals for our banking customers.

In my current capacity, I have the opportunity to interface with our America's base customers who need to process self-service financial transactions in an efficient, secure, and reliable environment.

In addition to our financial business unit, NCR has a proud heritage in retail transaction processing, and also includes our Teradata Solutions Group which provides database management solutions and general-purpose computing products to global customers.

NCR's history in providing solutions for the financial industry extends back to the initial develop of magnetic ink character recogni-

tion (MICR) based solutions for check clearing and the use of single number account control (SNAC) based transaction processing.

These early products not only are featured in the Smithsonian, but our modern solutions are being deployed by cutting-edge institutions in every corner of the globe as we speak. NCR is a publicly traded corporation that employs over 31,000 people globally.

Mr. Chairman, while the subject of today's hearing is protecting the Social Security number, the fundamental issue is protecting our shared confidence, confidence in payment mechanisms, ubiquity and acceptance, and confidence in individual security and privacy.

Without confidence that significant financial transactions can be negotiated with both efficiency and security, we will continue to witness gradual erosion in consumer confidence.

And as is significant from a business point of view, we will fail to realize the significant economic benefits that improving technology and quick response to consumer financial needs can bring.

However, balance demands that we do our utmost to protect vital information belonging to individual consumers. A diminished ability for consumers to obtain credit due to identity theft or fraud will be as chilling to economic activity as a diminished ability to grant credit due to cumbersome processing.

While I do not particularly envy the task of the subcommittee, you are to be thanked for taking the initiative to strike a balance while improving the security of Social Security numbers.

According to independent industry analysis, 200 million applications for credit were processed as recently as 1997. Outstanding balances from top 10 United States issuers of "general purpose" credit cards reached $387 billion in 1999, and represented 11 percent growth in 1 year's time.

Mortgage refinancing represents a significant portion of the Nation's mortgage business, but second mortgages, home equity lines of credit or HELOCs, and debt consolidation offers also continue to grow in volume.

These consumer credit obligations, as well as revolving credit, can be issued using not much more than the postal service and a Social Security number. Clearly, the need to improve security is increasing with these industry figures.

Numerous organizations have recognized the need to enhance and increase security levels associated with identification instruments. The Department of Defense recently began to reissue identification cards leveraging chip-based smart card technologies. In Europe, VISA and Mastercard are pursuing EMV-based card and card reading solutions to make fraudulent duplication more difficult.

In Asia, Mastercard is testing fingerprint-imbedded in magnetic slurry to ensure authorized use only. While all these systems do a better job tying individuals to account numbers and authorization IDs, they are predicated on specific chip or stripe reading technologies which are not presently ubiquitous.

And, while the advent of technology may find chip readers in every telephone, that promise is far from immediate. Unfortunately, the need for secure Social Security numbers is present.

The fundamental problem the committee will encounter is not entirely dissimilar to that which ATM owners and operators face.

Specifically, how can we be certain that the individual presenting themselves to transact business on a particular account is, indeed, authorized to do so?

While not foolproof, the methods currently employed by ATMs may bear review for potential use with Social Security numbers. The card and PIN system functions well in its limited capacity.

Specifically, a Social Security number could function as the card, and a PIN assignment to the number could add a level of security.

The system, as described, could be built and managed, which generates authorizations for applications of credit above a significant specified dollar value. The authorizations would be issued and verifications returned by a system which allows credit issuers to pass through authenticated requests. A conceptual diagram of this model is attached for your review.

Is this system foolproof? No, it is not. But it does offer a more secure environment for the use of numbers in significant financial transactions. It is very analogous to the car lock on your car door. While no one assumes that ensures the car would never be stolen, no consumer would buy a car without a car lock.

Current transaction processing and switching technologies could handle the volume requests in the system today. Our Nation's ATM infrastructure switches nearly 12 billion transactions annually, as a point of reference.

The cost for a new system to authenticate Social Security numbers and verifications would depend on how the process is defined. If advance notifications of revised procedures and processes should be required, then a re-issue of Social Security number cards would be desired, with PINs sent in separate mailings.

These start-up costs, in addition to the switching technology, could average in the teens of dollars per account. The ongoing operating costs could be dollars per account on a speculative basis.

I would be happy to take any questions at this time.

[The prepared statement of Mr. Evans appears in the appendix.]

Senator BREAUX. Thank you very much, Mr. Evans, and thanks to all of the witnesses, for your testimony. Now we will proceed to questions.

Mr. Willox, does LexisNexis buy and/or sell Social Security numbers?

Mr. WILLOX. Yes. We acquire information that does contain Social Security numbers.

Senator BREAUX. How do you do that?

Mr. WILLOX. We acquire them from numerous different types of sources, which are public record sources, which are outlined in the bill.

Senator BREAUX. What group out there goes out and assimilates Social Security number and sells them to you?

Mr. WILLOX. Public record sources.

Senator BREAUX. That is who you buy them from?

Mr. WILLOX. No, no, no. We buy documents that contain Social Security numbers by files that contain Social Security numbers. Public records.

Senator BREAUX. I mean, is there a service out there that goes through all the public records and collects all this, or does LexisNexis have a team that does that yourselves?

Mr. WILLOX. We acquire it from other third parties as well as collect if from ourselves.

Senator BREAUX. Well, the third parties that you all acquire it from, how do you know that they are legitimate sellers?

Mr. WILLOX. There is due diligence on those companies. They are legitimate, large organizations that acquire that type of data.

Senator BREAUX. This is a first impression for me, Senator Kyl, so excuse my density of questions. How long has this been going on that you have an ongoing business of companies that go out and simply engage in collecting public information that sells it to someone like you, your company?

Mr. WILLOX. It has been going on for decades at this point in time. Certainly, as technology has increased over the years, the requirements for more and more information to prevent fraud and manage risk has become even more important. Therefore, the data and information that is available today or needed today to prevent fraud and prevent identity theft is far more important than even it used to be.

Senator BREAUX. Tell me, if you can, why is it important for you to have a Social Security number in acquiring information to identify a person? I know you said you had so many thousands of Robert Joneses living in America.

Why would it not be sufficient to have the name of the person, the address of the person, the race of the person, the age of the person, and be able to narrow it down eventually to a single person without having the Social Security number which then can be used in a fraudulent manner from a theft standpoint? Why is the SSN number so important?

Mr. WILLOX. That is a good question. I will try to give you a short answer. I am not necessarily an expert on that type of technology that does that comparison and analysis. But it is very, very difficult to match files, match names, and match people without having a unique identifier to be able to do that.

Senator BREAUX. So you could do it, but this is a faster, easier way to do it if you got the single number.

Mr. WILLOX. More accurate way to do it. Far more accurate way to do it.

Senator BREAUX. I take it, as you made nice comments about the legislation before the committee and the work of Senator Feinstein, but after that you said you did not like anything that they did.

Mr. WILLOX. No, no, no.

Senator BREAUX. Is there anything in the bill you like, and if so, what?

Mr. WILLOX. Yes. I mean, they have done a great job with the bill. The criminal sanctions, the restriction to the general public to consumers. I mean, all of those things are great things. We have worked with Senator Feinstein and the committee, and I applaud all of their efforts. Our comments are really geared towards just the unintended consequences of a couple of the things that they are trying to do.

Senator BREAUX. But you do not agree with the limitation on the use of the Social Security numbers on public records that they are recommending, do you?

Mr. WILLOX. Well, our concern is that the States or local——

Senator BREAUX. You do not? Do you agree with that?

Mr. WILLOX. No. We do not right now in its present form.

Senator BREAUX. You do not agree with it.

Mr. WILLOX. Correct.

Senator BREAUX. Is there any limitation on the use of the Social Security number on public records that you would agree to?

Mr. WILLOX. We do not believe that consumers should have access to it, or the general public should have access to that data. What we do not want to have happen, is that——

Senator BREAUX. If it is public record?

Mr. WILLOX. Correct. We do not, exactly.

Senator BREAUX. You do not think there should be a limitation? I am trying to figure out, is there any limitation on the use of the Social Security number associated with public records that you would agree with? I got the impression from your testimony—

Mr. WILLOX. Yes, we agree it in the form that it is in, with the exception that our concern is that the States would have a dual system that they would have to maintain. Therefore, as a result of the cost and the limitations upon the States, they would be forced to only manage on one system.

If they did that, they would, at that point in time, manage a system that would redact the data, and therefore we would not have access to it. Even though there is a legitimate business purpose for us to get access to it, if the States, the local government agencies, or organizations do not manage two systems because of a cost factor, then we would not be able to access that data at that point in time.

Not because the bill does not allow us to do that. It does. But it would be because of a financial hardship, or whatever reason the other organizations would take that position that would create that problem.

Senator BREAUX. All right.

Mr. Evans, you suggested as one of your thoughts the concept of the PIN number being used along with a Social Security number as a protection. I am struggling to become a member of the Information Age, and it has not been easy.

Not too long ago I went to buy gasoline, and the gasoline pump tells me, when I put my card in—I have just gotten to the point of being able to do the card—it comes back and it says, "insert your PIN number." I said, what are you talking about?

It is like the movie about the American President. I had to call my office and say, what is this PIN number I am supposed to have on my gasoline credit card.

So my office has now provided me my PIN number, which has now been printed on the back of the credit card, which sort of defeats the purpose of having the PIN number. [Laughter.]

Mr. EVANS. True. That is a security risk.

Senator BREAUX. Not only that, I have got a PIN number on the back of the VISA card, which is the business card, and I have a different PIN number on the back of the VISA card which is my personal VISA card, and it is a different number. So, I have got more numbers than I am ever going to be able to keep track of. That is why they put them on the back of the card.

I mean, this is going to be a really confusing situation for the world if half of them are like me, where I have several credit cards, each one with a different PIN number, a Social Security number with a different PIN number, and I am not supposed to print it on the back of the card because it defeats the purpose of it. I am supposed to remember all of this in my head.

How is this going to work?

Mr. EVANS. Senator, first, I would like to take all of your cards and take the PINs of the back, if you would not mind. [Laughter.]

Senator BREAUX. We are hopeless. I have got it printed. It is a little sticker on the back of my card. You have got it on yours, too?

Mr. EVANS. I will tell you, as an ex-branch bank new accounts officer, that absolutely terrifies me. If it makes you feel anybody, I do recall being assigned to a new branch one time where they had written the combination to the automated teller machine on the back of the safe door so they could remember it easily. [Laughter.] That turned out to be problematic a little bit later.

I appreciate all of your observations, and do not disagree. However, if we look at the model for uptake in ATM technology, the experience there was that fewer than 30 percent of an institution's checking account customers even asked for a card about 15 years ago, and less than half of them ever even used them.

Now we are to the point where the majority of transactions that are in the banking system are processed, just basic cash withdrawals, by ATMs.

So my suggestion is, the customer gets over it. The consumer learns and adapts over time. It is not quick, it is not easy. I applaud you on the efforts to come into the Information Age. But what we will find, is users will manage to adapt. Also, mechanisms are built in such that if you forget a PIN, you can reestablish one.

Senator BREAUX. I was wondering. There is the possibility that everybody in America will have a Social Security number. Are we headed to the point where every single American is going to have one single PIN number?

Mr. EVANS. Anecdotally, I can tell you that a number of folks do tend to consolidate a PIN. Most cards and most authorization process allow you PIN selection functions. I would certainly imagine that being allowed for within the system I have described.

So if you want the same four numbers on your credit card, your debit card, and your telephone card and your phone messaging system also to be your Social Security PIN, the user could do that as well. But I am not disagreeing that folks will lose them and folks will write them down on the Social Security card.

Senator BREAUX. Thank you very much.

Senator Kyl?

Senator KYL. Thank you, Mr. Chairman. I am glad I am not the only one that is hopeless.

The problem, it seems to me, and this is a more philosophical issue, but all of you have, in one way or another, touched on it and I think we have got to step back and try to answer this.

We have a need for a very specific number in our country that enables you to work and get certain benefits as a result of that from the U.S. Government. That is the Social Security number.

You do not even really need a Social Security card, and I am going to get to that in a minute.

We also have a need now for better security in this country because, unfortunately, identity theft, and terrorism, and other problems have reminded us that it is not like when we used to be able to leave our back door unlocked when we went on vacation, and so on. We live in a different world now.

But a third thing we have in this country increasingly is the need for free-flowing commerce, which includes various kinds of identifiers. They have to be secure enough for the specific purpose for which they are intended, but not so cumbersome as to make it impossible for people like Senator Breaux and me to get along in this world.

It seems to me that one of the obvious conclusions that you draw from that, is that Senator Feinstein is on to something when she suggests that the Social Security card ought to be cut back to its original purpose, and commerce maybe should find ways to create identifiers other than the Social Security number. That would both provide more security, and also return the Social Security number to its original purpose and not allow it to be abused.

