PREVENTING IDENTITY THEFT BY TERRORISTS AND CRIMINALS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

AND THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS

OF THE

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

NOVEMBER 8, 2001

Printed for the use of the Committee on Financial Services and the Committee on Ways and Means

Serial No. 107–50

(Committee on Financial Services)

Serial No. 107–51

(Committee on Ways and Means)

U.S. GOVERNMENT PRINTING OFFICE

76–259 PS 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

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa
MARGE ROUKEMA, New Jersey, *Vice Chair*
DOUG BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Texas
BOB BARR, Georgia
SUE W. KELLY, New York
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
DAVE WELDON, Florida
JIM RYUN, Kansas
BOB RILEY, Alabama
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
DOUG OSE, California
JUDY BIGGERT, Illinois
MARK GREEN, Wisconsin
PATRICK J. TOOMEY, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
GARY G. MILLER, California
ERIC CANTOR, Virginia
FELIX J. GRUCCI, JR., New York
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
PATRICK J. TIBERI, Ohio

JOHN J. LAFALCE, New York
BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
KEN BENTSEN, Texas
JAMES H. MALONEY, Connecticut
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
MAX SANDLIN, Texas
GREGORY W. MEEKS, New York
BARBARA LEE, California
FRANK MASCARA, Pennsylvania
JAY INSLEE, Washington
JANICE D. SCHAKOWSKY, Illinois
DENNIS MOORE, Kansas
CHARLES A. GONZALEZ, Texas
STEPHANIE TUBBS JONES, Ohio
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
RONNIE SHOWS, Mississippi
JOSEPH CROWLEY, New York
WILLIAM LACY CLAY, Missouri
STEVE ISRAEL, New York
MIKE ROSS, Arizona

BERNARD SANDERS, Vermont

Terry Haines, Chief Counsel and Staff Director

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

SUE W. KELLY, New York, *Chair*

RON PAUL, Ohio, *Vice Chairman*
PETER T. KING, New York
ROBERT W. NEY, Texas
CHRISTOPHER COX, California
DAVE WELDON, Florida
WALTER B. JONES, North Carolina
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
ERIC CANTOR, Virginia
PATRICK J. TIBERI, Ohio

LUIS V. GUTIERREZ, Illinois
KEN BENTSEN, Texas
JAY INSLEE, Washington
JANICE D. SCHAKOWSKY, Illinois
DENNIS MOORE, Kansas
MICHAEL CAPUANO, Massachusetts
RONNIE SHOWS, Mississippi
JOSEPH CROWLEY, New York
WILLIAM LACY CLAY, Missouri

HOUSE COMMITTEE ON WAYS AND MEANS

BILL THOMAS, California, *Chairman*

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

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

SUBCOMMITTEE ON SOCIAL SECURITY

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

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

ROBERT T. MATSUI, California
LLOYD DOGGETT, Texas
BENJAMIN L. CARDIN, Maryland
EARL POMEROY, North Dakota
XAVIER BECERRA, California

CONTENTS

WITNESSES

THURSDAY, NOVEMBER 8, 2001

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

JOINT HEARING: PREVENTING IDENTITY THEFT BY TERRORISTS AND CRIMINALS

THURSDAY, NOVEMBER 8, 2001

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
AND THE
SUBCOMMITTEE ON SOCIAL SECURITY,
COMMITTEE ON WAYS AND MEANS,
Washington, DC.

The subcommittees met, pursuant to call, at 10:10 a.m., in room 2128, Rayburn House Office Building, Hon. Sue W. Kelly, [chairwoman of the Subcommittee on Oversight and Investigations], and E. Clay Shaw, Jr., [chairman of the Subcommittee on Social Security], presiding.

Present from Subcommittee on Oversight and Investigations: Chairwoman Kelly; Representatives Weldon, Inslee, Tiberi, Jones, Shows and Clay.

Present from Subcommittee on Social Security: Chairman Shaw; Representatives Matsui, Cardin, Becerra, Doggett, Collins, Brady, and Ryan.

Also attending was Congresswoman Hooley.

Chairwoman KELLY. This joint hearing of the Committee on Financial Services Subcommittee on Oversight and Investigations, and Committee on Ways and Means Subcommittee on Social Security, will now come to order.

I welcome today my colleagues, Clay Shaw, and Ben Cardin. I'm delighted that we also have other colleagues here—Darlene Hooley. Thank you very much.

I look forward to hearing what the witnesses have to say.

We're here this morning to see how we can prevent the awful crime and terrible tragedy of identity theft by terrorists and criminals. Our special intention is to protect the families of the deceased from such theft and financial fraud at their most vulnerable moment—when they are grieving from the shock of their loss.

Through the rapid transmittal of the information in the Death Master File from the Social Security Administration to the financial services industry and the immediate use of that information by the industry, we can prevent these crimes and spare the families pain.

James Jackson and Derek Cunningham stole hundreds of thousands of dollars in gems and watches from deceased executives of our major corporations before being caught by law enforcement. They stole the identity of the late CEO of Wendy's International

within days after his death and were not arrested until about 2 months later.

In the past 2 months, we learned that identity theft could be a tool of the hijackers who murdered thousands of our fellow citizens, and of their accomplices as well.

Last week, the Inspector General of the Social Security Administration testified that some of the 19 hijackers used phony Social Security numbers to perpetrate their murders. And we know that Lofti Raisi, an Algerian held on suspicion that he trained four of the hijackers how to fly, used the Social Security number of a New Jersey woman who has been dead for 10 years.

Even after these events, and after three of us serving on the Financial Services Committee requested the SSA to ensure the rapid transmission of the Death Master File, we've received no commitment from the SSA to take any specific action.

The file is still physically shipped to an agency at the Commerce Department, where copies are made and physically shipped to subscribers.

In other words, "snail-mail."

There has been no reduction for years in the time that it takes for the SSA to officially notify the financial services industry of a death. Identity theft is now part of the first war of the 21st Century, but the Federal Government is still treating it in a 1960s way.

That must end. That is why we asked the General Accounting Office to study the matter and report their findings to the committee. That is why we're so pleased that the Ways and Means Subcommittee on Social Security, chaired by my colleague, Representative Clay Shaw, can join us in holding a joint hearing today.

We need the Social Security Administration to take bold and immediate action to get the information to the financial services industry. We will hear from the SSA, the Commerce Department, the General Accounting Office, and we expect an innovative and effective solution.

We also need the financial services industry to ensure that the information is immediately integrated into databases and available for permanently deactivating Social Security numbers of the deceased.

Moreover, with the passage of the USA Patriot Act, there will soon be Treasury Department regulations requiring them to verify the identification of new account-holders and for customers to provide the identification requested by the companies.

We know that the SSA and financial institutions can meet this challenge. In the past 3 years, they've already met two difficult challenges—the Y2K conversion and the aftermath of the terrorist attacks.

The SSA was a leader among Government agencies in successfully avoiding the Y2K glitch and the financial institutions breezed through the turn of the millennium without a single major problem.

As the acting SSA commissioner testified last week before Representative Shaw's subcommittee, the SSA regional offices in the New York and Pennsylvania area reacted with fortitude and compassion to assist the victims and their families, and I want to

thank the Social Security Administration for their wonderful assistance to New Yorkers, including the many of those in my district.

After the horrendous destruction in New York City interrupted the financial markets and killed many, financial institutions there and across the country picked themselves up, dusted off, and got back to work with an amazing speed and grace, even while mourning their compatriots.

And all of them did all of that, the Y2K conversion and the recovery from the attacks, without any specific mandate in Federal law.

Surely, we can work together to meet this challenge before us now. I urge all parties to get together and, based on the GAO's findings, leapfrog over the antiquated system now used, and stop identity theft of the deceased.

Representative Shaw will chair the hearing for the first panel of witnesses. I will chair the hearing for the second panel.

Thank you.

[The prepared statement of Hon. Sue W. Kelly can be found on page 47 in the appendix.]

Chairman SHAW. Thank you, Ms. Kelly. We appreciate being here in your committee room and being able to join with you in this hearing this morning.

Today, our two subcommittees join together to examine ways to prevent identity theft by terrorists and criminals. When Social Security numbers were created 65 years ago, their only purpose was to track a worker's earnings so that Social Security benefits could be calculated. But today, use of the Social Security number is pervasive.

Our culture is hooked on Social Security numbers. Businesses and Government use the number as their primary source of identifying individuals. You can't even conduct the most frivolous transaction, like renting a video at your local store, without someone asking you first to render your 9-digit Social Security ID.

Interestingly enough, I had a doctor's appointment last Friday. It was a doctor I had never been to before. And I noticed when I was signing in, my Social Security number was required.

I mentioned that to him back in the examining room and I told him, I said, the time is going to come when you're not going to be able to get that number. And he said, well, I hope it does, because he had been a victim of identity theft and it took him many years through the various layers of collection agencies to finally show that he was not the one that ran the tremendous debt up on the credit cards.

Your Social Security number is a key that unlocks the doors to your identity for any unscrupulous individual who gains access to it. Once the door is unlocked, the criminal or terrorist has at their fingertips all the essential elements needed to carry out whatever dastardly act that they conceive.

We now know that some terrorists involved in the September 11th attacks illegally obtained Social Security numbers and used them to steal identities and obtain false documents, thus hiding their true identities and their motives. These unspeakable acts shine an intense spotlight on the need for the Government and the private industry to be vigilant in protecting identities. It also de-

mands that safeguards to prevent identity theft are put in place and put in place now.

Earlier this year, I, along with several of my Ways and Means colleagues, introduced H.R. 2036, the Social Security Number Privacy and Identity Theft Prevention Act of 2001. This bipartisan bill represents a balanced approach to protecting the privacy of Social Security numbers, while allowing for their legitimate uses.

Because of its broad scope, the bill has also been referred to the Committee on Energy and Commerce and the Committee on Financial Services, in addition to Ways and Means. I urge prompt action by all three committees so that we may bring this important legislation to the floor as quickly as possible.

It is a needed part of our Nation's response to terrorism.

Sadly, identity theft is a crime not perpetrated just against the living. A *Washington Post* article on Saturday, September 29th, reported that a man detained in Great Britain and suspected of training the terrorists who hijacked the airliners on September 11th, used the Social Security number of a New Jersey woman who died in 1991.

The Associated Press reported on October 31st, that an individual from North Carolina had been indicted on charges he tried to steal the identity of someone killed in the terrorist attack at the World Trade Center.

Therefore, today, we will take a hard look at the sharing of death information. The Social Security Administration maintains the most comprehensive file of death information in the Federal Government. How this information is compiled, its accuracy, and the speed with which it is shared with the public will be explored.

Because the financial services industry relies fundamentally on Social Security numbers as the common identifier to assemble accurate financial information, they are in a unique position to assist in the prevention of Social Security number fraud and abuse. Their timely receipt of death information and prompt updating of financial data is key in preventing identity theft.

In the past, some businesses have not been enthusiastic about further restricting the use of Social Security numbers. It is my hope they will rethink their resistance in light of September 11th.

Identity theft is a national security threat involving life and property. Safeguards will be made and I predict sooner rather than later.

Mr. Cardin.

[The prepared statement of Hon. E. Clay Shaw Jr. can be found on page 49 in the appendix.]

Mr. CARDIN. Thank you, Mr. Shaw. Let me thank both Chairman Shaw and Chairwoman Kelly for convening this joint hearing today.

This is an extremely important subject. We're working in a very bipartisan way to do everything we can to prevent identity theft.

The FBI considers identity theft to be one of the fastest-growing crimes in the United States. 350,000 cases a year.

We can do better.

The focus of today's hearing is going to spend a lot of time on the SSA's Death Master File, where it compiles the names and Social Security numbers of those individuals who have recently died.

Questions have been raised as to whether those files are as up-to-date as they need to be and whether that information is being shared, particularly with financial institutions, in the most effective way in order to reduce the amount of identity fraud.

I think there's a joint responsibility here and when the panel presents their testimony, I hope that they will deal with this. There's clearly a responsibility by SSA to have the information available so that we can prevent identity theft.

But there's also responsibility in the private sector, particularly of financial institutions, as to how they deal with identity in the use of fraudulent or false information.

Both need to work together in order to accomplish it.

The Chairmen have given us examples that should chill all of us. The fact that several of the hijackers had fraudulent SS numbers, that is something that is unacceptable. The fact that a terrorist apprehended in Britain had a Social Security number that was from a deceased person that was 10 years old is unacceptable. We can do better than that.

There is now, of course, a ring of thefts involving recently-deceased business executives. Ms. Kelly mentioned the Wendy's executive.

We need to be wiser in how we deal with the Social Security numbers and updating the data bank at the public level, sharing with the private sector, to avoid these types of crimes.

I think the questions being raised is whether we can update these Death Master Files in a more effective way, would that have prevented some of these ID thefts?

But I must at least raise some additional questions here as we go through this hearing.

We have the question that the primary purpose, the primary mission of the SSA's use of the Social Security card is to maintain earnings records and pay benefits in the case of death, retirement and disability.

I have concern about making the list more up-to-date and easier to use, could compromise individual privacy and have the unintended consequence of making it easier, rather than more difficult, for people to steal and use false SSNs.

So there are tradeoffs here.

We also have the challenge of joint accounts, where one person dies and you have another person account. If we all of a sudden freeze those assets, in a way, we may be causing unintended problems for our constituents.

So these are not easy issues.

But the bottom line is we cannot accept the number of thefts that are occurring today through the use of Social Security numbers. We need to do a better job. And we look forward to working with the people who will be here today on our panel and others so that we can effectively combat this criminal activity.

Thank you, Mr. Chairman.

Chairman SHAW. Thank you.

Mr. Weldon, do you have a statement?

Mr. WELDON. No, thank you, Mr. Chairman.

Chairman SHAW. Mr. Inslee.

Mr. INSLEE. No statement, Mr. Chairman.

Chairman SHAW. Mr. Tiberi.

Mr. TIBERI. No, thank you, Mr. Chairman.

Chairman SHAW. Ms. Hooley.

Ms. HOOLEY. Thank you, Chairman Shaw, and Chairwoman Kelly.

We've heard numerous times today identity theft is an equal opportunity crime. It affects victims of all ages, all incomes, and all ethnic backgrounds.

Ms. Kelly told us about Wendy's CEO. But more often than not, identity theft is something that affects the ordinary citizen, the person who is working hard, paying their taxes, and trying to do their best in life.

For example, a little over a year ago, a young man from Oregon named Sean Bolden, appeared before the full Banking Committee to testify about his personal nightmare with identity theft.

In Sean's case, identity thieves had opened dozens of financial accounts with his Social Security number and, as a result, at age 23, he was unable to obtain any credit whatsoever, including student loans.

And then there's the case of the little boy in Salem, Oregon, named Tyler Bales. Tyler was 16 months old when he lost his battle with a rare genetic disease called Hurler's Syndrome.

Now there's nothing more tragic than losing a child. Unfortunately, the heartache of Tyler's loss hasn't been eased for his parents.

Not only isn't it hard enough losing a 16-month-old child, but last spring, the Bales learned, courtesy of the Internal Revenue Service, that someone claimed Tyler as a dependent on their 2000 income tax return and, as a result, the Bales' income tax return was rejected.

As disturbing as that is, it gets worse.

Because of Federal disclosure issues, the IRS cannot give out the name of the identity theft to the Salem Police Department, even though identity theft is a felony offense in Oregon. The thief could live right down the street or 3000 miles away. But because of a loophole in the IRS, the Bales and the police department will never know who stole their son's personal information.

Mr. Chair, I submit that Tyler Bales and Sean Bolden are more than a name, a date of birth, or a Social Security number, and that's why I've been a strong advocate of stamping out the crime of identity theft.

In Tyler's case, I introduced H.R. 2077, the ID Theft Loophole Closure bill. It is in the Ways and Means Committee. It is a very simple bill that says the IRS, in fact, can give out the information to the local police.

I know our economy in a large degree depends on the flow of free information. However, it's imperative that we recognize that private information is just that—private—and not a salable commodity or something to be exposed by unscrupulous individuals.

Literally, this is the fastest-growing crime there is. The numbers are outrageous. And I could spend some times with numbers, but I don't want to do that. What I want to express today is this is happening more and more frequently. It's happening with people who are committing other crimes.

In Salem, the police department has said that in the last 2 years, ID theft has increased by over 38 percent and much of that is related to also methamphetamine abuse, is the motivating factor.

We need to close some of these loopholes. We need to do something with identity theft, instead of just talk about it. And I think today's hearing is a good start and I yield back my time.

Chairman SHAW. Thank you very much.

Now I'd like to introduce our first panel this morning.

We first have:

The Honorable Philip Bond, who is the Undersecretary of Technology at the United States Department of Commerce;

Jim Huse is no stranger to the subcommittees, he is the Inspector General of the Social Security Administration;

Fritz Streckewald, Acting Assistant Deputy Commissioner for Disability and Income Security Programs of the Social Security Administration;

Barbara Bovbjerg, the Director—Barbara, if I ever fail to mispronounce your name, would you please call me down on it?

[Laughter.]

Ms. BOVBJERG. It's "Bo-berg," and everyone has trouble with it.

Chairman SHAW. And it seems, as long as I've known you, I'd have gotten it right by now.

[Laughter.]

But you certainly are no stranger to the subcommittees, because you're the Director of Education, Workforce and Income Security of the General Accounting Office.

And Richard Hillman, who is the Director of the Financial Markets and Community Investment of the General Accounting Office.

Welcome to all the witnesses. We have your full statements and they'll be made a part of the record. You may proceed as you see fit.

Mr. Bond.

STATEMENT OF HON. PHILIP J. BOND, UNDER SECRETARY FOR TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Mr. BOND. Thank you, Mr. Chairman, Chairwoman Kelly, Members of both subcommittees. I want to thank you for inviting me here to address an important issue, obviously of combatting fraudulent use of Social Security numbers of decreased individuals.

The National Technical Information Service, NTIS, is a component of the Department of Commerce. It's involved in this issue because it makes available to the public the Social Security Administration's Death Master File extract.

Let me just say by way of preface that as someone who spent 7 years working in the people's house, sitting back there in the staff row, it's a special and deep honor for me to come back here and work with you in trying to work toward a solution and improvement in the system in this regard.

Obviously, September 11th has caused all of us to revisit and reassess what we're doing in every branch of Government, and certainly that is true at the Department of Commerce, where Secretary Evans has us involved deeply in that reassessment.

So I want to commend you for holding this hearing, for the leadership, and for bringing some attention to this matter. And I'm con-

fident that as the subcommittees look into this, that they'll find that technology is part of the solution.

First, very quickly, a bit about NTIS.

For over 50 years, NTIS has collected, organized and permanently preserved most of the research and technical reports of the Federal Government. There are today about 3 million information products in its permanent collection.

NTIS, I want to stress, received no appropriated funds. It is self-sustaining, basically on the sale of these largely technical manuals and reports.

Many agencies in the Federal Government work with NTIS because they know the agency has the ability to make their information products more widely available, beyond their normal constituency, and in different formats.

Clearly, it would be more expensive if all of the agencies tried to replicate this infrastructure.

A quick example. The Defense Technical Information Center provides its technical reports directly to the folks in their community. But they turn to the NTIS for the release of unclassified research to the public at large.

Similarly, the Social Security Administration distributes the Death Master File to Federal agencies, some State and local agencies, but they turn to the NTIS to make it available to others, in part because SSA does not currently have the capacity or the distribution networks.

Very quickly, my principal comments here will address what NTIS does with the files once we receive them and I'll defer to that agency on a description of the preparation of the files, other than to say that, on a quarterly basis, they do the full Master File and then monthly updates beyond that.

The Death Master File contains only basic information—Social Security number, last name, first name, date of death, date of birth, State or county of residence, zip code for the last residence, and last lump-sum payment.

Obviously, the Death Master File can be a great help for detecting erroneous or fraudulent payments.

Accordingly, SSA makes it available directly to a number of agencies that pay benefits or have other needs for this information, such as preparing statistical studies and to States which use the list to detect fraud or administrative errors, including fraudulent or erroneous food stamp payments, for example.

At the same time, SSA makes the Death Master File available to these Federal agencies, they make it available to NTIS for reproduction and distribution to others.

We receive this information on a cartridge via overnight mail and copy the information onto magnetic tape or cartridge or CD, depending on what our end-user has requested.

And I want to stress that NTIS will of course be pleased to consider other formats.

It typically takes 1 to 3 days for NTIS to complete this production process, having received the cartridge and then turning it around.

We send the file to more than one hundred subscribers, either via overnight mail or first-class mail, if that is their preference. All formats are sent out at the same time.

The turn-around time does depend in part on the size of the file, but it is not generally a function of the fact that NTIS offers it in various formats.

That is not the source of delay.

We understand that the Social Security Administration is exploring new approaches to making the file available in a more timely technological manner. These include sending the file to NTIS electronically and sending updates on a weekly, rather than monthly, basis.

Clearly, electronic transfer would certainly reduce the turn-around time. Subscribers would probably find it easier to obtain just the updates electronically rather than the massive Master File.

In any event, we are committed to working with SSA to improve the delivery of this important product.

Finally, let me express—I understand there's a desire in the financial community for a web-based search capability. That is an interesting proposal that we will certainly look at.

And again, NTIS is pleased to look at that further. If there's anything that we can or should do to expedite the process, we want to do it as soon as possible.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Philip J. Bond can be found on page 57 in the appendix.]

Chairman SHAW. Thank you, Mr. Bond.

Mr. Huse.

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

Mr. HUSE. Good morning, Mr. Chairman. Thank you for having me. Chairwoman Kelly.

While I have testified on the issue of identity theft before various committees in both the House and Senate, the issues of September 11th lend a renewed urgency to this issue.

Identity theft was already a significant problem facing law enforcement, the financial industry, and the American public before September 11th. In the weeks since that terrible day, it has become increasingly apparent that improperly obtained Social Security numbers were a factor in the terrorists' ability to assimilate themselves into our society while they planned their attacks.

While this has heightened the urgency of the need for Congress, the Social Security Administration, and my office to take additional steps to protect the integrity of the Social Security number, it has not altered the nature of the steps that must be taken.

The Social Security number, no matter how much we avoid labeling it as such, is our national identifier. As such, it is incumbent upon those of us gathered here to do all in our power to protect it and the people to whom it is issued. There are three stages at which protections must be in place: upon issuance, during the life of the number holder, and upon that individual's death.

With respect to the issuance of SSNs, or what the Social Security Administration refers to as the enumeration process, our audit and

investigative work has revealed a number of vulnerabilities and resulted in a number of recommendations.

The most critical of these recommendations centers around the authentication of documents presented by the individual applying for an SSN or a replacement Social Security card.

If we are to preserve the integrity of the SSN, birth records, immigration records, and other identification documents presented to SSA must be independently verified as authentic before an SSN is issued.

Further, if immigration records are to be relied upon, the Immigration and Naturalization Service must be required to authenticate those records.

Regrettably, this will subject the enumeration process to delays. But just as we must endure lengthy waits at airports in the name of higher security, so must we now sacrifice a degree of customer service in the name of SSN integrity.

H.R.2036, introduced by the Social Security Subcommittee, moves us closer to these protections, the importance of which cannot be overstated. If we cannot stop the improper issuance of SSNs by the Federal Government, then no degree of protection after the fact will have any significant effect.

It would merely be closing the barn door after the horse has gone.

The second and most difficult stage of protecting the SSN comes during the life of the number-holder. Because the SSN has become so integral a part of our lives, particularly with respect to financial transactions, it is difficult to give the number the degree of privacy it requires, but there are important steps we can take.

We can limit the SSN's public availability to the greatest extent practicable, without unduly limiting commerce. We can prohibit the sale of SSNs, prohibit their display on public records, and limit their use to valid transactions. And we can put in place enforcement mechanisms and stiff penalties to further discourage identity theft.

Finally, we must do more to protect the SSN after the number-holder's death. The Social Security Administration receives death information from a wide variety of sources and compiles a Death Master File, which is updated monthly and transmitted to various Federal agencies. It is also required to be offered for sale to the public and can be accessed over the internet through a number of sources, as we've already heard.

My concern under the current system is with the accuracy of the death information. Accuracy in this area is critical to SSA in the administration of its programs, to the financial services industry, and to the American people. Our audit work has revealed systemic errors in the Death Master File and we have recommended steps that SSA can take to improve the reliability of this critical data.

Among these recommendations were matching the Death Master File against auxiliary benefit records to ensure that individuals receiving benefits in one system are not listed as deceased in another, and reconciling 1.3 million deaths recorded in SSA's benefit payment files that do not appear in the Death Master File.

We are faced with striking a balance between speed and convenience, on the one hand, and accuracy and security on the other.

This is true in the case of the Death Master File, just as it is true in the enumeration process.

At all three of these stages of an SSN's existence, improvement is needed. H.R. 2036 addresses many of these concerns. The Social Security Administration, my office, the Congress, and the American people must act together to accord the SSN the protections appropriate to the power it wields.

Thank you very much.

[The prepared statement of Hon. James G. Huse, Jr. can be found on page 62 in the appendix.]

Chairman SHAW. Thank you, Mr. Huse.

Mr. Streckewald.

STATEMENT OF FRITZ STRECKEWALD, ACTING ASSISTANT DEPUTY COMMISSIONER FOR DISABILITY AND INCOME SECURITY PROGRAMS, SOCIAL SECURITY ADMINISTRATION

Mr. STRECKEWALD. Chairman Shaw, Chairwoman Kelly, Members of the subcommittees, thank you for asking me to appear before you today to discuss the Social Security Administration's collection, maintenance and distribution of death information.

We use this information for a number of important program purposes and the integrity of this information is of utmost importance to us.

SSA's Death Master File was created because of a 1980 Consent Judgement resulting from a lawsuit brought by a private citizen. Under the Freedom of Information Act, we are required to disclose the Death Master File to members of the public.

SSA obtains death reports from many sources, with 90 percent of the reports obtained from family members and funeral homes. The remainder of the information comes from States and other Federal agencies through data exchanges and reports from postal authorities and financial institutions. We match death reports of the approximately 2.5 million people who die annually against our payment records and terminate benefits for those individuals who are deceased. We annotate the deaths on our master Social Security and Supplemental Security Income beneficiary records and on the Social Security number record file for beneficiaries and nonbeneficiaries.

Since studies have shown that death reports from family members and from funeral homes are over 99 percent accurate, we do not verify these reports. For our beneficiaries, we are currently verifying reports from financial institutions and postal authorities after terminating benefits. However, we are changing our policy to verify these reports before taking any action.

Reports obtained through data exchange require verification through our field offices before an individual's death is posted to our payment records and their benefit is terminated. This includes death data received from the States.

We do not verify death reports on persons who don't receive Social Security benefits, and it would be difficult for us to do so since we do not have addresses or other identifying information on these individuals.

The Death Master File is updated daily based upon reports SSA receives and contains approximately 70 million records, including

Social Security beneficiaries and non-beneficiaries, with verified and unverified reports of death.

If available, the file contains the deceased's SSN, first name, middle name, surname, date of death, date of birth, State, county, zip code of the last address on our records, and the zip code of the lump-sum death payment. The record is also annotated to indicate where the report was verified.

Federal agencies, State and local government, and the private sector use the national death data file, and we are reimbursed for the cost of providing this information. Currently, as required by law, SSA shares the full Death Master File with Federal benefit-paying agencies that use the data to conduct matches against their own beneficiary rolls, such as the Department of Defense and the Office of Personnel Management.

Under the matching agreement with SSA, these agencies are required to independently verify the fact of death before taking any adverse action.

The publicly available Death Master File is provided monthly to the Department of Commerce, National Technical Information Service, or NTIS, which in turn makes it available to the public under the Freedom of Information Act. NTIS distributes it to subscribers by either tape file or CD-ROM version. Some of these private companies, including genealogical publishing companies, create their own files from the Death Master File. Some private websites have these files on line.

In response to issues raised by the subcommittee Members, we are exploring electronically transmitting our Death Master File to the NTIS, rather than sending them through Federal Express.

We are prepared to do that immediately, as soon as NTIS is ready to receive it. Transmitting the data more frequently is also possible, perhaps on a weekly or bi-weekly basis.

SSA also has an electronic data exchange of all States and a large number of Federal agencies. This is an electronic overnight query process that enables requesters to enter a query for any individual. Using this process, State agencies can access our death records so they can ensure that benefits are not paid to deceased individuals.

Finally, I'd like to briefly mention recent initiatives to strengthen the enumeration process.

In response to the events of September 11th and the indication that some terrorists had Social Security numbers and cards, some of which may have been fraudulently obtained, SSA formed a high-level response team to re-examine the enumeration process.

The response team, which includes representatives of SSA's Office of the Inspector General, will help determine what changes need to be made to ensure that we are taking all necessary precautions to prevent those of criminal intent from using Social Security numbers and cards to advance their operations.

Thank you again for the opportunity to discuss with your committees how SSA gathers and distributes death information.

I will be glad to answer any questions.

[The prepared statement of Fritz Streckewald can be found on page 73 in the appendix.]

Chairman SHAW. Thank you.

Mrs. Bovbjerg.

STATEMENT OF BARBARA D. BOVBJERG, DIRECTOR, EDUCATION, WORKFORCE AND INCOME SECURITY ISSUES; AND RICHARD J. HILLMAN, DIRECTOR, FINANCIAL MARKETS AND COMMUNITY INVESTMENT ISSUES, GENERAL ACCOUNTING OFFICE

Ms. BOVBJERG. Thank you, Mr. Chairman, Members of the subcommittees.

