

**PRESERVING THE INTEGRITY OF SOCIAL SECURITY
NUMBERS AND PREVENTING THEIR MISUSE BY
TERRORISTS AND IDENTITY THIEVES**

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS

AND THE

SUBCOMMITTEE ON IMMIGRATION,
BORDER SECURITY, AND CLAIMS

OF THE

COMMITTEE ON THE JUDICIARY

OF THE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 19, 2002

Serial No. 107-81

(Committee on Ways and Means)

Serial No. 102

(Committee on the Judiciary)

Printed for the use of the Committee on Ways and Means and the Committee
on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 2003

84-170

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

COMMITTEE ON WAYS AND MEANS

BILL THOMAS, California, *Chairman*

PHILIP M. CRANE, Illinois	CHARLES B. RANGEL, New York
E. CLAY SHAW, JR., Florida	FORTNEY PETE STARK, California
NANCY L. JOHNSON, Connecticut	ROBERT T. MATSUI, California
AMO HOUGHTON, New York	WILLIAM J. COYNE, Pennsylvania
WALLY HERGER, California	SANDER M. LEVIN, Michigan
JIM McCRERY, Louisiana	BENJAMIN L. CARDIN, Maryland
DAVE CAMP, Michigan	JIM McDERMOTT, Washington
JIM RAMSTAD, Minnesota	GERALD D. KLECZKA, Wisconsin
JIM NUSSLE, Iowa	JOHN LEWIS, Georgia
SAM JOHNSON, Texas	RICHARD E. NEAL, Massachusetts
JENNIFER DUNN, Washington	MICHAEL R. McNULTY, New York
MAC COLLINS, Georgia	WILLIAM J. JEFFERSON, Louisiana
ROB PORTMAN, Ohio	JOHN S. TANNER, Tennessee
PHIL ENGLISH, Pennsylvania	XAVIER BECERRA, California
WES WATKINS, Oklahoma	KAREN L. THURMAN, Florida
J.D. HAYWORTH, Arizona	LLOYD DOGGETT, Texas
JERRY WELLER, Illinois	EARL POMEROY, North Dakota
KENNY C. HULSHOF, Missouri	
SCOTT McINNIS, Colorado	
RON LEWIS, Kentucky	
MARK FOLEY, Florida	
KEVIN BRADY, Texas	
PAUL RYAN, Wisconsin	

Allison Giles, *Chief of Staff*

Janice Mays, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

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

SAM JOHNSON, Texas	ROBERT T. MATSUI, California
MAC COLLINS, Georgia	LLOYD DOGGETT, Texas
J.D. HAYWORTH, Arizona	BENJAMIN L. CARDIN, Maryland
KENNY C. HULSHOF, Missouri	EARL POMEROY, North Dakota
RON LEWIS, Kentucky	XAVIER BECERRA, California
KEVIN BRADY, Texas	
PAUL RYAN, Wisconsin	

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
GEORGE W. GEKAS, Pennsylvania	BARNEY FRANK, Massachusetts
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLEY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
STEVE CHABOT, Ohio	MELVIN L. WATT, North Carolina
BOB BARR, Georgia	ZOE LOFGREN, California
WILLIAM L. JENKINS, Tennessee	SHEILA JACKSON LEE, Texas
CHRIS CANNON, Utah	MAXINE WATERS, California
LINDSEY O. GRAHAM, South Carolina	MARTIN T. MEEHAN, Massachusetts
SPENCER BACHUS, Alabama	WILLIAM D. DELAHUNT, Massachusetts
JOHN N. HOSTETTLER, Indiana	ROBERT WEXLER, Florida
MARK GREEN, Wisconsin	TAMMY BALDWIN, Wisconsin
RIC KELLER, Florida	ANTHONY D. WEINER, New York
DARRELL E. ISSA, California	ADAM B. SCHIFF, California
MELISSA A. HART, Pennsylvania	
JEFF FLAKE, Arizona	
MIKE PENCE, Indiana	
J. RANDY FORBES, Virginia	

Philip G. Kiko, *Chief of Staff-General Counsel*

Perry H. Apelbaum, *Minority Chief Counsel*

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

GEORGE W. GEKAS, Pennsylvania, *Chairman*

DARRELL E. ISSA, California	SHEILA JACKSON LEE, Texas
MELISSA A. HART, Pennsylvania	BARNEY FRANK, Massachusetts
LAMAR SMITH, Texas	HOWARD L. BERMAN, California
ELTON GALLEGLEY, California	ZOE LOFGREN, California
CHRIS CANNON, Utah, Vice Chair	MARTIN T. MEEHAN, Massachusetts
JEFF FLAKE, Arizona	
J. RANDY FORBES, Virginia	

George Fishman, *Chief Counsel*

Lora Ries, *Counsel*

Art Arthur, *Full Committee Counsel*

Cindy Blackston, *Professional Staff*

Leon Buck, *Minority Counsel*

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

	Page
Advisory of September 12, 2002, announcing the hearing	2
WITNESSES	
Social Security Administration, Hon. James B. Lockhart III, Deputy Commissioner	11
U.S. Department of State, Charisse M. Phillips, Director, Office of Fraud Prevention Programs, Bureau of Consular Affairs	48
U.S. Secret Service, Robert Bond, Deputy Special Agent in Charge, Financial Crimes Division	54
Federal Bureau of Investigation, Grant D. Ashley, Assistant Director, Criminal Investigative Division	62
Social Security Administration, Hon. James G. Huse, Jr., Inspector General ...	66

Stylecraft Interiors Inc., Matthew James Reindl	73
Electronic Privacy Information Center, Chris Jay Hoofnagle	78
SUBMISSIONS FOR THE RECORD	
Social Security Advisory Board, Hon. Hal Daub, statement	104

American Federation of Government Employees, National Council of SSA Field Operations Locals, Baltimore, MD, Witold Skwierczynski, statement ..	108
American Immigration Lawyers Association, letter	111
ERISA Industry Committee, National Association of State Retirement Administrators, National Council on Teacher Retirement, National Rural Electric Cooperative Association, and Profit Sharing/401(k) Council of America, joint statement	112
Federation for American Immigration Reform, Dan Stein, letter	114
National Council of La Raza, and National Immigration Law Center, joint letter	115

**PRESERVING THE INTEGRITY
OF SOCIAL SECURITY NUMBERS
AND PREVENTING THEIR MISUSE BY
TERRORISTS AND IDENTITY THIEVES**

THURSDAY, SEPTEMBER 19, 2002

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

AND

COMMITTEE ON THE JUDICIARY,
SUBCOMMITTEE ON IMMIGRATION,
BORDER SECURITY, AND CLAIMS,
Washington, DC.

The Subcommittees met, pursuant to notice, at 1:05 p.m., in room 1100 Longworth House Office Building, Hon. E. Clay Shaw, Jr., and Hon. George W. Gekas (Chairmen of the Subcommittees) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
September 12, 2002
No. SS-16

CONTACT: (202) 225-9263

Shaw Announces Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves

Congressman E. Clay Shaw, Jr. (R-FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a joint hearing with the Subcommittee on Immigration, Border Security, and Claims of the Committee on Judiciary, chaired by Congressman George W. Gekas (R-PA), on preserving the integrity of Social Security numbers and preventing their misuse by terrorists and identity thieves. **The hearing will take place on Thursday, September 19, 2002, in 1100 Longworth House Office Building, beginning at 1:00 p.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Subcommittee and for inclusion in the printed record of the hearing.

BACKGROUND:

Although Social Security numbers (SSNs) are used for many legitimate purposes, wide availability, and easy access to this very personal information has greatly facilitated Social Security number-related crimes and fueled growing concern for safeguarding individuals' privacy.

Identity theft is considered the fastest growing financial crime in the country, affecting an estimated 500,000 to 700,000 people annually, regardless of age, gender, or race. Older Americans will become an increasingly attractive target by criminal elements, since they hold substantial wealth and because seniors are often dependent on caregivers. In addition, the rising cost of this crime increases the cost of banking, insurance, and credit cards for all Americans.

Worse yet, according to the Federal Bureau of Investigation, terrorists have utilized Social Security number fraud and identity theft to obtain employment, access secure locations, and finance their operations, thereby posing a significant threat to our national security. Forged documents, whether bogus birth certificates, fake SSN cards, or false immigration documents, are increasingly available from those who make their living selling false identities. There are now illegal markets throughout the cities of the United States where anyone can acquire a false or stolen identity.

The Social Security Administration (SSA) serves as the front line of defense in ensuring SSN integrity, because it is responsible for accurately assigning SSNs and ensuring the wages earned and Social Security benefits claimed on that number are only those of the number holder. Last year, SSA issued 18.1 million SSN cards, of which 5.8 million were new and 12.3 million were replacement SSN cards. The SSA's Inspector General (IG) has long criticized the agency's failure to verify the authenticity of identification documents, and in a recent report estimated that of the 1.2 million SSNs issued to non-citizens in 2000, nearly 100,000 were based on invalid or inappropriate immigration documents. This year, the SSA began verifying supporting immigration records before issuing SSN cards. The agency is also work-

ing with the Immigration and Naturalization Service (INS) and the U.S. Department of State (DoS) to implement new data sharing initiatives and an Enumeration at Entry initiative.

Each year the SSA receives about 250 million wage reports from employers covering approximately 150 million workers. For tax year 2000, employers reported almost 9.6 million wage items, equaling almost \$50 billion in wages, that could not be credited to individuals due to lack of key information or submission of erroneous information, although further efforts to reduce these discrepancies is ongoing. According to the SSA, after all processing is complete, 2 to 3 percent of wage items will remain unmatched. Earnings that cannot be matched to a particular worker are recorded in separate file known as the Earnings Suspense File (ESF).

According to the SSA IG, the ESF contains over 237 million wage items and \$375 billion in wages accrued between tax years 1937 and 2000. However, approximately two-thirds of growth in the file occurred between 1990 and 2000. The IG has referred to the ESF as a “major management challenge” for the agency because of its potential impact on benefit amounts and administrative costs, and because it represents a significant portion of SSN misuse. This year, the SSA extended its outreach to employers by sending letters to all employers who submitted earnings records that did not match SSA’s records and asking them to provide corrected information. In addition, the SSA began piloting an on-line system to supplement existing verification procedures and more quickly enable employers to verify the names and SSNs of newly hired employees.

Although SSA issues SSNs in order to track individual’s wages and right to Social Security benefits, the agency assigns SSNs for limited non-work purposes to certain individuals who are not U.S. citizens and are not authorized to work by the INS. Today, SSA only issues non-work SSNs to these individuals if Federal statute requires one to access a particular benefit or service, or State or local law requires one to get general assistance benefits. However, despite their “non-work” designation, in tax year 2000 approximately 600,000 individuals with non-work SSNs earned over \$21 billion, though in some cases individuals may have become authorized to work without notifying the SSA.

In announcing the hearing, Chairman Shaw stated: “This Subcommittee has extensively examined identity theft by criminals and heard first-hand testimony of the personal devastation caused by this type of robbery. In the year since the September 11 attacks, we have also learned how SSN fraud can enable terrorism. That is why my legislation to improve the privacy of SSNs has generated bipartisan support. The SSN protection must be an integral part of a comprehensive effort to strengthen homeland security. It is one very tangible way we can help prevent the American public from being further victimized by terrorists.”