What do all of you think about that general philosophy in her legislation? In other words, could commerce get along without the Social Security number by creating other kinds of numbers, PINs and so forth, and would it not be possible for LexisNexis, for example, to adjust to that situation without having this unique identifier called a Social Security number to deal with things that have absolutely nothing to do with Social Security?

Mr. WILLOX. I will be happy to start the discussion.

Senator KYL. Sure.

Mr. WILLOX. That is a real good question, and something that I think we have all looked hard and long at. It creates some very significant challenges for us. The Social Security number, and information in our society, is really the new currency of the new world for us. It is such a critical fiber and such a significant weave, that to extract it or change it would be very, very complex and costly.

I would support it, in theory. I think it is a good idea. Can it practically be done? Can it cost-effectively be done? I am not an economist, but of all of the folks that we have dealt with on this issue, and it has been substantive, it would be a very challenging issue.

Regarding a new number, knowing that I spent the last 15 years studying identity fraud and identity theft, knowing the criminal, if we replaced it with a new number or a series of new number numbers, they would attack those new numbers as well and find ways to get access to those numbers to be able to commit the frauds that they are committing today. So, it may slow the process down, but I am not sure it would prevent the problem that we have today.

Senator KYL. Does anybody else want to comment on that?

Mr. EVANS. Yes, Senator. The primary appeal of the use of the Social Security number is simply its ubiquity and the fact that it is absolute. I think, in opening questions, Chairman Breaux mentioned, why could you not use a street address or some other number? But those change over time.

The Social Security number does not change. That is one of the reasons that it is very appealing. So you would be challenged to find a numbering system that had that type of authority, that is established once and it does not change.

My suspicion is——

Senator KYL. May I just interrupt you on that? I apologize. I see where you are going here. But how much authority does it really have? For example, does the Social Security Administration check the identity documents that are used to establish the legitimacy of a claim for a number?

Mr. LOCKHART. Would you like me to answer, Senator?

Senator KYL. Well, you are probably in the best position. The answer is no, I think. Right?

Mr. LOCKHART. The answer is, we check the identity documents, we check birth records. We have checked, for non-citizens, which is probably the bigger issue. We have historically checked with the INS to verify the records if a person is applying to us 30 days after they arrive in the country.

INS did not have the system to do it quicker than that. Starting next week, we will check every identity document with the INS.

Senator KYL. So far, though, I do not remember whether Mr. Huse testified to this or not, but there are at least thousands of people, and perhaps hundreds of thousands, who have illegally obtained Social Security numbers, among other things, because of a failure to adequately verify identity documents. That is the situation, is it not?

Mr. LOCKHART. There are people who have gotten Social Security numbers through fraud. Yes, sir.

Senator KYL. And it is in the thousands, if not tens of thousands, if not hundreds of thousands.

Mr. LOCKHART. Well, it is in the thousands, and probably tens of thousands. I am not sure if it is hundreds of thousands. But there is a significant number.

Senator KYL. And Mr. Willox, do you undertake any effort to determine the validity of the information that you purchase for use in all of the different legal ways that you use that information?

Mr. WILLOX. We test our data for accuracy, and compliance, and things like that. But we typically represent our data in the same format that we acquire it from. So if we acquire data from the courthouses, then that data would be an accurate representation of what the courthouse has provided to us.

Senator KYL. So you know there is a certain amount of it that is not valid. You cannot easily figure out what that is, and you simply represent that that is the fact when you sell your information or services.

Mr. WILLOX. Correct.

Senator KYL. Would it be a good idea not to issue replacement Social Security cards, since that is a method for false identification and identity theft?

Mr. LOCKHART. We share your concern, Senator, about replacement Social Security cards. Last year, for instance, we issued 12.6 million replacement cards, of which about a million were to non-citizens. This is an expensive process. It clogs up our offices.

Potentially, it could lead to misuse, although the Social Security card has features on it that make it hard to change the numbers and names. It still could potentially be misused.

We are certainly looking at that, and it is one of the key agenda items for our enumeration task force, to potentially reducing the number of replacement cards an individual could receive.

Senator KYL. Is there any need for a Social Security card to be possessed by somebody?

Mr. LOCKHART. The need for a Social Security card. That is a good question. We have actually looked at that, and there is a debate in the agency. But right now, the key use is, after you are hired, an employer can ask to see the card to make sure you are a legitimate worker in this country.

Senator KYL. Mr. Huse, what do you think about that?

Mr. HUSE. Of course, we concur with the Agency and have been part of the debate on the efficacy of the Social Security card and whether it is even needed. It is a mantra that we have chanted for many years, at least in the work we have done advancing this whole issue of uses and misuse. It is the number, not the card, that counts.

Even though the card bears a caveat that it is not to be used for identification, really the only reason people seek a replacement is either for that purpose, or the fact that in some instances people, because of their seniority, feel that they need it. To be specific, the card probably does not have much efficacy anymore.

Senator BREAUX. Senator Lincoln?

Senator LINCOLN. Thank you, Mr. Chairman, especially for calling a hearing on such an important issue.

I wanted to compliment Senator Feinstein and Senator Gregg for their leadership on this issue, and thank the panel for being here with us today.

Mr. Chairman, at least once a month I receive a letter from someone in Arkansas who is concerned about their identity theft. I am sure other offices are getting the same kind of response.

I have heard horror stories from folks whose Social Security numbers were used by criminals to apply for credit cards and open bank accounts, all at a great financial loss to them.

I think we all recognize, when we attempt to protect Social Security numbers and identity, we really must protect the delicate balance between consumer privacy and making sure that the SSN information is available for appropriate uses by government and business interests as well. I think you all have brought a lot of important issues to the table here.

Mr. Lockhart, I want to thank you for being here. I have to say, with the Chairman's indulgence, on a personal note, Mr. Lockhart, I would like to thank you. You may not know it, but on loan to me in my office has been one of your most gifted policy analysts, Mike Anzek, who has been working in my office since January and has been absolutely wonderful.

Mr. LOCKHART. I am glad to hear that.

Senator LINCOLN. Although he is leaving me in August to rejoin the Social Security Administration, despite my attempts to keep him on board, I might add.

I want you to look after him and make sure that his talents are certainly utilized. I know he will be a great asset to you.

But we thank you for the comprehensive overview on how the use of the SSN has evolved. I understand that most cases of identity theft have largely been the result of the growing use in our society of SSNs, not as a result really of an action or failure to act by the Social Security Administration. We are glad to hear about your efforts in response to September 11th.

Can you tell me a little more about the work of the task force that SSA has organized, and maybe, perhaps, what your assessment of the Feinstein bill is in terms of, how would the SSA be affected most.

Mr. LOCKHART. Right. Turning to the task force, there are really three ways that Social Security numbers can be used for identity theft. One, is they use a number that is given to them by Social Security. Another, is they steal an identity. The third one, is they just make up the SSN, which apparently most, if not all, of the terrorists actually did.

Our initial focus is on the numbers assigned by SSA because our primary responsibility, is to make sure that the number that we issue is to someone that has the right to have the number, and we also want to make sure that valid documents were submitted for those numbers. Our enumeration task force has really been centered on ensuring that we protect issuance of the number and only give it to the people who deserve to have it.

So we have gone through a whole series of steps that we have taken and we have a whole series of steps we are moving forward on, and others that we are still looking at. But some of the things we have done so far, is we have gone through a whole retraining process in our 1,300 field offices, especially for the enumerations of non-citizens.

We have convened a task force with the INS, the Department of State, and also Homeland Security has joined that effort. We have, as I said, eliminated driver's licenses as a reason for non-work Social Security numbers. We are now verifying the birth records of everybody over age one.

We have piloted—and this may answer one of Senator Kyl's questions a little bit—a Social Security number verification system. There will be an electronic system that employers can actually go onto and verify a number and the name, and therefore would not need the Social Security card in that case. It is only at the pilot stage, but it is moving very well. We have six users and it is looking very good.

We are starting something called Enumeration At Entry, which I mentioned, which is, again, having the INS and the State Department look at the documents and tell us electronically that this person is legally in this country.

Senator LINCOLN. So instead of having an actual document that needs to be authentic in some way, you are actually electronically receiving that from the INS itself.

Mr. LOCKHART. Exactly. And I think that will obviously be more efficient, and also lead to less fraud.

In the meantime, as of next week we will have total verification of the documents with the INS. That means, even if we cannot do

it electronically, we are going to send them a copy of the documents and they are going to respond to us. We are not going to issue an SSN until we get that verified.

We do verify SSNs for employers. We also do it occasionally for financial institutions. We actually verify about 750 million SSNs a year, and we are going to continue to do that and expand that.

Then one thing we are just starting, which I think will also be another way to prevent identity fraud is creating enumeration centers. We are starting in Brooklyn in September.

We are going to gather together our employees, the Inspector General employees, and INS employees that are really experts in looking at these documents. We hope, by having everybody in place, we can prevent fraud, and also, if there is fraud, take action right there.

Senator LINCOLN. You have got 1.5 million non-citizens that get Social Security numbers. Is there any indicating that shows that that individual is a non-citizen? Is there a temporary status, or an asterisk, or anything?

Mr. LOCKHART. On the face of the card, if a person gets a card that says he or she is not authorized to work, it says on the face of the card, "Not Valid For Employment." If a non-citizen that is authorized to work gets a card from a temporary visa, or whatever, it says, again, on the face of the card, "Valid For Work Only With INS Authorization."

Senator LINCOLN. Why would a non-citizen in this country that is not authorized to work need a Social Security number?

Mr. LOCKHART. There is one exception left. We now only give Social Security numbers to people that are eligible for State or Federal assistance programs. That is really designed to prevent fraud more than anything, so that there is a number to track them by.

Since we made the change from not giving Social Security numbers for drivers' licenses, it looks like there is going to be about 20,000 of these non-work numbers given out per year.

Senator LINCOLN. I am sorry. How many?

Mr. LOCKHART. Twenty thousand out of the 5.8 million that we give a year. So, it is a relatively small number. Because we eliminated the drivers' license as a valid reason, the number will be something like 70 percent less than we have had historically.

Senator LINCOLN. There is no "temporary" attached to it? It is still the same nine-digit Social Security number?

Mr. LOCKHART. It is nine digits. But it does say "Not for Work" on the face of the card. But, no, it is not temporary. Social Security numbers, historically, have been permanent.

Senator LINCOLN. Even to non-citizens?

Mr. LOCKHART. Even to non-citizens.

Senator LINCOLN. And non-working citizens as well.

Mr. LOCKHART. Yes.

Senator LINCOLN. Thank you.

Well, my only other question, Mr. Chairman, was to Mr. Evans, because I do have a considerable amount of elderly in my State of Arkansas, and I was concerned about them remembering their PINs. But since the Chairman and the Ranking Member, I do not want to ask that question anymore. [Laughter.] So, I will pass.

Mr. HUSE. I just want to verify, you do not have your PINs written on the back of any card?

Senator LINCOLN. No, no.

Mr. HUSE. All right. Very good.

Senator BREAUX. Mr. Arterberry, you have been quiet because we have not asked you any questions. I would like to ask, if you can, to comment on the type of people that are doing the thievery? I mean, who are the folks that are out there engaged in this type of activity of stealing Social Security numbers in order to commit fraud.

Are we talking about street criminals? Are we talking about organized crime, or are we talking about the potential for terrorists using this to gain access? Give us a little bit of a flavor of the concerns about who might be doing this.

Mr. ARTERBERRY. Mr. Chairman, unfortunately, I think the short answer would be all of the above. Senator Feinstein, in her testimony, referred to an identity theft sweep that the Attorney General announced at the Department back in May.

In that sweep, we had 73 cases charging 134 individuals in 24 districts around the country. We saw a wide range of people committing these offenses. Some of them were career criminals.

Some—and I think this illustrates a vulnerability—were people within organizations and businesses who had access to information, private financial information.

Some, I think, were people who are migrating from perhaps street crime, drug activity, what have you, into identity theft because it is a crime that—at least viewed by the criminal—is one that is cleaner, the rewards can be very significant, and I think there is a perception that there is not the degree of punishment that may be attached to other crime.

Senator BREAUX. It seems to me that it would be difficult to continue doing this. Is this on a month-to-month basis, and once the original owner of the number starts getting the bills, things are shut down?

Is it able to be continued for an inordinate amount of time, or is there a limitation because of the practicalities of the person whose number has been stolen is starting to get the bills and is saying, wait a minute, something is wrong here.

Mr. ARTERBERRY. Senator, I cannot give you precise information or data to back this up, but I think it would be our impression that the period of time in which these schemes can be perpetrated against one individual is probably shortened because I think the system is getting better at reacting.