I'm really pleased to be here before the subcommittee again and to meet a new subcommittee to me, with my colleague, Richard Hillman, to discuss the distribution of death information to financial institutions.

As we've heard, the Social Security Administration collects and records the names and Social Security numbers of the more than two million Americans who die each year. This information is critical to the integrity of the Federal benefit system.

Properly used and distributed, death information can also help prevent the fraudulent use of Social Security numbers to steal identities, to obtain false identification documents, and to commit financial fraud.

In light of the recent terrorist attacks, it is more important than ever to safeguard Social Security numbers from criminal use.

Accordingly, our testimony today addresses three points. First, how death information is collected and distributed and how long this takes. Second, how the financial services industry uses such information. And third, possible steps to improve timeliness of distribution.

Our observations are based on prior GAO work, preliminary work at the SSA and the National Technical Information Service, and our discussions with financial services institutions.

First, let me describe the collection and distribution process.

As we've heard, SSA receives about 90 percent of its death information from funeral homes and relatives of the deceased, and most of this information reaches SSA within a week of death. SSA takes another week to process the information and add it to individual Social Security records.

At the beginning of each month, SSA extracts this death information from its records to the Death Master File, and sends it to the NTIS. NTIS receives this information by the fourth or fifth day of each month and mails it to subscribers on tape or on CD-ROM within another 2 to 4 days.

Overall, most death information reaches these subscribers within 1 to 2 months of death, depending on when the death notice first reaches Social Security.

The remaining ten percent of death information comes to SSA from other Federal agencies that learn of deaths through data matches or undelivered benefit checks and from State vital statistics bureaus. However, these death reports are less timely than those sent directly from families and funeral directors to SSA, and require verification by SSA before they can be added to the Master File and distributed.

Death information may not reach SSA from State reports until 3 to 4 months after the date of death and is not available to private subscribers.

Let me now turn to how financial services institutions use this information.

Representatives of such institutions told us they did not use a formal process or a central data source to identify deceased customers, although most receive death information either from family members or, in the case of Social Security beneficiaries with direct deposit, from SSA directly.

However, most also told us that they subscribe to fraud prevention products or services offered by credit reporting agencies for evaluating new credit applications. All three credit reporting agencies subscribe to the Master File and make this information available to their customers through these proprietary fraud prevention products.

Most institutions we contacted expressed an interest in receiving timely death information with frequent updates. Some of these institutions were aware of the Master File, but unfamiliar with the information they provide, or of the ability to subscribe, while others were not aware of it at all.

Finally, let me turn to possible steps for improving the distribution and use of death information.

As you've heard, SSA is exploring ways to speed up this process and has stated that it would be relatively easy to produce updates on a weekly, rather than a monthly, basis. SSA and NTIS officials have stated that it should also be possible for SSA to transmit updates to NTIS electronically and that NTIS could transmit the information to subscribers electronically as well.

SSA is also piloting the electronic death registration system, which would enable States to collect and report deaths electronically to SSA, both streamlining and centralizing the collection reporting of such information.

However, existing restrictions on distribution of State-provided data could complicate adoption of such an approach.

In conclusion, most death information is available to the public within 2 months and improvements to the collection and transmission processes could make this information more complete and more timely. Educating the financial services industry about the availability and contents of the Master File would also be helpful.

Such measures are tangible steps that could act to narrow the window of time in which a criminal can open new accounts using a deceased person's identity and would raise the likelihood that such behavior would be detected.

However, improving the use and timeliness of death information will not by itself eliminate identity theft and is not a panacea for addressing the larger issue of criminal misuse of Social Security numbers.

That concludes my statement, Madam Chairwoman. Mr. Hillman and I would be happy to answer any questions you have.

Chairwoman KELLY. Thank you very much.

Mr. Hillman, have you a statement, or is yours the same? It's a joint statement?

Mr. HILLMAN. Yes, Madam Chairwoman.

[The prepared joint statement of Barbara D. Bovbjerg and Richard J. Hillman can be found on page 87 in the appendix.]

Chairwoman KELLY. All right. Thank you very much.

I appreciate you all indulging us up here as some of us are leaving to vote. This way, we can keep the hearing going without keeping you all in your seats for too long a period of time. I'm going to open the questioning.

Mr. Streckewald, I have a question for you. Actually, I have a couple of questions for you.

On page 6, in your testimony, you describe the State verification and exchange system that allows some States and some Federal agencies to verify a death within one day. Have you considered whether to open it to access by the financial services industry?

Mr. STRECKEWALD. We use that for, as you said, the State governments. We have, as far as I know, not looked into using it for financial institutions.

We do have the ability for employers to verify Social Security numbers in a batch mode, which is like an overnight type of mode as well. And so, employers can send us batches or individual Social Security numbers, so that we can verify for them.

I'm not aware that we have specifically looked at the financial services' access to the information.

Chairwoman KELLY. I think that looks like the basis for a system that's needed by the financial institutions, so that they could do rapid verification.

Since the Patriot Act requires them to verify the identity of any new account-holder, I don't understand why the SSA can't commit to allowing that system to be used as part of verification procedures.

Mr. STRECKEWALD. We can certainly take a look at that and get back to the subcommittees on what we find.

[The information referred to can be found on page 82 in the appendix.]

Chairwoman KELLY. I wish you would, please. And to that effect, I'm going to send a letter to the Secretary of the Treasury with that recommendation to put into their regulations, because I think that that's a way of rapidly helping our financial institutions.

I also wondered if the SSA and the NTIS had ever collaborated on a study to determine a faster means of getting the information to the financial services industry, including this one, and including sending it electronically or even perhaps, that difficult word, contracting out the entire process, from extraction to dissemination.

Mr. STRECKEWALD. I think with recent events, we've come to the conclusion with NTIS that we do need to get this information to them quicker and that they need to be able to distribute it quicker.

I think what remains to be worked out is just the details of that. It's certainly technologically feasible and as we've heard this morning, it seems like both agencies are willing to move to perhaps a weekly or biweekly update of the information and to transmit electronically rather than through overnight mail.

Chairwoman KELLY. That I read in the testimony. My question is, I really want to know how rapidly you're doing that, but also there's another piece of this.

There's a victim. I had my credit card stolen. I think there's a lot of people who have had things like that go on. I want to know with regard to the Social Security number what you're doing to help the victims who have their identity stolen, or the families of victims.

Mr. STRECKEWALD. We have a series of actions that kick into place when we hear about this type of event. First of all, we refer them to the inspector general hotline because it's perhaps a criminal event that needs to be investigated.

But we also work very closely with the person. We give them pamphlets that explain who they can contact. We give them referrals to some of the national financial services organizations so they can clarify and correct their credit ratings.

So we do have procedures in place for referrals to hotlines and other services that can help correct the problem.

Chairwoman KELLY. It's been my experience in working with those that they are not terribly rapid. It takes a while. And it takes going through several people to get it done.

I'm going to ask you this, Mr. Bond, and I would like you both to answer both those questions, the prior question and this one.

What's the possibility of allowing people to do this kind of thing, to do it perhaps electronically with something as a follow-up that would be a verification.

Mr. BOND. I'm sorry? Just to understand, a verification of the receipt of the information or a verification of falsely secured numbers?

Chairwoman KELLY. I'm extending this to the people who are the victims of identity theft from the Social Security Administration numbers.

Those people would have to, when you have that happen, if it's in your family, you have to deal with a lot of different people. What's the electronic possibilities of letting people do that electronically, deal with people and do it rapidly, rather than having to make a lot of telephone calls?

Mr. HUSE. If I may be permitted, Chairwoman Kelly.

Chairwoman KELLY. By all means.

Mr. HUSE. The Federal Trade Commission and our office of the inspector general have a reciprocal information exchange that going forward will only get better. But in the last 2 years, has rapidly improved the transmission of victim information so that it gets to the credit-reporting bureaus better than it used to.

Can it be improved? Yes. Like many other things in Government, it is based on this application of resources and we're certainly changing our approach to the amount of resources we apply to this as this crisis has developed over the last 5 years.

But that's the way it's done. It's better today, and does use, by the way, e-mail and electronic transmission, if victims have that available to them, to get the information to us.

From that clearinghouse, then, this information becomes available to local, county and State law enforcement.

Again, I'm not trying to paint a rosy picture here, but at least we have the dots on the paper and we're connecting them a little bit better than we used to.

Chairwoman KELLY. What's the timeline on that?

Mr. HUSE. It all depends on the application of resources. We work in our budget submission process to try and gain those to do this.

The technology is already there. It really is a matter of adjusting IT resources and the human capital that you need to make this happen.

We're just learning that this is an issue that the people care about a great deal.

Mr. BOND. Madam Chairwoman, if I could add to that, too.

Technologically, of course, there's no reason you can't expedite things via the internet and secure communications and so forth. It really becomes part of a very fundamental e-government initiative that both the Congress and the Administration have to join hands on.

The Administration has sent up an aggressive proposal in that regard and appointed people at OMB to oversee it, to try to really push the agencies more toward quicker, more rapid response for our shared constituents.

But it's going to be a very fundamental effort to apply technology to the service of constituents.

Chairwoman KELLY. What's your timeline?

Mr. BOND. There is a multi-year plan out of OMB which does require some significant funding here on the Hill. And that will be one of the many issues in final appropriations discussions for this year because the request was not fully funded coming out of the two chambers.

Chairwoman KELLY. So it's a matter of appropriated funds from Congress.

Is that correct?

Mr. BOND. Absolutely, to upgrade the IT capabilities in many of the Federal agencies.

Mr. STRECKEWALD. If I could, I would reinforce Mr. Bond's comments that the Federal Government as a whole, through the leadership of OMB and through individual agencies' initiatives, is looking at customer-oriented electronic services.

In some ways, SSA has been providing this with our online applications. But this particular example that you're using, which is to help people correct identity theft problems, would have to be a broad spectrum of stakeholders, financial services, Government agencies, States, would have to come together and plan this out and construct the communications lines and the procedures for solving this.

But it is technologically feasible and OMB is trying to lead us to a more electronically-focused, customer-oriented Government.

Chairwoman KELLY. Mr. Huse.

Mr. HUSE. One more thought on all of this.

I think we understand now, with this identity fraud crisis issue and victim assistance as a key part of it, we've learned a lot the last few years that our traditional approaches to this just don't cut it. They don't work.

We have advanced a proposal in the budget process for innovative ways to change this model, so that law enforcement, Federal law enforcement integrates itself better with local law enforcement

because it's a total issue. It just can't be relegated to the Federal Government or a burden on local governments.

And this model means non-traditional approaches. The key to it is rapid and effective information exchange. The work is there and the ideas are there.

In fact, some of this is in 2036. Some of the pieces that we need to get this done is in 2036. But I really want to assure you, Madam Chairwoman, that we are committed to trying to do this.

But, as I said, as in everything in Government, it is resource-dependent.

Chairwoman KELLY. Most people who come before these subcommittees ask for resources. That's not a surprise.

Mr. HUSE. No.

Chairwoman KELLY. But we're essentially in a terrorist war situation.

One of the things that America has always had is ingenuity. This may be the time to do more with less. And I'm not saying that you can't get the resources. What I'm simply saying is that we have a limited budget. We all know that. And ingenuity is going to have to be the order of the day for all of us.

This may be the time, when you need to have that larger meeting, discuss how it's going to go and do it sooner rather than later, so you can get help from the financial institutions as well as from anyone else who is an interested stakeholder in this.

I want to ask the GAO, since there's no one else who has come back from the vote yet, I want to ask you, Barbara, if you don't mind, have you considered whether the Social Security Administration can open the State verification and exchange system to the financial services industry to allow the companies to verify?

Is that something that you've thought about?

Ms. BOVBJERG. GAO has done a lot of work on data sharing and the importance, on the one hand, of sharing information that allows you to safeguard benefits and safeguard identity and, on the other hand, being concerned about privacy and retention of personal information.

The death records are already public information, at least for the most part. What remains to be worked out with the States is this question of State restrictions on information that they provide that is not verified by SSA. That seems to be one of the sticking points. And we do hear about a resource question.

I think we have been interested and have asked about the feasibility of doing some sort of online look-up, web-based approach that financial institutions could go to directly. And we're not in a position to make any recommendations. We would have to look at the cost versus benefits. But we thought that that might show promise.

Chairwoman KELLY. Perhaps we should ask for a cost/benefit analysis of something like that.

Ms. BOVBJERG. Well, may I add something?

Chairwoman KELLY. Yes.

Ms. BOVBJERG. Excuse me, Ms. Chairwoman.

We are doing some work that I wanted to call to your attention for Congressman Johnson on the Social Security Subcommittee that looks at law enforcement and identity theft across governments.

And one of the questions that he has us addressing is looking at the lead Federal and State law enforcement agencies with responsibilities in identity theft investigation and looking at how they cooperate across jurisdiction, including across Federal agencies.

I'm not sure when that work will be published. That's being done in another team. But I think that that will help get at some of the issues that have been raised this morning.

Chairwoman KELLY. Thank you, and thank you for volunteering that.

What exposure did you find that financial institutions have? If a name is in the Master File and the institution processes a payment any way?

Mr. Hillman, do you want to answer that?

Mr. HILLMAN. I'm not exactly sure what the exposure may be to a financial institution who processes information and maybe provides funds out to an individual of a deceased person.

But we could find that out for you and let you know.

Chairwoman KELLY. I would appreciate your taking a look at that because that goes to the next question. And that is whether or not—I'm trying to get the acronym here—the FFIEC, the exam procedures, perhaps should take that into account.

I don't know if it does or not, but I think it's worth taking a look at.

I'm concerned also with the education of financial institutions with regard to what their exposure is and the appropriate usage of the Death Master File.

So perhaps you could take a look at look at that also.

Mr. HILLMAN. We'd be happy to do that. We have looked at the examination procedures, as you might expect, that financial Federal regulators follow in looking at the financial services industry.

And in general, those examination procedures look to the safety and soundness of those depository institutions to ensure that they have sufficient funds to conduct their businesses.

They haven't in all cases looked at other important areas such as concerns with individuals or constituents. And I agree with you that that would be an important topic to further study.

Chairwoman KELLY. Thank you very much.

Mr. Brady, do you have any questions?

Mr. BRADY. Thank you, Madam Chairwoman. I'm sorry I missed the last part of the testimony. But, obviously, to solve this problem will take a combination of prevention and enforcement in the process.

We need to do all we can in prevention of identity theft. But I think what everyone understands is that, in this open society, it will be difficult to close that barn door completely, in this open, information-based society.

So focusing a bit on the enforcement and the punishment side of it, what are the chances someone engaging in identity theft is going to get caught? What are the consequences in real life when they do?

Who's the best responsible and available to do that, State or Federal Government? What role can the business community play in catching them?

And the bottom line, what would it take to make the consequences harsher to be a real deterrent to people engaging in it? And I'll open it up to anyone who's got an opinion.

Mr. HUSE. I'll take the first cut at an answer, Mr. Brady.

Mr. BRADY. All right.

Mr. HUSE. We don't do a great job from a criminal justice perspective with identity thieves because it's a relatively new crime.

We have a mixed result if you look across the Federal judicial system in terms of sentencing on these crimes. We need to do better.

One of the outreach efforts I think we need to make now with the post–9/11 consciousness that we have is to educate United States attorneys to the fact that these crimes need to be a priority concern in each of the 94 judicial districts.

That may or may not be the case depending upon where you are in the United States. Other trendier crimes get priority.

Most States have very vigorous and good identity crime statutes themselves. So we need to cooperate more with local and State law enforcement to prosecute there where we can.

Clearly, though, the key to identity fraud because it transcends all boundaries is there has to be a better information-sharing mechanism. And the Congress, when it passed the Identity Theft Deterrence Act several years ago, an Assumption Deterrence Act several years ago, and established the clearing house in the FTC, I assure you that that is working and will only get better as we engage it more.

So that's my first try at an answer.

Mr. STRECKEWALD. If I could just elaborate a little bit. That particular law that was passed in 1998, which for the first time made it a Federal crime to fraudulently obtain identification, sell identification, or misrepresent yourself on obtaining any type of identification.

And for the first time, the Social Security number was included as a means of identification. So that did provide law enforcement with an added tool for enforcement.

Mr. BRADY. How many prosecutions have there been?

Mr. HUSE. We can get that for you and follow that up. One thing I want to add, Mr. Brady, is one of the provisions of 2036, if it's passed, gives us some great civil money penalty tools.

Also, for those identity crimes that fall maybe under the prosecutorial thresholds in a given judicial district, but still have a fact pattern that supports an offense, we can sting those people with some money penalties, and I think that's a good thing, too.

Mr. BRADY. In real life, what are the consequences for getting caught? What's an average sentence, punishment, for identity theft?

Mr. HUSE. Well, with sentencing guidelines, probably for a first offender, it is several years of confinement. It depends on the criminal history involved.

Mr. BRADY. Sure.

Mr. HUSE. But it's a 10-year felony, the misuse is a basic Federal felony.

Mr. BRADY. Is there a feel for what first-time, second-time offenders, what they traditionally get? I'm not pushing. I'm just curious.

We all know what guidelines are. We all know what happens in real life.

Mr. HUSE. As I said, it's confinement for several years. It hasn't reached the point, even though the violation is just as bad, of having, for example, the emotion involved of a bank robbery or something like that. But it's just as pernicious.

Mr. BRADY. What role—can I keep, while I'm on a roll?

Two questions, really. How can Washington help? Is it to create more resources here at the Federal level, or to complement better State prosecution efforts?

Second, what role can the business community play in helping us catch and enforce this?

Mr. HUSE. I'll let Barbara answer that.

Ms. BOVBJERG. I'll step into the breech.

We have talked in GAO about the need for both prevention and for law enforcement. One of the things that we're doing right now at the request of Chairman Shaw is looking at uses in Government at all levels—Federal agencies, various departments in State government, local government, and the courts, looking at uses of the number and looking at how the number is being safeguarded and developing options that could be considered for safeguarding.

So my answer to your question is more in a prevention side and working with SSA as they try to have the balance of making information available, but at the same time safeguarding it.

That's always an issue with some of these web-based——

Mr. BRADY. And clearly, we need to do both. I'm not discounting either. I was just focusing on that side because I'm not as aware of it.

And second, it just seems, when you look at the number of people who have been hurt by identity theft and fraud, the average time it takes to try and clear their name, the costs to them, and then on September 11th, we had people who stole identities and then stole thousands of people's lives as a result of it.

So the obvious question is, what can we do to punish them to the fullest extent, or to deter the next person who has that in mind?

That was my focus.

Ms. BOVBJERG. And then I turn it over to the law enforcement end of the table.

Mr. HUSE. Well, I just wanted to take the piece of the question, is it all about resources? And that goes to Chairwoman Kelly's earlier comment.

It doesn't necessarily just mean resources, although some modest adjustments are needed here and there because you're short some capacity.

But basically, the key to this is rethinking this particular crime top to bottom, and rethinking how we focus on this crime.

We're trying to apply an old model to this that just doesn't work. If we could just understand how serious it is, that's a big, huge step, and then work with ways to, using the magnificent technology that we have, to communicate better.

I think that's really the answer, rather than some new agency or the like.

Mr. BRADY. Thank you. Thank you all very much.

Chairman SHAW. Before I go to Ms. Hooley, I do have a question for you, Mr. Huse.

Does the law distinguish in the case of identity theft between a living person's identity who has been stolen or a deceased person?

Mr. HUSE. I don't believe it does. I think the law deals with the identity theft. I do know that a deceased person has no rights because they're not here to have them. But in terms of the identity theft, it still stays the same under the law.

Again, my staff——

Mr. BOND. I want to add, my understanding on that is that an individual under law is considered to be a living individual. And so the rights do not extend to the deceased.

So when you talk about privacy laws, those are applied to living individuals and that is a fine point that I think some of the Executive agency lawyers would want to talk to the committee staff about in doing forward on your legislation.

Chairman SHAW. OK. If that answer needs sharpening up, let us know.

Mr. BOND. OK.

Chairman SHAW. Ms. Hooley.

Ms. HOOLEY. Thank you, Mr. Chair.

In the case of Tyler Bales, you could not give the information to local law enforcement agencies, even though identity theft is a crime in Oregon.

So I want to know, do we need to as a body fix that?

Mr. HUSE. Congresswoman, when you were speaking, I jotted down on a card that case and I passed it back to our chief investigator and I said, we should look at this case.

I don't know why under the IRS rules they didn't disclose. And that may be some arcane rule. I mean, they're governed by rules. We are at Social Security.

But, usually, I'd like to see if there wasn't a way that the Social Security Administration might not be able to work with that case and take it forward.

And I'm not criticizing IRS. I'm just not sure.

Ms. HOOLEY. What I'm looking for is if we can do that, in the case of Oregon where identity theft is a crime.

Mr. HUSE. Right.

Ms. HOOLEY. And I'm just trying to figure out, do we need to fix it or if it's some rule that can be fixed.

Mr. HUSE. That's why I'd like to look at that.

Ms. HOOLEY. OK.

Mr. HUSE. And we'd be glad to talk to your staff about that and look into that case and then get back to you, if that's OK.

Ms. HOOLEY. OK. I have a couple of other questions.

The Death Master File, it contains everything that a thief would need to get up and running. It's now being transmitted, I understand, to 104 customers, up from about 51 in 1999.

Is that correct?

Mr. BOND. Yes, that's about right.

Ms. HOOLEY. And all of the customers are paying for the information.

Mr. BOND. Correct.

Ms. HOOLEY. And do they use it for the purpose to flag financial holdings of the deceased individuals or is the information being used for other purposes? And if so, what are the other purposes?

Mr. BOND. It is a wide variety of purposes, from security to checking for fraud, obviously. I'm just flipping through here to try to see, because I had asked that question myself. Having just been sworn in on October 30th, I'm trying to find out everything I can quickly.

Ms. HOOLEY. I think sort of the irony of this thing is——

Mr. BOND. There are a couple of things that you need to know about. One is just the private genealogy sites that people talked about. That is one that is used, that you can go to. I did my own search and found that the Jasper County Public Library in Indiana has got the full Death Master File available there.

So there's a variety of uses out there.

But the private sector is checking mostly for fraud in financial transactions.

Ms. HOOLEY. I guess sort of for me the irony is that the Internal Revenue Service can't pass the information on to law enforcement, but they can sell it to other organizations to be used.

And I just have a bit of a problem with that. Should I?

Mr. HUSE. I don't think any of us here are tax experts. We won't even go near there.

Mr. BOND. All I can add is that by the time it gets to NTIS, it is, as was explained, considered subject to the FOIA laws, and so it's out there.

Mr. STRECKEWALD. I have a little more information on the uses of that, at least in terms of the customers.

About 20 percent of the purchasers of the Death Master File are public sector groups. Some colleges use it, perhaps for research or checking against their databases of students. In addition, several private insurance companies use it extensively, along with a few banks.

But there are not a lot of financial institutions on the list.

Mr. BOND. Here's the actual breakdown from NTIS, Congresswoman. It's 20 percent State and local, 20 percent information brokers, 15 percent insurance companies. Medical and cancer research organizations make up 15 percent. Security providers, five. Marketing companies, around five percent. Credit reporting bureaus and agencies, five percent. Pension funds, five percent. Banks and financial institutions, three. And genealogy, three.

Ms. HOOLEY. Thank you. Thank you and I yield back my time.

Chairman SHAW. Thank you.

I want to pursue the question of Ms. Hooley. I want to know, those death files, when they're put out, the Social Security numbers are on them. And I guess they're readily obtainable.

We know from experience and testimony before these subcommittees that they still have value to those that would attempt identity theft.

At the hearing that we had last week, we found that those numbers do survive the decedent and have a real purpose in State tax returns and things of this nature as an identifier.

And we also found that the numbers stay exactly the same. There's no D for decedent or something put after the number. So

those numbers are still out there and for the layman looking at it, wouldn't know whether that was a decedent or somebody who was very much alive.

What is the suggestion—and I open this to any member of the panel, that any of you might have—with how we could safeguard those numbers and yet, release them for legitimate purposes?

Obviously, insurance companies need them and some public officials need them—public agencies need them, rather.

Are there any thoughts on that?

Mr. STRECKEWALD. Yes. Let me see if I can give a couple thoughts on that.

I think it goes to the whole purpose of the Death Master File. Originally, it was a court settlement that required us to do this under the Freedom of Information Act law. But we sell the Death Master File for commercial purposes through NTIS, so that those with a reason to know individuals' Social Security numbers will know which numbers belong to deceased individuals. If a number comes through their system and it matches up with a number on the Death Master File, there's a problem.

So, in fact, the number is flagged. It is annotated when you compare it against our Death Master File.

If the Death Master File is not used extensively, then, of course, people won't have awareness of it.

So, on the one hand, if it's out there, anybody can use it and try to take a number from it and create an identity or use it to apply for a credit card. But if the financial services and insurance companies and others make greater use of the Death Master File, then they'll know which numbers belong to deceased individuals.

Chairman SHAW. How can we safeguard that, those lists being misused?

We have to assume that if they're out there, they're being marketed, that they are available to the bad guys.

Mr. STRECKEWALD. From Social Security's perspective, if a person uses a Social Security fraudulently to work—sometimes numbers are used fraudulently for working—if earnings are reported on that number the year after the real number-holder dies, then we automatically investigate because we know that number belongs to a person who is shown as deceased on our records.

We issue an alert to the field office and they call the employer and ask who is this person that's giving these wages under this number. On our records, it shows that the number belongs to deceased individuals.

So, again, from the original purposes, earnings recordation, we do track back and see if it belongs to a dead person and if so, why are earnings being recorded.

Chairman SHAW. It takes a year. You know the person is dead, money is coming in, it is going into his account. Why wouldn't it be kicked out in the first——

Mr. STRECKEWALD. Well, if a person works in January, February and dies in March, those earnings are reported to us after the end of the year. So we know that we haven't heard from the IRS yet until the year is over.

The next year, if we receive earnings from that person, that's suspicious and that triggers an alert.

Chairman SHAW. Yes, that would be suspicious. How do we handle death in foreign countries? Someone has retired in a foreign country, their money is being electronically transferred to a bank down in Mexico. How is that dealt with?

Mr. STRECKEWALD. I believe that we receive from embassies lists of deceased beneficiaries in foreign countries—they have Social Security numbers—so we would annotate our records and we would terminate their benefits.

Chairman SHAW. How do the embassies accumulate that? Now here, the funeral home turns them in. The death record is required on that.

So where is it in countries that don't have that process in place?

Mr. HUSE. To get to a bottom line here, it's not a perfect system and it's totally dependent on cooperation in those countries to give that information back to the benefit officers that we have in foreign stations.

So what happens is, periodically, the agency does send out a survey team based on ages of beneficiaries—I think they set the number in the 1990s, but they're take a look to see if those people are still alive in the foreign population areas.

And those are done on a cycle basis by the international operations.

Mr. STRECKEWALD. It's the international operations. And in fact, for countries that are considered to be high risk, such as Yemen, they send a team out there.

Not only do they look at the elderly people, they ask to see in person every beneficiary in Yemen. That's one example. But we also go to the Philippines regularly and other countries.

Chairman SHAW. Would it help if we actually sent checks to foreign countries that required signatures, or is the expense of doing that more than the savings on electronic transfer?

Mr. STRECKEWALD. I think we'd have to take a look at that and get back to you. I'm not sure. It certainly would be an issue.

[The information referred to can be found on page 83 in the appendix.]

Chairman SHAW. And actually ask for an endorsement on the check. I think people would be a little less likely to endorse or forge somebody's name than they would be to just simply let the thing slide and let the money continue to accumulate in the bank account.

That's my off-hand opinion.

Anyway, any further questions? The gentleman from Wisconsin?

Mr. RYAN. No questions.

Chairman SHAW. OK. Well, at this point, I turn the gavel over to Ms. Kelly, who will preside over the next panel.

Chairwoman KELLY. Let me make the introductions of the second panel.

We have: Mr. Stuart Pratt, Vice President for Government Relations, Associated Credit Bureaus;

Tom Lehner, Executive Vice President for Government Affairs, American Financial Services Association;

Tom Sadaka, Special Counsel, Office of Statewide Prosecution, Orlando, Florida. We welcome you, Mr. Sadaka. Am I pronouncing that correctly?

Mr. SADAKA. Sadaka.

Chairwoman KELLY. John Dugan, Covington & Burling, representing the Financial Services Coordinating Council.

Mark Rotenberg, Executive Director, Electronic Privacy Information Center.

And Evan Hendricks, Editor and Publisher of *Privacy Times*.

We welcome you all. We look forward to your testimony. And I'd like to advise all Members and witnesses, I intend to keep to the 5-minute rule. So I'm going to remind witnesses when they have a minute remaining. Please check the clock.

I will also ask unanimous consent that all Members' questions be included in the record. I'd like to begin with you, Mr. Pratt.

STATEMENT OF STUART K. PRATT, VICE PRESIDENT FOR GOVERNMENT RELATIONS, ASSOCIATED CREDIT BUREAUS, INC.

Mr. PRATT. Thank you both very much for this opportunity to appear before this joint hearing today.

For the record, my name is Stuart Pratt and I am the Vice President of Government Relations for the Associated Credit Bureaus.

By way of background, the ACB, as we're commonly known, represents more than 500 consumer information companies and produce a wide range of products, including fraud prevention, risk management, credit reports, mortgage reports, tenant employment screening services, check fraud, and verification services.

And so the subject matter here today is obviously very relevant to us and all of our members.