Chairman Gekas added: “The privacy of the Social Security numbers of every American is under attack by terrorists, international criminals, and an increasing number of identity thieves. I believe the Social Security Administration can do more to tighten up its procedures for issuing Social Security Cards to prevent fraud.”

FOCUS OF THE HEARING:

The Subcommittees will examine: the role SSN fraud plays in crime and terrorist activities and methods by which criminal fraud is accomplished utilizing stolen SSNs; the integrity of the SSA’s enumeration and wage crediting process; Federal agency coordination and cooperation, including data sharing, to verify identification documents, and to detect and prevent fraud; and recommended legislative proposals aimed at combating SSN misuse and protecting privacy.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Due to the change in House mail policy, any person or organization wishing to submit a written statement for the printed record of the hearing should send it electronically to hearingclerks.waysandmeans@mail.house.gov, along with a fax copy to (202) 225-2610, by the close of business, Thursday, October 3, 2002. Those filing written statements who wish to have their statements distributed to the press and interested public at the hearing should deliver their 200 copies to the Subcommittee on Social Security in room B-316 Rayburn House Office Building, in an open and searchable package 48 hours before the hearing. The U.S. Capitol Police will refuse sealed-packaged deliveries to all House Office Buildings.

FORMATTING REQUIREMENTS:

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

1. Due to the change in House mail policy, all statements and any accompanying exhibits for printing must be submitted electronically to *hearingclerks.waysandmeans@mail.house.gov*, along with a fax copy to (202) 225-2610, in Word Perfect or MS Word format and MUST NOT exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

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

3. Any statements must include a list of all clients, persons, or organizations on whose behalf the witness appears. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers of each witness.

Note: All Committee advisories and news releases are available on the World Wide Web at <http://waysandmeans.house.gov>.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call (202) 225-1721 or (202) 226-3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Chairman SHAW. Thank you for being here. Mr. Gekas and I have sat in these chairs before at a joint meeting, and he just reminded me how well he did the last time we were here in cross-examining a certain witness and sort of nailed his hide to the barn door. When the newspaper—

Chairman GEKAS. The New York Times.

Chairman SHAW. When the New York Times wrote about it, they said how Clay Shaw tore this witness apart.

[Laughter.]

Chairman GEKAS. This time I sat in front of the right nameplate.

Chairman SHAW. Okay, today our Subcommittees will join together to examine efforts to preserve the integrity of Social Security numbers and how we can better prevent terrorists and identity thieves from using these numbers to abet their heinous activities.

I welcome my friend, Chairman Gekas. We were partners against crime on Judiciary a number of years ago, before I came to this Subcommittee.

I welcome Ms. Jackson Lee and all of the Members of the Judiciary Committee on the Immigration, Border Security, and Claims Subcommittee to the Committee on Ways and Means.

I appreciate the opportunity to work with you as we look for ways to ensure the security of individuals and the security of our Nation.

Although created solely for the purpose of tracking workers' Social Security earnings, our culture is hooked on Social Security numbers. Business and governments use the numbers as primary identifiers of individuals. Even the most trivial transactions, such as renting a video, require us to hand over our nine-digit ID before services can be rendered.

The Social Security number has become so woven into the fabric of American society that it has become the key that unlocks the door to an individual's identity for any unscrupulous individual who gains access to it. If someone such as a criminal or a terrorist unlocks the door, at their fingertips are all of the essential elements needed to carry out whatever dastardly act they can conceive.

Worse, as each day passes, we learn more about the degree to which terrorists use stolen identities and false Social Security numbers to establish cover employment, drivers' licenses, and credit cards, all enabling them to live within our borders and plan their crime against Americans.

No longer is Social Security number fraud simply a tool of common criminals. Sadly, it is now a tool of terrorists.

As we will hear today from our witnesses from the U.S. Department of State, the Federal Bureau of Investigation (FBI), U.S. Secret Service, and the Social Security Administration's Inspector General (IG), there is no limit to the creativity of the reprehensible acts perpetrated by criminals and terrorists.

Our Nation and this Congress has forced our attention on America's first line of defense since the attacks of September 11; the war on terrorism and protecting our borders. Next, we must enact increased privacy protections for Social Security numbers and more powerful tools for law enforcement.

To that end, I along with several of my Committee on Ways and Means colleagues introduced H.R. 2036, the Social Security Number Privacy and Identity Theft Prevention Act of 2001. It is a vital component of our country's response to terrorism.

The Social Security Administration serves as the frontline of defense in ensuring the integrity of Social Security numbers, a responsibility it takes very seriously. It is responsible for accurately assigning Social Security numbers as well as ensuring the wages earned and the Social Security benefits claimed on that number are only those of the holder.

As we will soon hear, since September 11, the agency has implemented a number of initiatives to help prevent identity theft. Yet, we will also hear there is more to do, particularly with regard to interagency cooperation. A solo approach by Federal agencies is not acceptable, as President Bush recognizes through his proposal to create a U.S. Department of Homeland Security.

Our Nation has been forever changed by the horrible attacks on our country. No longer can we sit idly by and not protect ourselves from domestic and foreign terrorists. Also, long before these attacks, individuals were fighting more personal battles with identity thefts.

We must implement changes that will prevent and deter future attacks on our national security and our personal financial security.

I look forward to hearing from each of our witnesses and thank them in advance for sharing with us their experience and their recommendation.

I now yield to my Co-Chair at this hearing, Mr. Gekas of Pennsylvania.

[The opening statement of Chairman Shaw follows:]

Opening Statement of the Hon. E. Clay Shaw, Jr., a Representative in Congress from the State of Florida, and Chairman, Subcommittee on Social Security

Today, our Subcommittees join together to examine efforts to preserve the integrity of Social Security numbers and how we can better prevent terrorists and identity thieves from using these numbers to abet their heinous activities. I welcome Chairman Gekas, Ms. Jackson-Lee, and all of the Members of the Judiciary Subcommittee on Immigration, Border Security, and Claims to the Committee on Ways and Means and appreciate the opportunity to work with you as we look for ways to ensure the security of individuals and our Nation.

Although created solely for the purpose of tracking workers' Social Security earnings, our culture is hooked on Social Security numbers. Businesses and governments use the number as the primary identifier of individuals. Even the most trivial transactions, such as renting a video, require us to hand over our 9-digit ID before services can be rendered.

The Social Security number has become so woven into the fabric of American society, it has become the key that unlocks the door to an individual's identity for any unscrupulous individual who gains access to it. If someone, such as a criminal or terrorist, unlocks the door, at their fingertips is all the essential elements needed to carry out whatever dastardly act they can conceive.

Worse, as each day passes we learn more about the degree to which terrorists use stolen identities and false Social Security numbers to establish cover employment, drivers' licenses, and credit cards—all enabling them to live within our borders and plan their crimes against Americans. No longer is Social Security number fraud simply a tool of common criminals; sadly, it's now a tool of terrorists.

As we will hear today from our witnesses from the Department of State, FBI, Secret Service, and the Social Security Administration's Inspector General, there is no limit to the creativity of the reprehensible acts perpetrated by criminals and terrorists.

Our Nation, and this Congress, has focused our attention on America's first line of defense since the attacks of September 11th—the war on terrorism and protecting our borders. Next, we must enact increased privacy protections for Social Security numbers and more powerful tools for law enforcement. To that end 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." It is a vital component of our country's response to terrorism.

The Social Security Administration serves as the front line of defense in ensuring the integrity of Social Security numbers—a responsibility it takes very seriously. It is responsible for accurately assigning Social Security numbers, as well as ensuring the wages earned and Social Security benefits claimed on that number are only those of the number holder. As we will soon hear, since 9/11 the agency has implemented a number of initiatives to help prevent identity theft. Yet we will also hear there is more to do, particularly with regard to inter-agency cooperation. A silo approach by Federal agencies is not acceptable, as President Bush recognized through his proposal to create a Department of Homeland Security.

Our Nation has been forever changed by the horrible attacks on our country. No longer can we sit idly by and not protect ourselves from domestic and foreign terrorists. Also, long before these attacks, individuals were fighting more personal battles with identity thieves. We must implement changes that will prevent and deter future attacks on our national security and our personal financial security.

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

Chairman GEKAS. I thank the Chairman. I begin by asking unanimous consent that the written statement that I have prepared to be my opening statement be received in the record.

Chairman SHAW. Without objection.

[The opening statement of Chairman Gekas follows:]

Opening Statement of the Hon. George W. Gekas, a Representative in Congress from the State of Pennsylvania, and Chairman, Subcommittee on Immigration, Border Security, and Claims

Chairman Shaw, it's a pleasure to join with you and your colleagues on the Committee on Ways and Means. Thanks for your kind words of welcome.

I agree with your concerns about the overuse of the Social Security Number and its lack of privacy.

Times have changed since the Social Security Administration began producing the little green cards in 1937. We in the Congress need to determine what remedies can be applied to the use of the card and to the practices of the Social Security Administration.

I am very supportive of the efforts of Chairman Shaw to bolster protection of the Social Security Number. At the same time, we need to look at what else is needed to address the problem comprehensively.

In some cases, old laws need to be updated.

There's no question in my mind that the criminal penalties for identity theft and for Social Security Number fraud, in particular, need to be strengthened.

We also need to look at whether tougher legal rules are needed so that the Social Security Administration will move faster to work with federal law enforcement agencies to stop the growth of identity fraud.

All Americans, especially Seniors and those approaching retirement, need to hear that the Social Security Administration is aggressive in preventing ineligible people from obtaining Social Security Numbers. It is only a short step from fraudulently obtaining Social Security Numbers to fraudulently obtaining benefits.

The structural problems of the Social Security program are well known and publicly debated. The problems with Social Security number fraud are much less well known, but equally important to protect benefits and the financial well being of the fund. I believe we can do much more to make it very difficult for terrorists, crooks and illegal workers to obtain Social Security Numbers.

Terrorists and crooks and the purveyors of illegal documents are getting smarter and many are experts in use of the Internet. We have to compel our government agencies and especially the Social Security Administration to get smarter too. We have to look at changing the business practices of the Social Security Administration to raise the bar against fraudulent and counterfeit source documents. We have to make it much more difficult for people to obtain two and three valid Social Security Numbers from this government agency.

The Social Security Number is the most common form of identification confirmation by Americans. It is absolutely vital that we make it extremely difficult for terrorists to abuse this fundamental key to the American identity.

I look forward to the testimony from the Deputy Commissioner of the Social Security Administration, and from our other excellent witnesses. I want to particularly recognize Mr. Matthew Reindl. He has come here today from Great Neck, New York, to tell us about the difficulty of operating a small family business with strict adherence to federal laws, when his competition freely employs illegal workers because of the lack of enforcement by federal agencies, including especially, the INS.

Chairman GEKAS. Hearing no objection from my colleagues, I will proceed to underline and endorse the concepts enunciated by the gentleman from Florida, Mr. Shaw, the Chairman, on the importance of the hearing and on the subject matter itself.

Perhaps the most ironic outcome of Social Security fraud and identity theft is that this great social program, one of the greatest ever attempted by any society in the history of the world, is also a potential and actual vehicle for terrorists who threaten our Nation and actually attack our Nation.

That is reason enough to convene such a meeting and to determine, once and for all, what we as legislators can do to prevent this kind of result that threatens the very lives of the people who are Social Security recipients and Social Security contributors across the land.