On the other hand, some identity thieves operate with an amount of, let us say, brass. They have been known to report the actual owner as the identity thief so that they can continue to operate, at least for some time.

Senator BREAUX. Do you, Mr. Arterberry, have any idea about the innocent person whose number has been stolen, and all of a sudden starts getting these bills for everything from gasoline purchases to a vacation trip to Paris, or a new car, or all the things they could do with it.

What is the obligation of the individual who has been the victim to prove that, no, I did not go to Paris, or no, I did not buy a car?

I mean, this is somebody else, and I do not know what happened. Can anybody comment on that? Mr. Huse?

Mr. HUSE. The obligation on the victim is total. It is their responsibility to prove that they have been victimized and to get their good name back. That is one of the great pieces of this crime that hurts people the most.

Senator BREAUX. So I have an obligation and get a bill to pay it. At least, the company that sent me the bill thinks so.

Mr. HUSE. Now, you do have some protections where you have ceilings on how much you are personally liable for on credit purchases, and so forth. But identity fraud extends across every aspect of financial crime. Every aspect. In fact, it is the key piece of any financial crime.

So when you are in one of these situations, it takes, as Senator Feinstein said, at least 18 months, on the average, of dogged effort to get your good name back, if you can succeed. Some people remain victims for years.

Senator BREAUX. Any other questions, Senator Kyl?

Senator KYL. Yes. Thank you, Mr. Chairman.

The first two bills that we got passed dealt with the problems you just identified, and in an imperfect way. But we tried to help the people who had been victimized get their good name back. We were not as effective at limiting the possibilities for crime in the first instance. That is what Senator Feinstein is trying to do with this next bill. We are going to need the cooperation of all of you, and others that you might identify.

Mr. Evans, I cut you off before and I did not mean to. I apologize for that. If you wanted to complete any thoughts you have, I would be interested in having you do that.

Mr. EVANS. I think the point we were making was with respect to the reason that Social Security numbers appeal to business and industry for use. It had to do with, you do not question whether or not this is an authoritative way to recognize an individual. My only suggestion with the point you were making, are there other methods to do that, they would need to be similar in singularity and authority, one issuing agency maintaining the authority of that number.

I would suspect, if you go to replace Social Security numbers, you will find similar concerns voiced by industry as were voiced at the point of the now-infamous Y2K type of conversion, where you have that nine-digit field hard-coded in software applications and information systems, that if you replaced it with something, it would need to look a lot like that without completely rewriting a lot of software.

Senator KYL. Well, clearly, if we end up with some kind of a guest worker program in this country and we mean to enforce the law with respect to immigration, we are going to have to have a tamper-proof personal identifier kind of card.

If we call it a Social Security card, fine, but it will have to be different than the one we have. Because the technology now exists to have fraud-proof cards, it seems to me we are going to have to go that direction.

But I think two other things are true. One, is that, at least now, this country will not stand for what is known as a national ID

card. Therefore, since the kind of card that I just described is critical for the administration of Social Security and also other work-related laws in the United States like a guest worker program or an amnesty program with whatever name you want to call it, and since business absolutely requires some kind of ubiquitous identifier that is as tamper-proof as possible, I see us actually developing two different systems.

One, is the government-issued, tamper-resistant, non-fraud card that is for one purpose and one purpose only, with very strict restrictions on its use. Then I see a variety of evolving techniques in the business community to achieve the needs of commerce and security in that area.

But I do think there is going to be resistance to further moving toward a doubly imperfect system of the Social Security number, which is not secure, which we cannot guarantee is valid, and which, second, exists ostensibly for a government purpose, but is now being required by all kinds of business and is, therefore, the ticket for identity fraud.

It seems to me we are fast approaching the point where you cannot have both, because we have, in a couple of cases, a vested interest in making the system work, and in the others, a public responsibility for finding a system that can work, and in the case of Mr. Lockhart, currently, to execute a set of laws, I am going to urge all of you to help us figure out how to do this.

I think we want to help Senator Feinstein and the others get to a point here where we reduce the possibility of ID theft, but we also understand the points that you have brought to us here that fall within the purview of the Finance Committee. I am not sure we are going to be able to figure this out without your help. So, I thank you for your testimony today.

Senator BREAUX. Thank you, Senator Kyl.

Gentlemen, we thank you for your presentations. I think they have been very, very helpful, and we look forward to working with you.

With that, the subcommittee will stand adjourned.

[The prepared statement of Senator Baucus appears in the appendix.]

[Whereupon, at 3:42 p.m. the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF HON. MAX BAUCUS

First, I want to thank Senator Feinstein for working with the Finance Committee as we consider this important legislation. The Senator from California has been very active on the issue of identity theft for many years and I know that this issue is very important to her.

I also want to thank Senator Breaux and Senator Kyl for agreeing to hold this hearing in their subcommittee. Finally, I thank all of the witnesses for their valuable testimony.

We are here today due to the problem of identity theft. This is a big problem and it is only getting worse. As we all know, identity theft occurs when another person steals your identity for profit or other illicit motive. It may be one of the fastest growing crimes in the United States. Recently, the Federal Trade Commission reported that identity theft was the largest complaint on the FTC's consumer complaint list last year, representing 42 percent of complaints.

Unlike most crimes where the victim is immediately aware of the assault, identity theft is often silent and invisible. Identity thieves do not need direct contact with their victims. All they need is access to some key component of a victim's personal information, and one key component is, of course, the Social Security number. That number—which is our de facto national identification number—is under the jurisdiction of the Senate Committee on Finance.

Again, I want to commend Senator Feinstein for her leadership on the issue of identity theft and I appreciate her being here today to discuss her bill with the Committee. I look forward to learning more about Senator Feinstein's legislation and the issues and alternatives that the other witnesses may present.

PREPARED STATEMENT OF ROB EVANS

Chairman Breaux, Senator Grassley, and members of the Subcommittee, my name is Rob Evans, Director of Financial Industry Marketing for the NCR Corporation. Thank you for the invitation to offer testimony today before your Subcommittee.

The company I represent, the NCR Corporation based in Dayton, Ohio, is the worlds leading manufacturer of ATMs. We also design, manufacture, and integrate a variety of specific purpose financial terminals for our banking customers. In my current capacity, I have the opportunity to interface with our Americas based customers who need to process self-service financial transactions in an efficient, secure, and reliable environment. In addition to our financial business unit, NCR has a proud heritage in retail transaction processing and also includes our Teradata Solutions Group which provides database management solutions and general purpose computing products to global customers.

NCR's history in providing solutions for the financial industry extends back to the initial development of magnetic ink character recognition (MICR) based solutions for check clearing and the use of single number account control, or SNAC based transaction processing. Not only are our earliest products featured in Smithsonian collections (the museum of American history Numismatic collection), but our modern solutions are being deployed by cutting edge institutions in every corner of the globe as we speak. The NCR Corporation currently employs over 31,000 people globally.

Mr. Chairman, while the subject of today's hearing is "Protecting the Social Security Number", the fundamental issue is protecting our shared confidence. Confidence

in payment mechanisms, confidence in ubiquity and acceptance, and confidence in individual security and privacy. Without the confidence that significant financial transactions can be negotiated with both efficiency and security, we will continue to witness gradual erosion in consumer confidence. And as significant from a business point of view, we will fail to realize the significant economic benefits that improving technology and quick response to consumer financial needs can bring.

However, balance demands that we do our utmost to protect vital information belonging to individual customers. A diminished ability for consumers to obtain credit due to identity theft or fraud will be as chilling to economic activity as a diminished ability to grant credit due to cumbersome processing. While I do not particularly envy the task of the subcommittee, you are to be thanked for taking the initiative to strike a balance while improving the security of social security numbers.

According to independent industry analysts, 200 million applications for credit were processed as recently as 1997. Outstanding balances from the top ten United States issuers of "general purpose" credit cards reached $387 billion in 1999, and represented 11% growth in one years' time. While mortgage refinancing represents a significant portion of the nations mortgage business, second mortgages, home equity lines of credit or HELOCs, and debt consolidation offers continue to grow in volume. These consumer credit obligations, as well as revolving credit, can be issued using not much more than the postal service and a social security number. Clearly, the need to improve the security of consumers social security numbers is increasing with these industry figures.

Numerous organizations have recognized the need to enhance and increase the security levels associated with identification methods and credit instruments. Recently, the Department of Defense begun to reissue identification cards leveraging chip based smart card technologies. In Europe, VISA are pursuing EMV based card and card reading solutions to make fraudulent duplication more difficult. In Asia, MasterCard is testing a user fingerprint embedded in magnetic slurry to ensure authorized use. While all these systems do a better job tying individuals to account numbers and authorization IDs, they are predicated on specific chip or stripe reading technologies which are not presently ubiquitous. And while the advent of technology which may find chip readers in every telephone is promising, it is far from immediate. Unfortunately, the need secure social security numbers is present.

The fundamental problem the committee will encounter is not entirely dis-similar to that which ATM owners and operators face. Specifically, how can we be certain that the individual presenting them self to transact business on a particular account is indeed authorized to do so? While not foolproof, the methods currently employed by ATMs may bear review for potential use with social security numbers. The card and PIN system functions well in its limited capacity. Specifically, a social security number could function as the card, and a PIN assignment to the number would add a level of security.

A system could be built and managed which generates authorizations for applications of credit above a specified significant dollar value. The authorizations would be issued and verifications returned by a system which allows credit issuers to pass through authenticated requests. A conceptual diagram is attached for your review.

Is such a system, as described, absolutely foolproof? No, it is not. It does, however, offer a more secure environment for the use of social security numbers in significant financial transactions. It is analogous to car locks on your car door. The lock is not a guarantee that the car will never be stolen, but the average consumer would not dream of purchasing a car that didn't have locks. This system could be activated and utilized via touch tone telephone, giving it a degree of ubiquity necessary for minimum disruption in current processes. While this system will not guarantee unauthorized use, it would make unauthorized use more difficult.

Current transaction processing and switching technologies could handle the volume of requests in the system today. The nations ATM infrastructure switches nearly 12 billion transactions annually, as a point of reference. The cost would depend on how the process is defined. For example, advance notifications of revised procedures and processes should be required, and a re-issue of social security number cards would be desired with PINs sent in separate mailings. These start up costs in addition to the switching technology could average in the teens of dollars per account. The ongoing operating costs could be dollars per account on a speculative basis.

There are problems with the conceptual model defined. Ensuring data integrity over the phone system via encryption of sensitive data would be desirable but is not present in the conceptual model. In current ATM systems, the bank who holds the account processes the PIN. This process is defined as a third party PIN issuer in the conceptual model, but the designated trusted third party would doubtlessly need

to develop methods to ensure confidentiality and security of PINs and account numbers.

NCR applauds the committee for its work on this sensitive subject. NCR appreciates the need for solutions which support the integrity of the current social security numbering infrastructure but add security mechanisms for individual account holders. NCR is ready to assist the committee in working on specific technical issues surrounding security in addition to assistance in developing and defining solutions as well.

Mr. Chairman, thank you and the committee very much for your time and attention to this matter.

PREPARED STATEMENT OF HON. JUDD GREGG

Thank you Senator Breaux and Senator Kyl for holding this hearing on S. 848, the Social Security Number Misuse Prevention Act of 2001, introduced by Senator Feinstein and myself. I appreciate the opportunity to testify on this important legislation.

On October 15, 1999, Amy Boyer, a young woman from Nashua, NH, was killed by a man who went on the Internet and was able to purchase her Social Security Number and other private information for $75. The company that sold the information to Amy's assailant obtained the Social Security Number and information about where Amy worked by hiring a "pretexer" who called her house and was able to secure the information and then sell it to the assailant.

As a result of this tragic event and thousands more, it became clear to me that the sale of Social Security Numbers (and indeed other private information) is dangerous and needs to be stopped. S. 848 was drafted to respond to this concern.

S. 848 would make the sale and display of Social Security Numbers to members of the public illegal, and would make it criminal for anyone to obtain a social security number with the intent to physically injure, harm, or use the identity of the individual for any illegal purpose.

Its' goal is to ensure that members of the general public, who have no legitimate reason to have another person's Social Security Number without their consent, would not be able to purchase the number or obtain the number off of a public record.

The goal of S. 848 is not, nor has it ever been, to affect the *use* of Social Security Numbers by legitimate businesses, law enforcement, national security officers or public health officials. In fact, maintaining that delicate balance has been one of difficult policy challenges—how to protect legitimate use and access to the number while limiting widespread public assess because of the significant risk of harm, invasions of privacy and the potential for misuse.

Senator Feinstein and I recognize the many ways in which the Social Security Number is used to actually help prevent harm. LexisNexis will offer testimony on many of those uses this afternoon.