I think it's clear, perhaps more than ever before, that how we authenticate, how we verify, and how we ensure the authenticity of information in various types of applications is an essential need in this country. Unfortunately, I think we've learned that for all of the wrong reasons.

But at the core of this need is also the availability of information to be used and deployed in the authentication of application processes. And at the core of all of that, in many cases still, is the need for the availability of the Social Security number, which plays a particularly important role in our ability and our members' ability to build authentication and fraud prevention products, which then in turn allow us to mediate disparate sets of information and bring them back together in order to partner with our financial services customer bases, insurance and so on, in ensuring that they are, in fact, opening up lines of credit, depository accounts and so on, for legitimate individuals and for legitimate purposes.

I want to applaud your subcommittee, of course, and the Congress as a whole for the enactment of the USA Patriot Act and the very fact that this Act itself recognizes the need to have a robust system of authentication, and in turn specifically directs the Secretary of the Treasury to establish minimum standards for financial institutions to verify account applicant information.

I think, further, Chairman Shaw, in your hearing last week, we heard additional challenges in terms of even the enumeration process, how do we authenticate and verify information about individuals who are making applications for Social Security numbers.

And in fact, I think we heard information in your hearing last week about the challenges even the States will face on a go-forward

basis in authenticating and verifying individuals who make applications for something as simple, but as consequential, as a driver's license.

So it's a changed world in which we live.

The ACB was asked to address some questions or some areas in our testimony and I thought I would attempt to do that very quickly. And then of course we can amplify on that in questions and answers that you may have.

You first asked how we, as consumer-reporting agencies, use the Social Security Administration's Death Master File. And let me start by discussing something about the scope of the industry that we represent.

Our three major credit reporting system members—Equifax, Experian, and TransUnion—each maintain databases of approximately 200 million files on credit-active consumers in this country.

In addition to that, members such as E-funds and Dole & Media, maintain Nationwide systems as well that help prevent checking account fraud and check fraud at the point of sale and further.

In fact, we estimate, easily, that more than a billion consumer reports are sold every year in this country. And those consumer reports can carry forward and do carry forward in most cases a notification where there is a Death Master File record that we have been able to obtain.

There are many members within our association who are, in fact, on that subscriber list. And I thought I would clarify one point that I think was lost perhaps in the previous round of testimony.

And that is that, when we say there were not many financial institutions on that listing of subscribers, that's in part, because the channel of distribution through which the DMF data is made available to a majority of the financial institution market place is through companies like the ones that we represent here with the ACB.

You've asked about technical problems with the current system and I think a lot of that has been covered in previous testimony. I think our members are also encouraged by the fact that there may be new and different technologies that could be brought to bear. There could be greater efficiencies achieved.

And I think those are the right questions and I think we'll have to work toward achieving the right answers.

Regarding other means of obtaining information, really, the only other way that the Associated Credit Bureau's members would be aware of an individual having died is through notifications that come through the systems directly from credit lenders.

When a credit lender is notified through a trustee of an estate, they in turn will notify through coding back to us the fact that that consumer's credit account is now associated with a deceased individual. And that would be a code that would then be included in a statement that would be included and referenced on that account in subsequent credit reports issued on that individual.

You've asked about outlining ways in which sources of information can be better integrated. And let me just say that today, integration is something that we achieve through the systems that we have.

Unfortunately, I do want to state that the FTC's rules under GLB restrain us significantly in terms of building fraud prevention products outside of the Gramm-Leach-Bliley Act or the Fair Credit Reporting Act.

And let me close by making just a couple of announcements. I see I'm slowly losing time here.

Chairwoman KELLY. Mr. Pratt, you've lost time.

[Laughter.]

So if you could sum up, that would be great.

Mr. PRATT. Two announcements. Number one, we've asked all of our DMF subscriber members of the Associated Credit Bureaus to convert to monthly receipt. All members will convert to monthly subscriptions with the DMF Master File, which I think will help escalate and help make information available.

And number two, our members have established and will work with a task force to work with the Social Security Administration in working through technology and legal issues that might be associated with escalating availability of information from the Administration.

[The prepared statement of Stuart K. Pratt can be found on page 100 in the appendix.]

Chairwoman KELLY. Thank you very much, Mr. Pratt.

We move now to Mr. Lehner.

STATEMENT OF THOMAS J. LEHNER, EXECUTIVE VICE PRESIDENT FOR GOVERNMENT AFFAIRS, AMERICAN FINANCIAL SERVICES ASSOCIATION

Mr. LEHNER. Thank you, Chairwoman Kelly, Chairman Shaw, Members of the subcommittees. Thank you for inviting me to testify today.

I'm Tom Lehner. I'm the executive vice president of the American Financial Services Association. AFSA is the leading trade association for market-funded financial services companies.

Our 400 member companies include consumer and commercial finance companies, auto finance/leasing companies, mortgage lenders, credit card issuers, and industry suppliers.

I'm here to address the issue of identify theft using Social Security numbers and, specifically, the industry's use of the Social Security Administration's Death Master File.

Social Security numbers are the most unique identifier of individuals in the United States. The financial services industry uses these identifiers for a variety of reasons, such as customer verification, credit checks, bankruptcy filings, and monetary judgments such as tax liens.

The use of Social Security numbers is not generally secure. They are readily available and, indeed, used by companies, State and local governments, motor vehicle departments, colleges, and even by consumers who willingly print the numbers on the face of their checks.

Thieves often steal Social Security numbers and ultimately the identity of individuals, both living and dead. Financial institutions such as credit card companies and banks have also incurred significant losses resulting from misuse of Social Security numbers.

Consumers have also experienced monetary losses, impaired credit and legal problems because others have amassed debts using their identities.

Financial firms have an obvious interest in making sure that individuals who open accounts are who they say they are. Companies rely on the Social Security Death Master File to protect against theft.

In most cases, firms do not directly subscribe to the Death Master File, but access it indirectly through credit reporting agencies or other vendors who do subscribe to it.

This is both more efficient and less costly to the consumer.

For example, bank issuers of credit cards routinely obtain consumer reports on card applicants from credit reporting agencies. Because the credit bureaus periodically update their files by comparing information to the Death Master File, the credit report will contain an indicator if the individual has been reported as deceased. And the bank can use this information to decline the application or investigate the circumstances.

Other financial firms such as securities broker/dealers also access the Death Master File as part of the account-opening process. This screening is typically done by third-party vendors who utilize Death Master File information.

Consumer lenders regularly use information from credit-reporting agencies to review and adjust the status of existing accounts as well. It also helps to verify customers seeking to refinance existing mortgages or those who are interested in other services offered by the financial institution.

Naturally, financial firms have other sources of information that might indicate that a customer has died and that access to the account should be frozen or terminated. The principal source is family members who called to notify the institution of the death of the customer and may request changes in the name on the account or the address where statements are sent.

Lawyers and estate executors are another source of this information.

Whether financial institutions obtain information about deceased individuals directly from the Death Master File or indirectly from other subscribers, they have an interest in obtaining information and data that is accurate and current. Delays between the date on which an individual dies and the date on which this information is made available to the public through the Death Master File increases the opportunity for identity thieves to defraud survivors, beneficiaries and financial institutions.

One of the disadvantages of the current Social Security numbering system is that the agency is not always immediately notified upon the death of an individual. There appears to be no requirement for local officials to notify the Social Security Administration when someone dies.

Despite their best intentions, having incomplete and incorrect information makes it very difficult for the Social Security Administration to issue an accurate Death Master File.

Many companies have established internal processes that deal with fraud and identity theft. In addition, companies work with

customers who are victims of identity theft and they also work with prosecutors to pursue those responsible.

AFSA supports the efforts to encourage the Social Security Administration to obtain death information promptly and report it more frequently. We also support the continued dialogue between credit-reporting agencies and financial institutions to facilitate the flow of the Death Master File information and bureau files.

For example, there may need to be a change in procedures so that when creditors report account status information to credit-reporting agencies, and this information is placed in a file of a customer about whom the bureau has received death information, the creditor is made aware of this fact on a timely basis.

We believe that more financial institutions would consider subscribing to the data directly if the information provided was in real time and more accurate. Whether financial institutions obtain information about deceased individuals directly from the DMF or indirectly from other subscribers, it's in our interest and that of the consumer that we obtain correct information.

We've hopeful that the Social Security Administration will make both the procedural and policy changes necessary to ensure the security of our individual unique identifiers, our Social Security numbers.

Thank you.

[The prepared statement of Thomas J. Lehner can be found on page 107 in the appendix.]

Chairwoman KELLY. Thank you very much and thank you for limiting your testimony to the time.

We now move to Mr. Thomas Sadaka.

STATEMENT OF THOMAS A. SADAKA, SPECIAL COUNSEL, OFFICE OF STATEWIDE PROSECUTION, ORLANDO, FL

Mr. SADAKA. Chairwoman Kelly, Chairman Shaw, I truly thank you for the opportunity to be here today.

For the record, my name is Thomas Sadaka and I am Special Counsel to the Statewide Prosecutor of Florida for computer crime and identity theft prosecutions.

As the only representative of State government, as well as State law enforcement, I think a bit of a background is in order.

Florida ranks third in the Nation currently in identity theft complaints, according to the FTC. As such, we have embarked on a rather strenuous effort to combat and to curb the epidemic of identity theft.

At the request of Gov. Bush and as a result of the Privacy Technology Task Force, which addressed issues of Social Security abuse, public records abuse, and identity theft in general, we have impaneled a State-wide grand jury and have partnered with the Florida Department of Law Enforcement to focus specifically on identity theft cases as well as what Florida can do to minimize the effects of identity theft and the victimization of her citizens.

As such, the use of the Social Security number and the use of other public records information has become apparent. It is the constant in all of the crimes that we have currently investigated.

The State of Florida, through my office, was instrumental in passing an identity theft statute. In 1999, the statute went into ef-

fect, and at that time, we were one of only three States in the Nation to actually criminalize identity theft on the local level.

That is improving. State law enforcement and legislatures are quick to enact these laws and are quick to operate on them.

As such, the investigation and the prosecution of these cases is moving along slowly. So while we've addressed the after-the-fact dealings of identity theft, we now need to turn to the issues of prevention of identity theft.

The use of the Social Security number and the use of other public records information is vitally important to the identity thief, as well as to the terrorists and others who want to shelter from society who they truly are.

From the law enforcement encounter with the individual on the street to the airport security checker who is relying on the State-issued identification card, identity theft has a very broad base, both public safety concern as well as financial industry concern.

Our public safety issues are much more in the forefront now since September 11th. But we've been addressing these issues over the past year to try to develop fraud-proof identification as well as uniform identifiers throughout the country so that we can rely on information that's provided from other States.

State driver's license offices rely heavily on the Social Security number. Every State requires a Social Security number to be provided. Yet, the States don't avail themselves of the information available from the Social Security Administration, nor the other required information that would be available.

Several of the States do check the Master Death File. The Florida legislature commissioned us in July to conduct a study on developing a fraud-proof Florida DL.

So as part of that, I have been researching what other States do in the issuance process of identification cards.

Of those that do some type of independent verification, only a select number of them interact with the death index on a real-time basis. And although the Social Security Administration has made limited availability for online data verification of Social Security, name and geographical region, there are no States currently that avail themselves of that ability.

The State of Florida is currently looking into the ability to expand their infrastructure such that they can rely on the information from the Social Security Administration.

There are two issues that face Congress. One is, the Social Security number has become basically our de facto national identifier. There are two subissues to that.

Do we want that to be the case? And if the Congress' decision is that, yes, that is to be the case, then there need to be laws and initiatives in place that can basically back up the integrity of that number.

There needs to be the ability of both the financial industry as well as State and local governments to verify that the Social Security number that's provided by the citizen or by the customer is truly that individual's Social Security number.

We need to confirm that the identify of that person is their true identity.

We rely heavily on breeder documents. There are currently 262 different birth certificates in circulation in the United States. Those linked with Social Security numbers and passports and documents that are available from other countries create an daunting task on the part of the administrator, who is issuing this identification card.

The Social Security Administration has within its grasp and within the other agencies of the Federal Government all of the information that is necessary to both the State and local governments, as well as the financial industry, to confirm the identity of the person who is before them. That information needs to be streamlined in its distribution and needs to be made available.

If the other alternative is to not allow the Social Security number to be used for that purpose, then we face another undaunting task of developing some other unique identifier, such that all of our citizens can be comfortable that the information that is represented to financial industries and to State and local governments is correct and accurate information.

Again, I want to thank you very much for the opportunity to be here today and I'd be more than willing to answer any questions at the close of the testimony.

[The prepared statement of Thomas A. Sadaka can be found on page 110 in the appendix.]

Chairwoman KELLY. Thank you very much.

We now move to Mr. Dugan.

STATEMENT OF JOHN C. DUGAN, PARTNER, COVINGTON & BURLING, ON BEHALF OF THE FINANCIAL SERVICES COORDINATING COUNCIL

Mr. DUGAN. Thank you very much, Madam Chairwoman, Mr. Chairman. It's a pleasure to be here today.

I'm testifying today on behalf of the Financial Services Coordinating Council, or FSCC, whose members are the American Bankers Association, the American Council of Life Insurers, the American Insurance Association, the Investment Company Institute, and the Securities Industry Association.

The FSCC represents the largest and most diverse group of financial institutions in the country, consisting of thousands of large and small banks, insurance companies, investment companies, and securities firms.

Together, these financial institutions provide financial services to virtually very household in the United States.

The FSCC continues to believe that the Social Security number plays a central role in deterring and detecting fraud and identity theft because Social Security numbers are the best unique identifier that financial institutions can use to determine whether an individual really is who he or she says he or she is.

To that end, the FSCC welcomes the attention the subcommittees are giving to the misuse of Social Security numbers of deceased individuals.

My testimony today makes three fundamental points. First, Social Security numbers are key unique identifiers that are essential to guard against identity theft.

Second, the SSA's Death Master File is a comprehensive record of deceased individuals' Social Security numbers, but delays in updating and disseminating this list can create opportunities for fraud and identity theft.

Third, because financial institutions ultimately rely, usually indirectly, almost exclusively on the Death Master File to determine whether a Social Security number belongs to a deceased individual, the more frequently the DMF is updated and disseminated and the more accessible that information is, then the more effective the list will be as a tool to detect and deter fraud and identity theft.

On the first fundamental point, following the lead of the Federal Government, the financial services industry has used the Social Security number for many decades as a unique identifier for a broad range of responsible purposes.

For example, our Nation's remarkably efficient credit-reporting system relies fundamentally on the Social Security number as a common identifier to compile disparate information from many different sources into a reliable credit report.

The banking, insurance and securities industries each use SSNs as unique identifiers for a variety of important regulatory and business transactions, primarily to ensure again that the person with whom the financial institution is dealing really is that person.

It's that essential need to verify a person's identity using a common unique identifier—the Social Security number—that leads financial institutions to rely on the reporting of deceased individual's SSNs to guard against identity theft.

We believe there are two keys to preventing the misuse of Social Security numbers of deceased individuals.

First, the list of such numbers must be kept current. Second, the current list must be widely accessible and easy to search and crosshatch against a given Social Security number.

Unfortunately, while the current DMF is used to accomplish both these goals, there's clearly room for improvement.

On the first point, with respect to the currency of information in the DMF, there can be significant delays in updating the list. These are delays caused by the time taken for deaths to be reported to the SSA, delays caused by the entry of inaccurate information, and delays caused by the fact that the SSA releases comprehensive updates on only a monthly basis.

On the second point, the DMF is not provided in a form that is readily searchable. As a result, because it contains such a large amount of information, the most practical way to use the list, at least for financial institutions, is through intermediaries that convert the DMF into a searchable database that can be used by financial institutions and others.

This service by third-party vendors is valuable, but it can be costly, and cost can thus be a deterrent to the widespread use of the DMF.

Obviously, if a centralized, searchable database containing the DMF were widely available at a reasonable price, it's likely that the DMF would be used more routinely for a wider variety of authentication checks.

Let me now conclude by talking about financial institutions' use of the Death Master File.

Although the main purpose of the DMF is to inform the SSA that an individual has died, it's also purchased by private information vendors. Financial institutions ultimately rely on these vendors for accurate information about the status of individuals' SSNs.

Therefore, while the accuracy of the DMF is crucial to saving the SSA money, it's equally crucial to financial institutions who seek to prevent fraud and identity theft.

For example, many large banks contract with information vendors to compare the bank's list of individuals who have been approved for credit cards against the DMF.

Similarly, banks, securities broker/dealers, mutual fund transfer agents, and insurance companies frequently use these information vendors to conduct the same kind of search with new account openings, changes in parties on accounts, to determine whether to allow a client to maintain a margin account, to locate lost shareholders, and for other purposes.

Simply put, the more current the DMF is, then the more current the vendor's data is, and the better financial institutions can be at uncovering identity theft and other fraud.

And with that, I would conclude. We certainly welcome suggestions for achieving both of the goals I've outlined in the testimony and we'd be happy to work with the subcommittees and their staffs to facilitate these efforts.

Thank you very much.

[The prepared statement of John C. Dugan can be found on page 113 in the appendix.]

Chairwoman KELLY. Thank you, Mr. Dugan.

We move next to Mr. Rotenberg. Mr. Rotenberg, I'm sorry I did not have your testimony before we had this hearing. Usually, I like to have a chance to read it before.

But I'm going to be very interested in what you have to say today.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY LAW CENTER

Mr. ROTENBERG. Well, thank you, Chairwoman Kelly, and Chairman Shaw. I would ask that my statement be entered into the record and I will briefly summarize the points that I'm going to make this morning.

I appreciate the opportunity to be here. I'm the Director of the Electronic Privacy Information Center. We are a public interest research group in Washington concerned with privacy issues relating to American consumers.

I have also been on the faculty at Georgetown for more than 10 years, where I teach the law of information privacy.

I think it's critical to make clear at the outset for the purposes of this hearing that there's a long-standing effort by Congress and by the courts to protect the privacy of the Social Security number in law. And this has been done from the outset out of recognition that the particular status of this number, which can be used in so many different contexts, is ripe for misuse and abuse and, as we've seen in the last few years, the growing crime of identity theft.

So, for example, Section 7 of the Privacy Act of 1974 makes very clear in the collection and use of the SSN that Federal agencies may only use the number for certain statutory purposes.

And I'd like to say at the outset that the efforts of Chairman Shaw and other Members of the subcommittees to move forward legislation, H.R. 2036, which would extend similar protections to the private sector and strengthen as well the protections in the public sector, is a very important measure that I hope you will move quickly in this session.

Now the second part of the problem to understand is that the ID theft problem results from the growing dependence of the Social Security number as a general form of identification unrelated to the original purpose, which was of course the management of SSA benefits.

And if I may, Chairwoman Kelly, to pick up on your opening statement, I'd like to make a brief observation about this case involving Lahfti Raisi, who is the Algerian who may be responsible, in fact, for training the hijackers in the great tragedy of September 11th.

Now it has been reported that Raisi took advantage of the Social Security number of a deceased person in the State of New Jersey, presumably to obtain access to facilities in other places that he would not otherwise be able to go.

But it's not clear, at least from the reports that we have reviewed, that Raisi sought the Social Security number of a deceased person.

In other words, this may have just been a nine-digit number pulled from the air that turned out, in fact, to be the number of a person who was deceased.

And I make this point because it's critical to understand that in the area of identity theft, there are many ways to create Social Security numbers that are not one's own that don't require access to a deceased's SSN.

You can spoof SSNs in a number of different ways. I can look at a Social Security number and probably determine whether it's accurate—in fact, a real Social Security number, computer programs and financial institutions do this on a regular basis.

But my point here is I think we need to understand that it is the growing dependence on the use of the Social Security number and whether that number comes from a person who's deceased or whether it's simply made up, is going to be an ongoing problem in systems of identification going forward.

Now this then relates to my third point about the expanded use of the Death Master File. And I fully appreciate the interest of the financial institutions in having more timely, more accurate information on an ongoing basis. So that when they are making these determinations about whether or not an SSN is the SSN of the person who represents it, they have better information on which to make that decision.

But in expanding the use of the DMF, I'm concerned also that it will create new opportunities for misuse and abuse by others, who will use that information for other purposes. Because, of course, now you will have access to a very convenient file in elec-

tronic format that will give the public a great deal of detailed personal information.

And so I think an assessment needs to be done. How do you ensure that that information will be used only by the financial institutions for the appropriate purpose and not by others for ill-intended purpose?

I'd like to conclude, then, with three recommendations.

The first recommendation, having worked on this issue now for more than 10 years, is to urge you once again to think about systems of identification that are not solely dependent on the Social Security number. It is the SSN that contributes to ID theft and our growing use of the SSN leads to more ID theft.

Second, as I suggested at the outset, I think the legislation before the subcommittees is excellent.

And finally, if you do go forward with the proposal to make the DMF readily available in electronic format, I urge you to create some mechanism of oversight, some way to evaluate, maybe a year out, how that information is being used, because it could well be the case that that file will become a new source of identity theft, and that could simply compound the tragedy.

Thank you.

[The prepared statement of Marc Rotenberg can be found on page 126 in the appendix.]

Chairwoman KELLY. Thank you very much.

We now move to Mr. Hendricks.

STATEMENT OF EVAN HENDRICKS, EDITOR AND PUBLISHER, PRIVACY TIMES

Mr. HENDRICKS. Thank you, Madam Chairwoman, and Mr. Chairman. My name is Evan Hendricks, Editor and Publisher of *Privacy Times*.

I've been qualified as an expert in identity theft cases by the Federal courts and I realize I'm the last witness between not only you and lunch, but the lunch of my son, Daniel, who has accompanied me here today.

Chairwoman KELLY. We welcome your son.

Mr. HENDRICKS. Yes, thank you.

Chairwoman KELLY. Welcome, Daniel.

Mr. HENDRICKS. Thank you. This is an important issue. I'm grateful to follow my colleague, Marc Rotenberg, because I concur in his remarks and incorporate them.

What we've seen in this terrible tragedy is that not only has identity theft figured in the use for passport and visa purposes, but also the terrorists supported themselves by committing identity theft and credit fraud.

We followed this in my newsletter, *Privacy Times*, which is in its 21st year; there is an excellent article in the November 4th, *Chicago Tribune* which summarizes many of the activities they did, including skimming, which is using a machine to swipe a card and steal all the information and then make a counterfeit card out of it.

There are two things that fraudsters want in this day and age: either a Social Security number so that they can do identity theft, or a credit card number and an expiration date.

We also know that the fraudsters are using stolen credit card numbers to buy people's Social Security numbers so that then they can commit more identity theft.

So it's becoming a vicious circle.

When the World Trade Center tragedy hit, unfortunately, it became somewhat like when there's a black-out in New York: the thieves know they can break into buildings because there's no electronic burglar alarms any more.

And unfortunately, one of the World Trade victim's friends took her credit card and went on a credit joyride, and I'm told by my friends at the Privacy Rights Clearinghouse and the Identity Theft Resource Center that a plane crash victim was going to be picked up by a limo driver who had all his information and then went on to commit identity theft.

As indicated by Congresswoman Hooley's opening remarks, there are some really sick people out there and a lot of them are now gravitating toward identity theft.

I come here to say that, like Mr. Rotenberg, the goal of privacy laws is to give people control over their personal information. And some of the gaps and the weaknesses in our current privacy laws help the fraudsters get control over other people's information.

One of the fundamental principles of privacy laws is the information collected for one purpose should not be used for another purpose without your knowledge and consent. And this is at the heart of the Fair Credit Reporting Act, which is one of the first privacy laws enacted in 1971, amended by Congress in 1996.

It's a good law and it recognizes in practice that there are other purposes. And so, the Fair Credit Reporting Act defines permissible purposes. And it also gives people remedies, private right of action, penalties.

And I think even my colleague down the table, Mr. Pratt, will agree, this privacy law has made the credit-reporting industry a better industry. They do a better job handling data. They have to be more responsive. And if things go wrong, people have a remedy.

And so I'm also here to dispel the myth because there is really not much of a conflict between privacy law and security: all of our existing privacy laws make exceptions for law enforcement, for health and safety, and for intelligence purposes.

I think if you get into an honest discussion with the investigators, you'll see that the privacy law has not impeded the investigations here.

But that's why we look for solutions, as Mr. Rotenberg said, we need to take advantage of information technology. We need automated exchanges of data.

Just as the Fair Credit Reporting Act defines purposes and gives people a degree of confidence that data will be used for permissible purposes, so we need to expand that concept to our larger society, including automating any sort of a Master Death File that will be shared with the banks on an instant basis, or with the credit-reporting agencies, too.

I also want to agree with Mr. Rotenberg that we need to have a national oversight office. Every other western country has an independent privacy commissioner that answers to the legislative branch.

We need one, too.

In terms of three practical solutions, the first is that, conceptually, people need to be plugged into their credit report. The technology allows for it today, and actually, we're gravitating toward this and we need to accelerate it. So if there's activity on your credit report, you should receive some sort of electronic alert.

This is not that difficult to set up and it would be one of the best ways to guard against identity theft.

Second of all, though the credit reporting agencies sell a service where they can do a trace on SSNs, it's not clear to me that they do an audit of their own systems to see how many names and addresses are associated with one SSN.

And if they did that simple audit function, they would guard against some real problems and help clean up the integrity of their databases.

The final thing I'd like to mention is something that's called single-use credit card numbers. And Ms. Chairwoman, I heard that you had your credit card number stolen. I don't know if it was by skimming or through a database.

One company that I work with, called Privasys, has developed these prototype cards. You punch your pin number into the credit card so it can issue you a single-use number that is only good for one purchase.

So if later that number is stolen, it's worthless.

And so, there are solutions that we need in law, in organizational practice, and in technology.

Thanks very much. I'd be happy to answer any questions.

[The prepared statement of Evan Hendricks can be found on page 131 in the appendix.]

Chairwoman KELLY. Thank you, Mr. Hendricks. I'm going to ask just a couple of questions.

Mr. Rotenberg, on page 2 of your statement, I have to say, I was multi-tasking up here and reading it at the same time.

I find this a fascinating statement. It is the financial services industry's misplaced reliance on the SSN, lacks verification procedures and aggressive marketing, that are responsible for the financial consequences of identity theft.

I want you to enlarge on that.

Mr. ROTENBERG. Well, my point, Chairwoman, is simply that the SSN has been moved from the realm of processing Social Security benefits within the Federal Government and the purpose of tax identification when it become recognized by Congress for that purpose in 1961, to a generalized identifier across the financial services sector.

Chairwoman KELLY. Yes, sir, I do understand that. My question is why you are blaming—it appears you're blaming the financial service industry's use and reliance on that Social Security number for some of the fraud.

As a matter of fact, that integrates with a comment by Mr. Pratt when he talks about the Gramm-Leach-Bliley effect on the FTC rules.

I'm wondering if the two of you can tell me—if what my interpretation is is a correct one. Are you saying that the Gramm-Leach-

Bliley bill has had an effect on the use of the SSN by the financial services industry that would increase the ability for fraud to exist?

Mr. PRATT. If I may, from our perspective, the point we wanted to make in the testimony was simply that the Gramm-Leach-Bliley Act did take into account that there would be a series of exceptions to a consumer's choice for how non-public personal information could be transferred. And one of those exceptions was for purposes under the Fair Credit Reporting Act.

But the FTC's interpretation appears to foreclose on a consumer reporting agency's ability once they have that information to then build fraud prevention products that might apply to other exceptions within the GLB 502[e] exceptions.

And clearly, to foreclose on our ability to build a fraud prevention or a verification product which would use identifying information outside of GLB and outside of the Fair Credit Reporting Act.

So, in that case, the law seems to have tightened down the screws a little too tightly on some information that we might be able to use.

Chairwoman KELLY. Do you agree with that, Mr. Rotenberg? Anyone is welcome to join in, but I want to ask that specifically of Mr. Rotenberg.

Mr. ROTENBERG. Well, I don't agree that one of the consequences of GLB was to make the Social Security number more widely available to financial institutions. I understand the point that it in some ways may restrict certain verification procedures.

But I do want to be clear about the point in my statement here. Clearly, the theft itself is not committed by the institutions. That's not what I said.

What I said, that the use of the SSN to link financial records across institutions means that when the theft has occurred, the damages are amplified.

And so, when I said earlier that we need to think about systems of identification that are not so dependent on the SSN, it is very much based on the experience that victims of ID theft have had. When their Social Security numbers get out, then they lose control of their bank account, their credit account, and the other accounts that they may have with financial institutions.

Mr. HENDRICKS. Madam Chairwoman, can I respond to that?

Chairwoman KELLY. Mr. Hendricks.

Mr. HENDRICKS. I'll give you one example.

Identity thieves are in the business of getting credit fraudulently. They're able to do that because they apply for credit in somebody else's name and Social Security number.

The first problem is the credit-reporting agencies are too liberal in disclosing the innocent victim's credit report in response to an application made by an imposter. In many of these cases, I've seen that the city is different, the address is different, and the spelling is different. Yet, they err on the side of maximum disclosure from the credit-reporting agency to the credit granter, and that's the first problem.

The second problem is that, if the imposter simply has your Social Security number, I've seen cases—if you write these two names down—Myra Coleman and Maria Gaten. If you have the same Social Security number, their algorithms work so, since there's an M

and an R and another letter in the first name, that it's similar enough to go ahead and disclose the information, even though the names are completely different.

So there are some real application problems that were built from earlier days when they were thinking—well, women get married, they change their last name. People move a lot. As opposed to now, where we have a clear threat of identity theft and they need to update their rules for disclosing consumers' credit reports.

Mr. DUGAN. Madam Chairwoman, I'd just like to make two points.