If that weren't enough to put us on guard on what has been happening to our Social Security number system, then we have to consider as well the attack on the system that identity fraud perpetrates with respect to diminution of the funding and the assets of the Social Security program. For everyone who falsely secures a Social Security number and starts to receive benefits, the pot of available funding is diminished by that much, to the detriment of

the current recipients and future recipients, not to mention the budgetary problems facing the Nation every single year, vis-à-vis the health of the Social Security fund and all that it touches in our society.

So, when we begin to listen to the witnesses here, we will have an eye and ear pinned to what it means in the day of the terrorist and what it means in the day of watchfulness on the health of the Social Security fund, what it means to try to prevent identity fraud and Social Security fraud in all its aspects.

I thank the Chair, and I yield back the balance of my time.

Chairman SHAW. Mr. Becerra, do you have an opening statement?

Mr. BECERRA. Thank you, Mr. Chairman.

First, let me say to the Chairman of the Subcommittee on Social Security of the Committee on Ways and Means, thank you very much for the several hearings that you have held on this issue of the Social Security number identity fraud and the importance to not just the people who will be recipients of Social Security but to all Americans who depend on such an important program, and, of course, to our government, which must dispense and implement this valuable program that has existed for over 75 years.

To our Co-Chair who is here today, Mr. Gekas, it is a pleasure to again have an opportunity to sit with him on a panel, as I did before when I served on the Committee on the Judiciary. I am pleased to join with my colleague, the Ranking Member of the Subcommittee on Immigration and Claims, Ms. Sheila Jackson Lee as well.

With all our colleagues that are here, I am looking forward to a hearing that will help us gain better insight on how we protect not just the Social Security number but Americans from identity fraud, how we protect them against invasions of that security that they had grown accustomed to. Now that we have seen what happened after September 11 and the fact that the 19 terrorists used Social Security numbers to help them obtain that fraudulent identity, it is important for us to try to move forward to see how we can secure not just our freedom and our privacy, but also the security of this country.

So, I am very much looking forward to the hearing, building upon what has been done through the Chairman's and the Members' good work on the Subcommittee on Social Security, and hoping that the testimony enlightens us on how to move forward and move forward quickly.

So, I thank you, Mr. Chairman. I yield back the balance of my time.

Chairman SHAW. Thank you, Mr. Becerra. Ms. Jackson Lee?

Ms. JACKSON LEE. Thank you very much, Mr. Chairman, and might I add my appreciation to Chairman Shaw and as well Chairman Gekas for having a hearing that gives example to government working at its best, Committees with their respective jurisdictions coming together. I'm pleased, of course, to join with the fellow Ranking Member of the Committee on Ways and Means and a former colleague on the Committee on the Judiciary, Xavier Becerra, and I think this very important issue.

It is good to see the Inspector General will be here. You testified earlier on some matters that we have before the Committee on the Judiciary, and I believe you gave great insight.

It is, of course, natural and important that we take leadership on the issues of Social Security fraud, theft, and issues that would impact negatively on the identity and the security of this Nation. Serving on the Subcommittee on Immigration and Claims, of course, I have to add my additional concern in words that I reflect most often; as we look to secure the Nation, we must also realize that we are a nation of immigrants, a nation of laws, even after September 11 and the unfortunate and tragic and horrific event that occurred, where so many of the terrorists and the perpetrators came in on legal visas that we still do not equate terrorism to immigration.

So I would hope, as look to this question, you will also have as a backdrop the fact that the recently passed immigration reform bill did not include a national identity card. We thought that that was not the direction to go, but it certainly is a direction to go with Mr. Shaw's concern about Social Security card fraud and identity fraud.

I hope that we will be cognizant of the technology that may put together a national Social Security card and the abuses that could occur. I also hope that we will avoid steps in this hearing and any legislation that would increase rather than diminish immigration-related discrimination that has already become a problem with the use of Social Security numbers by some employers.

So, we have our job cut out for us. I believe the American people will challenge us to do the right thing together, to provide enhanced security, but at the same time balance and respect the laws of this land, and certainly the civil rights and civil liberties of the people of this land.

With that, Mr. Chairman, I would ask that my entire statement be put into the record.

Chairman SHAW. Without objection, and without objection, any statement that any of the Members of this joint Committee hearing would like to put into the record will be made part of the record.

[The opening statement of Ms. Jackson Lee follows:]

**Opening Statement of the Hon. Sheila Jackson Lee, a Representative in
Congress from the State of Texas**

Good Afternoon Mr. Chairman. I would like to thank the Chairman and the Ranking Member of the Subcommittee on Social Security for inviting me and other member of the Subcommittee on Immigration, Border Security and Claims to participate in this important hearing on the importance of ensuring the integrity of Social Security Numbers (SSN) and preventing their misuse by terrorist and identity thieves. As many will note, the SSN is probably the most important number as it is the first step in access to so many things in our culture. If you need a drivers license you need a social security number. If you need credit you need a social security. It is central to American life.

On September 11, the United States experienced the worst attack on its soil since World War II. In the weeks following the attack, the U.S. government initiated a nationwide investigation into the reasons behind the failure of U.S. police and intelligence agencies to uncover the plot to destroy the Trade Center. In *Washington Post* stories earlier this year it was revealed that some of the September 11, 2001, hijackers had used identity theft and fraud to obtain false SSNs and other identification documents to facilitate training and preparation for the September 11, attacks.

First, let me emphasize that I, like you, condemn SSN fraud and its negative impact. None of us would approve of the fraudulent use of identification cards or any

other documentation. People who fraudulently use SSNs can and should be punished.

Our subcommittee held another Joint Hearing in Identity Theft and Fraud in June of this year with the Judiciary Subcommittee on Crime. Mr. Huse testified there, and I would like to let him know that it is good to hear from him again. I will say now as I said then, that efforts at stopping terrorism beg the question at which point is it best to stop the terrorist. Clearly, the best point to stop terrorists is prior to their entry into the country, before they have access to our social security administration, departments of motor vehicles and other infrastructure critical to secure identification documents. It should be pointed out that "18 of the 19 hijackers entered the United States on visitors visas." They made "concerted efforts to do so, so it is logical to assume that they believed that this type of entry, as visitors, made them less likely to come to the attention of federal authorities." This glaring fact underscores the difficulties faced by agencies in preventing terrorists from obtaining fraudulent SSNs and other identification. Again, it is better to get to terrorists prior to their entry into our country.

Effective measures will be difficult to achieve. The integrity of any SSN verification system hinges on the security of the documents which underlie it, and such "breeder" documents must also be secure. The birth certificate is a "breeder" document in that it can be used to obtain an identity document such as a U.S. passport, driver's license, military I.D. and a SSN.

However, if we are going to examine these issues, let us do so in a balanced fashion. We need to decide just how far we are willing to go in dealing with this problem. For instance, birth and death records are certain to be used, and we need to examine just what resources we need to dedicated to revamping these record-keeping systems. We must deal with issues of efficiency and resources in a complementary fashion as opposed to pitting these issues against one another. The same is true of revising SSA and INS databases. Are we willing to bear the costs of developing and maintaining such gigantic data bases? Again, examination of these issues must be done in a fair and equitable way.

The fight against SSN fraud and counterfeit documents should not become a fight against personal privacy that leads to a national ID card. I do not want a national ID card to be demanded of Americans every time they engage in what should be routine activity that can be conducted anonymously and without government intervention.

Technology has played a vital role in advancing freedom around the world, but it also has laid new temptations at the doorstep of business, government and criminals. Once the technology and a database are in place for a system such as a national ID, alternative uses for the system will arise. This potential abuse of such a system by unscrupulous businesses and governments and plain criminals could be devastating to our nation's average citizen.

Congress must also take care to avoid steps that would increase rather than diminish immigration-related discrimination that has already become a problem with the use of SSNs by some employers. In response to employer sanctions, some—but not all employers have screened out all "foreign-looking" or "accented" job applicants; or conversely have adopted the practice of looking only for illegal immigrants to hire in order to hold their status over these employees heads. They have selectively applied verification procedures only to "suspect" employees and demanded documents when hiring foreign-sounding employees when compared to other employees.

We also have to be mindful of states' rights. We should not become so aggressive in this area that states are turned into mere tools of the Federal Government in connection with the identity documents they issue.

Finally, Mr. Chairman, I hope that we can work cooperatively, and in the true spirit of bipartisanship to eliminate SSN fraud and make the necessary changes in the law that must be made. However, I would like to say for the record that although there is ample and substantial SSN fraud and theft, this hearing should in no way be used as a vehicle to discourage talented men and women from different countries from coming to the United States to study, to exchange creative thought and ideas, or to discourage businesses from temporarily moving their employees to contribute to our economy and our way of life. We should discourage SSN fraud, but not discourage fair and equal opportunity.

Thank-you Mr. Chairman.

Chairman SHAW. Now it is my pleasure to recognize the Honorable James B. Lockhart III, who is the Deputy Commissioner of So-

cial Security. I believe this may be the first time you have appeared before the Social Security Subcommittee.

Mr. LOCKHART. Yes, Mr. Chairman.

Chairman SHAW. It is my privilege to welcome you.

Please proceed as you see fit. We have your full statement which, without objection, will be made a part of the record, as will the full statements of all the witnesses this afternoon. So, you may summarize or proceed as you see fit, Mr. Lockhart.

STATEMENT OF THE HON. JAMES B. LOCKHART III, DEPUTY COMMISSIONER, SOCIAL SECURITY ADMINISTRATION

Mr. LOCKHART. Chairman Shaw, Chairman Gekas, and Members of the Subcommittees, thank you for asking me here today to discuss our work to preserve the integrity of the Social Security number and to prevent its misuse.

Commissioner Barnhart and I have made protecting the Social Security number a major stewardship priority. We have made many important enhancements and are reviewing other improvements.

We all know that Social Security number misuse can lead directly to identity theft with serious personal and economic consequences. On September 11, we also learned that it can have more far-reaching consequences, as the terrorists used made-up Social Security numbers.

As you know, the original purpose of the Social Security number was solely for tracking the earnings of people who worked in jobs covered by Social Security. Ever since, the use of the Social Security number has mushroomed as a way to identify people in records systems. It has become the identifying number for Federal and many other employee systems, taxpayers, noncitizens authorized to work in this country, beneficiaries of Federal- and State-funded programs, and some drivers' licenses.

By 1974, Congress became concerned about the widespread use of the Social Security number and passed the Privacy Act. It provides that except when required by Federal law, no government agency could withhold benefits from a person simply because of a refusal to give his or her Social Security number. Federal law does not restrict Social Security number use by private businesses or organizations.

As you can see, the Social Security number has become the personal identifier through a buildup over time. Unfortunately, it also has become the identifier of choice for criminals, including terrorists.

After September 11, the Social Security Administration formed a high-level response team to better prevent those with criminal intent from using Social Security numbers. We have put a new training emphasis on what we call enumeration for the 1.5 million noncitizens that we give numbers to every year.

On March 1, we stopped assigning Social Security numbers to noncitizens for the purpose of applying for a drivers' license. Noncitizens can now only get a Social Security number if they are authorized to work or if they need it for public assistance.

On June 1, we began verifying birth records of U.S.-born citizens older than age 1 who apply for a Social Security number, and we

are piloting an online system that lets employers verify the names and Social Security numbers of newly hired employees. That should help to strengthen our present verification systems.

We are also leading the government-wide e-VITAL project to improve the death master file and electronic birth records verification systems.

We are implementing a range of new initiatives with the Immigration and Naturalization Service (INS) and the State Department, which will be consistent with the requirements of the Privacy Act. We now verify all INS documents with that agency.