We understand that health care providers use the social security number to maintain our health records to ensure we are receiving the services we need;

Banks and financial institutions use them to prevent fraud—a social security number tells them that a loan applicant is exactly who he says he is;

The National Center for Missing and Exploited Children and the Association for Children for Enforcement of Support (ACES) use social security numbers to track down kidnappers and deadbeat dads;

Big Brothers/Big Sisters of America use social security numbers to do background checks on volunteers to make sure that they are not felons or child molesters.

A truly blanket prohibition that did not include any exceptions whatsoever would undermine these legitimate uses. In reality, nobody wants this. So we worked on striking a balance, and I believe S. 848, while it is not a perfect product, strikes that balance and permits every one of the previous examples of legitimate uses of the Social Security Number to continue, as well as the examples you will hear this afternoon from LexisNexis about how they use the number in their business.

Mr. Chairman, I will not describe the provisions of S. 848 in detail as I am sure the lead sponsor, Senator Feinstein will do that. However I wanted to let the Committee know that we are strongly committed to the principle of balance—of protecting both individual rights of privacy and legitimate uses of the number.

I understand that there are several issues that remain challenging, public records and preemption being the primary ones, however I am sure that between the great minds on this Committee and on the Judiciary committee we will be able to reach a solution that is both workable and effective and I look forward to participating in those discussions.

Every year as many as 700,000 instances of identity theft are reported. Limiting availability of the social security number is one important way we can address this issue. S. 848 is a well thought-out, tightly woven piece of legislation that effectively recognizes and balances the many concerns surrounding the uses of social security numbers. Passing this legislation is one of the most important things that Congress can do this year to reduce identity theft and protect individual privacy while permitting the continued legitimate and limited uses of the social security number. Thank you.

PREPARED STATEMENT OF HON. JAMES G. HUSE, JR.

Good afternoon, Chairman Breaux, Senator Kyl, and members of the subcommittee.

It is a pleasure to have the opportunity to discuss with this subcommittee the need for legislation to protect the keystone of this nation's social security programs—the Social Security number (SSN). That need, though certainly not new, has never been more acute than it is today. The SSN has grown in stature to where it is no longer merely a social insurance number, but a tool for financial crimes and a significant Homeland Security vulnerability.

Our audit and investigative work has identified three distinct areas in which legislation is critically needed.

Enumeration

The first is in the area of the Social Security Administration's (SSA's) enumeration processes. In calendar year 2000, SSA issued over 5.5 million original SSNs. Of these, 1.2 million were issued to non-citizens, and preliminary results of a study conducted by my office estimate that more than 100,000 were issued on the basis of fraudulent identity and/or immigration documents.

The laws and regulations which govern the issuance of SSNs were designed for a social insurance number, not a *de facto* national identification number. As a result, the SSN is not afforded the security measures one might expect.

To give credit where credit is due, SSA has made great strides to improve the integrity of the enumeration process on its own. But SSA can do only so much without a clear Congressional mandate. While SSNs are no longer issued for the sole purpose of obtaining a drivers' license, they are still issued to non-citizens when needed to obtain certain government benefits.

Most disturbing, in light of the events of September 11, is the continued inability of SSA to verify the authenticity of identification documents presented by non-citizens who apply for SSNs. The Immigration and Naturalization Service and SSA should find a way to authenticate immigration documents before an SSN is issued. We must ensure that *no* SSN is issued based on INS documents that a simple interagency check could have revealed to be fraudulent. The lack of adequate controls over this process creates a national security risk that both the Commissioner and I find unacceptable.

Controlling SSNs in Circulation

The second area in which legislation is overdue is in limiting the use and display of the SSN in the public and private sectors. Difficult decisions over appropriate uses remain subject to debate, but one easy decision can be made now. The public display of SSNs—on identification cards, motor vehicle records, court documents, and the like—must be curtailed immediately. Those who use the SSN must share the responsibility for ensuring its integrity. While we cannot return the SSN to its simple status of a half-century ago, *we can* ensure that identity thieves and other criminals cannot walk into a municipal court house and walk out again with the means of committing state-facilitated identity theft. The cost to the victims of identity theft, and to all of us, is too great. And the potential for these numbers to be used to commit acts of violence and terrorism is unthinkable.

Criminal, Civil, and Administrative Penalties

Finally, while no legislation can eradicate SSN misuse and identity theft altogether, the present panoply of criminal penalties is clearly insufficient to deter and/or punish identity thieves.

The felony provisions of the Social Security Act have no civil or administrative counterparts. Federal prosecutors cannot pursue every SSN violation criminally, or even civilly. Our Civil Monetary Penalty program has been a success in the area of program fraud, and could have a similar impact in the area of SSN misuse, if Congress would grant us such authority. We have asked before, and I ask again—

vest in us the authority to impose penalties against those who misuse SSNs. We can make a difference.

Conclusion

Various members of both houses of Congress have introduced legislation over the past several years to deal with the national dilemma presented by SSN misuse and identity theft. Very little has actually been enacted. I urge this subcommittee to bring its influence to bear so that we might at least take the first legislative steps necessary to turn the tide in the war against SSN misuse and identity theft. Thank you, and I'd be happy to answer any questions.

PREPARED STATEMENT OF HON. JAMES B. LOCKHART, III

Mr. Chairman and Members of the Subcommittee:

Thank you for asking me to be here today, to discuss Social Security Number (SSN) misuse. As the number of legitimate uses for Social Security Numbers increase, especially use in the private sector, so does the potential for misuse—and the consequences of misuse.

Social Security Number misuse can lead directly to identity theft and the resulting personal and economic consequences to the individual whose identity is stolen. But Social Security Number misuse also can create far-reaching consequences to our economy and our society as a whole.

The tragic events of September 11, and reports that some of the terrorists fraudulently used SSNs have brought home the need to strengthen the safeguards to protect against the misuse of the SSN. We have worked diligently towards this end ever since, with many important enhancements recently implemented and more to follow through the remainder of this year. We appreciate this Committee's interest in putting Social Security numbers beyond the reach of criminals.

Original Purpose of the Social Security Number and Card

To begin, I would like to discuss the original purpose of the SSN and the Social Security card. Following the passage of the Social Security Act in 1935, the SSN was devised administratively as a way to keep track of the earnings of people who worked in jobs covered under the new program. The requirement that workers covered by Social Security apply for an SSN was published in Treasury regulations in 1936.

Initially, the only purpose of the SSN was to keep an accurate record of earnings covered under Social Security and to pay benefits based on those earnings. The SSN card is the document SSA provides to show what SSN is assigned to a particular individual. The SSN card, when shown to an employer, assists the employer in properly reporting earnings. Early public education materials counseled workers to share their SSNs only with their employers.

Growth of SSN as an Identifier for Other Federal Purposes

In spite of the narrowly drawn purpose of the SSN, use of the SSN as a convenient means of identifying people in records systems has grown over the years in steps. In 1943, Executive Order 9397 required Federal agencies to use the SSN in any new system for identifying individuals. This use proved to be a precursor to a continuing explosion in SSN usage which came about during the computer revolution of the 1960's and 70's. The simplicity of using a unique number that most people already possessed encouraged widespread use of the SSN by Government agencies and private organizations as they adapted their record-keeping and business applications to automated data processing.

In 1961, the Federal Civil Service Commission established a numerical identification system for all Federal employees using the SSN as the identifying number. The next year, the Internal Revenue Service (IRS) decided to use the SSN as its taxpayer identification number (TIN) for individuals. And, in 1967, the Defense Department adopted the SSN as its identification number for military personnel. Use of the SSN for computer and other recordkeeping systems spread throughout State and local governments, and to banks, credit bureaus, hospitals, educational institutions and other areas of the private sector. At the time, there were no legislative authorizations for, or prohibitions against, such uses.

Statutory Expansion of SSN Use in the Public Sector

The first explicit statutory authority to issue SSNs did not occur until 1972, when Congress required that SSA assign SSNs to all noncitizens authorized to work in this country and take affirmative steps to assign SSNs to children and anyone receiving or applying for a benefit paid for by Federal funds. This change was prompt-

ed by Congressional concerns about welfare fraud and about noncitizens working in the U.S. illegally. Subsequent Congresses have enacted legislation which requires an SSN as a condition of eligibility for applicants for SSI, Aid to Families with Dependent Children (now called Temporary Assistance to Needy Families), Medicaid, and food stamps. Additional legislation authorized States to use the SSN in the administration of any tax, general public assistance, drivers license, or motor vehicle registration law within its jurisdiction.

At the same time, the Privacy Act was enacted in 1974 when Congress became concerned about the widespread use of the SSN. It provides that, except when required by Federal statute or regulation adopted prior to January 1975, no Federal, State or local government agency could withhold benefits from a person simply because the person refused to furnish his or her SSN.

In the 1980's, separate legislation provided for additional uses of the SSN including employment eligibility verification, military draft registration, commercial motor vehicle operators licenses, and for operators of stores that redeem food stamps. Legislation was also enacted that required taxpayers to provide a taxpayer identification number (SSN) for each dependent age 5 or older. The age requirement was lowered subsequently, and an SSN is now required for dependents, regardless of age.

In the 1990's, SSN use continued to expand with legislation that authorized its use for jury selection and for administration of Federal workers' compensation laws. A major expansion of SSN use was provided in 1996 under welfare reform. Under welfare reform, to enhance child support enforcement, the SSN is to be recorded in the applications for professional licenses, driver's licenses, and marriage licenses; it must be placed in the records relating to a divorce decree, support order, or paternity determination or acknowledgment; and it must be recorded in the records relating to death and on the death certificate. When an individual is hired, an employer is required to send the individual's SSN and identifying information to the State, which will verify the information with SSA. This "New Hire Registry" is part of the expanded Federal Parent Locator Service which enables States to find non-custodial parents by using the SSN.

Private Sector Use of the SSN

Currently, Federal law places no restrictions on the use of the SSN by the private sector. People may be asked for an SSN for such things as renting a video, getting medical services, and applying for public utilities. They may refuse to give it. However, the provider may, in turn, decline to furnish the product or service.

There are two basic ways the providers use the SSN. Within an organization, the SSN is typically used to identify specific persons and to maintain or retrieve data files. The second use is for external exchange of information, typically to transfer or to match data. For example, individual companies can track buying habits and customer preferences through the use of such data.

Continuing advances in computer technology and the ready availability of computerized data have spurred the growth of information brokers who amass and sell vast amount of personal information including SSNs. When possible, information brokers retrieve data by SSN because it is more likely than any other identifier to produce records for a specific individual.

The SSN as an Identifier

As you can see, Mr. Chairman, the current use of the SSN as a personal identifier in both the public and private sectors is not the result of any single step; but rather, from the gradual accretion over time of extending the SSN to a variety of purposes. The implications for personal privacy of the widespread use of a single identifier have generated concern both within the government and in society in general.

The advent of broader access to electronic data through the Internet and the World Wide Web has generated a growing concern about increased opportunities for access to personal information. Some people fear that the competition among information service providers for customers will result in broader data linkages with questionable integrity and potential for harm, and make it easier for identity thieves to ply their trade.

On the other hand, there are some who believe that the public interests and economic benefits are well served by these uses of the SSN. They argue that it would enhance the ability to more easily recognize, control and protect against fraud and abuses in both public and private activities. All Federal benefit-paying agencies rely on data matches to verify not only that the applicant is eligible for benefits, but also to ensure that the benefit paid is correct. Other federal agencies may be able to provide information about other socially beneficial uses of the SSN, including its use in research and statistical activities. The SSN often is the key that facilitates the ability to perform the matches.

Identity Theft

When most people think of identity theft they are referring to the use of the personal identifying information of another person to "become" that person. Identity theft also includes enumeration fraud, which uses fraudulent documents to obtain an original SSN for establishing identity. Finally identity theft also includes identity creation, which uses false identity, false documents and a false SSN.

Skilled identity thieves may use a variety of methods—low and hi-tech—to gain access to personal data. We, at the Social Security Administration want to do what we can to help prevent identity theft, to assist those who become victims of identity theft, and to assist in the apprehension and conviction of those who perpetrate the crime.

Preventing identity theft can play a role in the prevention of any future terrorism. Identification documents are critically important to terrorists, and a key to such documents is the Social Security number. The integrity of the SSN must be ensured to the maximum extent possible because of the fundamental role it can play in helping unscrupulous individuals steal identities and obtain false identification documents.

Identity thieves may get personal information by stealing wallets and purses, mail, personal information on an unsecured Internet site, from business or personnel records at work, buying personal information from "inside" sources, or posing as someone who legitimately needs the information such as an employer or landlord. We ask that people be careful with their Social Security number and card to prevent identity theft. The card should be shown to an employer when an individual starts working, so that the employment records are correct and then it should be put in a safe place.