Number one, we think the Gramm-Leach-Bliley Act, in fact, makes the misuse of Social Security numbers much more unlikely because it gives individuals more control over the ability of a financial institution to share that information with any non-affiliated third party, number one.

And number two, to the extent that information is provided for permissible purposes under the Gramm-Leach-Bliley Act, like fraud prevention, then the law specifically prohibits the recipient from using it for any other purpose.

So we think that that goes to that point particularly.

The second point I wanted to make was, it's nice to say that it's easy to steal a Social Security number, and, therefore, it's easy to steal someone's identity. But think what it would be like if you did not have a Social Security number used at all for identification purposes.

What Mr. Sadaka was saying earlier, you have to have some way to have a common, unique identifier in many circumstances, which is precisely what financial institutions use it for, to make sure that they know you are the Madam Sue Kelly that comes in the door and not a different Sue Kelly.

There have to be ways to link that up. And the use of the Social Security number is the way we do that. Without it, and with improper restrictions on its use, it would increase the occurrence of identity theft, not decrease it.

Chairwoman KELLY. Thank you very much. I have just one follow-up for Mr. Pratt.

What percent of your membership gets the DMF?

Mr. PRATT. I actually don't have a good answer for you, but I'll be happy to follow up.

Chairwoman KELLY. I wish you would, please.

Mr. PRATT. And I think your question is in terms of the total customer base, how many customers are using the DMF product that our members produce.

Is that it?

Chairwoman KELLY. I'm going to withhold any of my further questions because I've run out of time, and go to Chairman Shaw.

Chairman SHAW. I'd like to direct my question to Mr. Pratt again.

Our subcommittee has heard from many victims of identity theft over the last 2 years and there are stories that raise some very troubling issues pertaining to harassment and other matters.

First of all, fraudulent accounts were opened using their Social Security numbers, even though all of the information on the application was actually incorrect, including their names, addresses, and

even their birthdays. And the Social Security number was the only piece of information that was correct on these applications.

A second troubling issue is that credit-reporting agencies verified this incorrect information. Verifications of a name, address, place of employment, age, or spouse's name were not questioned. If the Social Security number matched up, the information was verified and the fraudulent application was approved.

First of all, can you explain how these fraudulent applications could have been verified or accepted?

Mr. PRATT. Well, let me go to, if I could break out your question into some parts.

Chairman SHAW. Maybe you could start just by telling us, what is the process and what are the checkpoints?

Mr. PRATT. The checkpoints that we use are the Social Security number, the name, the address, and, when available, we may be also able to cross-check previous address. Those would be the principle cross-checks.

Clearly, where we have 3 million consumers each year with last names changing, our cross-checks try to accommodate the fact that marriage and divorce occur and names can change in cycle.

Date of birth, some of the other identifying elements that you've indicated might have been on the application are not transmitted to the consumer reporting systems.

These may be issues that are addressed today differently than they may have been previously, but the cross-checks we use today are Social Security number, name and address.

In terms of why an application was approved, I'm not trying to put the monkey on someone's else back, but of course I can't tell you why the application was approved.

We transmit the information. We show the lender what information we believe in our file matches——

Chairman SHAW. Do you have any indication of where the system failed in this event?

Mr. PRATT. Well, no, sir, I really don't, because I don't have the facts in front of me specific to those particular situations.

I'd have to look at those, I suppose, to better understand where the failure occurred.

Chairman SHAW. Let me ask the question of liability because, from your previous answer, it sounds like it's nothing but negligence on the part of whoever is putting this information together.

Under the current law, are creditors and credit-reporting agencies accountable when their negligence contributes to identity theft and to other Social Security number misuses?

Mr. PRATT. Well, I have to resist the industry being characterized as negligent under the Fair Credit Reporting Act.

Chairman SHAW. I'm not characterizing the industry. I'm just saying, in the event of negligence, are they liable?

That's a simple, straightforward question.

Mr. PRATT. The answer to the question would be, under the Fair Credit Reporting Act, we're liable for being accurate. And therefore, if we're not accurate and a lender in turn is also liable as a user and as a furnisher under the same Fair Credit Reporting Act.

Chairman SHAW. So it's your testimony that they would be liable in the cases of negligence.

Mr. PRATT. There is negligence, there are willful and negligent standards under the Fair Credit Reporting Act and there are liabilities associated with the accuracy of the information and the use of the information.

Chairman SHAW. I'll have to go to the Act and see exactly what it says. What does it say—willful negligence, or do you know?

Mr. PRATT. There are two standards of civil liability, for example, and then of course there's administrative enforcement through the Federal Trade Commission and other functional regulators under the Act.

But the civil liability standards are willful and negligence.

Chairman SHAW. Ordinary negligence.

Mr. PRATT. Yes.

Chairman SHAW. And that makes them liable.

Mr. PRATT. Those are two standards of liability depending on the fact pattern, depending on how the suit is brought, against any one of the parties that is regulated under the Act.

Chairman SHAW. Do you think the creditors and credit-reporting agencies should be liable for these kinds of mistakes?

Mr. PRATT. Well, I think we're on the same side of this along with you. We don't want these mistakes to happen and we want accurate information in our files, sir, really.

Chairman SHAW. If we weren't on the same side, I wouldn't be here listening to you.

Mr. PRATT. I appreciate that.

Chairman SHAW. We're trying to figure this thing out so that we don't disrupt a system of a national identifier that, for good reason or bad reason, has been in place now for a number of years.

But we do know that there's been serious misuse. We do know that this is the fastest-growing crime in the country today.

And I personally believe and I think many other people personally believe, and I think Mr. Sadaka would agree with me on this—Mr. Sadaka, I think you agree that failure to do something is going to create a snowball effect and that this thing will be totally out of control after a reasonable period of time.

Do you agree with that?

Mr. SADAKA. Yes, sir, I do.

Chairman SHAW. Thank you. I yield back my time.

Chairwoman KELLY. Thank you.

We go to Mr. Hooley.

Ms. HOOLEY. Thank you, Just a couple of quick questions.

Anyone from the industry side can answer the first question. And that is, I understand the need for the industry to have this master list, so you can flag your files to prevent compromise by an identity thief.

What else do you do with the information? I mean, you use it to flag your files. What else do you do with the information?

Any one of you.

Mr. LEHNER. Well, as I mentioned in my testimony, it's oftentimes used to verify information on existing accounts, if people change the status of their account for some of our mortgage lenders. If a customer is refinancing their home, they're changing credit products within a company.

Usually, that information is asked as a means to verify that they are who they say they are.

Mr. PRATT. Our members as subscribers are using it principally for fraud prevention.

Ms. HOOLEY. That's what I assume, all of you are using it for fraud prevention.

Mr. DUGAN. There are other reasons to use the information: to track down or locate lost shareholders, or to review loan applications. But principally, it's to make sure that the person is who they say they are.

Ms. HOOLEY. Would you have any opposition to having it in law that the information is solely used to flag the file of a deceased individual or for fraud prevention?

Mr. PRATT. Like all good trade associations, I'd have to go back and talk to the members, I guess, and find out whether there's anything out there that I'm just not aware of here today.

Ms. HOOLEY. OK. By the way, Mr. Pratt, thank you very much for clearing up the file of Sean. I really appreciate your doing that.

Mr. PRATT. Thank you.

Ms. HOOLEY. For either Evan or Marc Rotenberg, are you aware of any instances where information from the Death Master File has been intercepted by identity thieves?

Are you aware of that at all?

Mr. HENDRICKS. No, not per se. The cases that I've heard of, the identity is just doing straight to the local government agency and getting information off death certificates. I've heard about cases like that and I've asked for more documentation of that.

Ms. HOOLEY. Do you think we should use it solely for flagging the files, using the Death Master list solely for flagging the files or for fraud?

Mr. HENDRICKS. Yes. You create an automated information exchange here and you specify what those purposes are and you create penalties for people that violate that and remedies for individuals whose privacy is violated.

I think that's the way to go. And I think if you look at the kind of privilege that goes between a lawyer and a client or a doctor and a patient, the privacy privilege is not so people can hide or keep data secret. It's to allow for the open exchange of information for the purposes you need—better health care, better legal advice.

And I want to take that concept and expand it to everything in our society. So privacy is protected within certain spheres, but that allows for open data exchange within the approves spheres.

Ms. HOOLEY. Thank you. That's all the questions I have.

Chairwoman KELLY. Thank you very much. I have a couple of other questions. One for all of you as panel members.

I'd like to know if you can commit to participating on a task force with the SSA to solve this problem.

I think that if we put together—if there's a task force of the SSA, the GAO, the Commerce Department, and all of you, we could probably get to the root of the problem and get it solved much more quickly than every agency acting without consulting the others.

So I'd like to ask for a commitment from all of you to being a part of that task force. Can you commit to that?

Mr. DUGAN. Madam Chairwoman, we'd be delighted to commit to do that.

Chairwoman KELLY. Am I hearing that from all of you?

Mr. PRATT. Our testimony already indicates we support doing that.

Mr. SADAKA. Absolutely, yes.

Mr. LEHNER. Absolutely.

Mr. HENDRICKS. Yes.

Mr. ROTENBERG. Yes.

Mr. SADAKA. We'd be very willing to commit as well.

Chairwoman KELLY. I thank you very much.

One final thing for you, Mr. Hendricks. Your son is going to have to wait for lunch for one second.

You said in your testimony that there was an independent national office to oversee and enforce the privacy law, was a recommendation of the U.S. privacy protection study commission in 1976.

I think it's time we consider something like that and I hope that you will consider that within the framework of this task force.

That being so, then I would like to, if there's no more questions, the Chair notes that some Members may have additional questions for this panel that they may wish to submit in writing.

So without objection, the hearing record is going to remain open for 30 days for Members to submit written questions to these witnesses and to place their responses in the record.

On behalf of the subcommittees, I want to thank all of the witnesses for taking the time to be here today. I believe it's been a very productive hearing that has highlighted a problem that can be solved with regards to identity theft.

This panel is excused with our appreciation. I want to thank Chairman Shaw and his staff and other Members and all of their assistants, and my staff, for making the hearing possible.

The hearing is adjourned.

[Whereupon, at 12:25 p.m., the hearing was adjourned.]

A P P E N D I X

November 8, 2001

Opening Statement—*Prepared, not delivered*

Chairman Michael G. Oxley

Committee on Financial Services

"Preventing Identity Theft by Terrorists and Criminals"
November 8, 2001

Thank you, Chairwoman Kelly, for your continued leadership on this issue. By uncovering this problem and organizing today's hearing, you have brought to light a subject that we need to address now more than ever. Identity theft has always been a despicable crime, but the theft of the identities of the September 11 terrorist victims is something we absolutely must not let happen.

I'd also like to welcome our colleagues from the Ways and Means Committee. Chairman Shaw and Ranking Member Matsui, I believe that by working together we can put a stop to one of the most shameful crimes in America.

As we shall hear today, current practices of the Social Security Administration make crime easier for terrorists and con artists who are the white-collar equivalent of grave robbers. By not immediately notifying the financial industry of death information, the Social Security Administration is giving the evildoers a window of opportunity. The technology is out there to stop this, and the financial services industry needs us to ensure that government is doing its job by making use of new technologies. I am confident that the industry can then take additional measures to meet this challenge, as it has with other challenges it faces in the course of business.

Identity theft is a problem that has grown increasingly more prevalent in the past few years. According to the Federal Trade Commission, identity theft was the top consumer complaint received last year, with the rate of complaints and inquiries increasing at an alarming rate with the widespread use of Internet technology. There are currently over 1,700 cases of stolen identity **per week** that are being reported.

In Ohio, a retired airline pilot who spoke to my staff had his identity stolen by a California man who purchased two homes with his credit information. Another Ohio victim had been dead for 10 days when two felons assumed his identity and stole $300,000 from his life savings to buy jewelry for resale on the black market.

All too often, the victims or their families must spend countless hours trying to resolve an identity theft with banks, credit card companies and the Social Security Administration. Credit histories are ruined for the living, and the families of deceased victims face additional burdens at the worst possible time. We need to close the loopholes that are allowing criminals to do this.

Once again, Madam Chairwoman, thank you for providing leadership on this issue.

Opening Statement

Chairwoman Sue W. Kelly

Subcommittee on Oversight and Investigations
Committee on Financial Services
"Preventing Identity Theft by Terrorists and Criminals"
November 8, 2001

We are here this morning to see how we can prevent the awful crime and terrible tragedy of identity theft by terrorists and criminals. Our special intention is to protect the families of the deceased from such theft and financial fraud at their most vulnerable moment, when they are grieving from the shock of their loss. Through the rapid transmittal of the information in the Death Master File from the Social Security Administration to the financial services industry, and the immediate use of that information by the industry, we can prevent these crimes and spare the families further pain.

James Jackson and Derek Cunningham stole hundreds of thousands of dollars in gems and watches from deceased executives of our major corporations before being caught by law enforcement. They stole the identity of the late CEO of Wendy's International within days after his death and were not arrested until about two months later.

In the past two months, we learned that identity theft could be a tool of the hijackers who murdered thousands of our fellow citizens, and of their accomplices as well. Last week, the Inspector General of the Social Security Administration testified that some of the 19 hijackers used phony Social Security numbers to perpetrate their murders.

And we know that Lofti Raissi, an Algerian held on suspicion that he trained 4 of the hijackers how to fly, used the Social Security number of a New Jersey woman who has been dead for ***10 years***!

Even after these events, and after three of us serving on the Financial Services Committee requested SSA to ensure the rapid transmission of the Death Master File, we have received no commitment from SSA to take any specific action. The file is still physically shipped to an agency at the Commerce Department, where copies are made and physically shipped to subscribers. There has been no reduction for years in the time that it takes for SSA to officially notify the financial services industry of a death.

Identity theft is now part of the first war of the 21st century, but the federal government is still treating it in a 1960's way. That must end. That is why we asked the General Accounting Office to study the matter and report their findings to the Committee.

That is why we are so pleased that the Ways and Means Subcommittee on Social Security, chaired by my colleague, Rep. Clay Shaw, can join us in holding this joint hearing today. We need the Social Security Administration to take bold and immediate action to get the information to the financial services industry. We will hear from SSA, the Commerce Department, and the General Accounting Office, and we expect an innovative and effective solution.

We also need the financial services industry to ensure that the information is immediately integrated into databases and available for permanently deactivating Social Security numbers of the deceased. Moreover, with the passage of the U.S.A. PATRIOT Act, there will soon be Treasury Department regulations requiring them to verify the identification of new accountholders, and for customers to provide the identification requested by the companies.

We know that the SSA and financial institutions can meet this challenge. In the past three years they have already met two difficult challenges, the Y2K conversion and the aftermath of the terrorist attacks.

The SSA was a leader among government agencies in successfully avoiding the Y2K glitch, and financial institutions breezed through the turn of the millennium without a single major problem. As the Acting SSA Commissioner testified last week before Rep. Shaw's subcommittee, the SSA regional offices in New York and Pennsylvania reacted with fortitude and compassion to assist the victims and their families. And I want to thank the Social Security Administration for their wonderful assistance to New Yorkers, including those in my district. After the horrendous destruction in New York City interrupted the financial markets and killed many, financial institutions there and across the country picked themselves up, dusted off, and got back to work with amazing speed and grace, even while mourning their compatriots.

And all of them did all of that, the Y2K conversion and the recovery from the attacks, without any specific mandate in any federal law. Surely we can work together to meet this challenge before us now. I urge all parties to get together and, based on the GAO's findings, leapfrog over the antiquated system now used and stop identity theft of the deceased.

Rep. Shaw will chair the hearing for the first panel of witnesses, and I will chair the hearing for the second panel.

Committee on Ways and Means
Subcommittee on Social Security
Joint Hearing with Committee on Financial Services'
Subcommittee on Oversight and Investigations on
Preventing Identity Theft by Terrorists and Criminals
Opening Statement of Chairman Shaw
November 8, 2001

Today, our two Subcommittees join together to examine ways to prevent identity theft by terrorists and criminals.

When Social Security numbers were created 65 years ago, their only purpose was to track a worker's earnings so that Social Security benefits could be calculated. But today, use of the Social Security number is pervasive.

Our culture is hooked on Social Security numbers. Businesses and governments use the number as their primary source of identifying individuals. You can't even conduct the most frivolous transaction --like renting a video at your local store – without someone asking you to first render your 9 digit ID.

Your Social Security number is the key that unlocks the door to your identity for any unscrupulous individual who gains access to it. Once the door is unlocked, the criminal or terrorist has at their fingertips all the essential elements needed to carry out whatever dastardly act they can conceive.

We now know that some terrorists involved in the September 11th attacks illegally obtained Social Security numbers and used them to steal identities and obtain false documents, thus hiding their true identities and motives. These unspeakable acts shine an intense spotlight on the need for government and private industry to be vigilant in protecting identities. It also demands that safeguards to prevent identity theft are put in place now.

Earlier this year, I along with several of my Ways and Means colleagues, introduced H.R. 2036, the "Social Security Number Privacy and Identity Theft Prevention Act of 2001."

This bipartisan bill represents a balanced approach to protecting the privacy of Social Security numbers while allowing for their legitimate uses. Because of its broad scope, the bill has been referred to the Committee on Energy and Commerce and Committee on Financial Services, in addition to Ways and Means. I urge prompt action by all three committees so we may bring this important legislation to the floor as quickly

as possible. It is a needed part of our nation's response to terrorism.

Sadly identity theft is a crime not perpetrated just against the living. A *Washington Post* article on Saturday, September 29, reported that a man detained in Great Britain, and suspected of training four of the terrorists who hijacked the airliners on September 11, used the Social Security number of a New Jersey woman who died in 1991. The Associated Press reported on October 31 that an individual from North Carolina had been indicted on charges he tried to steal the identity of someone killed in the terrorist attack at the World Trade Center.

Therefore today, we will take a hard look at the sharing of death information. The Social Security Administration maintains the most comprehensive file of death information in the federal government. How this information is compiled, its accuracy, and the speed with which it is shared with the public will explored.

Because the financial services industry relies fundamentally on Social Security numbers as the common identifier to assemble accurate financial information, they are in a unique position to assist in the prevention of Social Security number fraud and abuse. Their timely receipt of death information and prompt updating of financial data is key in preventing identity theft.

In the past, some businesses have not been "enthusiastic" about further restricting the use of Social Security numbers. It is my hope they will rethink their resistance in light of September 11. Identity theft is a national security threat involving life and property. Safeguards will be made and I predict sooner, rather than later.

Opening Statement of the Hon. Benjamin L. Cardin,
a Representative in Congress from the State of Maryland

- Chairman Shaw and Chairwoman Kelly, thank you for calling this joint hearing to learn about the use of Social Security numbers by terrorists and criminals, including the use of numbers belonging to deceased persons.

- Our subcommittee has been investigating this issue for several years now, yet identity theft continues to rise. The FBI considers it the fastest-growing crime in the U.S., and cases have hit 350,000 a year.

- It has now come to light that the 19 hijackers had SSN's – 13 of them legitimately, while 6 obtained fraudulent numbers. All used other aliases, as well, which presumably would include Social Security numbers.

- The focus of today's hearing is on SSA's death masterfile – its database of the names and Social Security numbers of 69 million people who have died. Questions have been raised about whether this file can be updated more frequently and shared expeditiously with the financial services community, to help prevent damage before it is done.

- I will be focusing on two concerns as we hear the testimony:

  - Is SSA doing its part to share death information? Can any more be done on that end?

  - Are members of the financial services industry doing their part to obtain and use this data, and prevent fraud and misuse?

- For example, a suspected terrorist detained in Britain was found to have used the Social Security number of a woman who died in 1991. Apparently, he added a digit to his 8-digit driver's license number to create a fake Social Security number, and it happened to have belonged to this woman. According to the Inspector General, her death was entered into SSA's death masterfile in 1991. How is it that this man's use of her SSN was not detected?

- And what can be done about identity theft involving existing accounts of deceased persons, as opposed to attempts to open new lines of credit under a stolen identity? For example, USA Today reported last year on a ring of thieves who targeted the bank accounts of prominent business executives who had recently died, including the CEO of Wendy's, International.

  Would more frequent updating of the death masterfile have prevented these thefts? Do banks and credit card companies regularly update their account information using the death masterfile? Or is it the responsibility of families and friends to notify banks of the death of an account-holder? What about case of joint accounts, where only one of the account-holders has died?

- I welcome the chance to hear more from the financial services representatives about what

their industry is doing to combat Social Security number misuse. We could pass a bill in our subcommittee to improve SSA procedures, but we want to be sure that this effort is met by equal and appropriate response on the part of users of this file, and those who perhaps should be using it but aren't today.

- We also need to consider the tradeoffs inherent in making SSA's death information more readily available. There is a cost to doing this that could take away from SSA's priority mission: to maintain earnings records and pay benefits in the case of death, retirement or disability. And I have concerns about whether making the list more up-to-date and easier to use could compromise individual's privacy, and have the unintended effect of making things easier for criminals, too.

OPENING STATEMENT OF
LUIS V. GUTIERREZ
RANKING DEMOCRAT
SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS
"PREVENTING IDENTITY THEFT BY TERRORISTS & CRIMINALS"
November 8, 2001

The easy accessibility of our social security number contrbutes significantly to the widespread increase of identity theft, which the government estimates strikes 750,000 victims per year and accounts for more than $2 billion in fraud losses.

The fact that passwords, user names and other data used by financial institutions and utility companies to verify identity, such as an account holder's Social Security number, driver's license information and a mother's maiden name are readily accessible in countless databases on the web contribute to the problem. Several web sites even advertise they can provide Social Security numbers.

One common target for fraud is the recently deceased individuals because their credit cards and bank accounts are not automatically canceled or transferred to survivors. Some thieves have even taken the identity of a deceased child to establish a clean credit history.

Identity theft has been a serious problem for decades and the number of victims is increasing dramatically each year. Allegations of identity theft using Social Security numbers more than doubled last year from 26, 531 to 62,000 cases nationwide. For example, a woman who had been receiving title II disability benefits since the mid-1070s had obtained a license as a Certified Nurses Assistant in July 1999 using the Social Security number (SSN) of her deceased stepfather; a man who defrauded Social Security programs of $30,000 when he continued to receive and spend his mother's Social Security widow's survivors benefits following his mother's death. More recently, a man suspected of training four of the hijackers of the Sept 11th attacks was able to use the Social Security number of a woman who had died ten years ago. Sadly, these are only three of the thousands of identity theft cases that occur in this country every year.

If we continue to accept the use of our social security number for a wide array of activities, such as joining a gym or when filling out a rental video card application, it will be difficult to reduce the incidence of identity theft.

I hope that with the information that will be gathered at this hearing we will be able to work toward meaningful initiatives to help better protect our privacy.

RON PAUL
14TH DISTRICT, TEXAS

FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEES:
VICE CHAIRMAN
OVERSIGHT AND INVESTIGATIONS
CAPITAL MARKETS, INSURANCE, AND GOVERNMENT-SPONSORED ENTERPRISES
DOMESTIC MONETARY POLICY, TECHNOLOGY, AND ECONOMIC GROWTH

INTERNATIONAL RELATIONS COMMITTEE
SUBCOMMITTEES:
INTERNATIONAL OPERATIONS AND HUMAN RIGHTS
WESTERN HEMISPHERE

Congress of the United States
House of Representatives
Washington, DC 20515–4314

203 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2831

312 SOUTH MAIN
SUITE 228
VICTORIA, TX 77901
(361) 576-1231

200 WEST 2ND STREET
SUITE 210
FREEPORT, TX 77541
(979) 230-0000

Ron Paul

Statement of Congressman Ron Paul
on "Preventing Identity Theft by Terrorists and Criminals"
11-08-01

Madam Chairwoman, thank you for holding this timely hearing on the important topic of identity crimes committed against the victims of the September 11 attacks on the Pentagon and the World Trade Center. I would also like to thank the Social Security Subcommittee of the Ways and Means Committee for participating in this hearing. It is hard to imagine a more shocking exploitation of the September 11 tragedy than targeting the victims of the terrorist attacks for identity theft.

I would also like to thank the Chairwoman for leading the effort to ensure the Social Security Administration is making full use of the "Death Master File" in order to help reduce the incidents of identity theft. It is long-past time we recognized the ways in which Congress' transformation of the Social Security number into a *de facto* uniform identifier facilitates identity crimes. Since the creation of the Social Security number, Congress has authorized over 40 uses of the Social Security number as an identifier. Thanks to Congress, today no American can get a job, open a bank account, get a professional license, or even get a drivers' license without presenting their Social Security number. Federal law even requires Americans to produce a Social Security number to get a fishing license!

Because of the congressionally-mandated abuse of the Social Security number, all an unscrupulous person needs to do is obtain someone's Social Security number in order to access that person's bank accounts, credit cards, and other financial assets. As supportive as I am of efforts to ensure that the Social Security Administration minimizes the risk of identity theft, the only way to ensure the federal government is not inadvertently assisting identity criminals is to stop using the Social Security number as a uniform ID. I have introduced legislation to address the American people's concerns regarding the transformation of the Social Security number into a national ID, the Identity Theft Prevention Act (HR 220). The major provision of the Identity Theft Prevention Act halts the practice of using the Social Security number as an identifier by requiring the Social Security Administration to issue all Americans new Social Security numbers within five years after the enactment of the bill. These new numbers will be the sole legal property of the recipient, and the Social Security Administration shall be forbidden to divulge the numbers for any purposes not related to the Social Security program. Social Security numbers issued before implementation of this bill shall no longer be considered valid federal identifiers. Of course, the Social Security Administration shall be able to use an individual's original Social

Security number to ensure efficient transition of the Social Security system.

Madam Chairwoman, while I do not question the sincerity of those members who suggest that Congress can ensure citizens' rights are protected through legislation restricting access to personal information, legislative "privacy protections" are inadequate to protect the liberty of Americans for several reasons. First, it is simply common sense that repealing those federal laws that promote identity theft is more effective in protecting the public than expanding the power of the federal police force. Federal punishment of identity thieves provides cold comfort to those who have suffered financial losses and the destruction of their good reputation as a result of identity theft.

Federal laws are not only ineffective in stopping private criminals, they have not even stopped unscrupulous government officials from accessing personal information. Did laws purporting to restrict the use of personal information stop the well-publicized violation of privacy by IRS officials or the FBI abuses by the Clinton and Nixon administrations?

My colleagues should remember that the federal government lacks constitutional authority to force citizens to adopt a universal identifier for health care, employment, or any other reason. Any federal action that oversteps constitutional limitations violates liberty because it ratifies the principle that the federal government, not the Constitution, is the ultimate judge of its own jurisdiction over the people. The only effective protection of the rights of citizens is for Congress to follow Thomas Jefferson's advice and "bind (the federal government) down with the chains of the Constitution."

In conclusion, Madam Chairwoman, I once again thank you and the other members of the subcommittee for holding a hearing on this important issue, and for your efforts to take steps to protect the American people from government-facilitated identity theft. However, I would ask my colleagues to remember that efforts to protect the American people from identity crimes will not be effective until Congress addresses the root cause of the problem: the transformation of the Social Security number into a national identifier.

JANICE D. SCHAKOWSKY
9TH DISTRICT, ILLINOIS

COMMITTEES:
FINANCIAL SERVICES
GOVERNMENT REFORM

FLOOR WHIP

515 CANNON HOUSE OFFICE BUILDING
Telephone: 202-225-2111
Fax: 202-226-6890
TTY: 202-225-1904

Congress of the United States
House of Representatives
Washington, DC 20515-1309

5533 N. BROADWAY
CHICAGO, IL 60640
Telephone: 773-506-7100
Fax: 773-506-9202

2100 RIDGE AVENUE, ROOM 2203
EVANSTON, ILLINOIS 60201
Telephone: 847-328-3399
Fax: 847-328-3425

6767 N. MILWAUKEE AVENUE
NILES, IL 60714
Telephone: 847-647-6955
Fax: 847-647-6954

Financial Services Subcommittee on Oversight and Investigations and Ways & Means Subcommittee on Social Security joint hearing on "Preventing Identity Theft by Terrorists and Criminals"

STATEMENT OF CONGRESSWOMAN JAN SCHAKOWSKY
NOVEMBER 8, 2001

Thank you Mr. Chairman for calling this important hearing today about preventing identity theft by terrorists and criminals. The FBI states that identity theft has become the fastest growing crime in America with 1,700 complaints a week and somewhere between 350,000 and 500,000 individuals per year falling victim to this crime.

The terrorist attacks on our nation on September 11th revealed disturbing realities about our nation's security systems and the ease by which criminals can obtain false identities and documents. I am particularly disturbed with the ease the terrorists entered, exited, and moved about the country. The INS and other authorities still can not track how 6 of the 19 hijackers entered the country.

I am further appalled at the level of opportunism some criminals demonstrate. There have already been three people indicted for using the identities of people who perished in the World Trade Center terrorist attacks. One of the men indicted is said to have gotten an American Express card and tried to obtain a $750,000 mortgage under the name of a man who died on Flight 175, which crashed into the World Trade Center. According to the authorities, it is commonplace that identity thieves prey upon those who have recently deceased.

Since Congress passed the Federal Identity Theft Law in 1998, the dramatic increase in identity theft can be attributed to the Internet, advanced computer graphics, and other technological advances and upgrades. We must find ways to use this technology to our advantage. I also introduced broad and comprehensive consumer rights legislation last Congress that included provisions to expand consumer protections against identity fraud. We also recently passed legislation that seeks to curtail the usage of false identification in establishing financial accounts.