By the end of the year, under the Enumeration at Entry Project, we will assign directly Social Security numbers to newly arrived immigrants based on the information the State Department and INS collect as they authorize noncitizen entry into the country.

We are also taking major steps to improve the accuracy of the 250 million annual wage reports that we receive, as they are critical for correctly calculating benefits. Despite improving our matching routines, almost 10 million of those 250 million wage reports a year are placed in the suspense file because the name and the Social Security number do not match. We have been writing letters to employees, asking them to correct the information. Over the last several years, we have greatly increased the no-match letters to employers.

Let me say that we appreciate the Subcommittee's effort to strengthen Social Security number privacy and prevent identity theft. The provisions in H.R. 2036 which strengthen the penalties and enforcement for Social Security number misuse would help in our efforts to locate and eliminate abuses.

Adding civil monetary penalties as proposed to existing criminal penalties for Social Security number misuse would provide another level of deterrence. We believe it would strengthen our ability to deal with cases of misuse that are not criminally prosecuted by the U.S. Department of Justice.

In closing, I would like to emphasize that the Social Security Administration is committed to doing all that it can to protect the integrity of the Social Security number by strengthening our enumeration and misuse detection capabilities. Commissioner Barnhart and I look forward to continuing to work with you on this vital national issue. I would be happy to answer any questions.

[The prepared statement of Mr. Lockhart follows:]

**Statement of the Hon. James B. Lockhart III, Deputy Commissioner
Social Security Administration**

Mr. Chairmen and Members of the Subcommittees:

Thank you for asking me to be here today to discuss the process of assigning and issuing Social Security Numbers (SSN), and the role that the SSN has in our society today. As the number of legitimate uses for SSNs increases, especially in the private sector so does the potential for misuse—and the resulting consequences of misuse.

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

The tragic events of September 11, and reports that some of the terrorists fraudulently used SSNs, have brought home the need to strengthen the safeguards to protect against the misuse of the SSN. Since Commissioner Barnhart and I have been at Social Security we have made protecting the SSN a major stewardship priority.

We have made many important enhancements this year and are reviewing other improvements.

Original Purpose of the Social Security Number and Card

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

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

Growth of SSN as an Identifier for Other Federal Purposes

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

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

Statutory Expansion of SSN Use in the Public Sector

The first explicit statutory authority to issue SSNs did not occur until 1972, when Congress required that SSA assign SSNs to all noncitizens authorized to work in this country and take affirmative steps to assign SSNs to children and anyone receiving or applying for a benefit paid for by Federal funds. This change was prompted by Congressional concerns about welfare fraud and about noncitizens working in the U.S. illegally. Subsequent Congresses have enacted legislation which requires an SSN as a condition of eligibility for applicants for SSI, Aid to Families with Dependent Children (now called Temporary Assistance to Needy Families), Medicaid, and food stamps. Additional legislation authorized States to use the SSN in the administration of any tax, general public assistance, drivers license, or motor vehicle registration law within its jurisdiction.

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

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

In the 1990's, SSN use continued to expand with legislation that authorized its use for jury selection and for administration of Federal workers' compensation laws. A major expansion of SSN use was provided in 1996 under welfare reform. Under welfare reform, to enhance child support enforcement, the SSN is to be recorded in the applications for professional licenses, driver's licenses, and marriage licenses; it must be placed in the records relating to a divorce decree, support order, or paternity determination or acknowledgment; and it must be recorded in the records relating to death and on the death certificate. When an individual is hired, an employer

is required to report this event to the State's New Hire Registry. This "New Hire Registry" is part of the expanded Federal Parent Locator Service which enables States to find non-custodial parents by using the SSN.

Private Sector Use of the SSN

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

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

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

The SSN as an Identifier

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

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

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

e-VITAL

I also want to mention that SSA is actively involved in an interagency initiative (e-VITAL) which is pursuing electronic data exchanges between other federal agencies and the States. This "e-VITAL" program consists of 2 projects that are being undertaken to maximize efficiency and improve customer service to citizens and businesses. One project is working with State agencies and funeral homes to expand and improve electronic notification of deaths. The second project is an electronic query system that allows State and Federal agencies to access birth and death information. This information would be used to improve the accuracy of our records and ensure that proper benefits are paid to individuals.

Identity Theft

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

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

Preventing identity theft can play a role in the prevention of any future terrorism. Identification documents are critically important to terrorists, and a key to such documents is the SSN. The integrity of the SSN must be ensured to the maximum ex-

tent possible because of the fundamental role it can play in helping unscrupulous individuals steal identities and obtain false identification documents.

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

SSA Response to SSN Misuse

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

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

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

In July, we began verifying any documents issued by the INS with them before assigning an SSN. We are verifying many of these electronically. But if the immigration document is not recorded in the INS system within ten days, we request written confirmation from INS that the documents submitted are bona fide and that the individual is authorized to work. This new verification process was fully implemented earlier this month.

We are also planning to pilot a Social Security Card Center that would be an interagency specialist group designed to provide quick and efficient service while ensuring the integrity of the enumeration process.

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

We also implemented changes to speed up the distribution of our Death Master File. SSA receives reports of deaths from a number of sources, and from computer matches with death data from Federal and State agencies. This information is critical to the administration of our program and is made available to facilitate the prevention of identify theft of the SSN's of deceased persons. Many of the private sector companies purchasing this information are credit card companies and financial institutions.

Furthermore, we are also limiting the display of SSNs on our correspondence. As of October 1, 2001 we no longer include the first five digits of the SSN on Social Security Statements and as of December 2001 on Social Security Cost-of-Living Notices. We do use the full SSN on other correspondence because there may be legal requirements for display of the SSN on the notice especially on termination and award notices. However, to ensure the confidentiality of the SSN on mail we do not show the addressee's SSN on the envelope, if mailing an envelope to an individual. If requesting information from third parties, we do not show the SSN for the purpose of associating the reply with the file when it is returned.

The good news is that over 80% of our beneficiaries receive their payments by direct deposit, which means for this large group there are no SSNs to be stolen or paper checks that can be lost or stolen. For those that do not use direct deposit, the Department of the Treasury prepares and mails all government checks including those for Social Security and Supplemental Security Income recipients. Effective with the September 1, 2000 benefit payments, the SSN printed on Social Security and Supplemental Security Income checks is no longer visible through the envelope window. Additionally, to protect the privacy of recipients who are paid by check and help prevent identity theft, Treasury is taking steps to remove all personal identification numbers, including the SSN, on all check payments. The goal for completing the project is early 2004.

Detecting SSN Misuse

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

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

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

Of course SSA's OIG has played an ongoing role in the investigation of fraud and misuse of the SSN, as shown in the following examples. As you know, SSA OIG agents have participated along with the US Department of Justice in "Operation Tarmac". In this joint effort, individuals have been identified who misused SSN's to fraudulently obtain security badges, and to date, a significant number have been sentenced. Further, SSA's OIG, INS, and local law enforcement authorities investigated an organization in Utah that manufactured and sold counterfeit documents. To date, nine individuals have been sentenced to jail time and/or deportation, and the investigation continues. In another combined effort, OIG, Postal Service, Federal Bureau of Investigations and the Secret Service investigated and arrested individuals in Seattle who established more than 50 false identities to open bank accounts.

Another important pillar in the effort to safeguard program integrity is the joint SSA-OIG General Cooperative Disability Investigations Program (CDI). Its mission is to detect fraud in the early stages-at the time of application for Social Security benefits or during the appeals process. The results of CDI investigations were used to support over 2,700 denials or terminations, allowing SSA to avoid improper payments to individuals.

Assisting Victims

To help victims, SSA provides hotline numbers to SSA's Fraud Hotline and the Federal Trade Commission ID Theft Hotline. We provide up-to-date information about steps that the person can take to work with credit bureaus and law enforcement agencies to reclaim their identity. We issue a replacement card if their Social Security Card is stolen. We help to correct their earnings record and issue a new SSN in certain circumstances. If the victim alleges that a specific individual is using

the SSN, SSA develops the case as a possible fraud violation. If appropriate, we refer the case to the OIG for an investigation and work closely with the OIG to facilitate their investigation.

Suspense File

As I mentioned earlier, the primary purpose of the SSN has always been to allow us to accurately record and keep track of a worker's earnings. This is SSA's core business process, and it ensures that a worker and his family receive benefits that reflect his work history. The earnings suspense file is an electronic holding file for reported earnings items that cannot be recorded to the earnings records of individual workers because the name and SSN on the items do not match SSA's records.

Currently, we receive and process about 250 million annual wage reports (Forms W-2) for employees from about 6.5 million employers. In recent years, after electronic and manual processing, about 97 percent of these items are ultimately posted to the Master Earnings File (MEF), which contains a record of the lifetime earnings of each individual worker. The remaining items, about 3 percent, are ultimately placed in the earnings suspense file. For 2000, after electronic processing, 10 million reports of wages were sent to the suspense file representing over \$54 billion in wages. The suspense file contains all mismatches since 1937 about 237 million reports of wages representing \$376 billion in earnings.

So, why is this issue significant? As I stated earlier, the wages reported to SSA on the Forms W-2 are used to maintain a record of every working individual's earnings. This earnings record is the basis for computing retirement, survivors, and disability benefits. If a worker's earnings are not recorded, he or she may not qualify for benefits or the benefit amount may be lower. When a person files for benefits, the earnings record is reviewed and an effort is made to establish any earnings that are not shown. However, it may be difficult to accurately recall past earnings and to obtain evidence of them. Thus, it is better to establish and maintain accurate records at the time the wages are paid.

We have a number of initiatives to assure that wage items are credited to the correct individual's earnings record and do not go into suspense. These include:

- Encouraging the filing of wage reports electronically or on magnetic media which has increased to 78.0% percent in 2001.
- Using over 23 software routines to match names to SSNs which initially do not match SSA records—for TY1999, software matched 16 million (about 60 percent) of the initial mismatches.
- Notifying employees of name/SSN errors and requesting corrections. In the last five years we have sent an average of 8 million letters a year to individuals or to their employers if we do not have a record of the employee's address.
- Notifying employers of name/SSN errors. In 2002, we increased these "no match" letters from about 110,000 to 870,000. This is because we sent these letters to all employers who submitted W-2 forms with information that did not match our records instead of only to employers with relatively large number of mismatches. We will be reviewing the effectiveness of this change.
- Providing outreach to the employer community to reinforce the need for accurate name/SSN reporting.

We are building a new Earnings Suspense File process that looks promising. It would electronically find millions of additional matches and post them to the correct earnings record.

Under this new process, we are estimating that at least 30 million items will be removed from the suspense file and credited to the records of individual workers. If so, benefits for several hundred thousand beneficiaries would be increased. If the test we have planned for the fall of this year is successful, we expect to begin the new process early in 2003 and have it completed by the end of 2004.

Improving Enforcement

Mr. Shaw's bill (H.R. 2036) is aimed at the need to limit private and public sector use, display and sale of the SSN and to increase penalties for misuse of the number. We appreciate Mr. Shaw's commitment to these objectives.

We support efforts to strengthen the penalties and enforcement for SSN misuse, which would be of great help to the agency in our consistent efforts to locate and eliminate abuses to the program. While current law provides criminal penalties for SSN misuse, the addition of civil monetary penalties for SSN misuse would provide another level of deterrence for those who would misuse the SSN. Such measures

would help to strengthen our ability to deal with instances of misuse that are not criminally prosecuted by the Department of Justice.