SSA Response to SSN Misuse

In response to the events of September 11, SSA formed a high-level response team which has met regularly ever since to recommend and track progress towards policy and procedural enhancements to help ensure that we are strengthening our capability to prevent those with criminal intent from using Social Security numbers and cards to advance their operations. Just as there have been delays at airports as a result of heightened security, we recognize that some of these initiatives may result in a delay in the receipt of SSNs for some citizens and non-citizens. However, these measures are necessary to ensure the integrity of the SSN and to ensure that only those who should receive an SSN do so.

Soon after 9/11, we began a new training emphasis on the rules for enumeration, and especially for enumerating non-citizens. We started with refresher training for all involved staff, but are following this up with periodic special training and additional management oversight. On March 1 we stopped assigning SSNs to non-citizens for the sole purpose of applying for a driver's license, so that non-citizens can now only get an SSN if they are authorized to work or where needed for a Federal funded or state public assistance benefit to which the person has established entitlement. On June 1, we began verifying with the custodians of the records, any birth records submitted by U.S. born citizens over the age of one applying for an SSN. Further, we are piloting an online system for employers to verify the names and SSNs of newly hired employees. I should note however, that for more than twenty years SSA has a system for employers to verify employees SSNs for wage reporting purposes.

Throughout this year we are also implementing a range of new data sharing initiatives with the Immigration and Naturalization Service (INS) and the Department of State (DoS) that will improve integrity goals with respect to non-citizens. As we have in the past, SSA will proceed with the data matching initiative in a manner consistent with the requirements set forth in the Privacy Act. We expect to have in place by the end of the year the first phase of what we are calling Enumeration At Entry (EAE). EAE is an integrity measure we have been working on collaboratively with the INS and DoS for some time and it will work similarly to our highly successful Enumeration at Birth program under which most U.S.-born infants are assigned SSNs based on requests by their parents in the hospital right at birth, eliminating the need for document verification. EAE will eliminate immigration documents from the process also. Under EAE, SSA will assign SSNs to new arrivals based on data collected by the DoS, as it approves the immigrant visa right in the foreign service post, and refined by the INS, right as entry into the country is authorized. SSA would receive the data electronically from the INS with no need for further document review and verification.

For non-immigrants who initially will not be part of Enumeration at Entry, additional verifications are planned. First, we have already worked out and implemented additional data sharing with DoS for refugees. Then beginning this month, we will

start verifying any documents issued by the INS for other arrivals with that Agency before assigning an SSN. We hope to be able to verify many of these electronically. But where this is not possible, we will request written confirmation from INS that the documents submitted are bonafide and that the individual is authorized to work. We expect this new verification process to be fully implemented by September.

We have developed this multi-pronged approach to make SSNs less accessible to those with criminal intent as well as prevent individuals from using false or stolen birth records or immigration documents to obtain an SSN.

We also implemented changes to speed up the distribution of our Death Master File. SSA receives reports of deaths from a number of sources, and from computer matches with death data from Federal and State agencies. This information is critical to the administration of our program and is made available to facilitate the prevention of identify theft of the SSN's of deceased persons. Many of the private sector companies purchasing this information are credit card companies and financial institutions.Furthermore, we are also limiting the display of Social Security Numbers on our correspondence. As of October 1, 2001 we no longer include the first five digits of the SSN on Social Security Statements and as of December 2001 on Social Security Cost of Living Notices. We do use the full SSN on other correspondence because there may be legal requirements for display of the SSN on the notice especially on termination and award notices. However, to ensure the confidentiality of the SSN on mail we do not show the addressee's SSN on the envelope, if mailing an envelope to an individual. If requesting information from third parties, we do not show the SSN for the purpose of associating the reply with the file when it is returned. We use other means such as a unit number. Additionally, to protect the privacy of recipients who are paid by check and help prevent identity theft, Treasury is taking steps to remove all personal identification numbers, including the SSN, on all check payments. The goal for completing the project is early 2004.

The good news is that over 80% of our beneficiaries receive their payments by direct deposit, which means for this large group there are no SSNs to be stolen or paper checks that can be lost or stolen. For those that do not use direct deposit the Department of the Treasury prepares and mails all government checks including those for Social Security and Supplemental Security Income recipients. Effective with the September 1, 2000 benefit payments, the SSN printed on Social Security and Supplemental Security Income checks is no longer visible through the envelope window. Instead of the Social Security Number, Treasury includes the check number, which is assigned during payment processing, in the window area. Treasury uses this number to locate and hold payment prior to delivery when SSA has determined the payment is not due. Likewise, arrangements have been made with the U.S. Postal Service to use the beneficiary name and address to locate and return payments identified by SSA under the check intercept process.

Detecting SSN Misuse

One way that a person can find out whether someone is misusing their number to work is to check their earning records. About three months before their birthday, anyone 25 or older and not already receiving Social Security benefits, automatically receives a Social Security statement each year. The statement lists earnings posted, to their Social Security record as well as providing an estimate of benefits and other Social Security facts about the program. If there is a mistake in the earnings posted they are asked to contact us right away, so their record can be corrected. We investigate, correct the earnings record and if appropriate, we refer any suspected misuse of a Social Security number to the appropriate authorities.

SSA may learn about misused SSNs in a variety of other ways including alerts from our computer systems while matching Federal and State data, processing wages, claims or post entitlement actions, reports from individuals contacting our field offices or teleservice centers and inquiries from the Internal Revenue Service concerning two or more individuals with the same SSN on their income tax returns.

We have another tool that has been used successfully to detect instances of fraud and abuse. This tool, called the Comprehensive Integrity Review Process (CIRP), is a review and anomaly detection system. Known fraudulent patterns are first identified and then transactions that fit these fraudulent patterns are provided to SSA managers for their review. If upon investigation, the SSA manager believes that fraud or misuse has occurred, they prepare a referral to the Inspector General (IG).

Assisting Victims

To help victims, SSA provides hotline numbers to SSA's Fraud Hotline and the Federal Trade Commission ID Theft Hotline. We provide up-to-date information about steps that the person can take to work with credit bureaus and law enforcement agencies to reclaim their identity. We issue a replacement card if their Social

Security Card is stolen. We help to correct their earnings record and issue a new Social Security number in certain circumstances. If the victim alleges that a specific individual is using the Social Security Number, SSA develops the case as a possible fraud violation. If appropriate, we refer the case to the IG for an investigation and work closely with the IG to facilitate their investigation.

S. 848

The provisions of S. 848 clearly reflect the Congress's growing concern with identity theft and its effects. The bill addresses the need to limit private and public sector use, display and sale of the SSN and to increase penalties for misuse of the number.

We note that the bill provides for civil monetary penalties for misuse of the SSN. While current law provides criminal penalties for SSN misuse, the addition of civil monetary penalties for SSN misuse would provide another level of deterrence for those who would misuse the SSN. We support this provision, which will strengthen our ability to deal with instances of misuse that are declined for prosecution by the Department of Justice.

We also support the provision in S. 848 that would prohibit access to the SSNs by prisoners employed by Federal, State or local governments.

Closing

I would like to conclude by emphasizing that we, at the Social Security Administration want to do what we can to help prevent identity theft, to assist those who become victims and to assist in the apprehension and conviction of those who perpetrate the crime.

In a larger view, though, the Social Security Administration is only one of many institutions that have to be on guard for identity theft. As the Chairman knows, this is a very difficult area. In our experience, most instances of identity theft have resulted not from any action or failure to act by SSA, but from the proliferation of personal information in our society. SSA cannot police the disclosure of Social Security numbers made by private citizens and organizations. Mr. Chairman and members of the Committee we thank you for asking us to testify.

RESPONSE TO A QUESTION FROM SENATOR KERRY

Question: Is the Social Security Administration aware of the disruption this new procedure [Immigration and Naturalization Service (INS) verification of all non-immigrants' legal status before SSA will issue a Social Security number (SSN)] is causing and are you taking prudent steps to accommodate the needs of these exchange programs?

Answer: We appreciate your support for efforts to enhance the integrity of our enumeration process and share your concern that some initiatives may result in a delay in receipt of an SSN or replacement card. Our procedural changes are designed to assure that only those who meet the enumeration requirements receive an SSN or replacement card.

The tragic events of September 11 compel us to give greater attention to integrity concerns associated with verifying documents, including those issued by the INS. Recognizing the legitimate needs of non-immigrants, SSA continues to work with INS and the Department of State to design practices and procedures to expedite document verification and minimize delays in the assignment of SSNs.

When a non-immigrant comes to this country as a participant in a program authorized by the Fulbright-Hays Act, INS determines the participant's work status, issues the individual certain authorizing documents reflecting that status and posts data to its SAVE (Systematic Alien Verification for Entitlements Program) system. Those non-immigrants authorized to work usually apply for SSNs shortly after entering the country. In the past, Social Security offices have relied primarily on a visual inspection of the INS documents to determine authenticity before processing the application for an SSN.

Recent improvements in the timeliness of INS data postings are making it possible to verify many documents electronically. During the period July-September 2002, SSA will phase in a more stringent verification process. First, SSA will attempt to verify the documents with INS through SAVE. We expect the validating information will be available online immediately or within a few days of the non-immigrant's entry into the country, and an SSN card can be issued quickly for many new arrivals. If the verifying information is not posted, SSA will request a paper confirmation from INS. No SSN will be assigned until SSA is able to directly verify the non-immigrant's status with INS. INS' response time can range from as little as 1 day to 20 working days or longer. However, we anticipate that most documents will be verified online within a few days. We believe situations requiring paper

verification should be limited, and expect those circumstances will decrease as the INS further improves its computer system.

An individual must apply for an SSN before seeking employment; however, an individual with proper INS documentation can begin working before the actual SSN is assigned. Employers in this situation should carefully document their actions with respect to reviewing the employee's documentation. It is advisable that this documentation include: 1) a statement that the new employee has applied for an SSN, but currently has not been assigned a number, and 2) the employee has been asked to provide the number to the employer upon receipt of the SSN.

We are committed to doing all we can to protect the SSN while striking a balance among the needs of individuals, employers and SSN integrity. We believe that this new process should provide adequate safeguards for the integrity of the SSN while permitting individuals and their employers to move forward with hiring decisions.

PREPARED STATEMENT OF NORMAN A. WILLOX, JR.

I. INTRODUCTION

Good afternoon. My name is Norm Willox, and I am Chief Officer for Privacy, Industry, and Regulatory Affairs for LexisNexis, a division of Reed Elsevier Inc. On behalf of LexisNexis, I appreciate the opportunity to be here today to discuss the importance of preserving access to social security numbers ("SSNs") by responsible businesses like LexisNexis, and to share with the Subcommittee our comments on S. 848.

LexisNexis leads the information industry with the largest online information service, providing critical information to legal, business, and government professionals. LexisNexis maintains a database four times the size of the Internet. The LexisNexis service contains more than 3.9 trillion characters and approximately 4 billion documents in more than 15,150 databases covering 34,190 sources. It adds 8.8 million documents each week.

Today, over two million professionals in 60 countries worldwide—lawyers, law enforcement officials, accountants, risk managers, financial analysts, journalists, and information specialists—subscribe to the LexisNexis services.

One of the distinguishing aspects of the LexisNexis service is our extensive collection of public records information. Indeed, we have the largest collection of public records in the world. Use of our public records information is an indispensable tool for gathering information and providing accurate answers to prevent and detect fraud, verify identities, locate individuals, perform due diligence searches, and provide risk management solutions and employment screening for businesses and governments worldwide. The overwhelming majority of the information sources on the LexisNexis service are public in nature, all of which are available to the general public through their public libraries, the local newsstand or bookstore, or from government offices.

LexisNexis would like to take this opportunity to thank Chairman Breaux and the other members of this Subcommittee, as well as Senators Feinstein, Hatch, and Gregg for their invaluable work on the important issue of SSN privacy. Our company is committed to the responsible acquisition and use of SSNs, and shares the Subcommittee's concern about the potential misuse of data for identity theft and other harmful purposes. Indeed, in the fight against identity theft, where verifying an individual's identity is crucial, information from commercial databases such as LexisNexis is absolutely essential.

The use of commercial databases is also an important tool in the global battle against terrorism. Information provided by LexisNexis was instrumental in locating suspects wanted in connection with the September 11th attacks. LexisNexis has supported the federal law enforcement community and other agencies for more than 30 years and is currently supporting the Department of Justice, Department of Defense, Treasury Department and other federal agencies in their ongoing efforts to combat terrorism. The use of SSNs is essential to these important efforts.

Due, in large part, to the efforts put forward by Senators Feinstein, Hatch and Gregg and the other members of the Senate Judiciary Committee, S. 848 has improved significantly. The exemptions in the bill that would allow for continued business and government uses of SSNs are critical to crafting a workable approach to this complex issue.