We must remain vigilant in overseeing the effectiveness of the laws we pass and creating new laws to stop both terrorists and criminals. I look forward to this discussion on how to expedite the processing of information regarding deceased individuals and using technology to our advantage in stopping identity thieves and maintaining security.

STATEMENT OF

PHILLIP J. BOND

UNDER SECRETARY FOR TECHNOLOGY

DEPARTMENT OF COMMERCE

ON

IDENTITY THEFT

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

HOUSE COMMITTEE ON WAYS AND MEANS

AND THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

HOUSE COMMITTEE ON FINANCIAL SERVICES

NOVEMBER 8, 2001

Thank you for inviting me here today to address the important issue of combating the fraudulent use of social security numbers of deceased individuals. The National Technical Information Service (NTIS), a component of the Technology Administration of the Department of Commerce, is involved in this issue because it makes available to the public the Social Security Administration's Death Master File Extract.

As someone who has put six years of his life into working in the People's House, it is truly an honor to have this opportunity to return and work with you to defend Americans against identify theft. The events of September 11 are causing us all to revisit and reassess what we are doing and how we are doing it. I commend you for holding this hearing, and look forward to further discussions to make America more secure. I am very confident that these Committees will find technology to be a solution to closing the loopholes that make identities vulnerable to theft.

First, let me tell you a bit about who NTIS is and what it does. For over 50 years, NTIS has been collecting, organizing, and permanently preserving most of the research and technical reports produced by federal agencies and their contractors and grantees. It has almost 3 million information products in its permanent collection and makes them available to business, industry, the academic community, and the general public. NTIS is one of the Government's means for transferring technology from the shelf where it might otherwise sit and collect dust to those who can turn it into new products, new businesses, and new jobs. NTIS receives no appropriated funds and sustains itself primarily from the sale of these reports.

Over the years, NTIS has developed close working relationships with many federal agencies. Many agencies work with NTIS because they know it has the ability to make their information products widely available beyond their traditional constituency and that NTIS can distribute their information in a variety of formats, depending on customer needs. It would undoubtedly be more expensive if individual agencies tried to replicate this infrastructure for individual products. For example, the Defense Technical Information Center will provide its technical reports to any registered member of the Defense community but provides all unclassified research to NTIS for distribution to the public at large. The intelligence community collects and translates information from newspapers and radio broadcasts around the world so Government policymakers can learn what's going on and how information is being reported locally. The community provides the information to NTIS so it can make it available to the public. Similarly, the Social Security Administration (SSA) distributes the Death Master File within the Federal Government and to certain state and local agencies, but uses the services of NTIS to make it available to others, in part because they do not currently have the capacity or established distribution networks to handle large numbers of subscribers.

My principal comments will address what we do with the files we receive from SSA. I will defer to that agency to address any questions regarding accuracy or timeliness, except to note that (a) every calendar quarter, SSA extracts information from its various filing systems and creates a complete Death Master File, which now contains almost 67

million names, and (b) it also prepares a monthly update containing new deaths and changes or deletions to the master file.

The Death Master File contains only basic information: Social Security Number, Last Name, First name, Date of Death, Date of Birth, State or County of Residence, and Zip Codes for the Last Residence and Last Lump Sum Payment.

Obviously, the Death Master File can be a great help for detecting erroneous or fraudulent payments. Accordingly, SSA makes it available directly to a number of agencies that pay benefits or have other needs for this information such as for preparing certain statistical studies; and to states, which use the list to detect fraud or administrative errors including fraudulent or erroneous food stamp payments.

At the same time that SSA makes the Death Master File available to these various federal and state agencies, it makes it available to NTIS for reproduction and distribution to other users. NTIS receives this information on cartridge via overnight mail. It then copies the information onto magnetic tape, cartridge, or CD-ROM, depending on customer preferences. NTIS will, of course, be pleased to consider other formats if there is sufficient demand. It typically takes one-to-three days to complete the production process and to send the file to its more than 100 subscribers via overnight mail, or other means, depending on the subscribers' preferences. All formats are sent out at the same time. The turnaround time depends in part on file size, but is not generally a function of the fact that NTIS offers the file in various formats.

We understand that the Social Security Administration is exploring new approaches to making the file available in a more timely manner. These include sending the files to us electronically and sending updates on a weekly, rather than monthly, basis. Electronic transfer would certainly reduce turnaround time. Subscribers would probably find it easier to obtain just the updates electronically. In any event, we are committed to working with SSA to improve the delivery of this important information product.

Finally, we understand that there is some desire in the financial community for a web-based search capability. This is an interesting proposal that merits consideration. We note, however, that the proposed improvements under consideration by SSA may resolve many of the issues regarding timeliness. NTIS will be pleased to look into this further.

In conclusion, NTIS is proud of its relationship with the Social Security Administration and honored that they look to NTIS to make this important product available to the public. I would welcome any suggestions to help NTIS distribute this important list more effectively. Thank you.

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security

And

The Committee on Financial Services Subcommittee on Oversight and Investigations

Testimony

Preventing Identity Theft Committed by Terrorists and Criminals

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

November 8, 2001

Preventing Identity Theft Committed by Terrorists and Criminals

Testimony of: James G. Huse, Jr.

Inspector General of the Social Security Administration

Good morning, and thank you for the opportunity to appear today to discuss the prevention of identity theft by terrorists and criminals. While I have testified on the issue of identity theft before various Committees in both the House and Senate, the events of September 11th lend a renewed urgency to this issue.

Identity theft was already a significant problem facing law enforcement, the financial industry, and the American public before September 11th. In the weeks since that terrible day, it has become increasingly apparent that improperly obtained Social Security numbers were a factor in the terrorists' ability to assimilate themselves into our society while they planned their attacks. While this has heightened the urgency of the need for Congress, the Social Security Administration, and my office to take additional steps to protect the integrity of the Social Security number, it has not altered the nature of the steps that must be taken.

The Social Security number, no matter how much we avoid labeling it as such, is our national identifier. As such, it is incumbent upon those of us gathered here to

do all in our power to protect it and the people to whom it is issued. There are three stages at which protections must be in place: upon issuance, during the life of the number holder, and upon that individual's death.

With respect to the issuance of SSN's, or what the Social Security Administration refers to as the enumeration process, our audit and investigative work has revealed a number of vulnerabilities and resulted in a number of recommendations. The most critical of these recommendations centers around the authentication of documents presented by the individual applying for an SSN or a replacement Social Security card. If we are to preserve the integrity of the SSN, birth records, immigration records, and other identification documents presented to SSA must be independently verified as authentic before an SSN is issued. Further, if immigration records are to be relied upon, the Immigration and Naturalization Service must be required to authenticate those records. Regrettably, this will subject the enumeration process to delays, but just as we must endure lengthy waits at airports in the name of tighter security, so must we now sacrifice a degree of customer service in the name of SSN integrity. H.R. 2036, introduced by the Social Security Subcommittee, moves us closer to these protections, the importance of which cannot be overstated. If we cannot stop the improper issuance of SSNs by the Federal government, then no degree of protection after the fact will have any significant effect—it would merely be closing the barn door after the horse has gone.

The second, and most difficult, stage of protecting the SSN comes during the life of the number holder. Because the SSN has become so integral a part of our lives, particularly with respect to financial transactions, it is difficult to give the number the degree of privacy it requires, but there are important steps we can take. We can limit the SSN's public availability to the greatest extent practicable, without unduly limiting

commerce. We can prohibit the sale of SSNs, prohibit their display on public records, and limit their use to valid transactions. And we can put in place strong enforcement mechanisms and stiff penalties to further discourage identity theft. These measures can be accomplished only in cooperation with the financial services industry, and only in a spirit of compromise and mutual accommodation. Again, H.R. 2036 takes important steps in this direction.

Finally, we must do more to protect the SSN after the number holder's death. The Social Security Administration receives death information from a wide variety of sources and compiles a Death Master File, which is updated monthly and transmitted to various Federal agencies. It is also required to be offered for sale to the public, and can be accessed over the Internet through a number of sources. Whether making this information publicly available is wise, is a policy issue that Congress may wish to consider in light of recent events; certainly it exposes a large number of issued SSNs to the public. My concern under the current system is with the accuracy of death information. Accuracy in this area is critical to SSA in the administration of its programs, to the financial services industry, and to the American people. Our audit work has revealed systemic errors in the Death Master File, and we have recommended steps that SSA can take to improve the reliability of this critical data. Among these recommendations were matching the Death Master File against auxiliary benefit records to ensure that individuals receiving benefits in one system are not listed as deceased in another, and reconciling 1.3 million deaths recorded in SSA's benefit payment files that do not appear in the Death Master File.

We are faced with striking a balance between speed and convenience on the one hand and accuracy and security on the other—this is true in the case of the Death Master File, just as it is true in the enumeration process and in the protection of SSNs

during the life of the number-holder. In the post-September 11th environment, we must be particularly cautious in striking that balance, and any attempt to accelerate the death reporting process must be undertaken in full awareness of the importance of accuracy.

At all three of these stages of an SSN's existence, improvement is needed. H.R. 2036 addresses many of these concerns. But legislation, and more importantly, cooperation, is critical. The Social Security Administration, my office, the Congress, and the American people must act together to accord the SSN the protections appropriate to the power it wields.

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

SOCIAL SECURITY
Office of the Inspector General

December 19, 2001

The Honorable Michael G. Oxley
Chairman, Committee on Financial Services
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

This letter is in response to your request dated November 21, 2001, for further information in connection with my November 8, 2001, testimony concerning preventing identity theft by terrorists and criminals. You submitted a list of questions and asked that I answer them for the record.

My answers are shown on the enclosed list, which also repeats your questions. As you requested, we are also emailing the answers to fsctestimony@mail.house.gov .

If you need further information, please call me or have your staff call Douglas Cunningham at (202) 358-6319.

Sincerely,

James G. Huse, Jr.
Inspector General of Social Security

Enclosure

Panel One, Question 3(a):

What are your thoughts on scaling back the use of the social security number as a national identifier? Would this offer us any kind of a solution to minimizing the public's access to social security numbers and thereby minimize theft?

In many ways, the Genie is already out of the bottle, and it would be futile to try and totally reverse the course. With respect to financial transactions and many government transactions, the Social Security number is so intertwined in our daily lives that a sudden ban, or even a significant "scaling back" on its use in these transactions would create havoc. Moreover, it would then have to be replaced by a new identifier that would be equally prone to abuse and theft.

That said, I do advocate limiting the role of the Social Security number in areas where its use is more a matter of convenience than necessity. The sale and purchase of Social Security numbers cannot continue. The use of Social Security numbers as identification numbers by institutions such as schools and hospitals needs to be stopped. And the public display of Social Security numbers is a dangerous habit from which we must now wean ourselves.

We can never return to the days when the Social Security number was used only for Social Security. But we can, and must, exercise more care in how the numbers are issued and how they are used in commerce.

Additional Questions:

1. **In your testimony, you seem to be concerned about the availability of death information to the public, since it exposes a very large number of issued Social Security numbers (SSNs). As a policy matter, should the SSNs of those who have died not be made public in your view?**

   Certainly there are many voices on this issue, from Courts to public interest groups. My perspective is that of the official charged with protecting the integrity of the Social Security number, so I will always favor more restrictive practices with respect to the display and availability of SSNs, regardless of whether the number-holder is still with us.

   The reality is that if death reporting is timely and accurate, public availability of the SSNs of deceased individuals is of little use to would-be thieves. But the reality, as I testified, is that the system is imperfect. As such, I would certainly welcome a change to existing law that would make the Death Master File unavailable to the public. But I am enough of a pragmatist to understand that there are many legitimate uses to which that information is put, and that the Courts have spoken as to the need to make that information available under existing law.

2. You mention your office has made recommendations to the agency to improve the reliability of its death information. How accurate is the death master file? Has SSA implemented your recommendations?

The accuracy of the Death Master File (DMF)—which contains approximately 69 million records—is reliant on two types of recordkeeping. Therefore, pinpointing the DMF's accuracy is complicated.

First, the DMF does not contain every deceased SSN holder and therefore the absence of a particular person in the DMF is not necessarily proof the person is alive. Our audit work has concluded that SSA is aware of a particular grouping of 1.3 million deaths of SSN holders that are not listed in the DMF. Specifically, in our July 2000 audit report, *Improving the Usefulness of Social Security Administration's Death Master File* (A-09-98-61011), states we found that about 1.3 million beneficiary deaths were not recorded on the DMF. The report also noted that SSA does not verify the accuracy of death reports on the DMF for non-beneficiaries. (SSA only verifies death reports for individuals who are receiving Old-Age, Survivors and Disability Insurance benefits or Supplemental Security Income payments.)

Second, the DMF contains lists of individuals who are not actually deceased. In our June 2001 audit report, *Old-Age, Survivors and Disability Insurance Benefits Paid To Deceased Auxiliary Beneficiaries* (A-01-00-20043), we estimated that, as of June 1999, the DMF contained 4,152 OASDI auxiliary beneficiaries erroneously listed as deceased. Further, 4,077 of these 4,152 beneficiaries had their personal identifying information (date of birth and SSN) available to the public on the Internet.

We have recommended steps that SSA can take to improve the DMF's reliability. Among these recommendations were matching the DMF against auxiliary benefit records to ensure that individuals receiving benefits in one system are not listed as deceased in another, and reconciling the 1.3 million deaths recorded in SSA's benefit payment files that do not appear in the DMF.

Below is a summary of our prior recommendations related to DMF information, including a status of SSA's progress in implementing them.

Report	Issues Identified	Recommendations/Current Status
The Social Security Administration's Procedures to Identify Representative Payees Who Are Deceased (A-01-98-61009) issued by SSA/OIG in September 1999	Incorrect death information was recorded on SSA's DMF and payment records. Specifically, the OIG estimated that 465 representative payees were recorded as deceased even though they were still alive.	SSA should identify and correct instances in which a payment record contains an erroneous date of death for a representative payee. [SSA issued instructions to its field offices to address deceased rep payee situations in February and March 2001.]
Performance Measure Review: Summary of Pricewaterhouse Coopers, LLP Review of SSA's Performance Data (A-02-00-20024) issued by SSA/OIG in March 2000	Individuals who are alive and currently receiving OASDI and/or SSI benefits are listed as deceased on the DMF.	SSA should develop policies and procedures for the resolution of unmatched items in its Death Alert, Control, and Update System (DACUS) and establish a work group with primary responsibility for resolution. [SSA formed a workgroup in March 2001. The workgroup prepared a report containing recommendations, and SSA's Office of Policy is reviewing this report. DACUS Release 5, which is currently unscheduled for implementation, will be the vehicle for incorporating changes recommended by the workgroup.]

Report	Issues Identified	Recommendations/Current Status
Improving the Usefulness of the Social Security Administration's Death Master File (A-09-98-61011) issued by SSA/OIG in July 2000	SSA's master payment files contained death information that had not been included in its DMF. OIG determined that about 1.3 million deaths remained unrecorded on it death file. It also reported that the DMF did not identify which deaths had been sufficiently verified by SSA as a basis for awarding or terminating benefits.	SSA should reconcile the 1.3 million deaths that were recorded on its payment files, but not recorded on the DMF and ensure that, in the future, all deaths are included on the DMF. SSA should annotate the DMF to identify which deaths have been sufficiently verified by the Agency prior to awarding or terminating benefits. [SSA reported in December 2001 that its Office of Systems was addressing the need to reconcile the 1.3 million deaths. Also, SSA has included the second recommendation in its Client/Enumeration Five-Year Plan which is expected to upgrade DACUS with verification information in release 3.1.]
Old-Age, Survivors and Disability Insurance Benefits Paid to Deceased Auxiliary Beneficiaries (A-01-00-20043) issued by SSA/OIG in June 2001	The OIG estimated that 4,152 auxiliary beneficiaries receiving OASDI payments had dates of death recorded on SSA's death file even though the beneficiaries were actually alive.	SSA should periodically (at least annually) match the DMF against its auxiliary payment records to identify records in which a date of death is posted on the DMF but for which payment records show current benefit payments. [As of August 29, 2001, SSA matched a portion of the payment records—approximately 3.4 million records—with the DMF. The results are currently being analyzed in an effort to refine the matching criteria in order to limit the personal contacts by SSA to verify a death prior to terminating benefits.]

3. **When you testified before our Subcommittee last year regarding the use and misuse of SSNs, you provided suggestions to prevent its misuse. One of the recommendations was regulating the sale of SSNs. In your testimony today, you again give this recommendation and state that cooperation is needed to impede the misuse of the SSN. Can you expound on what type of cooperation is needed among Federal agencies and between the government and the financial services industry?**

   It was not my intention to tie the need for cooperation between Federal agencies to the sale of SSNs. Certainly inter-agency cooperation is critical to the overall protection of the integrity of SSNs, as I pointed out in my testimony when discussing the need for Immigration and Naturalization Service (INS) verification of INS documents presented in support of SSN applications. However, the cooperation to which I referred in discussing regulation of the sale of SSNs is more in the spirit of compromise of each party accepting less than they might want. For effective change to occur, SSA must be prepared to accept the importance of the SSN in the private sector, while the financial services industry must acknowledge that the need to tighten controls over the SSN may prohibit certain practices. I think there is already a firm understanding of the need to strike this balance on the part of both parties, and I am confident that as we seek to provide better protection for the SSN in the months to come, that awareness will continue to grow.

For Release on Delivery

Collection and Use of SSA's Death Data

JOINT HEARING WITH
HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
AND
SUBCOMMITTEE ON OVERSIGHT AND
INVESTIGATIONS OF
THE COMMITTEE ON FINANCIAL SERVICES

NOVEMBER 8, 2001

FRITZ STRECKEWALD
ACTING ASSISTANT DEPUTY COMMISSIONER FOR
DISABILITY AND INCOME SECURITY PROGRAMS
SOCIAL SECURITY ADMINISTRATION

Ways and Means Social Security Subcommittee
Committee on Financial Services Subcommittee on Oversight and Investigations
November 8, 2001

Chairman Shaw, Chairman Kelly, Representative Matsui, Representative Gutierrez, and Members of the Subcommittees:

Thank you for asking me to appear before you today to discuss the Social Security Administration's (SSA) collection, maintenance, and distribution of death information, which is critical to the administration of our programs. We use this information to determine continuing eligibility for benefits, as a lead for entitlement to benefits, and for other program and integrity purposes. We take our role as program stewards seriously and the integrity of this information is of utmost importance.

Death Information

Collection

First, I would like to provide some background on our death data. The Death Master File (DMF) was created because of a 1980 consent judgement resulting from a lawsuit brought by, a private citizen under the Freedom of Information Act. As a result of that consent judgement, which specifically requires that identifying information including the Social Security number be divulged, SSA now maintains a national file of death information, the DMF. Under the Freedom of Information Act, we are required to disclose the DMF to members of the public.

SSA obtains death reports from many sources, with 90 percent of the reports obtained from family members and funeral homes. The remainder of the information comes from States and other Federal agencies through data exchanges and reports from postal authorities and financial institutions.

We match these death reports of the approximately two and one half million people who die annually against our payment records. We terminate benefits for those individuals who are deceased. This data is also used as a lead for entitlement to benefits for surviving family members. We annotate the death on our master Social Security and Supplemental Security Income beneficiary records and on the Social Security number record file for beneficiaries and non-beneficiaries.

Since studies have shown that death reports from family members and funeral homes are over 99% accurate we do not verify these reports, and immediately take action to terminate benefits. For our beneficiaries, we currently are verifying reports from financial institutions and postal authorities after terminating benefits. However, we are changing our policy to verify these reports before taking any action. Reports obtained through data exchanges require verification through our field offices before an individual's death is posted to our payment records and their benefit is terminated. This includes death data received from the States.

We do not verify death reports on persons not receiving Social Security benefits, and it would be difficult for SSA to do so since we do not have address or other identifying information on these individuals.

Verification of death means that a reporter, usually someone in the beneficiaries' home, a representative payee, a nursing home, a doctor or hospital, has agreed that the person is deceased and, if the date of death is an issue, corroborates the date reported.

Once death reports received from States are verified, the state data is then considered SSA data. This is important, because some states limit (re)disclosure of their records to only Federal benefit paying agencies. Section 205 (r) of the Social Security Act (42 U.S.C. 405 (r) gives the States this authority to limit SSA's (re)disclosure of their death records. Therefore, if SSA is providing death information to other parties we are careful that the information that we release is SSA data.

Maintenance

It is important to know that the DMF is updated daily based on reports SSA receives and contains approximately 70 million records, including Social Security beneficiaries and non-beneficiaries, with verified and unverified reports of death. If available in our records, and as required by the consent judgement, the file contains the deceased's SSN, first name, middle name, surname, date of death, date of birth, state, county, zip code of the last address on our records, and zip code of the lump sum payment.

Distribution

Federal agencies, State and local government, and the private sector use the national death data file. We are reimbursed for the cost of providing this information.

Currently, as required by law, SSA shares the full DMF with Federal benefit paying agencies that use the data to conduct matches against their own beneficiary rolls. Under the matching agreement with SSA these agencies are required to independently verify the fact of death before taking any adverse action. These agencies include the Railroad Retirement Board, Department of Defense, Department of Veterans Affairs, Department of Labor and Office of Personnel Management.

Other Federal agencies that use the information on the DMF include the State Department, Department of Education, National Institute for Occupational Safety and Health, Internal Revenue Service, Brooks Air Force Base, Department of the Treasury, and the Department of Commerce. In addition, several State and local agencies receive this information.

The publicly available DMF, which is the version that has no state data, is provided monthly to the Department of Commerce, National Technical Information Service (NTIS) which in turn makes it available to the public under the Freedom of Information Act. SSA currently does not have the capacity to provide a large number of individual subscribers with this information, and NTIS, because of its established distribution network, is the more appropriate agency to undertake any such distribution.

NTIS distributes it to subscribers by either a tape file or CD ROM version. Due to the large number of cartridges customers are encouraged to purchase the full file on CD-ROM. Purchasers who intend to keep their DMF current need to purchase a subscription to the DMF, which includes the full file, issued quarterly, and monthly updates.

Some of these private companies, including genealogical publishing companies create their own files from the DMF. Some private web sites have these files online.

Improvements

We are currently upgrading the DMF. These improvements will help to ensure that death data is posted to the correct record, that the most reliable source of death is used, that incorrect deaths are removed from all records and that field office staff are able to resolve cases where SSA's files contain inconsistent death data. We expect to have the upgrade completed within the next year.

We are also piloting an electronic transfer of death information from the States. This system is designed to enable SSA to receive death reports within 24 hours of receipt in the State vital statistics. SSA can then take action on those cases to terminate benefits.

Another improvement I want to mention is that we are currently exploring electronically transmitting our DMF data to the NTIS rather than sending it to them by Federal Express. We are prepared to do that immediately, as soon as the NTIS is ready to receive it. In

fact, we transmit the DMF to the Office of Personnel Management electronically now. Transmitting the data more frequently is also possible, perhaps weekly or biweekly.

Electronic Data Exchange

It is also important to mention that SSA also has an electronic data exchange, known as the State Verification and Exchange System (SVES), with all States and a large number of Federal agencies. This SVES is an electronic overnight query process that enables requesters to enter a query for any individual.

If the individual is shown as deceased on our payment record, the requestor is notified within 24 hours of the request. This system processes approximately 2 million records on a daily basis. Using the SVES, State Food Stamp agencies can access our death records so that they can ensure that benefits are not paid to deceased individuals.

Social Security Number Safeguards

I would also like to discuss an issue that deeply disturbs all of us at the Social Security Administration, we are deeply affected by the tragic events that occurred on September 11. There are indications that some of the terrorists had Social Security numbers and cards, which may have been fraudulently obtained.

As soon as we learned of this, we formed a high-level response team, which includes participation from our Office of the Inspector General and from the New York and San Francisco Regions. The response team is reexamining our enumeration process to

determine what changes we need to make in our policies and procedures to ensure that we are taking all necessary precautions to prevent those with criminal intent from using Social Security numbers and cards to advance their operations.

The response team is also reviewing the recommendations the Inspector General has made over the last five years with respect to enumeration. They are also looking at several initiatives that SSA already had underway to identify those that can be accelerated.

The team has completed its early assessments and we are evaluating their first set of recommendations. They are just the beginning of our efforts to strengthen the process.

One recommendation that we have already acted on is to establish an interagency task force on enumeration. The focus initially will be to strengthen enumeration policies with respect to those who have recently entered the country. Later the interagency taskforce will undertake a comprehensive review of policies and procedures for enumerating immigrants and develop cooperative strategies between the agencies.

Over the last few years we have made changes to our Social Security number process to improve our security procedures. Those changes sought to strike a delicate balance between measures to ensure the integrity and security of the enumeration process and a desire to get a number issued to the applicant as quickly as possible. But we all know

that the world changed on September 11, and we need to reassess that balance between customer service and security.

That brings me to your bill, Mr. Shaw, H.R. 2036, the Social Security Number Privacy and Identity Theft Prevention Act of 2001, which you have developed over the last few years, with Mr. Matsui and other members of the Social Security Subcommittee who have cosponsored the legislation. This Administration supports the goals of your legislation to enhance privacy protections for individuals and to prevent the fraudulent misuse of the Social Security number, and we look forward to working with you and the Subcommittee members to best achieve those goals.

Conclusion

Thank you for the opportunity to discuss with your committees how SSA gathers and distributes death information. I will be glad to answer any questions.

The Privacy Act of 1974, as amended, generally prevents an Agency from disclosing records contained in a system of records, such as those at issue here, without the written consent of the subject of the record unless one of twelve exceptions apply. The only possible applicable Privacy Act exception that might apply is the routine use provision. However, SSA has not established a routine use for disclosure to financial institutions and by regulation can only establish a routine use to administer SSA programs or to administer other programs with similar purposes.

SSA has established electronic routines for providing SSN verification (identity verification) to non-public third parties such as financial institutions with the written consent of the SSN holder. While none of these routines allow online verification, they do provide overnight verification. Third parties that wish to obtain SSN verifications with written consent may enter into a formal agreement with SSA whereby they can submit requests electronically, while retaining consent statements that have been previously approved by SSA.

We believe that electronic payments actually enhance our ability to learn of deaths of beneficiaries living abroad because the bank provides us with another source of death information.

Also, the benefits of payment via electronic funds transfer (EFT) versus checks result in the safety, convenience and timeliness that direct deposit provides, given the delays and difficulties associated with overseas mail delivery. This is more significant now than ever before due to recent events affecting both domestic and international mail delivery. Normal delivery of checks to foreign countries can delay receipt to our beneficiaries by up to 2 weeks, whereas payment by EFT usually results in timely deposit into their accounts.

Wherever available in foreign countries, we think EFT provides the same type of excellent public service to beneficiaries living in those countries that has come to be expected by those living in the United States.

Questions Submitted by the Subcommittee on Social Security and Congressman Luis Gutierrez - November 8 Hearing on Preventing Identity Theft by Terrorists and Criminals

Congressman Gutierrez

What does SSA consider to be the main reason for the fast number increase of identity theft cases?

- Since most identity crime does not involve SSA or its programs, and SSA's own data are extremely limited, we have no basis on which to respond. We defer to our Office of Inspector General (OIG) and the Federal Trade Commission (FTC) for more specific information.

- Over the last three years, an average of about 40% of the calls to the Office of the Inspector General (OIG) hotline were related to the Social Security number. In August 1999, an OIG study based on a sample of allegations indicated that over 80% of allegations relate to identity theft.

Subcommittee on Social Security

In your testimony, you say your agency does not have the capacity to provide a large Number of individual subscribers with this information. Can you explain why? What would it take for you to be able to link up with individual subscribers electronically?

- The Death Master File (DMF) consists of nearly 70 million records. Each of these records is about 100 positions, or bytes long. Given the existing transmission capabilities between SSA and DMF requesters, it is not possible to transmit the full DMF to requesters. Such a transmission would take several days with the current connections.

- We have the ability to electronically transmit updates to DMF monthly and we are currently doing this with OPM. We are working with the other Federal agencies to whom we provide monthly updates to assist them to establish an electronic transmission process.

- Our current systems architecture supports the existing process, which requires us to provide direct updates to a limited number of Federal agencies and to NTIS, who provides this data to private sector customers. Changing to a process where SSA provides the DMF and updates directly (bypassing NTIS) would require a study of the various alternatives to design the appropriate systems architecture and could involve significant costs.

I'm pleased to see that you are exploring electronically transmitting the death master file data to the National Technical Information Service (NTIS) at Commerce, rather than sending it to them by Federal Express. You say you are ready to do this immediately as soon as Commerce is ready to receive it. When will that be? (Office of Systems)

- We are working with NTIS to determine when they will be ready to receive DMF data electronically. We defer to the Department of Commerce to provide further information.

You also say transmitting the data more frequently is possible. Will you do this? When? How often -Weekly? Biweekly?

- Yes, we are working with NTIS to determine how and when they will be ready to receive DMF data electronically, and we can provide weekly electronic updates. We defer to the Department of Commerce to provide further information.

In your testimony you discuss your pilot of electronic transfer of death information with the States. Can you tell us more about that pilot? How many States are involved, what have been the results? Are you planning to implement such transfers nationwide and how soon? Could you set up this same sort of exchange with private sector groups? If not, why not?

- Electronic Death Registration (EDR) would replace the current paper driven process for collecting, filing and sending death certificate information in the States. Under Section 205 of the Social Security Act, SSA is required to obtain death certificate information from the States. This reengineered process would enable SSA to obtain more timely and accurate death data from the State sources to administer our programs and to share with our DMF customers.