Closing

I would like to conclude by emphasizing that we at the Social Security Administration are committed to protecting the integrity of the SSN. We want to do what we can to help prevent identity theft, to assist those who become victims and to assist in the apprehension and conviction of those who perpetrate the crime. We are committed to improving the accuracy of the records of workers earnings and thereby helping to ensure accurate retiree, disability, survivors and SSI payments.

In a larger view, the Social Security Administration is on guard for identity theft. This is a challenging task. In our experience, most instances of identity theft have resulted not from any action or failure to act by SSA, but from the proliferation of personal information in our society. The disclosure of SSNs by private citizens and organizations are prime among them. While SSA cannot control the disclosure of SSNs, we can and are doing a better job in areas that we can control, such as enumeration and misuse detection.

Thank you for asking us to testify on this issue.

Chairman SHAW. Mr. Lockhart, if someone comes into this country, perhaps on a student visa or whatever, opens a bank account, the bank will require that person to supply their Social Security number. This is needed for the reporting of interest and things of that nature that account might be subject to.

Is there any indicator on the Social Security number as to the status of that particular person? Is there any indication on the Social Security card as to the status of that particular person? Now, this is not on a work visa.

Mr. LOCKHART. Yes. First of all, if a student comes into the country with a J-1 or F-1 visa, and is not authorized to work, we will not give him a Social Security card. So, that's the first step. They have to be authorized to work to get a Social Security number.

Let's assume that the university tells us that they are authorized to work, and we get a letter from the university to that effect, and we do the verification with the INS about the visa, we would then give them a Social Security number. The Social Security number itself has nothing special on it, but the card would say that the employer should check the INS documents in that case.

Chairman SHAW. If the person who the card is issued to then decides to go to work and supplies that identification number to the employer without showing him that card, what happens at that particular time, assuming then that the person takes the job and the Federal Insurance Contributions Act (FICA) wages are paid into the Social Security Administration?

Mr. LOCKHART. Again, assuming that he or she got the card legitimately, there is no problem. That is what is supposed to happen, that they will pay the FICA taxes in, and assuming we have verified the documents with the INS, the card was given legitimately. The employer still is supposed to look at the documents to make sure that they are legitimate.

Chairman SHAW. I understand the employer would be liable for other penalties for not properly checking the resident status or exactly why that person happens to be in the country, whether they be a citizen or a noncitizen.

Mr. LOCKHART. Now, in the circumstances that you posed at the beginning, if they were not authorized to work, if we did not

give them a Social Security number, in theory, they can go to the U.S. Department of the Treasury and get a taxpayer number. That is a 900 series. It looks like a Social Security number, but that is a separate series and is not part of the Social Security system.

Mr. JOHNSON. Would the gentleman yield?

Chairman SHAW. I am a little confused here. I will be glad to yield in just a moment, but I am a little confused here because the person who you issued the Social Security number to may not be authorized to work or may not be here on an actual work visa. Is that not correct?

Mr. LOCKHART. Under our new procedure, that should not happen. As of September 1, we are verifying all documents with the INS, and they are telling us that the document is good before we give the Social Security number out.

Unfortunately, I think in the past, before the new procedure, there was a procedure at Social Security, where, if someone had been in the country only 30 days, our field office looked at the documents, put them under black lights and checked them to see if they were real. If they were a really good forgery, they might have been faked or something, and they could have possibly gotten a Social Security number on documents that were counterfeit.

Chairman SHAW. The gentleman from Texas?

Mr. JOHNSON. Thank you, Mr. Chairman.

I would like to follow up on that because just in Dallas, Texas, this month, they caught a bunch of illegals in an 18-wheeler, some of which died. You are aware of that case, I am sure.

My question is, there were 26 of them that were released on the spot in the United States and told they could get a Social Security number from you and go to work. Now, how do you account for that kind of thing?

Mr. LOCKHART. I am not actually aware of who made that statement.

Mr. JOHNSON. The lady who runs the district office for the Immigration and Naturalization Service there in Dallas. They let them go for 2 months, and she told me that they would get Social Security numbers and be given work permits. Three of them were allowed to go, one to Chicago and two to New York City, from Dallas.

Mr. LOCKHART. Well, under our present procedures, they would have had to have a document from the INS saying that it was valid for them to work. If the INS had given that document to them, yes, if you bring in a valid document—

Mr. JOHNSON. You give them a Social Security number just on the basis of the Immigration and Naturalization Service letting an illegal have a work document temporarily? Do you put any time limit on the Social Security number? How do you know they are not all terrorists?

Mr. LOCKHART. Again, our job is to give a Social Security number when we have valid documents from the Immigration and Naturalization Service. We get the documents, we look at them, we check them, we go into the INS system, we check it against the INS system. If it is not in the INS system, then we send a paper request to the INS to get them to verify that there is a real document that authorizes them to work.

It is not the Social Security Administration's job to decide whether they are authorized to work. It is our job to give them a number once they are authorized to work, so that they will pay taxes into the Social Security fund and to the Internal Revenue Service (IRS).

Chairman SHAW. Reclaiming my time, there are situations where someone can get a nonworking Social Security number. Now, that Social Security number, can an employer or anybody look at that number and say, "Hey, that's a nonworking Social Security number"? That is my question.

Mr. LOCKHART. Yes, there are circumstances. Historically, there were more circumstances. As of March this year, we are only giving them to people who are not working that are required by some benefit system—I think we will give about 20,000 or 30,000 out a year from now on. Previously, we did it for a driver's license, but those cards themselves say "not eligible for work." There is no special number, and we are looking at a special number. It is one of the things we are looking at.

Chairman SHAW. That is what I wanted to get at. I think that when we do issue a nonwork Social Security number, it ought to have something on it, a letter, a prefix, or something, that would identify it as "this is not for purposes of work."

Mr. LOCKHART. We are looking at a special series, just like, as I mentioned, the Treasury Department has the 900 series. We are looking, potentially, at a special series for anybody that doesn't have a permanent right to work in this country.

Chairman SHAW. Do you know if you can do that without legislation from us? I believe you can.

Mr. LOCKHART. I believe we can. Yes, sir.

Chairman SHAW. If you need legislation, come back, and we will work on it. Mr. Gekas?

Chairman GEKAS. Yes, I thank the Chair.

Mr. Lockhart, pursuing some of the questions that emerged from the statements and questions that were posed by the gentleman from Texas, Mr. Johnson, you said that after September 11, you undertook several initiatives to pin down the ability to grant Social Security numbers to only those who deserved them. The questions posed by Mr. Johnson implicate the Immigration and Naturalization Service in the wholesale admission of people first into the country and then to allow them to seek and gain Social Security numbers. Were there any recommendations made by the Social Security Inspector General in his recent report with respect to this problem, the reliance of Social Security on INS in its processing of prospective new numbers?

Mr. LOCKHART. Well, the Inspector General has recommended, I think for several years, to do what we just implemented. One of the points I would like to make is that both Commissioner Barnhart and I came in after September 11, and we looked at all these things, and we saw that there were holes in our system, and we want to correct them. We have corrected a lot, but we have more room to go. We are very concerned about this issue, and we will work on it.

The key recommendation that the Inspector General had made is that we verify every document with the INS. Every document that authorizes someone to work, we first go into the computer sys-

tem. If it is not in their computer system, then we actually send a copy of the document to the INS and ask them to verify it.

So, that is our procedure, and we are following it now. It may, in some cases, slow up persons getting a Social Security number, but we think it is well worth it.

Chairman GEKAS. Do you hold up issuance of the number until submissions are made to you by the INS so that you are perfectly—

Mr. LOCKHART. Under our new procedure that we began implementing about 3 months ago and finished September 1, that is correct. We do not issue a Social Security number if the documents have not been verified by the INS.

Chairman GEKAS. Speaking of the recommendations of the Inspector General, were they before September 11 or after, or both?

Mr. LOCKHART. As I remember, they were both.

Chairman GEKAS. Do you have a scorecard on the recommendations made and where you are in implementing or attempting to implement those recommendations?

Mr. LOCKHART. Yes, Mr. Chairman, we do have a scorecard. We have been working very diligently. This task force that I mentioned in my testimony has a whole series of initiatives. We have implemented a lot of the major ones, but we are looking at other ones. For instance, the one that Chairman Shaw mentioned about a special series of numbers for nonpermanent Social Security cards.

So, we are working very diligently through this list. As I said, both Commissioner Barnhart and myself are really extremely serious about making sure that only people who are authorized to work, only people who should get Social Security numbers, are getting them in this country.

Chairman GEKAS. I would like, personally, and perhaps the other Members would also benefit from it, if we could actually produce such a scorecard, that is, to list the recommendations on the left and then give us completed or implemented or about to be implemented or on the way, some kind of indication as to what the recommendations were and what progress has been made in implementing those recommendations. I would be interested in that kind of graph.

Mr. LOCKHART. We certainly will be happy to provide that for the record, Mr. Chairman. I think as you talk to our Inspector General when he comes up in the next panel, I think he will tell you that we are making extremely good progress on this issue.

Chairman GEKAS. Well, you will have time to do it right before he takes the stand.

[Laughter.]

Mr. LOCKHART. Well, I have some versions of it here, but—

Chairman GEKAS. You can start the conversation now. I yield back the balance of my time.

Chairman SHAW. Thank you, Mr. Gekas. Mr. Becerra?

Mr. BECERRA. Thank you, Mr. Chairman.

Thank you for your testimony, Mr. Lockhart. I appreciate it.

Let me make sure, before I ask the particular questions that I have, I want to make sure that I understand something correctly. There are some 600,000 Social Security numbers that come to your

attention that are based on nonwork-authorization Social Security numbers, correct?

Mr. LOCKHART. Yes, let me explain it. We have, really, three major categories of Social Security cards.

One is, you are authorized to work. You are either a citizen and you got it at birth, you have been authorized to work, or you have been permanently allowed in the country. The second one is that you are authorized to work with INS documentation, and the third one is that you are not authorized to work. We used to give those out because many State driver's license departments required them, and we have given out, unfortunately, many millions of those.

Every year, as we get the wage earnings reports in, those 250 million that I mentioned in my testimony, we get about half a million wages on nonwork Social Security numbers. Now, that doesn't mean that they are not authorized to work because they may not have come in to us again to get their Social Security card updated.

Mr. BECERRA. That was going to be my point, because I am familiar, being from California, that there are a lot of folks who start with a nonwork Social Security number but then ultimately obtain the authorization to work. Then, for whatever reasons, either they or the employer, somehow the information doesn't get to the Social Security Administration immediately. So, until that information gets to you, they are categorized as nonwork-authorized Social Security numbers.

Mr. LOCKHART. That is correct.

Mr. BECERRA. Okay. Let me get back to the whole issue, because it is becoming clear, now that Social Security has been able to give us more and more information, that you are trying to clean up these files, which for years have been building up and up in terms of the number of cases where we haven't been able to identify all the pertinent information for an individual.

My understanding is you obtain, on a yearly basis, claims or numbers or information on cases for about 250 million Social Security numbers.

Mr. LOCKHART. What we receive are wage reports from employers. Oftentimes, people change jobs, so there are actually less people working than the number of wage reports.