However, LexisNexis is concerned that the bill's treatment of public records will prompt state and local governments to close off access to SSNs in public records, cutting off access to this important information at the source. We also have concerns with the scope of the Attorney General's rulemaking authority, the lack of preemp-

tion of state laws, and the civil cause of action provisions. Our comments on S. 848 are presented in Section IV below.

My remarks today will focus on the following three areas: First, I will describe how LexisNexis uses SSNs and the importance of ensuring continued access to and use of SSNs for business-to-business and business-to-government purposes. Second, I will provide the Subcommittee with examples of some of the important uses of SSNs by business and government customers. Finally, I will make some observations about the impact of S. 848 upon the continued use of SSNs by businesses, government agencies, and non-profit organizations that depend on this information to do their jobs.

II. LEXISNEXIS' USE OF SSNS

LexisNexis is committed to the responsible use of information and has been at the forefront of the privacy debate, leading industry efforts to balance consumer privacy interests with responsible uses of information for important and socially beneficial purposes. We recognize that key to the SSN issue is striking the appropriate balance between consumer privacy and ensuring that important uses of this information can continue.

LexisNexis uses the SSN for important indexing, matching, and verification purposes to ensure the accuracy of information used by professional and government agencies. The inability to use SSNs for indexing and verification would, ironically, result in more rather than less identity theft and undermine many of the positive uses of SSNs which I will describe below.

For our general customer base, LexisNexis has made a policy NOT to display full SSNs except if they appear in the context of a public record. Some databases are searchable by SSN where the user already has the SSN in their possession. However, the results of that search will not display the SSN.

By allowing our customers to use SSNs as a search term, and at the same time prohibiting the display of full social security numbers to our general customer base, our approach prevents people from discovering anyone's social security number from a commercial source, thereby protecting privacy. At the same time, it preserves the ability of people who already know someone's social security number, typically in a commercial, governmental, or law enforcement context, to use a commercial database for important public purposes, such as finding "deadbeat parents" for child support enforcement. As explained below, the result is a significant increase in the effectiveness of our customer's ability to verify identities and locate individuals, as seen through the significant statistical improvements in the effectiveness of our customers who use our services in connection with child support enforcement efforts and locating pension fund beneficiaries.

LexisNexis' policy does allow the full display of SSNs to a limited and selective set of customers that qualify through our stringent "SSN access" process. These customers consist of federal, state and local law enforcement officials, federal, state and local government agencies, specialized investigative units of companies where that department was created to investigate fraud and subrogation units of qualified insurance companies.

III. IMPORTANT AND BENEFICIAL USES OF SSNS BY LEXISNEXIS' BUSINESS AND GOVERNMENT CUSTOMERS

Government agencies, businesses, researchers, and others rely on information contained in commercial databases to do their jobs. Commercial database companies like LexisNexis play a vital role in this effort by collecting information from numerous sources and creating comprehensive data collections that allow users to easily search and locate information. Without this critical public records information, the effectiveness of these government agencies, businesses, and researchers would be dramatically reduced.

The use of SSNs is essential for person identification and record matching purposes and is critical in ensuring the accuracy of the information in these databases. SSNs allow persons to be identified accurately and assure that records for different individuals do not get co-mingled providing a false result. There are more than 43,000 Robert Jones' in the U.S. today. How else can someone distinguish one from another? A unique identifying number like the SSN is important to ensure that information collected on individuals is pertinent and accurate.

The following examples describe some of the important ways in which commercial database services, such as LexisNexis, are used by our customers to help people, protect consumers, locate missing children, prevent fraud and assist law enforcement efforts:

- *Preventing and investigating terrorist activities*—The use of commercial databases like LexisNexis is an important tool in the global battle against terrorism. Information provided by LexisNexis was instrumental in locating suspects wanted in connection with the September 11th terrorist attacks. Since September 11th, the Department of Justice found that LexisNexis public records were mission critical in bolstering cases against terrorists. As a result, more than 10,000 agents, investigators, attorneys and analysts have full access to LexisNexis public records and other information. The SSNs contained in the LexisNexis database are a critical tool used by the FBI and other federal law enforcement agencies to locate suspects and witnesses and in investigating and building cases against suspected terrorists.
- *Locating and recovering missing, abducted and exploited children*—LexisNexis has partnered with the National Center for Missing and Exploited Children to help that organization locate missing and abducted children. Locating a missing child within the first 48 hours is critical. After that time, the chance of recovering the child drops dramatically. In many of these cases, it is the noncustodial parent who has taken the child. The use of SSNs is critical in locating the noncustodial parent and recovering the missing child.
- *Identifying and preventing fraud*—Banks and other financial institutions routinely rely on SSNs in public record information contained in LexisNexis' databases to detect fraudulent credit card applications. With the use of LexisNexis, a major bank card issuer recently experienced a 77% reduction in dollar losses due to fraud. Insurance companies have experienced similar successes through the ability to use SSNs. The use of SSNs in public records and other sources is key to preventing fraud.
- *Locating witnesses and helping make arrests*—Lawyers are major users of these databases. Access to SSN information in these databases, even when it is not displayed, is critical to tracking down witnesses in connection with civil litigation. Law enforcement agencies also are major users of commercial databases. For example, in 1998, the FBI made over 53,000 inquiries to commercial online databases. This information led to the arrests of 393 fugitives and the location of nearly 2,000 suspects and more than 3,000 witnesses [1].
- *Preventing and investigating financial crime*—LexisNexis is the preferred provider of public records at the Financial Crimes Enforcement Network (FinCEN) under the U.S. Treasury Department. FinCEN supports federal, state and local law enforcement agencies in financial investigations and is heavily reliant on SSNs in these investigations. In addition, LexisNexis is working on a project with the American Bankers Association to develop best practices to be used by banks and other financial institutions to prevent money laundering and ensure compliance with the USA PATRIOT Act. The use of SSNs by financial institutions to verify and validate information on prospective customers will be critical to the success of that program.
- *Enforcing child support obligations and government assistance programs*—Public and private agencies rely on SSNs in public records and other information contained in commercial databases to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for Enforcement of Support (ACES), a private child support recovery organization, has stated that SSNs are the most important tool for locating parents who have failed to pay child support. ACES has had tremendous success in locating nonpaying parents using LexisNexis. For example, ACES has found that the ability to use an ex-spouse's social security number as a search term has nearly doubled the success rate in locating a delinquent parent as compared to relying upon prior address information. Additionally, government agencies use SSNs in the administration of assistance programs to prevent or detect the fraudulent collection of benefits.
- *Helping locate pension fund beneficiaries*—The task of locating former employees is becoming increasingly difficult. Americans move on average every five years, particularly when they change jobs. Their names may change as a result of marriage or they may list slightly different names (*e.g.*, leaving out a middle initial) on employment documents. To ensure that pension fund beneficiaries receive the money owed them, plan administrators and sponsors are required by federal law to use a commercial locator service, such as LexisNexis, to search for missing pension beneficiaries. These services are by far the most cost-effective and efficient way to find these former workers. Pension Benefit Informa-

[1] Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, before the U.S. Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State and the Judiciary and Related Agencies, March 24, 1999.

tion, a leading service locating these workers, reports that searching with a retiree's SSN results in an 85–90% success rate in locating an individual, compared to a success rate of only 8% without use of this information. Loss of SSNs from public records and commercial locator services would dramatically increase the costs of locating former employees. Moreover, in many cases, employers would be unable to find former employees, resulting in a loss of pension benefits.

- *Security screening*—PeopleWise, a LexisNexis company, conducted background checks on more than 70,000 workers and volunteers for the 2002 Olympic Winter Games in Salt Lake City. The use of SSNs was critical in verifying and validating the information on each Olympic worker and volunteer and ensuring the safety and security of the athletes and spectators. SSNs are also used by organizations such as Big Brothers Big Sisters of America to perform background checks to ensure the safety and security of those connected to their programs.
- *Locating heirs and beneficiaries of trusts and unclaimed funds*—Commercial database services are used to locate heirs, beneficiaries of trusts, and beneficiaries of unclaimed funds. Access to SSN information, even when not displayed, offers a cost-effective means by which an estate's attorney or executors can locate heirs. Similarly, trustees use SSNs to locate beneficiaries and banks use SSNs to locate persons who have failed to close accounts and beneficiaries to unclaimed funds and safety deposit boxes, avoiding having unclaimed property and money escheat to the state.
- *Assisting with debt collection activities*—The use of SSNs is critical to our credit economy. Collection of debts is important to maintaining credit cost factors at levels that are affordable to a broad cross-section of the population. SSNs allow debtors to be identified and located quickly and accurately. Access to SSN information often provides the sole means by which creditors can track down debtors.

IV. IMPACT OF S. 848 ON THE CONTINUED AVAILABILITY AND USE OF SSNS

We applaud Senators Feinstein, Hatch, and Gregg for recognizing legitimate business and government uses of SSNs and we will continue to work with them to help ensure that this bill accomplishes its important objective of preventing the misuse of SSNs. We do have several comments on the bill. We believe that S. 848 would make it difficult now and in the future to ensure the continued access to and use of SSNs for many of the important and positive uses outlined above. Specifically, we are concerned about the following four issues:

1. Public Records

The issue of SSNs in public records is a highly complex issue that will have far-reaching implications. Public records are an important source of information used by LexisNexis in compiling data for our online service. We routinely use SSNs in public records to accurately match records from disparate data sources. In addition, our clients, including financial institutions, insurance companies, government agencies and others routinely rely on our public record databases containing SSNs for identity verification and validation purposes, to identify, prevent, and investigate identity theft and fraud and for other important purposes.

When we refer to public records, we mean government records that typically and historically have been made available to the public. Examples of public records include titles to real property, real property tax assessor records, bankruptcies, judgments, liens, state professional licenses (and their suspension and revocation), corporation filings, and birth and death records. This information traditionally has been available to anyone who presents themselves at the courthouse.

We believe the public record provisions in S. 848 are unworkable. The bill would effectively construct a two-tiered system for public records and would require state and local governments to maintain two sets of books (one copy of records for public disclosure in which SSNs are redacted, and another copy for other purposes in which the SSNs are included). This two-tiered system of record keeping would be highly burdensome and costly to state and local officials, and would result in confusion concerning who could access the non-redacted records. Faced with such problems, many state and local officials would simply eliminate all SSNs from records. The result would be that we would be cut off from critical public record information at the source. The important exemptions in the bill for legitimate and business and government uses are of little value if the SSNs are no longer available at the source.

As the General Accounting Office confirms in its May 2002 Report to Congressional Requesters on Social Security Numbers, redacting SSNs from public records would be a difficult and challenging process. The complexity of this issue is underscored by the fact that the GAO itself did not provide a recommend approach. The report states that record custodians do not believe that redaction of SSNs is a practical alternative. These custodians reported that redaction would be time-consuming, labor intensive, difficult, and in some cases, would require a change in law.

Public records are a unique class of information that have historically been made available for public inspection. Therefore, we are concerned with any limits on the dissemination of this information. The proposals to date that attempt to address the issue of SSNs in public records are unworkable and would result in significant restrictions on this information. Until a viable approach is developed, public records should be exempted from the bill.

2. Attorney General Rulemaking

The proposed rulemaking provision is overly broad and could result in excessively restricted access to SSNs. The bill should clarify the scope of the Attorney General's ("AG") rulemaking authority, and ensure that the AG's rule will implement the business-to-business and business-to-government exceptions. We are concerned that the broad factors included in the bill could result in the promulgation of unduly restrictive rules for SSN access. In addition, we are concerned that the bill provides the AG with broad discretionary authority to selectively approve or reject individual companies, and determine which ones will qualify for access to SSNs under the exceptions outlined in S. 848.

We believe that the AG's discretionary authority should be limited, and the factors to be considered in promulgating the regulations limited to those specific factors necessary to ensure the continued uses of SSNs by legitimate businesses, rather than focusing on general assumptions of risk or harm.

3. Preemption

Preemption is critical given the current state of piecemeal legislative efforts in numerous states, including Florida, California, Illinois, Texas, Michigan, and Indiana, to restrict the use of SSNs by businesses. Given the uniquely federal nature of SSNs and their importance to businesses engaged in interstate commerce, the bill should preempt state laws. The lack of preemption of state laws would render the business-to-business and business-to-government exemptions somewhat hollow in that access to SSNs would be cut off at the source if the states decide not to recognize these business and government exemptions.

4. Civil Actions

Although we recognize that the Feinstein-Hatch substitute has limited the available damages, we question whether a private right of action is even necessary. The other provisions of the bill, which include hefty administrative penalties by the AG and criminal and civil penalties, provide more than adequate means of enforcement by the Justice Department. The use of the SSN is engrained in many sectors of our society. The requirements and exemptions of this section may be subject to differing interpretation. Government enforcement will permit some flexibility to address interpretations in the early years following enactment. By contrast, a private cause of action could result in a chaotic and burdensome transition.