- In September 1999, SSA awarded a contract with the National Association for Public Health Statistics and Information Systems (NAPHSIS) to develop standards and guidelines for the States to use when implementing their EDR systems. Also under this contract, we tested a concept that allows us to receive an SSN for verification and return the response to the source, and to receive an electronic death report within 5 days of the person's death. NAPHSIS worked with the State of New Jersey to modify their existing EDR system. Preliminary results show that the proof of concept pilot, completed in October 2001, was successful.

- In May 2001, NAPHSIS published a Standards and Guidance document on their web site for the States to use when implementing EDR. SSA awarded a FY 2001 contract to NAPHSIS to assist States in implementation of EDR and provide training. NAPHSIS will also do some marketing of EDR to the various death registration participants professional associations.

- In September 2001 we awarded contracts to partially fund EDR in New Hampshire and the District of Columbia. This begins a national rollout of EDR. By FY 2003 SSA will verify SSNs of decedents in real time online and take immediate action on the death records it receives. We continue to support a national rollout of EDR and expect to continue partially funding this project as the budget permits.

- EDR is a more efficient process for SSA to use for collecting State death reports. It is not a data dissemination system. We will use information we get via EDR to update the DMF. The DMF will continue to be our method of disseminating death information to users.

Is the task force you mentioned regarding enumeration being operated by SSA or are you a member of it? Have the other agencies invited to these meetings shown a willingness to participate? What product do you anticipate coming forth from the taskforce? Is the scope of the taskforce limited? If so, to what topics and objectives? When do you see the task force developing policies? Do you have any sense of how quickly some of these might become procedure?

- SSA made a commitment to the White House to work with INS and the Department of State to review SSA's enumeration policies and determine how best we could work together to prevent the issuance of Social Security numbers (SSNs) to noncitizens who are not eligible for a number. As a result of an invitation issued by SSA, we had our first meeting with INS, the State Department, The Office of Refugee Resettlement, and OMB on November 9, 2001. Since then, we met separately with the Department of State to determine the usefulness of their data for verifying the status of refugees who are applying for an SSN. We have also had several conversations with INS.

- While the taskforce focused on ways to improve SSA's enumeration process, we are open to further data exchanges with INS and the State Department. Those discussions are just beginning but we hope to have some new procedures in place by early 2002. Also, we are exploring long-range ideas that could be implemented within the next 12 months. Our ultimate goal is to make sure that SSA's enumeration policies and procedures both serve and protect the American public.

- In response to the events of 9/11, SSA also immediately formed an Enumeration Response Team, tasked with reviewing SSA's enumeration policies and procedures. In October the Team presented a set of near-term recommendations for change to then-Acting Commissioner Massanari. Mr. Massanari approved them immediately. These recommendations will be implemented within 90 days of approval. The Team has also completed a review and analysis of the recommendations over the last several years from SSA's Office of the Inspector General regarding enumeration. Where possible, activities on recommendations that had been accepted by SSA are being accelerated and recommendations to which SSA had previously disagreed are being reconsidered. In addition, the Team will provide longer-term recommendations for the Commissioner's consideration.

You also state in your testimony that SSA is reimbursed for the cost of providing the death information. How does this occur? How much do you receive annually? How is this money used?

- SSA enters into annual reimbursable agreements with the 12 agencies that currently purchase the DMF. The total current annual cost to SSA for these exchanges is approximately $80,000. The agencies that receive the DMF are billed quarterly and payment is made to SSA's Office of the Deputy Commissioner for Finance, Assessment, and Management. The amount recovered is detailed by Common Accounting Codes and returned to the offices providing the services, SSA's overhead account, and the Information Technology (IT) fund.

In light of the news that a terrorist obtained the SSN of a woman who had been deceased for approximately 10 years, some have suggested deactivating SSNs. What is your opinion on this? Is it feasible?

- It is important to understand that we only issue a Social Security number once. It is never used again.

- Once we receive a report of death, our records are flagged indicating that the person is deceased.

- We maintain that record because earnings during the year of death need to be applied to that account. Where earnings after the year of death are applied, there is an alert that is generated so an investigation can be undertaken.

- The account remains there, too, because family members of that numberholder, for example, a child or widow, could later file for benefits on that account.

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Financial Services; and Subcommittee on Social Security, Committee on Ways and Means

For Release on Delivery
Expected at
10:00 a.m., EST
on Thursday
November 8, 2001

SOCIAL SECURITY

Observations on Improving Distribution of Death Information

Statement of Barbara D. Bovbjerg, Director
Education, Workforce and Income Security Issues and

Richard J. Hillman, Director
Financial Markets and Community
Investment Issues

GAO-02-233T

Chairwoman Kelly, Chairman Shaw, and Members of the Subcommittees:

Thank you for inviting us here today to provide you with our observations on the gathering of death information and its distribution to financial institutions. Over the past few years, Congress, law enforcement, and others have expressed concern over the use and misuse of Social Security numbers (SSNs). Accurate and timely death information (i.e., notification of death), including the SSN, is critical to the integrity of the federal benefits system and can help protect consumers' financial assets against fraud. However, the SSN also is a key identifier used by unscrupulous individuals to steal identities, obtain false identification documents, and commit fraud.[1]

In light of the recent terrorist attacks, your committees have considered actions to prevent potential terrorists and criminals from creating false identities using SSNs and, in particular, to prevent the misuse of a deceased person's Social Security number. Accordingly, you asked us to examine the process for gathering death information and distributing it to financial institutions. Specifically, our remarks will focus on (1) how long each stage of the process takes, (2) what actions the financial services industry reported taking to prevent the misuse of a deceased person's Social Security number, and (3) what possible steps could be taken to improve the timeliness of collecting and transmitting death information. Our observations are based on prior GAO work, preliminary work at the Social Security Administration (SSA) and the National Technical Information Service (NTIS), and discussions with the three national credit reporting agencies, eight of the largest credit card issuers, and two national trade associations. We have not independently verified the timing of the process for distributing death information, nor have we assessed the costs associated with improving the timeliness of this process.

In summary, death information collected by SSA generally reaches financial institutions and other entities within 1 to 2 months of a person's death, although delays in processing and distributing information sometimes occur. Complete files of recent deaths are distributed quarterly and updated monthly with information from a number of sources. SSA receives direct reports of deaths from relatives and friends of the deceased and from funeral homes. SSA also obtains further data by cross-checking its own

[1] *Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited* (GAO/GGD-98-100BR, May 1998).

files with information from other federal and state agencies. The financial services industry relies on Social Security numbers as one of the primary identifiers to establish the identity of customers, to assess the creditworthiness of customers, and to protect against fraud. Financial institutions check personal information provided by those seeking new credit, and many subscribe to fraud prevention products. The financial services representatives we spoke with expressed interest in receiving more timely death information. SSA is exploring ways to accelerate the process of receiving and processing death information, including producing updates weekly rather than monthly, and transmitting death information to NTIS electronically. In a long-term initiative, SSA is participating with state and local officials to develop an Electronic Death Registration System that could reduce the time to report death information to SSA. However, cost and legal issues remain to be resolved before the electronic system can be fully implemented.

Background

Each year, about 2.5 million people die in the United States. SSA is responsible for keeping track of death information on beneficiaries of the Social Security system, but it gathers such information on non-beneficiaries as well. SSA collects reports on deceased persons from a number of sources, including funeral homes, relatives, other federal agencies, and state vital record offices. SSA places information from the reports, such as the date of death, in its Numerical Identification File (NUMIDENT)—the master file of Social Security number holders. It contains information collected when an individual applies for a Social Security card, when a change of name or other correction is recorded, and when a death is reported. SSA periodically extracts death information from this file to generate the Death Master File (DMF). SSA may make death information available to the public under the Freedom of Information Act.

SSA makes the DMF file available to the public, including financial institutions, through NTIS. NTIS offers this file as a single issue or a subscription. Purchasers who wish to keep their DMF current are required to purchase a subscription, which includes the full file and monthly updates. NTIS makes this information available to its 107 subscribers on magnetic tape or CD-ROM. NTIS subscribers include churches, computer companies, federal and state agencies, insurance companies, non-profit organizations, universities, the national credit reporting agencies, and other financial services organizations.

Death Information Is Distributed to Financial Institutions Within 1 to 2 Months

Death information is collected and transmitted through several steps. Relatives, friends, or funeral homes are generally the first to report deaths to SSA, and the reports typically reach SSA field offices and processing centers within a week of the death.[2] According to SSA, these sources account for about 90 percent of the death information it receives. The remaining reports come from other federal or state agencies.

Processing information from relatives, friends, or funeral homes generally takes another week after SSA receives the notification. After a death report arrives at a field office or processing center, SSA checks the Master Beneficiary Record or the Supplemental Security Record to determine whether the deceased was a Social Security program beneficiary.[3] Death information is recorded directly on NUMIDENT within a few days of the report's receipt. If the deceased was a beneficiary, benefits are also terminated on the Master Beneficiary Record.

In some cases, death reports are delayed or SSA requires more than a week to complete the processing of a report. About 5 percent of the deaths reported to SSA, for example, are identified from SSA computer matches with records of deceased individuals provided by other federal agencies, such as Veterans Affairs and the Centers for Medicare and Medicaid Services, or state agencies, such as state vital statistics bureaus. SSA field offices must verify any death report that was based solely on information from these matches before terminating any benefits or recording the death information on NUMIDENT. Because death data provided by states to SSA is restricted,[4] some deaths may not be recorded on the DMF distributed to financial institutions.[5] Over time, the number of death records that are

[2]For example, funeral home directors, who are generally responsible for submitting death certificates to the state vital statistics bureaus, report deaths to SSA by submitting a form to local SSA field offices.

[3]The Master Beneficiary Record and Supplemental Security Record are the principal SSA payment files for the Old Age, Survivors, and Disability Insurance and the Supplemental Security Income programs, respectively.

[4]According to the National Association for Public Health Statistics and Information Systems (NAPHSIS), states restrict the disclosure of their death information to secure compensation for its use and to maintain confidentiality. NAPHSIS is a not-for-profit organization representing most of the state registrars and directors of vital statistics.

[5]42 U.S.C. 405(r) permits SSA to restrict state-supplied death information to federal benefit-paying agencies.

affected by this restriction is unclear. Once SSA field offices verify the state-supplied death information with another source and take the necessary action to terminate benefits and update its benefit records, disclosure of the death information is no longer restricted. However, the time period from the date of death until these deaths are recorded on NUMIDENT may be quite long, because death reports from states may be 90 to 120 days old when they arrive at SSA.

The remaining 5 percent are based on files from the Department of the Treasury of payments returned by postal authorities or financial institutions. A Department of the Treasury official told us that it was likely that these reports require more than a week from the date of death to reach SSA. However, we did not verify this information and could not determine how much more than a week might elapse.

At the beginning of each month, SSA extracts death information from the NUMIDENT for the DMF and sends the file to NTIS. According to NTIS officials, the files generally arrive within the first week of the month. NTIS generally needs another 2 to 4 days to produce and send the magnetic tapes and CD-ROMs to its subscribers. In total, about 1 to 2 months elapse between a person's death and the time when the death information is available to financial institutions and other NTIS subscribers, depending on when the death notice is first received by SSA.

Actions Taken By Financial Institutions to Prevent Misuse of Deceased Individuals' Social Security Numbers

The financial services industry relies heavily on SSNs as a key identifier for a number of purposes, such as the reporting of information to the Internal Revenue Service or the accurate processing and recording of customer financial transactions. The timely receipt of death information and prompt updating of financial data are key factors in the industry's ability to prevent fraud and identity theft involving the SSNs of deceased individuals.

In our discussions with representatives from the financial services industry, they reported taking a number of steps to verify information on customers applying for new credit. For example, financial institutions check the creditworthiness of customers by obtaining the credit history of an applicant from credit reporting agencies, using the SSN as one of the key identifiers. However, for existing accounts, most financial institutions we spoke with did not use a formal process or central data source to identify deceased customers. Instead, they relied primarily on family members and on executors or trustees of the estate to provide this information. For existing customers receiving Social Security benefits via direct deposit,

Social Security stated that it generally notifies the financial institution of a beneficiary's death within 24 hours of receiving notice. However, as we discussed above, there could be delays in SSA receiving such notices.

Some of the institutions we spoke with were aware of the Death Master File but were (1) unsure about the information it contained or (2) not aware that they could subscribe to the file from NTIS. Others were not aware that the Death Master File existed. According to the NTIS subscriber list, very few banks subscribe through NTIS for the Death Master File. Only one of the financial institutions we spoke with reported tracking losses or the frequency of fraud associated with deceased customers. However, the financial institutions we spoke with reported that their losses or the frequency of occurrence were not material. Most financial institutions told us that they subscribed to fraud prevention products or services offered by the credit reporting agencies that included alerts for deceased persons' Social Security numbers.

All three national credit-reporting agencies reported subscribing to and receiving the monthly updates to the DMF. However, one credit reporting agency relied solely on the quarterly Death Master File and not on the monthly updates for its normal credit reporting and fraud services. We also found that the credit reporting agencies made the data from the DMF available only for subscribers to their proprietary fraud prevention products. In contrast, death information reported directly to the credit reporting agencies by credit issuers and family members was made available to all their users, along with other credit information on a customer's credit history. This information was generally provided within one to two billing cycles.

Financial institutions also subscribe to other sources for death information. One information service we contacted primarily used the Death Master File and supplemented it with information from other sources, such as funeral homes and local governments. It provided screening and matching services to its clients, to identify deceased customers. The representative we spoke with indicated that his service's clients often lacked the necessary technology infrastructure to process and maintain the Death Master File. This representative also noted that the timeliness of data contained in the DMF had greatly improved since the move to the monthly updates (from quarterly updates). However, the representative said that more frequent updates—weekly or daily—were needed.

Two credit card associations that we contacted have also taken some steps to help prevent the misuse of Social Security numbers of deceased individuals. For example, they cosponsored a verification system for bankcard applications. This system was designed to verify such things as an applicant's address, telephone number, and Social Security number, and whether he or she has provided any questionable data on the application. This system, which was designed to help members reduce losses attributed to fraud, had several fraud alert codes, one specifically designated to flag the use of the Social Security number of a deceased individual.

In our discussions with representatives from the financial services industry, most expressed an interest in receiving more timely death information to narrow the window of opportunity in which criminals can perpetrate fraud. The credit reporting agencies expressed an interest in receiving more frequent DMF updates, but their responses varied regarding how frequently SSA needed to provide those updates. Some could handle the updated information daily; some could process the updates only biweekly. Some recommended that SSA provide a Web-based "look-up" service to verify death information.

Possible Steps for Improving the Collection and Transmission of Death Information

SSA is exploring ways to speed up the collection and processing of death reports and the transmission of death data to financial institutions. In the near term, SSA and NTIS are discussing ways to speed up the transmission of death information to users, such as financial institutions. SSA officials have stated that it would be relatively easy to produce updates on a weekly rather than monthly basis. Additionally, SSA and NTIS officials stated that it should be possible for SSA to transmit updates electronically to NTIS, and that NTIS could also provide its updates to financial institutions electronically. SSA officials have indicated that it would be more difficult and costly to provide updates more frequently than weekly, or to bypass NTIS and provide electronic updates directly to financial institutions.

As we have previously reported, delays in SSA receiving some state death reports have hindered the prompt processing and distribution of such information. In a long-term initiative, SSA is participating in several pilot projects with state and local officials to develop an Electronic Death Registration System that, among other things, would enable the states to report deaths to SSA electronically. This system could improve the speed with which deaths are reported to SSA. For example, in a July 2001 SSA request for contract proposals of the new system, SSA required project plans to demonstrate the capability to send a "fact of death" report to SSA

within 5 days of a death, and within 1 day of receipt in the state bureau of vital records. However, state agreements with SSA preclude the agency from terminating benefits solely on the basis of state-provided death reports. Therefore, SSA also required project plans to demonstrate the capability to confirm death information electronically with entities originating the death report, such as funeral directors.

SSA and the National Association for Public Health Statistics and Information Systems officials also indicated that there are unresolved issues with the Electronic Death Registration System. These include the willingness of the states to adopt this system and SSA's ability to release state-provided death information to financial institutions. For example, SSA officials stated that it remains unclear whether states will be willing or able to pay the cost of installing automated terminals in the funeral homes, hospitals, medical examiner offices, and other locations involved in the death registration process. Additionally, SSA has not yet resolved legal issues that might preclude the release of state-provided death report information to financial institutions.

We inquired about the feasibility of SSA providing death information directly to financial institutions and others from an on-line, Web-based look-up service. SSA officials said that implementing such a system would require significant changes to various SSA systems and might raise privacy considerations.

SSA, NTIS, and the credit reporting agencies told us that additional resources would be required to process death information more frequently. However, NTIS officials expressed some concern that there should be a demonstrated demand for the improved service before making these investments.

Conclusions

In conclusion, it appears that SSA and NTIS could improve the timeliness of the distribution of the Death Master File. Improving the timeliness of death information to the financial services industry would help to narrow the window of time that a criminal has to open new accounts using a deceased individual's identity. Additional education to the financial services industry about the availability and contents of the Death Master File would also be helpful. Providing more timely death information and making financial institutions more aware of a reliable source of such information are tangible steps that could be taken to deter criminals from using deceased individuals' Social Security numbers to obtain false

identities for use in fraudulent activities. However, improving the timeliness of death information would not by itself eliminate identity theft and is not a panacea for addressing the larger issue of the criminal misuse and theft of Social Security numbers.

Chairwoman Kelly and Chairman Shaw, this concludes my statement. We would be pleased to respond to any questions that you or other members of the Subcommittees may have.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director, or George A. Scott, Assistant Director, Education, Workforce, and Income Security (202) 512-7215, and Richard J. Hillman, Director, or Harry Medina, Assistant Director, Financial Markets and Community Investment (202) 512-8678. Individuals making key contributions to this testimony include Daniel F. Alspaugh, Emily R. Chalmers, Heather T. Dignan, Debra R. Johnson, Kay Kuhlman, and John M. Schaefer.

Responses from Barbara Bovbjerg and Richard Hillman, GAO for

Questions for the Record
Submitted by the Ways and Means Subcommittee on Social Security
to the Committee on Financial Services, Subcommittee on Oversight and Investigations
Joint Hearing Held on November 8th on
Preventing Identity Theft by Terrorists and Criminals

Page 1
Question 1(a)

Do you have any estimates on how much would it cost to implement the program that would speed up the transmission of death information to users?

We did not estimate how much it would cost the Social Security Administration (SSA) and the National Technical Information Service (NTIS) to improve the timeliness of the process for gathering death information and distributing it to financial institutions. Beginning in February 2002, SSA began providing the Death Master File (DMF) to the NTIS on a weekly basis, according to Social Security Administration (SSA) and National Technical Information Service (NTIS) officials. An SSA official told us that updates to the DMF, which SSA provided to NTIS on cartridge tape in the past, are now available electronically. SSA did not have a monetary estimate of its cost yet, but an official estimates the additional workload requirements to send information on a weekly instead of a monthly basis at 1/2 of a work year.[1]

Question 1(b)

Do you have any information about how other countries have reduced the problems of identity theft in the past? Is this a U.S. problem or is this a global problem?

How other countries have reduced the problems of identity theft in the past was not within the scope of our work. Identity theft is often a component of other crimes and could take place outside the United States as evidenced in the reported activities of some international crime rings, credit card fraud, and money laundering. However, we do not have specific information regarding the prevalence of identity theft on a global basis.

Page 3, Question 1

You state in your testimony that financial institutions, who rely heavily on the use of SSNs, do not use a formal process or central data source to identify deceased customers. Can you explain why?

[1] A work year is an estimate of the personnel requirement based on full-time equivalents and workload. The monetary amount of a work year would depend on the salary of the personnel involved and an overhead factor.

Most financial institutions we spoke with told us that they relied primarily on family members and executors or trustees of the estate to provide death information. These institutions told us that they received death information relatively quickly through these sources. In some cases notification was immediate but generally occurred within one to two billing cycles from the date of death. The institutions we spoke with did not perceive their current methods of receiving death information for existing customers to be problematic. The institutions also reported that their losses or the frequency of occurrence associated with fraud on a deceased customer's account were not material.

Question 2

You state that many financial institutions were unaware of the information contained in the DMF or were unaware of its existence. Can you tell us why?

The financial institutions we spoke with told us that the death information they received from current sources was reliable and had not explored other sources of death information, such as the Death Master File (DMF). However, most institutions reported that they subscribed to fraud prevention products or services offered by the credit reporting agencies. Others subscribed to an information service that provided screening and matching services. The primary source of death information for these products and services was the DMF. Although some of the institutions told us that they knew of the DMF, they were unaware that many of their subscription services used it.

Question 3

One of the financial institutions you surveyed stated that more frequent updates, such as weekly or daily, were needed. In your opinion, what are the technological capabilities of the users to process this information if the information were updated more frequently?

We did not assess the technological capabilities of the financial institutions we spoke with to process the Death Master File (DMF) or updates. However, most institutions expressed an interest in receiving more timely death information. All three consumer reporting agencies told us that they subscribed and received updates to the DMF. These agencies expressed interest in more frequent updates to the DMF and reported processing capabilities that ranged from daily to bi-weekly.

Question 4

Your testimony indicates that the financial services industry, including the credit reporting agencies, have many other sources of death records. Is this why they don't use the SSA data? If SSA did improve its death reporting, do you think companies would use or retain their current methods of death records?

As we stated earlier, the financial institutions have relied on a number of sources to provide them with information on customers' deaths. Our discussions indicated that SSA

data supplemented these sources and was considered "additive" in nature and most likely would not replace existing sources of death information.

Question 5(a)

Do state motor vehicle agencies ever subscribe to SSN death records?

Social Security Administration and National Technical Information Service officials told us that state motor vehicle agencies do not subscribe to SSA's Death Master File. However, under a memorandum of agreement between SSA and the states, SSA will verify certain information transmitted by a state motor vehicle agency. This information is limited to name, date of birth, and Social Security Number and will only be verified if all three fields transmitted by the agency match the information on SSA's NUMIDENT file. According to SSA, several states submit batched records directly to SSA for verification, while 17 states have the ability to verify information through a third-party, on-line service.[2] We were told that although this service does not provide for verification of specific death information, SSA may notify the state that there is a problem with a record submitted for verification that matches the personal identifiers of a deceased individual on SSA's NUMIDENT file.

Question 5(b)

Because states must issue death certificates, are there programs for the rapid reporting of deaths to motor vehicle agencies within and outside the state to prevent truly dangerous criminals from getting the photo ID?

Our discussions with driver licensing officials of five states indicate that state policies and practices for using death certificate data may differ. While officials in four states indicated that the state vital records office periodically provides death information to the state driver licensing office so that licensing records can be updated, one official indicated that the state does not attempt to match death information and driver licensing records.

Question 5(c)

There is a system that tracks drivers licenses nationally so that criminals cannot hold more than one license. Could reporting of SSN death information records to this data base be useful?

Reporting death information to national systems that track commercial and non-commercial drivers' licenses could help identify problem records, but matching identities would be difficult because there is no single integrated national drivers' license

[2] Seventeen states and the District of Columbia subscribe to AAMVAnet's Social Security Number On-Line Verification application: Alabama, Arizona, Idaho, Maine, Maryland, Massachusetts, Mississippi, Missouri, Nebraska, Nevada, New York, Ohio, South Dakota, Tennessee, Virginia, Washington, and Wyoming. AAMVAnet, a not-for-profit affiliate of the American Association of Motor Vehicle Administrators, provides computer applications and network services to its subscribers.

information system. Furthermore, two of the existing systems for information on non-commercial drivers do not use the Social Security Number as a standard identifier. Because these national systems rely on state records, some identities are likely to have been verified with SSA by the state of record, but currently less than half of the states appear to verify any personal identification information with SSA.

According to a recent report by the Department of Transportation (DOT) to Congress,[3] the Commercial Driver License Information System (CDLIS) requires the use of the Social Security Number as a standard identifier, but neither the Problem Driver Pointer System (PDPS), nor the Driver License Reciprocity (DLR) system uses a uniform identifier. Both CDLIS and PDPS are files that "point" to records that reside with the state motor vehicle agencies representing different driver populations. CDLIS, which is designed to prevent commercial vehicle operators from obtaining a license in more than one state, points to a single driver who has been issued a commercial drivers' license. In contrast, PDPS, which is a redesign of the National Driver Register for providing information about serious motor vehicle convictions in another state, can point to multiple adverse actions by the same driver. The DLR system, which provides the capacity to electronically transfer and close out the driver history records from one state to another, is not a central data base and lacks a uniform identifier, making inquiries difficult and subject to misidentification. The DOT report recommended that DOT and the states should proceed with the development of a single integrated drivers information system that uses a unique identifier, such as the Social Security Number.

[3] U.S. Department of Transportation. Report to Congress. *Evaluation of Driver Licensing Information Programs and Assessment of Technologies.* Washington, DC: 2001.

STATEMENT OF STUART K. PRATT

ASSOCIATED CREDIT BUREAUS, INC.

WASHINGTON, D.C.

HEARING ON

PREVENTING IDENTITY THEFT BY TERRORISTS

Before the Subcommittee on Oversight and Investigations of the House Financial Services Committee and the Subcommittee on Social Security of the House Ways and Means Committee

of the

United States House of Representatives

Washington, D.C.

Thursday, November 8, 2001

Chairmen Kelly and Shaw, thank you for this opportunity to appear before this joint hearing of the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security. For the record, my name is Stuart Pratt and I am vice president government relations for Associated Credit Bureaus.

ACB as we are commonly known is an international trade association representing 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services.

We applaud your willingness to hold this important hearing on the subject of the Social Security Administration's Death Master File (DMF) and its uses for fraud prevention. It is clear, now more than ever, that nothing is more vital than ensuring that this country's public and private sector have every information tool necessary to prevent fraud and illegal access to services. The key to ensuring that both the government and the private sector can fully authenticate identifying information on applications of all types is through a robust system of authentication and verification technologies. At the core of these technologies is the availability of validated consumer identification information for cross-matching purposes. The social security number plays a particularly important role in the accuracy and completeness of this cross-matching process by allowing systems to be linked to ensure that all relevant records are considered when authenticating consumer data.

Congress has already recognized and begun to act on this need for strong and effective consumer information authentication measures through the enactment of the USA PATRIOT Act, which requires the Secretary of the Treasury to establish minimum standards for financial institutions, which must verify account applicant data.[1] Further evidence of the need to authenticate the identities of applicants was heard last week in your very timely hearing, Chairman Shaw, wherein we learned from the Inspector General of the Social Security Administration that they are reevaluating the authentication systems they will need to ensure that misuse of our social security account numbering system does not happen easily.

The subject of today's hearing, which focuses on the Social Security Administration's Death Master File, is a key component in this broad assessment of how we verify identities and prevent illegal access to products, entitlements and services. Let me now address some of the specific questions you raised in your letter of invitation.

How do consumer reporting agencies use the Social Security Administration's Death Master File?

In answering this question, the Committees should consider the scope of our members' coverage of the current U.S. market place. The three major credit reporting systems, Equifax, Experian and TransUnion, which provide nationwide coverage for all credit active Americans (approximately 200 million files per data base), are subscribers to the

[1] PL 107-56, Title III, Subtitle A, Section 326.

DMF. Nationwide coverage is also provided by other key ACB member company DMF subscribers including eFunds and Dolan Media. In sum total more than a billion consumer reports of various types, which can carry DMF notifications, are sold each year to depository institutions, creditors, telecommunications companies, the insurance industry and even to governmental agencies.

In terms of uses of the death master file, these include notifying users of various types of consumer reporting and identity verification/authentication products that a particular social security number is likely associated with a deceased individual. Our members' services include providing DMF notification in products sold (such as credit reports) and also sweeping customer data bases to ID records associated with DMF records. As you can see, our members' product offerings are extensive and far-reaching.

Are there technical problems identified with the current system of providing DMF data to ACB member subscribers?

ACB will look into this question with our DMF subscriber members and respond in more detail for the hearing record. One of our members, Dolan Media, indicated to us that the Social Security Administration has made significant improvement in the DMF over the past two years. Specifically they report that data in the DMF, which used to be outdated by as much as six month is now reported more often within 30 to 60 days of the death.

What other means of obtaining information about deceased individuals are available in order for ACB members to put a "hold" on SSNs?

As with the previous question, ACB will need time to fully develop our answer. It is our understanding that ACB credit reporting system members, which are also subscribers to the DMF, do receive, at least in some cases, notification of death from lenders and other regular furnishers of information to our members' data bases. These notifications are included in special comment fields and codes, which are standardized through the association's data reporting format standard, Metro2. These comment codes are available to subsequent users of consumer credit reports.

Can you outline ways in which sources of information can be better integrated to prevent fraudulent uses of social security numbers?

Our members' systems are a good example of how the private sector is already integrating a range of information sources today. Key in this integration is the freedom to develop fraud prevention products for a range of industries.

Unfortunately, for example, the current FTC rules issued as a result of the enactment of the Gramm-Leach-Bliley Act (GLB) seriously impinge on the use of essential consumer identifying information for non-Fair Credit Reporting Act purposes. Due to the FTC interpretation of GLB, credit header data[2] is restricted even for use by other financial

[2] The term "credit header information" commonly includes information such as name, address, previous address, telephone number, and social security number.

institutions. But beyond GLB or permitted uses for consumer reports under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), under the FTC GLB rules, credit header is not available for eCommerce authentication products, location and verification of pension fund recipients, and a host of other uses which are not covered under either law. In fact, the rule may foreclose on any opportunity to use credit header for other types of security screening efforts, such as scanning airline passenger manifests.