Mr. BECERRA. The information I have is that there are some 250 million wage reports on an annual basis, representing about 150 million workers. When you run those through your checks, at the onset, there is about a 1 in 10 nonmatch for those wage reports, incorrect name, some information doesn't correspond. It doesn't mean that it is not a valid Social Security number. It just means that, of those 250 million, 1 in every 10 or so came up with some red flag.

Mr. LOCKHART. Right. It didn't match.

Mr. BECERRA. It didn't match. You are then able to reduce that to about 2 or 3 percent, versus about 10 percent, correct?

Mr. LOCKHART. Well, 3 percent yes.

Mr. BECERRA. Three percent, and that is your suspense file?

Mr. LOCKHART. Exactly.

Mr. BECERRA. Within that suspense file, my understanding is that you have a caseload of about—is it 250 million of these?

Mr. LOCKHART. Yes. We have, in the suspense file——

Mr. BECERRA. About 237 million.

Mr. LOCKHART. Yes, 237 million. Exactly.

Mr. BECERRA. So, 237 million. In tax year 2000, you received some 9.6 million more of these wage reports that went into the suspense file. Give me a sense of what it takes to close a case on one of these files. What does it take to do the final check, to determine if there was just an error or if we have to do some further checks?

Mr. LOCKHART. We have computer teams that catch about two-thirds, as you mentioned, of the mistakes. It can be typos. Someone's maiden name hadn't been changed in our records. Some Hispanic names get transposed. They are having that problem right now at the California Department of Motor Vehicles. I was out there a week or so ago, and there is a lot of activity there.

So, our routines catch some of that. So, as we have done for many years, we then send out to the employees whose wage report we are getting, a letter telling him we are having a problem with mismatching. We send close to 10 million of these letters out a year, and we have been doing it for years, and about 1 million-plus, we don't have a good address for the employee, so we actually send it just to the employer. We ask them to come to the Social Security office and straighten it out, submit a form called a W-2C for correction.

Mr. BECERRA. What is the resource requirement for you to do that along with administering all the retirement benefits, dealing with survivors' benefits, disability claims? What is the separate resource requirement to deal with the suspense file?

Mr. LOCKHART. I don't really know the number, to tell you the truth. The initial piece of it is pretty computerized, and so, the cost is reasonable, but when they start coming in with the information, then it takes up a lot of field office time.

It is an important thing to do because what we are trying to do is correct the record so that when people are disabled, when people are retiring, that we have the right amount of money and we give them the proper benefits. We think it is an important function of the agency.

Mr. BECERRA. My time has expired, so I will close and say that perhaps, Mr. Chairman, we can try to follow up and try to get a sense of what it takes for the Social Security Administration to really do the job of getting through that suspense file, because as Mr. Lockhart just mentioned, that is important work.

Thank you, Mr. Lockhart. Thank you, Mr. Chairman.

Chairman SHAW. Ms. Jackson Lee?

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

Mr. Lockhart, thank you again. Would you restate for me the categories of immigrants that you give a Social Security card to?

Mr. LOCKHART. There are a whole series of different visas that are created by the INS, and I am not an expert on all this, but really, there are two main categories, if you look at it that way. One is that they are permanently authorized to work, and maybe about a half million of the cards we give each year are that group. The other million or so that we give are temporarily authorized to work under a whole series of things. A lot of them are student-related. Then there are the whole series of people coming in for soft-

ware firms. The whole series that are given by the INS, but those are temporary.

Ms. JACKSON LEE. Do you feel comfortable in the procedures at the Administration, that you are accurately providing those who have documentation to work, that you are fairly accurate, or do you need additional resources or additional assistance in making sure you are accurate on the issuance of those types of cards?

Mr. LOCKHART. We feel, with the new procedures, we are doing a lot better job. Now what we are doing is verifying every document with the INS.

Now, new and better systems are needed because it is still a pretty paper-intensive process. The INS is starting to get more and more of the documents quickly into the system called the Systematic Alien Verification for Entitlements (SAVE) program. They have a student system coming up next year, which will help a lot.

We also have some other important procedures that I think will really help this and really put the workload where it should be. One of these that we are looking at is called Enumeration at Entry, which I mentioned, which would be that the State Department and the INS, when they are giving these work-authorizing documents, that they just send us an electronic message that this person is authorized, so we can issue them a Social Security number. Then we don't have to go through this roundabout procedure.

So that is the long-term solution, I think, for a lot of this.

Ms. JACKSON LEE. What kind of efforts are you making to get to that point? Certainly, it makes a lot of sense to me. You are talking about, by technology, send an e-mail, a note, a notice, if you will, to the Social Security Administration. Where are you on that?

Mr. LOCKHART. We have been working on that for several years. Our systems are all ready for it, and it is supposed to start next month, actually, with the State Department. Then, we will roll it out over time throughout the State Department and the INS.

Ms. JACKSON LEE. I think that is an important step to announce or to at least make known that you are moving toward that, because then that helps, if you will, keep the pathway of legality even more on track, because you are getting information as it comes. I think one of the difficulties is trying to go back and restructure documents and to look at what happened as opposed to getting that information as it is happening.

Mr. LOCKHART. That is correct. I think that will be a very important step forward. We are going to put a lot of resources in it. As I said, our systems are already ready to do it, and we hope to have it as a very high priority over the next year or two.

Ms. JACKSON LEE. To capture of the essence of the problem, you said millions of cards are issued for those with documents and allowed to work. Then there are about a million, if I understand, you left of an "S." You said there are about a million that may come in that don't have documentation or don't have authorization to work but ultimately may secure that. What kind of monitoring do you have to know the ones that are securing it and ultimately may need the right kind of Social Security card?

Mr. LOCKHART. Well, what I said, I think, is that there are about a half a million who have permanent authorization to work

and about a million a year that we give cards have some sort of temporary work permit.

Ms. JACKSON LEE. Then there is a group that—

Mr. LOCKHART. Then there is a whole group that is not authorized to work, and we do not give them Social Security cards. We do not give them Social Security numbers, except for a very, very small group, about now 20,000 to 30,000 a year, that get these non-work cards because they are authorized for some benefit program, but generally, they would not be a major threat.

Ms. JACKSON LEE. So you feel fairly confident that you are not giving now Social Security cards to those without the documentation to work? Do you feel fairly confident of that, in terms of immigrants?

Mr. LOCKHART. I visited our field offices in California a couple of weeks ago and watched them work, and it seems to be working, the new procedure. Again, we rolled it out over the last 3 or 4 months. We have 1,300 field offices countrywide. The last one just implemented it September 1.

We are very hopeful that this procedure will work and that people will follow it, and they seem to be following it very well.

Ms. JACKSON LEE. I thank you. My time is out. I will just simply say the suggestion or maybe what we might have read or heard of millions of individuals who may be immigrants who don't have authorization to work, such as that figure you gave, 20,000 to 30,000, is not as accurate as we may have heard. The number of cards that you are dealing with that are unauthorized to work are about 20,000 to 30,000, and not millions.

Mr. LOCKHART. Those that are nonwork cards. Now, there is obviously a whole series of people that are working in this country that do not have legitimate Social Security numbers. As we were talking earlier, some of those are showing up in our suspense file. A lot of our suspense file just may be typos and stuff like that, but there are people that are working, and it is probably in the millions, without proper Social Security cards and numbers in this country.

Ms. JACKSON LEE. We will work through that. Thank you very much.

Mr. JOHNSON. [Presiding.] Thank you, Ms. Jackson Lee. The Chair recognizes Mr. Hayworth.

Mr. HAYWORTH. I thank you, Mr. Chairman.

Mr. Lockhart, thank you for coming to testify today. I want to make sure that I understand exactly the status of foreign students who come to the United States to study at our colleges and universities, vis-à-vis Social Security cards. Now, you mentioned some distinctions here; those who come who are authorized to work, those who are on public assistance.

Help me nail down the student status. Do we classify that as an authorization to work? Authorized to study? What classification are they given?

Mr. LOCKHART. The general student status at, say, a university is, they are authorized to study. Then the INS, as I understand it, has authorized the universities to authorize them to work within the college, not somewhere else, just within the university.

The way the statute works is, if they come in with a letter from an authorized person from that university to say this person is authorized to work at the university and is expected to work at the university, then we will give them a Social Security number.

Now, what has happened, frankly, is some universities, because they may need Social Security numbers for these individuals for their records or something, are not actually putting these people to work, so that they are not actually working. And yet, we are getting a letter that says—

Mr. HAYWORTH. So, what you have are universities engaged in defrauding the Federal Government, saying they have people working who are not working, to get Social Security numbers?

Mr. LOCKHART. We may have some universities sending letters, and they may be interpreting differently than we are.

Mr. HAYWORTH. No, no. Let's get down to brass tacks here. If people are attempting to defraud and deceive the Federal Government in wartime for easy bucks, this is serious.

Mr. LOCKHART. Yes sir, and I know our Inspector General has looked at some cases. I have heard of situations where a university has actually advertised in foreign newspapers that "come to our school and we'll get you a Social Security number." You know, that is not right.

Mr. HAYWORTH. What is the name of the university that has done that?

Mr. LOCKHART. I am not sure. I heard about it in our Oklahoma City office, though.

Mr. HAYWORTH. Let me ask you a further question. This is very disturbing, to say the least. Maybe this is a question better suited for INS, but do we keep track of the nationalities of those who come to study? Do we know, for example, the number of Iraqi students who are in the United States on study programs or work study programs? Do you have any estimate today how many Iraqi students are here in the United States on a work study program?

Mr. LOCKHART. You are right, it is an INS question. We would not have that information in any of our databases.

Mr. HAYWORTH. Is there any particular reason not to keep that information?

Mr. LOCKHART. Again, what we are looking at is to make sure that people are paying their FICA taxes, and that is what the Social Security number has been created for. It is the INS's job to authorize people to work. That is what they are there for. That is their law. It is not our law.

Mr. HAYWORTH. Let me ask you this question. You say things have changed under the new programs, the combination of pre-September 11 reforms and post-September 11 reforms, and we are about 4 months into the situation now. How would you evaluate the level of communication between Immigration and Naturalization Service and the Social Security Administration? Are your computers able to talk to each other?

Mr. LOCKHART. Well, first of all, I think we are doing a lot better with communicating with the INS. In fact, I just talked to the Deputy Commissioner there this morning, and we are trying to work better than we have in the past. So, I think on the human level, it is working better. We are having many more meetings. I

think they understand our issues now a lot better, and we are beginning to understand theirs.

From the computer standpoint, they do have this SAVE program that does tell us when someone is authorized to work. We have access to it in our field office. A person right at the service window who is reviewing a document will have access to the system. I saw them bring one up when I was in California. Momentarily it comes up, and it says whether this person is authorized to work or not.

The problem is not all of the data is in there.

Mr. HAYWORTH. So, we have incomplete data. Again, as we opened this questioning period, I am very concerned about the status of some colleges and universities who seem to be playing fast and loose with work study.

There is perhaps, Mr. Chairman, an appropriate role legislatively to crack down on those who would deceive the government for work study dollars.

I see my time has expired. I thank you, and thank you, Mr. Chairman.

Mr. JOHNSON. The time of the gentleman has expired. The Chair recognizes Mr. Collins.

Mr. COLLINS. Thank you, Chairman Johnson.

Mr. Lockhart, you know, we talk about these Social Security numbers, and it seems as though we kind of hand them out in a manner that has no system to it. Do we do benefits the same way? They get these Social Security numbers and they are here and they work temporarily—

Mr. LOCKHART. First of all, I would say that we do have a system for handing out Social Security numbers. We do handout approximately 18 million a year. A major portion of those are actually replacement cards, but we handout about 5 million new cards a year.