V. CONCLUSION

LexisNexis is committed to the responsible acquisition and use of SSNs and other personally identifiable information and has been a leader in the industry. LexisNexis shares the Subcommittee's concern about the potential misuse of this information for identity theft and other harmful purposes. Nevertheless, as S.848 recognizes, legitimate uses of SSN information are absolutely essential in the fight against identity theft and fraud and other important uses. Congress should not take any steps that would jeopardize the usefulness of such services. We thank the Subcommittee for holding this hearing on these important issues and look forward to working with Congress to develop an appropriate solution.

CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

July 10, 2002

S. 848

Social Security Number Misuse Prevention Act of 2002

As reported by the Senate Committee on the Judiciary on May 16, 2002

SUMMARY

S. 848 would impose a variety of restrictions on the collection, use, public display, and sale of Social Security numbers (SSNs). The Attorney General would enforce those provisions through civil and criminal penalties. The bill also would require the Department of Justice to report to the Congress within one year of enactment on the use of SSNs in public records.

CBO estimates that implementing S. 848 would cost about $4 million in 2003 and $17 million over the 2003-2007 period, subject to the availability of appropriated funds. Pay-as-you-go procedures would apply because the bill's provisions related to civil and criminal penalties could increase both revenues and direct spending. However, CBO estimates that any such effects would be negligible.

S. 848 contains a number of intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), including limitations on the sale, display, and use of Social Security numbers by state, local, or tribal governments. While there is some uncertainty about the aggregate costs of those mandates on state, local, or tribal governments, CBO estimates that the costs likely would exceed the threshold established in UMRA ($58 million in 2002, adjusted annually for inflation) in at least one year over the next five years.

S. 848 also would impose private-sector mandates as defined by UMRA. The most costly mandate would require individuals and businesses that accept credit cards to electronically print truncated account numbers on receipts. CBO cannot estimate the aggregate direct cost of mandates in the bill because of uncertainty as to the number of credit card processing devices that would need to be upgraded and the wide range of replacement cost of those devices.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 848 is shown in the following table. The costs of this legislation fall within budget function 750 (administration of justice).

	By Fiscal Year, in Million of Dollars				
	2003	2004	2005	2006	2007
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level	5	3	3	3	3
Estimated Outlays	4	4	3	3	3

BASIS OF ESTIMATE

S. 848 would require the Attorney General to enforce new restrictions on the collection, use, and sale of Social Security numbers. Based on information from the Department of Justice, CBO expects that the agency would need to hire about 15 additional staff members, including Administrative Law Judges, attorneys, and paralegals, for this purpose. CBO estimates that salaries and expenses for those new hires would cost about $3 million a year, assuming the appropriation of the necessary amounts.

Under S. 848, the Department of Justice would conduct a year-long study on the use of SSNs in public records and on methods to remove them. CBO estimates that completing the report would cost about $2 million in 2003, subject to the availability of appropriated funds.

Because those who violate the provisions of S. 848 could be subject to civil and criminal fines, the federal government might collect additional fines if the bill is enacted. Collections of civil and criminal penalties are classified in the budget as governmental receipts (revenues). However, CBO estimates that any such increase in collections would be less than $500,000 per year.

Collections of criminal fines are deposited in the Crime Victims Fund and spent in subsequent years. Because any increase in direct spending would equal the amount of fines collected (with a lag), the additional direct spending also would be negligible.

PAY-AS-YOU-GO CONSIDERATIONS

The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. Although S. 848 could affect both direct spending and receipts, CBO estimates that any such effects would be negligible.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 848 would prohibit—beginning three years after the enactment of the bill—the display, sale, or purchase of a number of public records which contain SSNs. It also wold require state, local, and tribal governments to implement new procedures for handling public documents that contain SSNs. Such prohibitions and new requirements would be intergovernmental mandates as defined in UMRA.

The bill would prohibit—beginning three years after the enactment of the bill—the display, sale, or purchase of the following documents if they contain Social Security numbers: death certificates, professional and occupational licenses, property settlement documents, birth documents, land ownership records, marriage permits and licenses, bankruptcy documents, court judgments, child support documents, divorce petitions and decrees, and tax liens. Additionally, any public agency in possession of one of those documents must restrict internal access to the document and redact the Social Security number before providing the document to anyone who is not authorized to have access to SSNs.

State, local, and tribal governments that collect, maintain, and make documents available to the public would likely have to make systemic changes that alter their document maintenance and retrieval systems. Those changes may take the form of greater training for employees or changes in recordkeeping and computer systems used to generate the affected documents. Based on information from state and local governments and various interest groups representing them as well as survey data from the General Accounting Office (GAO), CBO believes it is likely that the aggregate costs of the requirements would be significant and would exceed the threshold established in UMRA for intergovernmental mandates ($58 million in 2002, adjusted annually for inflation) in at least one year over the next five years.

Costs are likely to be significant because SSN use is pervasive. The GAO study indicates that over 90 percent of governments they surveyed (both state and county) use SSNs on both paper documents and electronic records. While agencies at all levels of government are already taking some steps to safeguard SSNs—for example, all states have either stopped using SSNs on drivers licenses, or they allow the use of an alternative identification number—SSNs still appear in a number of other documents such as death certificates, property documents, professional licenses, and court documents.

Because of the large number of state and local governments (well over 80,000) in the United States, even fairly low-cost changes to document systems would quickly add up to aggregate costs exceeding the threshold in UMRA. For example, if less than half of the agencies potentially affected by the bill (i.e., health and vita statistics, criminal justice, licensing, education, and human services departments) at all levels of government were required to implement some system change (computer changes or employee training) and each spent as little as $5,000 on altering their systems or procedures over a three-year period, total costs would exceed the threshold at some point over the next five years.

The large number of municipal governments contributes significantly to the total estimated costs of complying with the mandates in this bill. And because there are so many of them (over 75,000), even small one-time costs—as little as $5,000—would add up to costs over $60 million in a given year. Counties and states are more dependent on SSNs for various recordkeeping and identification purposes and are thus likely to face significantly higher costs because of the complexity and scope of their recordkeeping systems. (Some counties estimate that altering their systems to use identifiers other than SSNs or to eliminate display of SSNs would result in one-time costs ranging from $40,000 to over $1 million, again depending on the county and the scope of the changes that would need to be made). Because there are fewer counties (about 3,600), however, total compliance costs for them would likely be lower than the aggregate costs attributable to municipalities.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 848 would impose a private-sector mandate by requiring individuals and businesses that accept credit cards to truncate the credit card account numbers to include no more than the last five numbers on an electronically printed cardholder receipt. The mandate would take effect four years from the date of enactment. According to the credit card processing industry, some systems are currently in compliance because they are capable of electronically printing truncated account numbers on customer receipts. In order to comply with this mandate, some merchants would have to make modifications to their systems, including software reprogramming, formatting changes to dial-up terminals, and purchase of new printing devices. CBO cannot estimate the direct cost of this mandate because of uncertainty as to the number of devices that would need to be upgraded and the wide range of replacement costs of those devices.

Under the bill, an individual or business entity would be prohibited from the purchase, sale, or display of an SSN to the general public, without the expressed consent of the individual. The purchase, sale, or display of SSNs would be allowed for business-to-business use or business-to-government use. According to the Federal Trade Commission (FTC) and industry sources, only a few entities currently display or sell Social Security number

information to the general public. Therefore, CBO estimates that the direct cost of this mandate would be minimal.

The bill also would impose a private-sector mandate on certain business entities by limiting the personal disclosure of SSNs for consumer transactions. Business entities could no longer require an individual to provide the individual's SSN when purchasing a commercial good or service unless the number is necessary to verify their individual's identity with respect to the specific transaction or to prevent fraud. According to the FTC and industry sources, some businesses currently require an individual to provide their SSN usually for the specific transaction identification or to prevent fraud. Therefore, CBO estimates that the direct cost to comply with this mandate would be small, if any.

ESTIMATE PREPARED BY:

Federal Costs: Ken Johnson
Impact on State, Local, and Tribal Governments: Leo Lex
Impact on the Private Sector: Paige Piper/Bach

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis

STATEMENT OF THE NATIONAL COUNCIL OF INVESTIGATION & SECURITY SERVICES, INC.

[SUBMITTED BY A. DALE WUNDERLICH]

I am Dale Wunderlich, President of A. Dale Wunderlich & Associates, of Parker Colorado, a firm I founded in 1979. I am a former police investigator and served as Special Agent in the Secret Service for over 13 years. I am presenting this statement on behalf of the National Council of Investigation and Security Services (NCISS), which I serve as President. NCISS is the association representing the nation's professional investigative agencies and private security organizations. Our members provide essential services to the judicial system, law enforcement and the American consumer.

As a profession that has been striving to assist victims of identity theft for many years and long before the Internet came into being, we applaud Congress' efforts to make it more difficult for thieves to assume someone else's identity. Social Security numbers and other highly personal information should not be made available to everyone with Internet access. Access to sensitive information should be limited to those who have a legitimate need for it.

Although restrictions on the display and sale of public and personal information will no doubt reduce instances of identity theft, Congress should not be under the illusion that it will end the crime. Our experience shows that most such thefts still occur from the mails and from the theft of documents, files, charge slips, credit cards, and wallets from restaurants, stores trash bins and private property.

USES OF PERSONAL DATA

Professional investigators utilize the Social Security number to help identify individuals for a number of purposes, including but not limited to:

Locating witnesses in both civil and criminal venues
Finding heirs and pension beneficiaries
Preventing and uncovering fraud
Recovering child support
Assisting victims of identity theft

One of the most helpful tools we have in identifying people for these purposes is access to the databases maintained by individual reference services. The Committee

should know that these services require that we contract with them in order to receive access to the data. We are required to maintain records to show the need for the data and how we determined that the client is bona fide. These information services are auditing investigators, and are even running sting operations to enforce their contracts.

We have recently surveyed our membership about how they have used the Social Security number and been able to assist victims of identity theft and other crimes. The following examples demonstrate the benefits of permitting licensed private investigators to access essential information using individual reference services. In all of these investigations, the SSN is critical to index, match and verify the accuracy of information. These anecdotes should give this Committee some idea of how investigators use this information on a variety of assignments:

A 43-year-old single mother of three in Illinois had recently received a promotion and was shopping for a new apartment to better her family's living conditions. Once she decided upon a new home, she completed the credit application in excitement. This predominantly Spanish-speaking woman was devastated to learn that she had an eighteen-page credit report with over $180,000 in bad debt in her name. Investigation revealed that a former neighbor had repeatedly rummaged through her trash discovering her personal identifying data and purloining pre-approved credit offers. It was determined this identity thief had been using the victim's credit for over four years without her knowledge. While her Social Security number was the key to her victimization, access to Social Security information through commercial databases played a key role in providing the associated addresses and other information needed to prove her innocence and to track down the offender.

In South Carolina, a Coast Guard Auxiliary member desperately sought answers when numerous creditors began sending threatening letters. The police even came to his door claiming he had purchased a new automobile under false pretenses. The investigation utilized Social Security numbers, credit header data, driving history information, and commercial and proprietary databases. It was determined that the man was one of several Coast Guardsmen who had been victimized. The matter was coordinated with Department of Defense investigators. The victim's name was eventually cleared, and the culprits caught.

A 22-year-old Missouri man was steadfast in his denial of responsibility for the false-pretense theft of a recent model Oldsmobile from a Kansas City dealership, despite a dealership employee picking him out of a photo line-up. The investigation, which included the use of drivers license photo identification records, SSN credit header data, and proprietary databases, revealed that the person actually responsible for the theft was a delinquent brother who had disassociated himself from the family years ago.

An equipment rental agency doing business in Indiana and Illinois was one of several in the area that had experienced a rash of false-pretense thefts. Persons using others' identification had rented equipment and failed to return it. Access to vehicle registration information, credit header data, commercial and proprietary databases made it possible to successfully identify and prosecute at least some of the persons involved.

A business owner in Tennessee asked for assistance in determining the legitimacy of a customer's claim that someone had stolen his identification and made purchases in his name. Utilizing proprietary databases which rely on the SSN identifier and surveillance techniques, it was determined this man had made the various purchases himself, then falsely claimed that his identity had been stolen in an effort to avoid financial responsibility for the payments.

A Texas business had experienced a significant false pretense theft of construction equipment. After extensive investigation utilizing criminal and vehicle registration records, credit header data, as well as proprietary database information, it was determined that the individual responsible was a member of a ring. Another ring member, acting as a mole, had taken hundreds of Social Security numbers and other identifying information from an unwitting employer. Utilizing the stolen identities, this ring had perpetrated dozens of acts of identity theft and false pretense theft. In most border states, stolen equipment is shipped directly to Mexico and faces little inspection or screening at the border. But in this case, much of the client's equipment was recovered in good condition in Colorado and the investigative results turned over to authorities.