Said differently, we need to ensure that current laws and regulations, including GLB, do not interfere with efforts to more fully integrate information sources for fraud prevention and general identity verification, in particular, where the use of credit header would take place outside of the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act.

Can you identifying steps the consumer reporting agencies are taking to update their systems to prevent fraudulent uses of the SSN.

We need more time to answer this question completely. However, we are very pleased to announce in support of your hearing that all of our members identified to date as subscribers to the DMF are ensuring that their systems are programmed to accept monthly updates of the DMF from the Social Security Administration. In fact, a majority of our members are already subscribers to the Social Security Administration's DMF monthly updates. This operational change by our members should ensure that our members' data is as updated as possible and in turn will allow creditors and other

subscribers to our members' systems to more effectively authenticate applicant information, including the social security number and prevent fraud.

Further, in closing my remarks, I am pleased to announce that ACB will create a new Task Force consisting of all members of the association which are also subscribers to the Social Security Administration's DMF. This task force will serve as a liaison with the Social Security Administration on technology and legal issues as they continue their own assessment of how best to deliver DMF data to subscribers.

Thank you again for this opportunity to appear before your committees. We support your efforts and I am happy to answer any questions.

Testimony before The House Committee on Financial Services,
Subcommittee on Oversight and Investigations
and
The House Ways and Means Committee,
Subcommittee on Social Security

November 8, 2001

Thomas J. Lehner, Executive Vice President
American Financial Services Association

Introduction

Chairwoman Kelly, Chairman Shaw, members of the committee, thank you for inviting me to testify. I am Tom Lehner, Executive Vice President of American Financial Services Association. AFSA is the leading trade association for market funded financial services companies. Our 400 member companies include consumer and commercial finance companies, auto finance/leasing companies, mortgage lenders, credit card issuers and industry suppliers.

I am here to address the issue of Identity Theft using Social Security numbers, and specifically the industry's use of the Social Security Administration's Death Master File (DMF).

Social Security numbers are the most unique identifier of individuals in the United States. The financial services industry uses these identifiers for a variety of reasons, such as customer verification, credit checks, bankruptcy filings, and monetary judgments such as tax liens. Unfortunately, the use of Social Security numbers is not secure. They are readily available and indeed used by companies, state and local governments, colleges, and even by consumers who print their numbers on their checks.

Thieves steal the Social Security numbers, and ultimately the identity of individuals both living and dead.

Financial institutions, such as credit card companies and banks, have incurred significant losses resulting from misuse of social security numbers. Consumers have also experienced monetary losses, impaired credit, and legal problems because others have amassed debts using their identities.

Industry use of the Death Master File

Financial firms have an obvious interest in making sure that individuals who open accounts are who they say they are. Companies rely on the Social Security Death Master File to protect against theft. In most cases, firms do not directly subscribe to the Death Master File, but access it indirectly via credit reporting agencies or other vendors who subscribe to it. This is both more efficient and less costly to the consumer.

For example, bank issuers of credit cards routinely obtain consumer reports on card applicants from credit reporting agencies. Because the credit bureaus periodically update their files by comparing information to the Death Master File, the credit report will contain an indicator if the individual has been reported as deceased, and the bank can use this information to decline the application or investigate the circumstances.

Other financial firms, such as securities broker-dealers, also access the Death Master File as part of the account opening process. Third party vendors who utilize Death Master File information typically do this screening.

Consumer lenders regularly use information from credit reporting agencies to review and adjust the status of existing accounts as well. It also helps to verify customers seeking to refinance existing mortgages, or who are interested in other services offered by the institution.

Naturally, financial firms have other sources of information that might indicate that a customer has died and that access to the account should be frozen or terminated. The principal source is family members, who call to notify the institution of the death of the customer, and may request changes in the name on the account or the address where statements are sent. Lawyers and estate executors are another source of this information.

Problems with the Death Master File

Whether financial institutions obtain information about deceased individuals directly from the Death Master File, or indirectly from other subscribers to the File, they have an interest in obtaining accurate and current data.

Delays between the date on which an individual dies and the date on which this information is made available to the public through the Death Master File increases the opportunities for identity thieves to defraud survivors, beneficiaries, and financial institutions.

One of the disadvantages of the current Social Security numbering system is that the agency is not always immediately notified upon the death of an individual. There appears to be no requirement for local officials to notify SSA when someone dies.

Despite their best intentions, having incomplete and incorrect information makes it very difficult for the Social Security Administration to issue an accurate Death Master File.

Steps the industry has taken

Many companies have established internal processes that deal with fraud and identity theft. In addition, companies work with customers who are victims of identity theft, and they also work with prosecutors to pursue those responsible.

Suggested improvements

AFSA supports efforts to encourage the Social Security Administration to obtain death information promptly and report it more frequently.

We also support the continued dialogue between credit reporting agencies and financial institutions to facilitate the flow of Death Master File information in bureau files. For example, there may be a need to change procedures so that when creditors report account status information to credit reporting agencies, and this information is placed in a file of a customer about whom the bureau has received death information, the creditor is made aware of that fact on a timely basis.

We believe that more financial institutions would consider subscribing to the data directly if the information provided was real time and accurate. Whether financial institutions obtain information about deceased individuals directly from the DMF, or indirectly from other subscribers to the DMF, it is in our interest and that of the consumer that we obtain correct and current data.

We're hopeful that the Social Security Administration will make both the procedural and policy changes necessary to ensure the security of our individual unique identifiers, our Social Security numbers. Thank You.

Statement of Thomas A. Sadaka, Special Counsel
For Computer Crime and Identity Theft Prosecutions, Florida Office of Statewide Prosecution

Testimony Before the Subcommittee on Social Security
Of the House Committee on Ways and Means

Hearing on the Preventing of
Identity Theft by Terrorist and Criminals

November 8, 2001

Mr. Chairman and members of the Subcommittee, my name is Thomas Sadaka and I am Special Counsel to the Statewide Prosecutor of Florida for Computer Crime and Identity Theft Prosecutions. The Florida Office of Statewide Prosecution is charged with the investigation and prosecution of multi-circuit organized crime and to assist other law enforcement officials in their efforts against organized crimes. Identity theft is among the cases handled by the Office and is currently the focus of a great deal of the resources of the office.

The Office of Statewide Prosecution was instrumental in aiding the Florida Legislature in the drafting and passing of a statute criminalizing the unauthorized use of another's personal identifying information. As a result of our involvement in this arena the Statewide Prosecutor, Melanie Ann Hines, was invited by Governor Jeb Bush to sit on the Governor's Privacy and Technology Task Force where the needs of technological advancements were balanced against issues of social security number abuse, public records abuse and general identity theft. As a result of the report generated by the Privacy and Technology Task Force, Governor Bush requested the empanelment of a Statewide Grand Jury to specifically focus on identity theft issues and what the State of Florida can do to combat this epidemic. The Office of Statewide Prosecution also serves as the legal advisors to the statewide grand jury. Since July, the Statewide Grand Jury has been devoting one week each month to the investigation of identity theft related cases.

Additionally, the Office of Statewide Prosecution has partnered with the Florida Department of Law Enforcement (FDLE) in an identity theft task force where special agents of FDLE have been assigned exclusively to the investigation of large scale identity theft cases. Cases generated by this partnership have been presented to the statewide grand jury and since July have resulted in the arrests of numerous individuals and the dismantling of several criminal organizations with identity theft losses in excess of one million dollars.

This Subcommittee is well aware of the vast impact identity theft has on our society. States are scrambling to fashion laws to criminalize this conduct and law enforcement is quick on the legislative heels to learn how to effectively investigate and prosecute these crimes. Identity theft case investigations are time and resource demanding and are impacting heavily on already budget tightening law enforcement agencies.

The victims of identity theft face their own unique problems in rectifying the damage to their good names, their credit; and restore their lives while dealing with a criminal justice system that is heavily imbued in the learning curve.

Federal, state and local law enforcement are developing a proficiency in the investigation of identity theft cases and the private sector is becoming a bit more accustomed to dealing with and assisting law enforcement and the victims of identity theft. So while the "after the fact" dealings are getting less cumbersome, the issues of prevention are becoming more important.

Society is becoming well schooled in the idea that individual social security numbers are extremely important and valuable. As such, we don't generally carry our social security cards on our persons any longer, and we take some precautions with our personal identifying information. What society has not become well schooled in is how readily available this information is to the would be identity thief through numerous sources.

It is well known to this Subcommittee how the social security number has become the de facto national identifier and is relied upon heavily by the financial industry, medical community, insurance industry, educational institutions and state and local government as a means to uniquely identify the customer. Each one of these entities reproduces the social security number within their own files and generated documents and makes this information available to others in some form. In spite of the fact that we don't carry our social security cards, the vast majority of us have our social security numbers emblazoned upon our medical insurance cards in the representation of our policy number. There are still a vast number of driver licenses from the various states in circulation that have the holder's social security number referenced as their license number.

Through the use of the Internet and the attendant speed at which information travels, the ability to gain access to personal identifying information, social security numbers and the ability to exploit that information from the perceived anonymity of a keyboard has empowered a new generation of identity thieves who have in turn made identity theft the fastest growing crime in the world. To further fuel this ability, we have information of lists of names and social security numbers routinely being auctioned off to the highest bidder on the Internet.

The push to put court files and other public records online only operates to increase the pool of information available to the identity thief. Court records are particularly attractive to the identity thief as they are, by nature, filled with personal identifying information, including social security numbers, ready for the exploit. Requiring the supplier of these records to redact social security numbers and other personal identifying information would be an immense undertaking and require far more resources than those agencies currently possess.

Through the investigation and prosecution of identity theft cases, the use of the social security number is constant. The identity thief relies more on the social security number of others than on any other personal identifying information. Evidence has shown misspelling in names, inaccurate dates of birth and incorrect addresses, however, the identity thief has success as long as they utilize a valid social security number.

When a living individual becomes the victim of identity theft, there is some ability on the part of the victim to intervene to stop the fraud. On average, victims become aware of the theft within a year of the occurrence with a great deal of victims becoming aware within a month. These victims have the ability to notify the consumer reporting agencies and the financial industry that their personal

identifying information has been compromised. Through fraud alerts and other overt acts on the part of the victim, the ability to continue the fraud is hampered. This is not the case when a deceased individuals social security number is utilized. In some instances, this type of fraud may never be discovered.

As you are aware, the Social Security Master Death File is made available to the public and private sector to determine if a social security number supplied by an applicant for credit, government benefits, state issued driver license or identification card, and the like, has been reported as belonging to a person who is deceased. In a study of state issued driver licenses and identification cards, we have learned that among those states that conduct some form of information validation, generally use the Master Death File to determine the validity of the supplied social security number. If a terrorist or an identity thief provides a social security number of a deceased individual to a state driver license administrator, prior to the updating of the Master Death File, then it is highly likely that that individual will be successful in their endeavor to obtain a state issued ID. Once that ID is issued, the possessor will be able to use it for identification until it is lost, confiscated or expires. Needless to say, this false identification will be in use for years and the downstream effect or consequence could be immeasurable.

All efforts need to be made to increase the speed at which the Social Security Master Death File is updated. Identity thieves rely heavily on obituaries and the up to six month lag time between death and the inclusion of the social security number in the Master Death File for the commission of their crimes. The current distribution method of mailing the list out on tape would seem to be outdated and obsolete.

Recommendations:

Since we all recognize the wide spread use of the social security number for purposes that far exceed the original intent, steps must be taken to provide those relying on the social security number with access to validation and confirmation information or to prohibit its use to anything beyond the original purpose and intent.

Current efforts to make online verification of social security numbers available to state governments, particularly driver license administrators, has not been effective. Very few states currently avail themselves of any real time verification of social security numbers provided by applicants. Several states interact with the Master Death File, but that interaction is not real time and as previously illustrated, once the DL or ID card is issued, it is nearly impossible to remove from the stream of commerce. Infrastructure enhancements must be employed to facilitate the interaction of states with the social security database to immediately confirm the validity of the supplied social security number and if it belongs to the person presenting the information.

Identity theft is an epidemic. The onus is upon the government to do everything in its power to prevent government's own information, primarily the social security number linked to other personal identifying information, from further victimizing her citizens.

Laws limiting the use of the social security number and punishing its unauthorized use or dissemination need to be enacted to provide the ability to prosecute those who would sell names and social security numbers to the highest bidder.

On a final note, I would recommend a campaign to educate the public as to the proper use of a social security number and to question those that request it for daily business transactions, school volunteer forms, health club memberships, and the like.

Thank you for the opportunity to be here today. I would be happy to answer any questions.

TESTIMONY
of
JOHN C. DUGAN
(Partner, Covington & Burling)

Representing the

FINANCIAL SERVICES COORDINATING COUNCIL

American Bankers Association
American Council of Life Insurers
American Insurance Association
Investment Company Institute
Securities Industry Association

BEFORE

THE SUBCOMMITTEE ON SOCIAL SECURITY
COMMITTEE ON WAYS AND MEANS

AND

THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

November 8, 2001

Testimony of Financial Services Coordinating Council

My name is John Dugan. I am a partner with the law firm of Covington & Burling. I am testifying today on behalf of the Financial Services Coordinating Council, or "FSCC," whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, Investment Company Institute, and Securities Industry Association. The FSCC represents the largest and most diverse group of financial institutions in the country, consisting of thousands of large and small banks, insurance companies, investment companies, and securities firms. Together, these financial institutions provide financial services to virtually every household in the United States.

The FSCC thanks the subcommittees for the opportunity to testify today on the misuse of the Social Security numbers ("SSNs") of deceased individuals. We continue to believe that SSNs play a central role in deterring and detecting fraud and identity theft because SSNs are the best "unique identifier" that financial institutions can use to determine whether an individual is really who he says he is. To that end, the FSCC welcomes the attention the subcommittees are giving to the issue of SSN misuse, especially the misuse of the SSNs belonging to deceased individuals.

As the subcommittee requested, my comments today focus on the Social Security Administration's ("SSA") maintenance of the Death Master File ("DMF"), on which financial institutions ultimately rely to update their records to prevent misuse of the SSNs of deceased individuals; the problems that financial institutions face in relying on the DMF due to notification lag times; and possible ways in which the system can be improved so that there is significantly less delay in updating and disseminating the DMF.

My testimony today makes three fundamental points:

- ***First,*** SSNs are key unique identifiers that are essential for financial institutions to use to guard against identity theft or other fraud or misuse (for example, use of SSNs is critical to the fight against money laundering, as has been recognized in the recently enacted anti-money laundering legislation).
- ***Second,*** the SSA's DMF is a comprehensive record of deceased individuals' SSNs, but delays in updating and disseminating this list can create opportunities for fraud and identify theft.
- ***Third,*** because financial institutions ultimately rely almost exclusively on the SSA's DMF to determine whether an SSN belongs to a deceased individual, the more frequently the DMF is updated and disseminated, and the more accessible such information is, the more effective the list will be as a tool to detect and deter fraud and identity theft.

The Integral Role of Social Security Numbers in U.S. Commercial Activities

As the GAO noted in its February 1999 report,[1] the SSA created SSNs 65 years ago as a means to maintain individual earnings records for the purposes of that program. But Congress soon realized the tremendous value to society of a unique identifier that is common to nearly every American. As a result, it began to require federal government use of the SSN as a "common unique identifier" for a broad range of wholly unrelated purposes, such as tax reporting, food stamps, Medicaid, Supplemental Security Income, and child support enforcement, among others. Moreover, as the GAO acknowledged, it has repeatedly

---

[1] "Social Security -- Government and Commercial Use of the Social Security Number is Widespread," February 1999, GAO/HEHS-99-28.

recommended in numerous reports that the federal government use SSNs as a unique identifier to reduce fraud and abuse in federal benefits programs.[2]

Following the federal government's lead, American businesses not only complied with federal requirements to use SSNs as identifiers for federal laws unrelated to social security, such as income tax reporting, but they also realized the powerful consumer benefits to be derived from comparable business use of SSNs as a common unique identifier. Thus, businesses began to use SSNs in a manner similar to the federal government. For example, businesses use SSNs to match records with other organizations to carry out data exchanges for legitimate business purposes such as transferring and locating assets, tracking patient care among multiple health care providers, and preventing fraud and identify theft. Many businesses also use SSNs as an efficient, unique identifier for internal activities.

Similarly, the financial services industry has used the SSN for many decades as a unique identifier for a broad range of responsible purposes that benefit consumers and the economy. For example, our nation's remarkably efficient credit reporting system relies fundamentally on the SSN as a common identifier to compile disparate information from many different sources into a single, reliable credit report for a given individual. Further, the banking, insurance, and securities industries each use SSNs as unique identifiers for a variety of important regulatory and business transactions, primarily to ensure that the person with whom a financial institution is dealing really is that person. It is that essential need to verify a person's identity using a common unique identifier—the SSN—that leads financial institutions to rely on the reporting of deceased individuals' SSNs to guard against fraud and identity theft. Thus, because SSNs are

---

[2] *Id.*

used so widely by government and businesses as the most reliable common unique identifier, it is critical that that reliability not be undermined by the theft and misuse of the SSNs of deceased individuals.

The Social Security Administration's Death Master File

A key method for preventing fraud and identity theft due to the misuse of a SSN is to identify the fraudulent use of a deceased individual's SSN. The linchpin of this prevention effort is the SSA's DMF. The SSA processes more than 2 million deaths each year and has compiled roughly 50 million deaths, total, in the DMF.[3] The death reports used to update the DMF come from a wide variety of sources. Nearly 95 percent of death reports come from family members, funeral homes, postal authorities and financial institutions. The remaining 5 percent come from all 50 states and the District of Columbia, which are required to provide death information to the SSA within 90 to 120 days after the month of death.[4]

The SSA takes the information it receives from these sources and updates the DMF on a monthly basis. The records of each deceased person include his social security number, last

---

[3] Nearly every record in the DMF relates to an individual who died after 1962, which is when the SSA began keeping the death records on computer. Jack Gehring, *Social Security Death Master File: A Much Misunderstood Index, at* http://www.ancestry.com/search/rectype/vital/ssdi/article.htm (last visited Nov. 6, 2001).

[4] *Social Security Administration's Program Integrity Activities: Hearing Before the Subcomm. on Social Security of the House Comm. on Ways and* Means, 106th Cong. (March 30, 2000) (statement of William A. Halter, Deputy Commissioner of Social Security), *available at* http://www.ssa.gov/policy/congcomm/testimony_033000.html (last visited Nov. 6, 2001).

In 1999, SSA contracted with the National Center for Health Statistics and the National Association for Public Health Statistics and Information Systems to begin developing a national electronic death registry, within which SSA could obtain death information from states within 24 hours of the state's receipt of that information. *Id.* However, that system is not in use at this time, and the SSA expects only 10 states per year to implement the electronic registry. *Id.*

name, first name, date of birth, date of death, state or country of residence, ZIP code of last residence, and ZIP code of lump sum payment of death benefits.[5]

The DMF is made available to the public for a fee, but it is not made available as a searchable, centralized database. Private entities may obtain the DMF in one of two ways. Entities in the United States, Canada, and Mexico may purchase a quarterly subscription for $6,900per year, which means the SSA will send those subscribers an entire, updated DMF every quarter. In the alternative, entities in the United States, Canada, and Mexico may purchase a full DMF for a one-time cost of $1,725 and then purchase a subscription to the Death Master Monthly Updates File for $2,760 per year. The SSA requires those entities who purchase a single, full DMF and who intend to keep their DMF current to purchase the monthly updates subscription, which only distributes the updates to the DMF, rather than the entire updated DMF, on a monthly basis.[6]

Because the DMF is not provided in a simple, searchable format, most financial institutions do not purchase it directly. Instead, when it is necessary to verify an SSN as part of an account opening procedure or otherwise, financial institutions generally rely on third party vendors, including credit bureaus, who purchase the DMF. For example, when provided with the SSN at the time an account is opened, a financial institution would typically provide that SSN to the third party vendor, and the vendor would use its databases to compare the number with SSA's updated DMF.

---

[5] NTIS, *Social Security Administration's Death Master File, at* http://www.ntis.gov (last visited Nov. 6, 2001).

[6] *Id.* Entities outside the United States, Canada, and Mexico may purchase the DMF Quarterly subscription for $13,800, a single DMF for $1,725, and the Death Master Monthly Updates file for $5,520. *Id.*

Financial institutions may also learn of an individual's death through the use of Death Notification Entries ("DNEs"). The SSA is one of the agencies that generates a DNE when a benefit recipient dies. The DNE is a zero-dollar entry with an addenda record. That is, rather than sending the financial institution a beneficiary's payment, the financial institution receives information about the individual's SSN, date of death, and the amount of the next scheduled benefit payment. The financial institution is then encouraged to flag the deceased recipient's account to prevent the account from accepting any post-death Federal benefit payments.[7]

Effectiveness of the Death Master File

There are two keys to preventing the misuse of SSNs of deceased individuals. First, the list of such numbers must be kept current. Second, the most current list must be widely accessible and easy to search and "cross-hatch" against a given SSN. Unfortunately, while the current DMF is used to accomplish both these goals, there is clearly room for improvement.

Currency of DMF numbers. With respect to the currency of the information in the DMF, there can be significant delays in updating the list. There are delays caused by the time taken for deaths to be reported to the SSA; delays caused by the entry of inaccurate information; and delays caused by the fact that the SSA releases comprehensive updates on only a monthly basis.

To be more specific, the SSA's Death Alert Control and Update System (DACUS) controls the processing of death information from the time an individual's death is reported to the time the DMF is updated. However, incoming death reports can be missing needed identifying information, such as date of death, or contain incorrect information, such as an

---

[7] *Returns–Reasons, DNE*, Green Book, *available at* http://www.fms.treas.gov/greenbook/returns/returns-a2.html (last visited Nov. 6, 2001).

incorrect SSN. In addition, where the SSA's Master Beneficiary Record contains information that is inconsistent with the information submitted to the DMF, the DMF cannot be updated, even though the Master Beneficiary Record is updated.[8] Further, SSA does not verify death reports of individuals who are not social security beneficiaries. This means that if multiple or incorrect death reports are submitted for a non-beneficiary, the SSA does not detect or correct the reports. In turn, erroneous death information for non-beneficiaries would be passed on to financial institutions.[9]

Thus, not only are DMF updates sent to subscribers only once a month, but where an individual's death record contains incomplete, incorrect, or inconsistent information, the delay in updating the DMF could be even longer. Unfortunately, a criminal can take advantage of that lag time by attempting to use the deceased person's SSN for fraudulent purposes, because the financial institution would not have the updated information to find out the true status of that SSN. Indeed, according to recent testimony by the SSA's Inspector General, the SSA's death reporting system still needs a great deal of work to ensure that the DMF is updated on a timely basis.[10]

---

[8] "Social Security—Most Social Security Death Information Accurate But Improvements Possible," Aug. 1994, GAO/HEHS 94-211, available at 1994 Westlaw 838092.

[9] "Social Security—Most Social Security Death Information Accurate But Improvements Possible," Aug. 1994, GAO/HEHS 94-211, available at 1994 Westlaw 838092.

[10] *Social Security Administration Improper Payment Issues: Hearing Before the Senate Committee on* Finance, 107th Cong. (April 25, 2001) (statement of James G. Huse, Jr., Inspector General of the SSA), *available at* http://www.ssa.gov/oig/testimony04252001.htm (last visited Nov. 6, 2001). The Inspector General's comments were directed toward the need to improve death reporting in order to ensure that social security benefits are not paid to an individual after his death; however, his comments illustrate the need for quicker death reporting as it relates to identify theft or misuse of deceased individuals' SSNs.

"Searchability" of DMF. As noted, the DMF is not provided in a form that is readily searchable. As a result, because it contains such a large amount of information, the most practical way to use the list is through intermediaries that convert the DMF into a searchable database that can be used by financial institutions and others. This service by third party vendors is valuable but can be costly, and cost can thus be a deterrent to the use of the DMF. Obviously, if a centralized, searchable database containing the DMF were widely available at a reasonable price, it is likely that the DMF would be used more routinely for a wider variety of SSN authentication checks.

Financial Institutions' Use of the DMF

Although the main purpose of the DMF is to inform the SSA that an individual has died and therefore should no longer receive payment of benefits,[11] the DMF information also is purchased by private information vendors, upon whom financial institutions ultimately rely for accurate information about the status of individuals' SSNs. Therefore, while the accuracy of the DMF is crucial to saving the SSA millions of dollars each year in overpayments, it is equally crucial to financial institutions who seek to prevent fraud and misuse of the SSNs of deceased individuals.

For example, many large banks contract with information vendors—including, but not limited to, the major credit bureaus—to compare the bank's list of individuals who have been approved for credit cards against the DMF. Similarly, banks, securities broker-dealers, mutual fund transfer agents, and insurance companies frequently use information vendors to conduct the

---

[11] The Office of Management and Budget "required that, beginning in March 1992, federal and federally assisted programs match SSA's death information against their payment files on a monthly basis to more quickly remove deceased beneficiaries from their roles and reclaim overpayments." "Social Security—Most Social Security Death Information Accurate But Improvements Possible," Aug. 1994, GAO/HEHS 94-211, available at 1994 Westlaw 838092.

same type of SSN comparison for new account openings, changes in parties on accounts, to determine whether to allow a client to maintain a margin account, to detect possible fraudulent transactions, to locate lost shareholders, and to review loan applications. Because the vendors receive their information about the status of SSNs from the SSA's DMF, if the information in the DMF is incorrect or incomplete because of delays in updating the list of deceased individuals, then financial institutions will receive incorrect information about the validity of the SSN that a potential customer has provided. Simply put, therefore, the more current the DMF is, then the more current the vendor's data is, and the better financial institutions can be at uncovering identify theft and other fraud involving the use of deceased individuals' SSNs.

Conclusion

The FSCC believes that the most effective way to combat fraud and identity theft stemming from the misuse of SSNs of deceased individuals is to make those numbers more current and more easily accessible at a reasonable price by all institutions, including smaller ones. We welcome suggestions for achieving both goals, and would be happy to work with the subcommittees and their staffs to facilitate these efforts. Thank you.

1a. You mentioned in your testimony some of the problems that financial institutions face when relying on the DMF due to notification lag-times. What approaches have been taken by the financial institutions to overcome these problems?

Financial institutions rely on information available from both public and private sources – with embedded Social Security numbers (SSN) to ensure correct identification – to check for inconsistencies that may suggest the occurrence of fraud or identity theft. For example, when it is necessary to verify an SSN as part of an account opening procedure or otherwise, financial institutions generally rely on third party vendors, such as credit bureaus, who purchase the DMF. Thus, more up to date and timely disclosure of DMF information will enhance these other sources of information and facilitate our ability to deter identity theft.

In the context of local community banks, the institution is able to glean certain information from the community. However, as the community becomes larger and more diverse, this approach becomes more difficult and impractical. Such an approach cannot be relied upon at larger institutions with diverse customer bases, both geographically and by product line.

1b. What do you think about initiatives/suggestions to make it more difficult for the Social Security number to be an all-purpose identifier (medical records, student id#s)? Do you think this will help reduce the rising number of identity theft cases?

Financial institutions use a variety of public records, including bankruptcy records; public records involving liens on real estate; and criminal and fraud detection databases, such as the National Fraud Center database. Access to information in public records, including SSNs, is important to financial institutions' efforts to uncover fraud and identity theft, to verify customers opening new accounts, and to maintain internal security operations. It is also important for third parties such as credit bureaus to have access to this information. Financial institutions rely upon these third parties to prevent and detect fraud and identity theft. Consequently, broad restrictions on the use of SSNs could make it easier, rather than harder, for individuals' identities to be stolen.

1c. What are the most recent numbers of financial losses that the credit card companies attribute to identity theft?

Accurate numbers are not available. Definitions and classifications of identity theft vary by card issuer, and some issuers do not make the numbers public.

1. **You state in your testimony the importance of timely updating and dissemination of the Death Master File to the prevention of fraud and identity theft. However, GAO in their testimony stated that despite the request for more timely updates, many financial institutions do not have the capability to use this information more frequently. Can you comment on this?**

   In fact, we do have the capability to use this information more frequently. More timely updating and dissemination of DMF information immediately would be incorporated into credit bureau information and other third party information, which all sizes of institutions rely upon to make various credit and deposit account decisions. This information is vital to financial institutions to uncover fraud and detect identity theft, verify customers when opening an account, assist in internal security operations, and make sound credit and other financial product determinations.

2. **You say that the Death Master File is important in preventing ID theft and fraud. How many cases of fraud has your membership uncovered in the past year? Who did you report the fraud to after it was discovered? Is there a requirement for you to report a case of ID theft to any agency including SSA or say, State motor vehicle agencies where stolen SSNs provide the key for getting a photo ID driver's license?**

   There is not an easily quantifiable number with respect to all fraud cases. One indication is provided by the ABA Deposit Account Fraud Survey Report 2000, which is limited to information with respect to check fraud. The survey found that 69 percent (up from 48 percent in 1997) of commercial banks, including 67 percent of community banks, 92 percent of mid-size banks, and all of the large institutions, suffered financial losses from check fraud. At banks that have experienced identity theft, an average of 29 percent of their check-related losses could be attributed to identity theft. Banks are required to file "Suspicious Activity Reports" or SARs on a variety of transactions that could be indicators of fraud. Those filings are with the Financial Crimes Enforcement Network, which is a bureau of the Department of the Treasury. In the most recent "SAR Activity Review," (October 2001) close to 40 percent of the total filings indicated potential fraud of some type. Identity theft is an offense that must be reported on a SAR.