We do have systems in place. We have significantly strengthened those systems, as I have already said, but there were systems in place before September 11 as well. There were procedures in place.

On the benefits side, we have a whole series of systems. I think I can say, having come to Social Security only 7 or 8 months ago, that the systems at Social Security are some of the best in government, and we are always well-rated that way.

For benefits, obviously we have some issues with the suspense file, which we already talked about, but I think we do a reasonable job of keeping track of people's benefits. We have maybe that 3-percent error rate, but we have a 97-percent match every year, which is significant. We are talking about \$4 trillion in wages a year.

So, our systems are doing what I consider a good job. We could do better, and I am not trying to say that we couldn't do better. We could do significantly better, and we are continuing to work on it. Commissioner Barnhart and I have made it very clear since we arrived here that we are not going to accept the status quo. We want to improve this agency dramatically.

Mr. COLLINS. Well, that is encouraging, and truthfully, I think you have. I have talked with the Commissioner on several occasions, and you too, and I think you have made some good strides.

I have a situation that has occurred in my district, which includes Fort Benning, Georgia. We have a local judge there who has

called on a number of occasions, but his first call was in reference to several who had appeared in his court. They were here illegally, didn't have any kind of identification.

This is really an INS problem, too, because when he called INS to report them and ask them to pick them up, and this was after September 11 of last year, they said they didn't have the time, didn't have the money, couldn't do it. It was very frustrating to this particular judge.

He did call 1 day and said that they had incarcerated a person who was working at Fort Benning. He had a work pass, a work permit, and on that work permit was a Social Security number, and this person was here illegally also.

So, he sent a copy of the work permit over the office, and we double-checked it with your office and found that the number had not been issued.

How much of that exists? Do we have any idea? That is what this judge said, how much? Fort Benning, too, says, you know, this is not an isolated incident.

Mr. LOCKHART. It is a big issue. People make up Social Security numbers. As far as we can tell, all 19 terrorists, or however many that did have a Social Security number, they were all made up, and that is a big, big issue. As I said earlier to a question, there are probably millions in this country with made up Social Security numbers.

What we are trying to do is develop—and we do already have in place for employers, for State agencies, the ability to check those numbers with us, either in person or by computers. The idea is that, if they bring in a name, and they bring in a Social Security number, we can tell them if it is real or not. If there is a mismatch, then they should know that there is an issue with the individual.

Mr. COLLINS. I am glad that you are communicating with the people over at INS, because it seemed like there was a lot of slack there. For an INS office to inform a judge we don't have the time to pick up people who are here illegally, already incarcerated, something is wrong with that type of system.

I think it is a real threat and a danger to us to have people with work permits file Social Security numbers here illegally, working on a military installation.

Mr. LOCKHART. Yes. As you may have read in the newspaper, many of the agencies represented on the next panel, including our Inspector General, have been very active at the airports in this area, in verifying Social Security numbers. We are very committed to helping out in those kinds of law enforcement activities because we do believe it is extremely important for this country.

Mr. COLLINS. Well, in closing, the Office of the Inspector General for Social Security has been very helpful in this case, too. They are investigating this and investigating the employer.

Thank you.

Mr. LOCKHART. Thank you.

Mr. JOHNSON. Some of my colleagues and myself would like to clarify the statement you made. Did you indicate that all the terrorists had illegal Social Security numbers?

Mr. LOCKHART. Well, what I said is, I am not sure if all of them had Social Security numbers, but as far as we can tell—and

the Inspector General has talked to the FBI, and the FBI I guess will be up—as far as we know at this time, none of the terrorists received a Social Security number at one of our offices. That is why we need to use the kinds of systems that we are building. We have had in place systems for 20 years for employers and other people to verify Social Security numbers. They just have not been used.

We now have a test, which, again, I mentioned in my testimony, with about eight major employers of an online system. I think over time, if we can do that, it will help protect the Social Security number from people that just make it up.

Ms. JACKSON LEE. Mr. Chairman, if you would just yield for just a brief moment?

Mr. JOHNSON. I yield to the gentlelady.

Ms. JACKSON LEE. There is a question that I left on the table, when you said millions of made-up numbers, you are not saying that there are millions of immigrants with made-up numbers? There are people all over the United States with made-up numbers. Is that what you are saying?

Mr. LOCKHART. You have to go back to that suspense file we were talking about. There are 10 million that we can't match every year. A lot of it is typos, wrong names, but there are certainly people in there that are working, whether they are immigrants, illegal or not, I don't know. There are certainly—I think most people would say many millions that are working without a proper Social Security number.

Ms. JACKSON LEE. Not all of one label?

Mr. LOCKHART. What?

Ms. JACKSON LEE. Not all of one label, one type of people, there are many—

Mr. LOCKHART. We just don't have the data. I mean, if we could find them, we could match them.

Ms. JACKSON LEE. We would find out.

Mr. Chairman, thank you. I do want to say that the INS is really trying to work on this issue, to the extent that I have visited sites, airports around the country I spent my time visiting. I will tell the Committee, if they have interest, that I literally saw the INS recognize undocumented individuals coming in from a country overseas, and was able to match the fact that their documents were fraudulent and was there to greet them. I saw the action when I was there. They were able to greet them immediately as they deplaned.

This is happening across the Nation. I think that we can be assured that they listen to Congress on the responsibilities that they have.

I thank the Chairman for yielding.

Mr. JOHNSON. I thank the lady for her comments. The Chair recognizes Mr. Hulshof.

Mr. HULSHOF. Thank you, Mr. Chairman. Welcome, Mr. Lockhart. We certainly welcome our colleagues from the Subcommittee on Immigration, Border Security, and Claims.

A lot of the questions to you, Mr. Lockhart, have been referenced around the issue of illegal immigrants that are here. What I would like to do is focus, as is also the subject of our hearing, on identity theft. Our Subcommittee, the Social Security Subcommittee, has heard some heart-wrenching stories from citizens, sometimes elder-

ly citizens, who have been bilked of thousands of dollars in personal savings, with credit histories being just turned upside down because of identity theft. So, I would like to ask a couple of questions along that line.

You mentioned about 18 million cards a year, some of those are replacement cards. What percentage per year are replacement cards?

Mr. LOCKHART. About 12.5 million of those, so two-thirds.

Mr. HULSHOF. A couple of hypotheticals. If I come in to get a replacement card, I presume I could get one. What if I had just been given a replacement card the week before?

Mr. LOCKHART. You can get one with the proper documentation. You just can't ask for it. Yes, assuming you had the proper documentation, you can come in.

At the moment, we don't have a limit. It is one of the areas we are really looking at, because not only is there an integrity issue here, there is also a tremendous workload issue. Some of our offices are spending a third of their time issuing replacement cards. So, we are looking at it to see if we should limit the number, to see if we should charge, to see if they even need a replacement card.

I mean, what is happening in many of these offices is we have the Supplemental Security Income, SSI, population that we serve, and many of them have mental impairments, are homeless, and they are always losing the cards. We have people that have had 30 or 40 cards, and they are being required by some State agency to produce it. Now, if we can go to more of a verification electronically, that might relieve some of that workload as well.

Mr. HULSHOF. So, the Inspector General's recommendation to put perhaps some limit on the number of replacement cards, with some exception for extraordinary circumstances, that would be something that you would support?

Mr. LOCKHART. I am about ready to get a white paper on the topic. There is a series of issues. Some of the people I have talked to in the field office say why not charge them something for it. Maybe that will discourage them. A limit would be another way. There is a whole series of ways.

I mean, what is important is actually the number, not the card, when you really think about it.

Mr. HULSHOF. A couple of other quick areas, as my time is dwindling. If the Social Security Administration receives a report from an employer that indicates that somebody is working in America, say in Phoenix, Arizona, using my Social Security number, do you let me know that?

Mr. LOCKHART. What we do, if there is more than one wage report on a Social Security number, we try to unscramble it, and that unscrambling may mean that we call someone. By the time we receive the information, we are receiving information well over a year old on wage reports by the time it is entered in the system. It is probably not very helpful, if your identity has been stolen. You would probably know by then anyway.

The other thing we do, though, is we also put out annually the Social Security statement, as you know. In that, when you see it, if there is an incorrect wage, you could call us, and we would unscramble it that way.

Mr. HULSHOF. Okay, the final area of questioning regards data sharing with law enforcement agencies. Of course, the Privacy Act does say that agencies can share information with another information for the purpose of civil or criminal law enforcement purposes, if the head of that agency makes a written request.

Yet, it is my understanding that regulations within your agency limit disclosure to law enforcement activities relating to serious crimes like murder and crimes of violence. What about identity theft itself? I mean, for instance, if law enforcement were to contact the Social Security Administration and say, "We are working on an identity theft case. We need some data from your agency to be shared with us," would you provide it to them?

Mr. LOCKHART. It is not only serious crimes but it also is fraud against a Social Security number, and it is also if our IG opens a case. So, if the law enforcement person comes to the IG, which is where they would come, and the IG opens a case, we would certainly provide the information. We are not protecting identity thieves, in any sense of the word.

Mr. HULSHOF. Local law enforcement would then have to go the Inspector General.

Mr. LOCKHART. Which is part of Social Security, yes.

Mr. HULSHOF. Okay. Thank you, Mr. Chairman. I yield back.

Mr. JOHNSON. Thank you. Mr. Brady, do you care to question? The gentleman is recognized for 5 minutes.

Mr. BRADY. Thank you, Mr. Chairman.

I want to follow up on Congressman Hulshof's questions on collaboration. First, I want to thank the Social Security Administration for your collaboration with law enforcement on Operation Tarmac, which was launched after September 11. It has uncovered a large number of individuals with security clearances working at our Nation's airports under false pretenses, obviously a practice that cannot be allowed to continue.

On the 9th of this month, in my community, just 2 days before September 11's anniversary, Operation Tarmac indicted 143 individuals working at Houston's Bush International Airport, the airport that I and many of my neighbors fly in and out of on a weekly basis.

These people acquired airport security badges by using a non-existent Social Security number of someone else's Social Security number.

From my viewpoint, the operation was a very solid preventative measure because these individuals each had access to airplanes, ramps, and tarmacs, regardless of their security clearance.

You have really addressed the question of what we can do to prevent this type of fraud in the future, but following on to Congressman Hulshof's question, is there not a way to increase cooperation with law enforcement, short of the IG opening up a case? Obviously, what we are trying to do here, the 143 who were indicted, perhaps and most likely there isn't a terrorist among them. Just as you arrest speeders before they cause an accident, someone who tries to buy a gun illegally, in hopes to prevent harm from happening later, it is important that we have these measures in place, even though they may seem to be small, preventative measures.

What can we do to increase, short of having to open up a case, to increase this type of cooperation with law enforcement?

Mr. LOCKHART. Really, the best way is for the security companies, everybody that is hiring at the airports or anywhere else, to use our systems. We have the systems, and any employer can come in and verify Social Security numbers when a hiring decision is made. That is the best prevention by far, just not to employ them to start with.

It is not being used as well as it should, and we are trying to get the word out that we have those systems in place, and they should be using them. So, that is the first thing that should be done.

The second thing is, we are continuing to work with our IG and our IG is continuing to work with all law enforcement to see how we can better fit our constraints.