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

A businesswoman in Atlanta, Georgia, asked our investigator to help an applicant who claimed his identity had been stolen. An imposter whose criminal record included nine felonies had stolen this man's Social Security number and date of birth. In the course of committing false pretense thefts in several states, the imposter's identity records became mixed with those of the victim. The applicant couldn't understand why he had been turned down for several jobs until this potential employer leveled with him. He then realized his identity had been stolen. Numerous law enforcement agencies told him they couldn't help him. The investigator arranged for the applicant to be fingerprinted and the Georgia Bureau of Investigation issued him a certificate stating he was not the same person as the imposter. He then carried the certificate to the three major credit bureaus to clear his name in their files. The investigator says had he not helped the victim through this maze, he would surely have been arrested in Georgia or Florida where warrants had been issued.

A recent investigation in California revealed a middle-aged suspect who had stolen his elderly father's identity launching a spending spree in Oregon and California. The attendant havoc created for his parents was not resolved before both parents passed away. The attorney for the estate turned to a private investigator to uncover the facts, clear the record of the deceased parents and obtain restitution. The Social Security numbers and credit header information were key to differentiating between the deceased victims and the perpetrator.

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

> "Over the years I have located a number of missing heirs in probate estate cases. One of my cases involved a young woman who was left a sizeable inheritance by her uncle in the form of a trust. The family had not had any contact with her for a number of years, so the attorney handling the trust asked for my assistance. Locating women who have remarried and changed their surnames complicates the location process. By using her Social Security number and credit header information, I was able to eventually determine she was recently married and living someplace in Utah. I located her husband's relatives and learned that she and her husband were destitute and living out of a pick-up truck either in Utah or Oregon. I sent her the requisite documentation in care of her husband's relatives and she rightfully obtained her substantial inheritance. Without access to such information, I would not have been able to locate her."

S. 848

We strongly support provisions of S. 848 that deny the public access to Social Security Numbers. We believe the bill goes a long way toward meeting the legitimate needs of business and government for the information they need. Of most importance to investigators are the "business to business" exceptions. These include fraud prevention, background checks and law enforcement purposes. It is essential that the language "but not limited to" these exceptions be maintained in the bill, as Congress cannot predict every essential business to business purpose which may arise.

Our members and the individual reference services to which we subscribe, must constantly rely on the Social Security Number as an identifier. While we abhor the misuse of the SSN by rogue information providers who advertise and sell to the general public without due diligence, we are concerned that segments of S. 848 will prevent the functioning of legitimate databases for legitimate purposes. The thoughtful exceptions which the bill appears to provide for business to business use would be of little value if the legitimate individual reference services are blocked from collecting the information at its source. This would not only limit our use of the information, but would destroy an important and critical tool for all law enforcement agencies.

Verification of the SSN is essential for all forms of security screening and background investigations. At a time when correct and timely information is critical, Congress needs to be sure it does not take away the tools to do the job. We are concerned that the discretionary powers provided to the Attorney General by S. 848 could result in the promulgation of regulations that do not reflect legislative intent. Altering a public record system that has served our country well for over a century is a risky proposition. Care must be taken to prevent unintended consequences which could be manifold and injurious to the country as a whole. We recommend the Committee consider tightening the guidelines for the Attorney General.

We also urge the committee to reconsider the provisions relating to public records. It is highly unlikely that courts and other holders of public records will expend the necessary resources to redact Social Security Numbers from documents for the gen-

eral public, but provide them for those excepted under the bill. In many instances, SSN's are listed throughout documents and will prove difficult to redact. At a practical level, it is difficult to see how this provision could work.

CONCLUSION

We believe that the identity theft laws recently enacted will help law enforcement to prosecute perpetrators once apprehended. We agree with the basic premise of S. 848 to limit SSN access for the general public.

But Congress should be aware that public law enforcement resources are stretched and crimes of this nature are not now a high priority. The losses, though devastating to the victims, are usually beneath the dollar threshold that many departments follow. The private sector will have to continue to augment public law enforcement. I know from my experience with the Secret Service at the White House and other assignments, how critical it is for law enforcement to be able to access civilian databases for information. The advent of terrorism on our soil only magnifies this need. If the databases are blocked from accessing the SSN identifier in public records, both the public and the private sector will suffer.

It is therefore essential that law enforcement and licensed private investigation and security firms not be precluded from accessing the essential data that assists us in helping victims of this insidious thievery. By eliminating the restrictions on access to public documents and clarifying the role of the Attorney General, Congress can assist public and private security to help fight identity theft and other crimes.

Thank you for the opportunity to express our views.

Public and Private Benefit Plan Sponsors
Urge Caution When Restricting Uses of SSNs

The undersigned organizations urge you to carefully consider the unintended consequences of legislation currently pending before the Senate Finance Committee. Without amendment, the Social Security Number Misuse Prevention Act of 2001 (S.848) could unintentionally hinder the delivery of benefits from, and the efficient administration of, public and private employee benefit plans.

We strongly support the bill's purpose of ensuring the integrity of the social security number (SSN). We are extremely concerned about the proliferation of identity theft and other financial crimes that exploit individual SSNs, and believe strong legislation should be enacted to combat such nefarious acts. As currently drafted, however, S.848 could make it more difficult to deliver comprehensive health and retirement benefits to public and private employees alike.

In general, public and private employee benefit plans use SSNs in plan administration because of the SSN's utility as a common identifier for a highly mobile workforce, and because of tax reporting requirements. Plan administrators take seriously the responsibility that the use of SSNs requires, and they use the utmost caution and security when SSNs are used in plan administration and communications.

Public and private sector defined benefit and defined contribution pension and savings plans, like 401(k), 403(b), and 457 plans, use SSNs to identify plan participants, account for employee contributions, implement the employee's investment directions, track "rollovers" from other plans, and allow employees to view their account activity or benefit accrual online (typically in conjunction with a secure "PIN"). S.848's broad prohibitions could impede, for example, an individual's ability to stay current on the accumulation of benefits for his or her retirement.

SSNs are also used as the primary identifier in many medical and health benefit and prescription drug plans to coordinate communications between the doctor, the medical service provider, and the plan. S.848's broad prohibitions could, for example, put at risk the delivery of appropriate medications to the individual.

The application of S.848's broad prohibitions could:

- **Unintentionally restrict access to employee benefit plans.** Section 7 of S.848 prevents "commercial entities" from requiring an individual's SSNs to complete the sale or purchase of a "commercial good or service." Without clarifying that section 7 does not

apply to public and private employee benefit plans, plan sponsors might be prevented from obtaining an individual's SSN for plan enrollment, benefit payments, and other routine plan administrative functions.

Exemptions to those prohibitions provided in section 7 for identity verification and fraud prevention, while helpful, do not go far enough. We strongly urge you to clearly and expressly exempt public and private employee benefit plans entirely from these prohibitions.

- **Unnecessarily limit the legitimate and beneficial use of SSNs**. Section 3 prohibits the "sale," "purchase," or "display to the general public" of an individual's social security number without expressed written consent. Those ambiguous definitions risk making legitimate and beneficial uses of social security numbers a violation of Federal criminal law.

- **Unwisely subject public and private employee benefit plans to regulations promulgated by a federal agency with no expertise in employee benefit plans.** Section 5 of S.848 grants the Attorney General authority to promulgate regulations to carry out the prohibitions against sale, purchase, and display of SSNs. Regulations that require the amendment of hundreds of thousands of public and private employee benefit plans should not be promulgated by an agency with no expertise or jurisdiction over the laws governing those plans.

Attached are proposed amendments to S.848 that are designed to enable the bill to achieve its sponsors' objective of limiting the misuse of social security numbers without interfering with the efficient and effective administration of public and private employee compensation and benefit plans.

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

Sincerely,

American Benefits Council
The ERISA Industry Committee
Financial Executives International's Committee on Benefits Finance
National Association of State Retirement Administrators
National Council on Teacher Retirement
National Rural Electric Cooperative Association
Profit Sharing/401(k) Council of America

Attachments

Proposed Amendments to S.848

The undersigned organizations propose the following amendments to S.848, the Social Security Number Misuse Prevention Act of 2001." Our proposed amendments are designed to enable the bill to achieve its sponsors' objective of limiting the misuse of social security numbers without interfering with the efficient and effective administration of public and private employee compensation and benefit plans. In each instance, new text is underscored, and deletions are [bracketed].

Section 2. Amend Section 2(2) of the bill to read as follows:

"(2) While financial institutions, health care providers, public and private employers, and other entities have often used social security numbers to confirm the identity of an individual, the general display to the public, sale, or purchase of these numbers has been used to commit crimes, and also can result in serious invasions of individual privacy."

Comment: This amendment clarifies Congress's recognition of the use of social security numbers by employers.

Section 3. Amend Section 3 of the bill as follows:

1. Amend Section 1028A(a)(1) (defining "display") to read as follows:

   "(1) DISPLAY – The term 'display' means to intentionally communicate or otherwise make available (on the Internet or in any other manner) to the general public an individual's social security number. As used in this section, the term 'general public' does not mean any person connected with any activity that is necessary to effect employment-related transactions that has a bone fide purpose unrelated to the use of the social security number.

Comment: This amendment clarifies that a social security number is not displayed to the general public when it is placed in a viewable manner in connection with an employment-related transaction that has a bone fide purpose unrelated to the use of the social security number, such as the administration of an employee benefit or compensation plan.

2. Amend section 1028A(a)(3) (defining "purchase") to read as follows:

   "(3) PURCHASE – The term 'purchase' means providing, directly or indirectly, anything of value in exchange for a social security number, but does not include any activity necessary to effect an employment-related transaction that has a bone fide purpose unrelated to the use of the social security number."

Comment: This amendment clarifies that a social security number is not purchased when it is obtained in connection with an employment-related transaction that has a bone fide purpose unrelated to the use of the social security number, such as the administration of an employee benefit or compensation plan.

3. Amend section 1028A(a)(4) (defining "sale") to read as follows:

"(4) SALE – The term 'sale' means obtaining directly or indirectly, anything of value in exchange for a social security number, but does not include any activity necessary to effect an employment-related transaction that has a bone fide purpose unrelated to the use of the social security number."

Comment: This amendment clarifies that a social security number is not sold when it is provided in connection with an employment-related transaction that has a bone fide purpose unrelated to the use of the social security number, such as the administration of an employee benefit or compensation plan.

4. As an alternative to the above amendments to Section 3, amend Section 1028A(f) to read, in part, as follows:

"(f) EXCEPTIONS- Except as provided in subsection (d), nothing in this section shall be construed to prohibit or limit the display, sale, or purchase of a social security number--

* * *

"(5) if the display, sale, or purchase of the number is for a business-to-business use, business-to-government use, government-to-business use, or government-to-government use

* * *

"(G) if such number is necessary or appropriate to effect, administer, enforce, or apply for benefits under any type of Federal, State, or local government program or public or private employer-sponsored compensation or benefit plan.

* * *

"(7) if such number is required to be submitted as part of the process for applying for any type of Federal, State, or local government benefit or program, including benefits related to employment with such governments.

Comment: These amendment are offered as an alternative to the other proposed amendments to Section 3 of the bill (amending the definition of "display," "purchase," and "sale." The amendments clarify that the prohibitions contained in Section 3 of the bill will not apply to public and private employer-sponsored plan uses of social security numbers. The amendments further clarify that all types of transactions between and among business and government are covered. The current text applies to simply business-to-business and business-to-government uses. This amendments also clarify that "government benefit or program" includes benefits related to employment with such governments.

Section 7. Amend Section 7 as follows:

1. Amend Section 1150A(a)(1) to read as follows:

"(a) IN GENERAL -- A commercial entity may not require an individual to provide the individual's social security number when purchasing a commercial good or service or deny an individual the good or service for refusing to provide that number except –

"(1) for any purpose relating to –

"(A) obtaining a consumer report for any purpose permitted under the Fair Credit Reporting Act;

"(B) a background check of the individual conducted by a landlord, lessor, employer, voluntary service agency, or other entity as determined by the Attorney General;

"(C) law enforcement; [or]

"(D) a Federal, State, or local law requirement; or

"(E) employment of the individual, including the provision of compensation or benefits; or

Comment: This amendment clarifies that Section 1150A does not apply in the context of the employer-employee relationship, such as the administration of an employee compensation or benefit plan.

American Benefits Council
The ERISA Industry Committee
Financial Executives International's Committee on Benefits Finance
National Association of State Retirement Administrators
National Council on Teacher Retirement
National Rural Electric Cooperative Association
Profit Sharing/401(k) Council of America

○