3. **In the majority of cases, family members of the deceased would be contacting banks and insurance companies quickly to protect assets or collect insurance benefits. Is this not an immediate source of death information that could be used to prevent ID theft if it were properly managed?**

   If the family provides such information, then, yes, it is a helpful source of information. However, sometimes it takes time for bereaving family members to resolve matters dealing with the estate. Consequently, depending on family members to report the information presents the problem at issue in the hearing: misuse of

SSNs that results from the time delay in updating and disseminating DMF information.

As stated above, financial institutions rely upon a wide range of sources of information in an effort to maintain accurate records and information. We suggest that facilitating DMF operations would help in this effort.

4. **You state that subscribing to SSA's death records through third parties can be costly and therefore a deterrent to use. But earlier you mentioned that SSA sells the same information for a few thousand dollars. What is the cost to a financial services firm if the death is not detected quickly, or worse, there is a case of ID theft? One would think that the potential liability to your business of having someone acquire an SSN and using another person's account and assets would be enormous. Do you have a financial or legal liability from giving due diligence for protecting your customer's accounts?**

Banks use Social Security Administration death records through various third party vendors such as credit reporting agencies and vendors selling fraud prevention filters. These third parties incorporate the DMF information into their products. The SSN information, when provided in this fashion, is more easily integrated into the banks' own systems. Thus, in many cases, there is no need to pay for the information separately.

For many institutions, purchasing DMF information may be costly, particularly if the institution is not a high risk for identity theft, such as a community bank in a rural area. Thus, if a centralized, searchable database containing the DMF were widely available at a reasonable price, it is likely that the DMF would be used more routinely for a wider variety of SSN authentication checks. In this regard, testimony indicates that some states make available real time verification of SSN information to their respective Department of Motor Vehicles. The Committee may want to consider exploring a broader application of such real time verification and authentication of SSN information.

The financial services industry is vigilant in its efforts to prevent identity theft. The responsible use and protection of personal financial information is a top priority of financial institutions. This protection is important to promoting the strength of our lending institutions as the engines of local economic development. Financial institutions use a combination of safeguards to protect customer information, such as employee training, rigorous security standards, encryption, and fraud detection. In addition, institutions work with law enforcement officials to pursue individuals who fraudulently use information. However, the amounts involved frequently are not high enough for law enforcement to devote resources, which is an ongoing problem for our institutions.

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, Electronic Privacy Information Center
Adjunct Professor, Georgetown University Law Center

Joint Hearing on

SSNs and Identity Theft

Before the
Subcommittee on Oversight and Investigations
Committee on Financial Services
and
Subcommittee on Social Security
Committee on Ways and Means

U.S. House of Representatives
November 8, 2001
2138 Rayburn House Office Building

My name is Marc Rotenberg. I am the executive director of the Electronic Privacy Information Center, a public interest research organization based here in Washington. I am also on the faculty of the Georgetown University Law Center where I have taught the Law of Information Privacy for ten years. I have written briefs in two of the leading cases involving the privacy of the Social Security Number (SSN), and I have had the pleasure of testifying before the Subcommittee on Social Security this past May on the use and misuse of the Social Security Number.

I appreciate the opportunity to testify this morning on one of the unfortunate results of the misplaced reliance on SSNs as universal identifiers. The problem of "identity theft", particularly of the deceased, cannot be solved by sharing SSN data more rapidly or other such stopgap measures. The problem lies rather in the dramatic expansion of the use and collection of the SSN that Congress should try to limit. I will briefly review the efforts to regulate the use of the SSN, discuss some of the problems with universal unique identifiers, and make a few brief recommendations. I believe that legislation to limit the collection and use of the SSN is appropriate, necessary, and fully consistent with US law. I also believe that if Congress fails to act, the problems that consumers will face in the next few years are likely to increase significantly.

History of the SSN and the Efforts to Regulate

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

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the Social Security Number that show a striking resemblance to the problems we are seeking to correct today. Although the term "identify theft" was not yet in use, Records Computers and the Rights of Citizens described the risks of a "Standard Universal Identifier," how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."[1]

At the time of its enactment, Congress recognized the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of this provision, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy

[1] *Records, Computers and the Rights of Citizens* at 135.

concerns in the Nation." Short of prohibiting the use of the SSN outright, Section 7 of the Privacy Act provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it."[2] This provision attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed where the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

Financial Services Use of SSN

The use of the SSN has expanded significantly since the provision was adopted in 1974. This is particularly clear in the financial services sector. In an effort to learn and share financial information about Americans, companies trading in financial information are the largest private-sector users of SSNs, and it is these companies that are among the strongest opponents of SSN restrictions. For example, credit bureaus maintain over 400 million files, with information on almost ninety percent of the American adult population. These credit bureau records are keyed to the individual SSN. Information is freely sold and traded, virtually without legal limitations.[3]

It is the financial service industry's misplaced reliance on the SSN, lax verification procedures and aggressive marketing that are responsible for the financial consequences of "identity theft."[4] Congress must encourage the industry to develop alternative, and less intrusive systems of record identification and verification. We have also suggested to this Subcommittee before that Congress fund a National Research Council study to explore new techniques that will enable record management while minimizing privacy risks. Moreover, the misuse of death records underscores the need for consumers to have easy access to view and correct their credit reports, and to have the ability to control the use and dissemination of personally identifiable information.

---

[2] (a)(1) It shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. (2) the provisions of paragraph (1) of this subsection shall not apply with respect to - (A) any disclosure which is required by Federal statute, or (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

See Pub. L. No. 93-579, 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A 552a (West 1996).

[3] Komuves at 557.

[4] See for example the GAO Report that details the high cost and difficultly involved with preventing social security card fraud and therefore its current unreliability as a unique identifier. See also the SSA's Office of Inspector General reports and testimony on the misuse of SSN. [http://www.ssa.gov/oig/hotreports.htm]

Social Security Administration's Death Master File

The Death Master File is publicly available from the Social Security Administration (SSA) for a little under $1,800 for a single issue ($6,900 for a quarterly subscription with monthly updates). Anyone can buy 60 million electronic records from the SSA on all Americans (and others with SSNs) that have died. These records contain important personal identifiable information, including the name, social security number, date of birth, date of death, state or country of residence, ZIP code of last residence, and ZIP code of lump sum payment to the decedent's beneficiary. These records are also accessible for free on the web at places like Ancestry.com. The records have over a 3% error rate, and provide information chiefly on those who died after 1960.

It is remarkable that such a data goldmine is made publicly accessible by SSA and is a sobering reminder of the urgent need to restrict access to sensitive personally identifiable information. Rather than focusing attention on how these records can be transmitted more rapidly and accurate to commercial and private users, Congress must first consider placing limitations on the use and access to such data. Unscrupulous users of this database for instance might be able to exploit the recently bereaved or take advantage of their changed financial circumstances. Separate from what residual privacy concerns might be there for the recently departed, it is important to appreciate the effect such disclosure has on the survivor's privacy where their spouse's or parent's name, SSN and location is made freely available. The database might arguably be of some help for those engaged in historical research, but the terms and conditions of such use can be regulated to protect the privacy of survivors.

It also seems obvious that the more widely disseminated this information is the more opportunities for financial fraud and identity theft will arise. If Congress chooses to make the Death Master File more readily available to the private sector, then I urge to adopt corresponding privacy rules that will limit the opportunities for abuse.

Conclusion

As I suggested in my testimony in May to this Subcommittee, I believe that it is appropriate, necessary and consistent with other privacy measures to develop and enact legislation in the 107th Congress that will safeguard the use of the SSN. The prospect that the Death Master File will be made more widely available outside of the federal government further underscores the need for legislation in this area.

We also believe it is important to take a long-term view of the SSN. The best legislative strategy is one that discourages the collection and dissemination of the SSN and that encourages organizations to develop alternative systems of record identification and verification. It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater

risk to personal privacy. Given the unique status of the SSN, it's entirely inappropriate use as a national identifier for which it is also inherently unsuitable, and the clear history in federal statute and case law supporting restrictions, it is fully appropriate for Congress to pass legislation.

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

References

Electronic Privacy Information Center, "Social Security Numbers" [http://www.epic.org/privacy/ssn/]

Flavio L. Komuves, "A Perspective on Privacy, Information Technology an the Internet: We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," 16 J. Marshall J. Computer & Info. L. 529 (1998)

GAO Report, "Mass Issuance of Counterfeit-Resistant Cards Expensive, but Alternatives Exist," (August 1998)

Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991)

Marc Rotenberg, *Privacy Law Sourcebook: United States Law, International Law, and Recent Developments* (EPIC 2001)

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

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

TESTIMONY OF EVAN HENDRICKS
EDITOR/PUBLISHER
PRIVACY TIMES

Before The Subcommittee On Oversight & Investigations
House Committee On Financial Services

Before The Subcommittee On Social Security
House Ways and Means Committee
November 8, 2001

Madame Chairwoman, Mr. Chairman and Members of the Subcommittees, thank you for this opportunity to testify on the important issue of preventing the misuse of Social Security numbers (SSNs) of the deceased.

By way of introduction, I am Evan Hendricks, Editor/Publisher of *Privacy Times*, a Washington newsletter that I founded 21 years ago. I have been qualified by federal courts as an expert on identity theft in Fair Credit Reporting Act cases. I currently serve on the Social Security Administration's expert panel on privacy, assisting the SSA formulate and apply Privacy Impact Analyses to existing and contemplated electronic services.

As a Sports fan, I often hear that "If you do the little things right, you get the big things right."

Unfortunately, when it comes to SSNs, as a nation, we have over the years made a series of bad decisions. The underlying mistake has been to expand the use of the SSN beyond that for which it was created: the numbering of personal accounts for the collection of taxes and benefits in the Social Security program. Since 1936, when the number was first established, Congress

has authorized its use for additional purposes, including drivers' licenses, financial records and Federal, State and local governmental agencies. In addition, many private companies -- insurers, health care organizations, universities and health clubs -- use the SSN as their primary personal ID number for customers.

Thus, in many significant ways, the SSN has become a *de facto* national identifier. This is of course is not consistent with the U.S. Government's original promise to the American people that the SSN would not be used for identification purposes. It also means that as a society, we have lost considerable control over the SSN. They are available in too many places: Web sites, court records and bulletin boards. They are available for sale from information brokers. They are vulnerable to unauthorized access, use and even sale wherever they are stored, be it a personnel department, a government database or a Web site.

The SSN is the first number that is sought by (1) credit-identity thieves; (2) by people trying to hide their true identities, like terrorists; and (3) people trying to enter or remain in the United States in violation of our immigration laws.

These factors, along with many others, point to the urgency of enacting legislation to protect the privacy of SSNs, and to support efforts by Chairman Shaw and other Members to enact such legislation. My May 22 testimony before Chairman Shaw's Subcommittee, in which I also called for comprehensive privacy legislation and oversight, is available at http://waysandmeans.house.gov/socsec/107cong/5-22-01/5-22hend.htm.

The New Paradigm: Identity Theft

Few people realized that the failure to protect the privacy of personal data and the SSN has made possible what is becoming the fastest growing crime of the information age: Identity Theft. The first piece of data an identity thief wants is the SSN. Identity theft occurs when an imposter steals a consumer's identity, usually a Social Security number and sometimes a name and address, for the purpose of exploiting the credit-worthiness of an innocent consumer, obtains credit in the name of the innocent consumer, and absconds with goods. This activity leaves the innocent consumer with the debris of a polluted credit history.

Identity theft was becoming an epidemic before the Internet became popular. The steady rise in the number of identity theft cases has been well documented. In May 1998, the General Accounting Office, relying on figures provided by the Trans Union Corp., reported that the number of consumer inquiries to Trans Union's fraud desk grew from 35,235 in 1992, to 80,013 in 1993; to 154,365 in 1994; 265,898 in 1995, 371,220 in 1996 and 522,922 in 1997. Trans Union estimates that about two-thirds of these inquiries relate to identity fraud. Two more recent sources of statistics -- the Federal Trade Commission and California police agencies -- indicate the epidemic is worsening. The problem promises to worsen because there are indications that organized crime gangs are gravitating towards identity theft as a "low-risk, high payoff crime."

Thanks to fine reporting by Robert O'Harrow, Jr. of the *Washington Post*, we know that identity thieves regularly use stolen credit card numbers to buy SSNs and other personal data from information brokers and then use the information to commit credit fraud.

Some of the key solutions to identity theft include prompt and regular consumer access to his or her credit report and or/notification to the consumer of new activity on the credit report, stricter duties on CRAs to ensure that an innocent consumer's credit report is not disclosed in response to a credit application by an imposter, and wider use of "disposable" or "one-time" credit card numbers.

According to the Privacy Rights Clearinghouse and the Identity Theft Resource Center, another disturbing method of operation is for identity thieves to gather news about recently deceased persons, either from local agencies that issue death certificates, or from the obituaries, and use the information to commit credit fraud.

These groups reminded me of press reports that one woman stole the identity of a victim she knew who died in the World Trade Center attack and committed credit fraud. Also, a California limousine driver, who was to pick up a man who died on a hijacked Sept. 11 jet, stole the man's identity and committed credit fraud.

SSNs Of The Deceased

In addressing the issue of the SSNs of the deceased, it's important to consider a fundamental flaw in the current system: While the use of and reliance upon the SSN is widespread (making it a *de facto* ID number), the system for issuing it, protecting it and expiring the SSN is antiquated, relative to advanced information technology.

The Social Security Administration maintains a "Death Master File," consisting of 60 million names and SSNs of deceased persons, available for sale by the National Technical Information Service (www.ntis.gov). But, as the NTIS Web site states, "The SSA does not have a death record for all persons; therefore, SSA does not guarantee the veracity of the file. Thus, the absence of a particular person is not proof this person is alive."

Although it is not entirely clear how SSA gathers information on deceased persons, it appears that the information comes from a variety of sources, including SSA beneficiary records, local government agencies that issue death certificates and relatives of the deceased. But the SSA's system can be described as "hit-or-miss," leaving the Death Master file incomplete.

It appears that a thorough overhaul of this system is necessary, particularly given the growth in the abuse of the SSNs of the deceased. What is needed is an automated system by which the local governmental agencies in charge of issuing death certificates can instantly report to SSA the names and SSNs of deceased persons. SSA, in turn, can report these names and SSNs to the three major credit reporting agencies (CRAs). The CRAs would then be responsible for ensuring that an identity thief did not exploit a deceased person's SSN for financial gain. Legislation could help facilitate creation of such a system, both by providing legal authorization and the necessary appropriations. Such legislation should specify that the system be created

solely for the purpose of ensuring accuracy of information systems that maintain SSNs of the deceased.

Privacy, The Purpose Test & Real Oversight

We live in an Age in which a plethora of personal information is available about all of us from a wide variety of sources. Protecting privacy in the Information Age does not mean shutting down all systems or locking up all personal data -- that will never happen, nor should it. An important aspect of protecting privacy in today's environment is defining the purposes for which information may be used. That is why the Fair Credit Reporting Act, the first information privacy law (1971, amended in 1996) defines the "permissible purposes" for which credit reports may be used. And, like the FCRA, privacy laws must create penalties to deter misuse of personal data and remedies for individuals whose privacy is invaded.

Another important aspect in the protection of privacy is oversight and enforcement. The United States lacks what every other Western nation has: An independent national office to oversee and enforce privacy law. Other nations get great value from their Privacy Commissioners, who typically report to Parliament, receive complaints from citizens, investigate, conduct audits of organizations' information systems, study new technologies, and serve as a public resource. The U.S. Privacy Protection Study Commission, a bipartisan panel created by the Privacy Act of 1974, recommended such an office in 1976.

Privacy is a very broad issue, affecting every aspect or our society: finance, medicine, employment, commerce, communications, law enforcement and counter-intelligence. It will be difficult if not impossible to ensure that privacy rules are administered effectively across these sectors without appropriate direction. An independent Office of Privacy Commissioner, created by statute and reporting to Congress, is the appropriate entity to provide that direction.

Madame Chairwoman, Mr. Chairman, again, thank you for this opportunity to appear before the Subcommittee. I'd be happy to answer any questions.

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Question: 2 a) You mentioned in your testimony that some of the key solutions to Identity Theft include stricter duties on credit reporting agencies (CRAs). What are some of your suggestions?

Answer: Federal courts may ultimately decide that some of the solutions I offer below are already required by the Fair Credit Reporting Act.

First, CRAs need to be more careful when disclosing a consumer's credit history in response to a credit application. Currently, CRAs error on the side of maximum disclosure because that is one of the ways that they make money. Identity thieves take advantage of this. I've seen cases in which the imposter's application for fraudulent credit had a different name and different address than the victim, but the CRA nonetheless disclosed the innocent victim's credit report, facilitating the granting of credit to the imposter. In the age of identity theft, CRAs must match sufficient indicia from the credit application to the consumer's credit history before disclosing that history.

Second, the three major CRAs need to make it easy for consumers to have secure, electronic access to their credit reports so that they are alerted promptly when there is activity on their credit report. This should be required for consumers who are certified victims of identity theft. If thousands of credit grantors enjoy instant access to a consumer's credit history, so should consumers enjoy such access to their own data, especially when doing so can guard against identity theft. I believe Equifax has launched such a service for a fee.

Third, CRAs should audit their own databases, starting with an SSN search that would reveal if more than one name/address were associated with one SSN. CRAs sell an "SSN Trace" to customers, but it's not clear they employ the same process for internal audits.

Second Set of Questions

1) Public opinion change since Sept. 11: Is the public moving from worrying about privacy to concerns over safety?

Clearly the Sept. 11 attack provoked a public opinion shift so that anything that would promote the security of America and its citizens was favored. The reality, which the public will increasingly understand as we improve our security, is that good privacy law and practice not only does not interfere with security, but contributes to it. For example, identity theft and credit fraud was a fundamental method of operation of al-Qaeda operatives. Second, existing privacy laws make exceptions for law enforcement, health and safety emergencies, etc., so that they don't interfere with exigent investigations like those following Sept. 11. Third, the goals of consumer privacy laws, i.e., stopping private companies from selling consumers' data without their consent, and giving consumers access to their own data, in no way interfere with the fight on terrorism. Fourth, the post-Sept. 11 investigations will further raise awareness about the widespread availability of everyone's personal data, and renew privacy concerns. All of these, and other factors, will swing the pendulum back to America favoring strong privacy protection for their own personal information, while making exceptions for approved purposes, like stopping terrorists.

2) Public reaction if it is learned that more terrorists used SSNs? What proscription on SSN use does the public want and what inconveniences are they willing to accommodate to insure their national safety?

The public already disapproves of the growing use of SSNs by institutions that are not required by law to use them. The public anger over this is being compounded by the growing use of SSNs by identity thieves. So, if there are further instances of terrorist using them, public anger will build even greater and more rapidly.

I don't see anyway that proscription on SSN use will inconvenience Americans. It will only inconvenience those companies that traffic in Americans' SSNs without their consent.

3) What private institutions will benefit most from getting early access to the Death Master File? Answer: CRAs and financial institutions. Of course, it will also remove an excuse for inaccuracy.

Do they use it now to stop theft? Answer: It's not clear. That would be an interesting GAO study.

Newer strategy to stop theft from these sources? Perhaps have those who access/obtain death data from local/State agencies certify that they are doing so for a permissible purpose.

What percent of identity theft could be thwarted using these improved methods?
Answer: Probably only 5-7%. This is a guess, as there are no reliable data at this point. But taking steps now could prevent the problem from growing to 10-20%.

COMSERV, Inc. - Computer Systems and Services

November 9, 2001

To the Subcommittee on Social Security of the Committee on Ways and Means:

Identity theft through the improper use of Social Security numbers is a very large problem, as you are becoming quite aware. For over 20 years now, my company, COMSERV, Inc. has been dedicated to helping corporations, financial institutions, federal and state government agencies, and other organizations in the detection of the fraudulent use of Social Security Number (SSN) for the purpose of identity theft, among other illegal uses.

In 1978, COMSERV, Inc., then ATL Corporation, realized that this was a major problem and initiated Freedom of Information Act (FOIA) litigation to require the Social Security Administration (SSA) to produce computerized files of all deceased persons. After two years of litigation, SSA was ordered to produce the requested computerized file. Using this file, COMSERV, Inc. pioneered the concept of a national death database (e.g. Death Information System) for the use of fraud detection within benefit plans and many other areas.

Because of my continuing dedication to this wide-spread problem, I find it very disturbing that one or more terrorists may have assumed the identity of deceased individual(s) to further their evil cause and harm American citizens, but I am not surprised. Too many agencies have not seen the need to run checks of SSNs to determine if the SSN has been reported as belonging to a deceased individual or if there are mismatches in other associated information provided with the SSN such as date of birth. I believe this processing deficiency is basically due to not understanding the potential consequences of not performing such checks. See the attached article that was published in the September 1, 2001 Palm Beach Post for evidence of this.

Even though I shudder to think that terrorists may be stealing our citizens' identities, I am now quite disturbed by your consideration to no longer allow death information to be distributed under the FOIA for two reasons. First, as with most everything, death information can be used for good and for bad. If we outlaw everything that can potentially be used for bad, we will be left with no freedoms. Further, by not allowing this information to be distributed, companies like my own will become handicapped in combating this serious problem. My company will continue to operate by getting death information from the many other sources we already gather it from, but the data will become less accurate, preventing us from helping various organizations to quickly and easily determine if someone is using a deceased person's SSN.

8625 Cory Dr., Bowie, MD 20720-4459
Voice: 301-805-1123, Fax: 301-805-4289, WWW.COMSERV-INC.COM

I am already in negotiations with the INS to provide my Social Security Number Validation System (SSNDTECT) product line, which includes a desktop software application that performs instant checks on SSNs with information provided to the utilizing agency. Other agencies, such as the U.S. Department of State's Consular Affairs (they are responsible for Visas and Passports), are not performing due diligence regarding SSN validation and the use of death information to combat identity fraud. Our SSNDTECT product includes a death check capability. Think of what having this capability in the past could have done to protect American lives. Now think of what it could do in the future.

Secondly, not distributing this information will not prevent identity theft through SSN use. There are too many readily available sources for death information. Further, people do not need to obtain the SSN of a deceased individual in order to assume an identity. Most states use the SSN as a driver's license number, and driver's licenses are used for identification purposes everywhere. My company gets numerous calls each year from individuals complaining that someone has stolen and is using their SSN in order to obtain credit cards and loans. This is a real problem for our citizens. My product, when used by credit card companies and banks, helps detect and prevent this illegal use of SSNs.

Finally, I wish to bring to your attention some of the following positive things that my company alone has done with death information:

- Helped financial institutions detect credit fraud through the use of stolen identities;
- Reduced expenses for organizations by purging deceased persons from mailing lists;
- Identified cases where retirement benefits and even salaries were being paid to people long after they died;
- Genealogy studies;
- Medical and research purposes;
- Identification of deceased voters;
- Identified resurrection fraud; and
- Identified improper use of SSNs on IRS filings.

All of these things have resulted in substantial cost savings to both the private industry and the government, and there are many other potential good uses as well. Cost savings in the private industry have likely resulted in things such as reduced overhead rates, making companies more competitive, lower rates of defaulted loans allowing financial institutions to offer lower interest rates, and more. Cost savings to the government could aid in increasing the Social Security surplus, and yes, even in identifying terrorists. The technology is available today for wide spread deployment within any government agency.

In closing, I ask you to consider that for private corporations such as COMSERV, Inc., death information is of paramount importance to combat identity fraud and detect erroneous payments. By making this information unavailable, you will be reducing both the private industry and government's ability to combat this very real problem.

Thank you so much for your consideration. Should you have any questions, please do not hesitate to contact me at 301-805-1123 or 301-520-1205.

Sincerely,

Robert D. Perholtz

President, COMSERV, Inc.
RDP@comserv-inc.com
WWW.COMSERV-INC.COM

ERIC
THE ERISA INDUSTRY COMMITTEE
1400 L Street, NW, Suite 350 Washington, DC 20005-3509 TEL: (202) 789-1400 FAX: (202) 789-1120

November 8, 2001

The Honorable Sue Kelly
Chair, Subcommittee on Oversight and Investigations
Committee on Financial Services
U.S. House of Representatives
Rayburn House Office Building
Room 2129
Washington, D.C. 20515

Dear Madam Chairwoman:

The ERISA Industry Committee (ERIC), representing the employee benefits interests of major employers, fully supports the goal of the Social Security Number Privacy and Identity Theft Prevention Act of 2001 (H.R.2036) to stem the proliferation of "identity theft," and other violations of individual privacy, including those that may be involved in future terrorist attacks. However, H.R.2036 as currently drafted would substantially interfere with the administration of employee benefit plans and seriously compromise the ability of employers to offer defined benefit pension plans, 401(k) accounts, prescription drug and other health and welfare benefits safely and efficiently to their employees and those employees' families.

The intention of H.R.2036 in general, and Title II of the bill in particular, is to prevent misuse of social security numbers. Title II prohibits the "sale," "purchase," or "display to the general public" of an individual's social security number. While the intention of that prohibition is clear, the definitions of "sale," "purchase," and "display to the general public" are not. Those ambiguous definitions risk outlawing routine plan administration.

ERIC understands that the intention of the bill's supporters is not to prohibit legitimate uses of social security numbers and we have been working with staff to find a solution through more precise legislative drafting. We have also sent a similar letter to Chairman Shaw of the Social Security Subcommittee of the Ways and Means Committee.

ERIC looks forward to working with staff and with your Subcommittee to effectively address the problem of identity theft without creating unintentional barriers to the provision of pension, health and other benefits to employees.

Please do not hesitate to contact us for more information about this matter.

Very truly yours,

Mark J. Ugoretz
President

Janice M. Gregory
Vice President

Cc: Members of the Subcommittee on Oversight and Investigations

ERIC

THE ERISA INDUSTRY COMMITTEE
1400 L Street, NW, Suite 350 Washington, DC 20005-3509 TEL: (202) 789-1400 FAX: (202) 789-1120

November 8, 2001

The Honorable E. Clay Shaw, Jr.
Chair, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
Rayburn House Office Building -- Room B-318
Washington, D.C. 20515

Dear Mr. Chairman:

The ERISA Industry Committee (ERIC), representing the employee benefits interests of major employers, fully supports the goal of the Social Security Number Privacy and Identity Theft Prevention Act of 2001 (H.R.2036) to stem the proliferation of "identity theft," and other violations of individual privacy, including those that may be involved in future terrorist attacks. However, H.R.2036 as currently drafted would substantially interfere with the administration of employee benefit plans and seriously compromise the ability of employers to offer defined benefit pension plans, 401(k) accounts, prescription drug and other health and welfare benefits safely and efficiently to their employees and those employees' families.

The intention of H.R.2036 in general, and Title II of the bill in particular, is to prevent misuse of social security numbers. Title II prohibits the "sale," "purchase," or "display to the general public" of an individual's social security number. While the intention of that prohibition is clear, the definitions of "sale," "purchase," and "display to the general public" are not. Those ambiguous definitions risk outlawing routine plan administration.

ERIC understands that the intention of the bill's supporters is not to prohibit legitimate uses of social security numbers and we have been working with staff to find a solution through more precise legislative drafting. We have also sent a similar letter to Chairwoman Kelly of the Oversight and Investigations Subcommittee of the Financial Services Committee.

ERIC looks forward to continuing to work with staff and with your Subcommittee to effectively address the problem of identity theft without creating unintentional barriers to the provision of pension, health and other benefits to employees.

Please do not hesitate to contact us for more information about this matter.

Very truly yours,

Mark J. Ugoretz
President

Janice M. Gregory
Vice President

Cc: Members of the Subcommittee on Social Security

NATIONAL COUNCIL
ON
TEACHER RETIREMENT

CYNTHIA L. MOORE
Washington Counsel
c/o The Moore Law Firm, PLLC
1911 N Fort Myer Dr., Suite 702
Arlington, VA 22209
TEL: (703) 243-1667 FAX: (703) 243-1672

November 8, 2001

The Honorable E. Clay Shaw, Jr.
Chairman
Subcommittee on Social Security
U.S. House of Representatives
1102 Longworth Building
Washington, DC 20515

RE: Submission of statement in connection with the hearing "Preventing Identity Theft by Terrorists and Criminals," November 8, 2001

Dear Mr. Chairman:

I would like to submit this letter on behalf of the 75 state and local government retirement systems that belong to the National Council on Teacher Retirement (NCTR). NCTR members appreciate your work on the pressing issue of reducing identity theft through the misuse of Social Security Account Numbers (SSANs). Your legislation, H.R. 2036, the Social Security Number Privacy and Identity Theft Prevention Act of 2001, will help achieve that goal by protecting individuals from fraudulent and other wrongful use of SSANs.

We understand that H.R. 2036 is not intended to prohibit legitimate uses of SSANs. As currently written, however, the bill's definitions of "sale," "purchase," and "display to the general public" as used in Title II of the bill are unclear and could interfere with the legitimate use of SSANs by retirement system administrators. For example, administrators use SSANs as a means to verify a retirement beneficiary's identity to ensure that the individual applying for the benefit is entitled to it. They also use SSANs to uncover fraudulent use of retirement benefits. When a plan participant dies, his/her next of kin does not always notify the retirement system so that the benefit can be discontinued. To avert this problem, administrators frequently compare death records of their retirement systems with death records provided by other entities.

We look forward to working with your staff to resolve these matters.

Sincerely,

Cynthia L. Moore

○