Our constraint really is that this is taxpayer information. It is protected by the Internal Revenue Code, and it is a very important issue with them, that taxpayer information is secure.

So, we are working with the IRS, and we are working through our IG with the various law enforcement officials.

Mr. BRADY. That is a very good answer. My thought was, in the case with Houston's airport, Federal agents went through, under the leadership of our U.S. attorney, Mike Shelby, went through some more than 21,000 individual files to make those match. The good news is, there are only 143 who didn't, which tells you there is a level of security there.

My thought was, can we not make it, with certain restrictions, as easy for law enforcement, again, under certain restrictions, to match those numbers as it would be for employers to go online to do it?

Mr. LOCKHART. It is an issue we talked about in the agency, and certainly we talked it over with the Inspector General, and he is certainly recommending it. Again, it is an issue that is partially out of our hands, from the standpoint that the taxpayer information belongs to the IRS. So, it is one of the issues that we have to continue to work with them on, as to what are the procedures.

We have certainly, as you said, been able to do it for Operation Tarmac, and we hope that we can do it whenever necessary.

Mr. BRADY. I was just thinking, if there was some law enforcement clearinghouse at some level that works directly with the Social Security Administration and the appropriate authorities to be able to access, so that you don't have 10,000 going on from different jurisdictions, but actually a good, cooperative, laid-out, disciplined process that speeds up having to run through 21,000 files, where we can do more security because we save time.

Mr. LOCKHART. It is certainly something we should consider, yes.

Mr. BRADY. Thank you, sir. Thank you, Mr. Chairman.

Mr. JOHNSON. Thank you. Let me follow up on that for just a second. I am told, and I would like for you to verify it, that if an employer called you with a number for you to check, you say it is okay or not, but you don't tell them whether the guy is dead or if he is on a nonwork Social Security number. Is that true?

Mr. LOCKHART. Yes, sir. That is true. That is a flaw in our system that we are in the process of correcting. I was not aware of that until very recently myself, and I had the same concern that you do, that it doesn't make any sense to verify in that circumstance, if someone is dead or they have a nonwork number. We are making the system changes so that our verification systems will tell that.

Mr. JOHNSON. You will be in the near future, then?

Mr. LOCKHART. We are implementing those changes. Yes, sir.

Mr. JOHNSON. Okay. Let me ask you one other thing. I believe the Social Security Administration Inspector General is on record as supporting Social Security privacy legislation. This bill would prevent numbers from being used as ID numbers for many purposes, including military ID. At a time when military personnel are deployed worldwide, and terrorists are trying to exploit our weaknesses in everything from the Internet to our own financial systems, I don't know if it is wise for the military to be using their Social Security number for everything from checking out equipment to cashing a check. I would like to hear your comments on that.

Mr. LOCKHART. There is certainly an overuse of the Social Security number in our society. It has become a de facto identifier one way or another. The problem is that, in many ways, something else will have to be substituted for it. In some cases, it is useful for prevention of fraud and prevention of terrorists. So, there are pluses and minuses to all this.

Certainly, in your legislation, there are a lot of reasonable things that we can think about on how to limit the use of the Social Security number, because it has really grown dramatically more than it was ever supposed to do in this country.

Mr. JOHNSON. You agree with the original concept, as far as Social Security and tax purposes, period?

Mr. LOCKHART. That is the original concept. Unfortunately, I think the cat's out of the bag.

[Laughter.]

Mr. JOHNSON. Okay. Let me ask you one other quick question. In reference to the illegals that I spoke of earlier, I recognize it is mostly an Immigration and Naturalization Service problem, but if you issue a temporary work permit and the Immigration and Naturalization Service then follows up 2 months later with a letter to these guys, saying, "You are going to be deported. Come on back home," maybe some of them will, how do you get termination on that Social Security number?

Mr. LOCKHART. The procedures of the agency have been that, once a Social Security number is issued, it is issued. If we think there has been some fraud, we do put in the record that there has been some fraud, and we won't issue a replacement card, but the numbers are not canceled.

Mr. JOHNSON. So, they are out there indefinitely? So, if the guy is deported back to Mexico, let's say, and then comes back across the border, he still has a good Social Security number?

Mr. LOCKHART. He still has a Social Security number. If we have entered into our records that we think fraud has been involved, if they came into our office, we could find that out, but it is something that we need to look at. It is an issue that I think

we need to look at, as to whether we should do anything to cancel a number. Historically, we never have. We have issued 415 million numbers.

Mr. JOHNSON. Thank you. I appreciate your honest testimony and openness with us. We thank you for the job you all are doing over there. Keep up the good work.

With that, we will close your testimony and ask the second panel to step up. I am going to turn the meeting over the Chairman Gekas.

Mr. LOCKHART. Thank you, Mr. Chairman.

[Questions submitted by Chairman Shaw to Mr. Lockhart, and his responses follow:]

Social Security Administration
Baltimore, Maryland 21235

1. During the hearing, Mr. Lockhart stated that SSA has a scorecard on the recommendations the Inspector General had made to tighten controls related to issuing Social Security numbers (SSNs). As requested by Chairman Gekas, we would appreciate your providing a copy of that scorecard to both of our Subcommittees.

Scorecard on Inspector General Recommendations to Tighten Controls on Issuing Social Security Numbers	
RECOMMENDATION	STATUS
Congressional Response Report—Terrorist Misuse of Social Security Numbers A-08-02-32041 October 3, 2001	
Expand the Agency's data matching activities with other Federal, State and local Government entities.	Ongoing. The Enumeration Response Team (ERT) is considering this as part of its long-term efforts.
Explore the use of other innovative technologies, such as Biometrics, in the enumeration process.	Ongoing. The ERT is exploring the use of biometrics in the enumeration process.
Increase the number of investigative and enforcement resources provided for SSN misuse cases	Ongoing. The FY 2003 IG budget request includes an additional 29 FTEs, which will be used for investigative and audit and the OIG technology plan.
Authorize SSA and SSA's OIG to disclose information from SSA files as requested by the DoJ and FBI in times of national emergency and in connection with terrorist investigations.	Partially Completed. OIG will take the lead for completing this initiative.
Audit of enumeration at Birth Program A-08-00-10047 September 27, 2001	
Reinvest some of the savings realized by the Enumeration at Birth (EAB) program and provide necessary funding, during future contract modifications, for the Bureaus of Vital Statistics (BVS) to perform periodic independent reconciliations of registered births with statistics obtained from hospital's labor and delivery units and to periodically verify the legitimacy of sample birth records obtained from the hospitals.	Ongoing. The current EAB contracts expire on December 31, 2002. Negotiations for the new contracts with the States began in March 2002. We have proposed the recommended review to the states in negotiations for the new contracts. We expect the negotiations to be completed by December 2002, with the new contracts effective from January 1, 2003 through December 31, 2007.

Scorecard on Inspector General Recommendations to Tighten Controls on Issuing Social Security Numbers	
RECOMMENDATION	STATUS
Enhance its duplicate record detection and prior Social Security number (SSN) detection routines to provide greater protection against the assignment of multiple SSNs.	Ongoing. SSA plans to enhance its system to prevent the assignment of multiple SSNs for identical cases with different birth certificate numbers, but an implementation date for this enhancement has not been determined.
Instruct FO personnel to exercise greater care when resolving enumeration feedback messages generated by the system.	Completed. Instruction issued via Emergency Message on December 27, 2001.
Cross-reference multiple SSNs assigned to the 178 children within the sample.	Completed. SSA has completed the cross-referencing of these SSNs.
Continue to monitor the timeliness of BVS submissions and work with those BVSs that are having difficulty complying with the timeframes specified in the contracts.	Completed. SSA has taken a number of actions with the States to assist them in complying with current contract timeframes. These include attending a yearly conference of all State registrars, presenting EAB findings to the participants, and establishing a "Frequently Asked Question" or FAQ, on SSA's Internet site.
Obstacles to Reducing Social Security Number Misuse in the Agriculture Industry. A-08-09-41004 January 22, 2001	
Expedite implementation of the initiative to improve communication of name/SSN errors to employers and employees.	Partially Completed. SSA began a pilot of its online Social Security Number Verification System (SSNVS) in April 2002, and expects to expand the pilot in early 2003.
Introduce legislation that would provide SSA the authority to require chronic problem employers to use Enumeration Verification System (EVS).	Ongoing. Currently IRS has the authority to penalize employers who do not comply with wage reporting requirements. IRS has recently announced that they will impose penalties. SSA is working with IRS to support them in this effort.
Collaborate with the INS to develop a better understanding of the extent that immigration issues contribute to SSN misuse and growth of the Earnings Suspense File (ESF). Additionally, reevaluate its application to existing disclosure laws or seek legislative authority to remove barriers that would allow the Agency to share information regarding chronic problem employers with the INS.	Ongoing. IRS has implemented a task force to review their policies and procedures regarding penalizing employers who send SSA bad names and SSNs. We are reviewing our regulations to determine if current SSA regulations provide sufficient authority to share information with other agencies, including INS, in situations that are consistent with the purpose of Social Security programs and SSA's disclosure policy.
Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications A-08-98-41009 September 19, 2000	
Accelerate negotiations with United States Immigration and Naturalization Service (INS) and Department of State (DOS) to implement the Enumeration at Entry (EaE) program. Once implemented, all non-citizens should be required to obtain their SSNs applying at one of these Agencies.	Partially Completed. SSA implemented the first phase of EaE in October 2002, and is working with INS on identification of the next phases.

Scorecard on Inspector General Recommendations to Tighten Controls on Issuing Social Security Numbers	
RECOMMENDATION	STATUS
Continue efforts and establish an implementation date for planned systems controls that will interrupt SSN assignment when multiple cards are mailed to common addresses not previously determined to be legitimate recipients (for example, charitable organizations) and/or when parents claim to have had an improbably large number of children.	Partially Completed. The Comprehensive Integrity Review Process (CIRP) was implemented in 1999. Based on certain characteristics of the information input into Modernized Enumeration System (MES), CIRP identifies high-risk transactions that are subject to a monthly management review (such as too many cards being sent to one address). SSA continues its efforts to implement enhancements to the MES, however, the timeline for these enhancements has been impacted by the implementation of the near-term changes recommended by the Enumeration Response Team.
Obtain independent verification from the issuing agency for all alien evidentiary documents before approving the respective Social Security number applications until the Enumeration at Entry program is implemented.	Completed. SSA now obtains independent verification for all alien evidentiary documents.
Propose legislation that disqualifies individuals who improperly obtain SSNs from receiving work credits for periods that they were not authorized to work or reside in the U.S.	Unable to implement. We are unable to implement this recommendation because INS does not have historical information on when an individual was or was not authorized to work.
Effectiveness of Internal Controls in the Modernized Enumeration System. A-08-97-41003 September 14, 2000	
Require field office (FO) management to perform periodic quality reviews of processed exception messages (EMs) and provide appropriate feedback and related training to FO personnel.	Ongoing. Management is required to perform quality reviews and as additional enumeration training needs are identified refresher training is provided to FO personnel.
Require FO personnel to document the basis of all resolution actions taken on EMs for an appropriate period of time to facilitate management review.	Ongoing. Most EMs require only routine review and decision; FO managers receive and review listing of pending EMs that are coded as suspect or fraudulent.
The Social Security Administration is Pursuing Matching Agreements with New York and other States using Biometric Technologies A-08-98-41007 January 19, 2000	
Pursue a matching agreement with New York so that the Agency can use the results of the State's biometric technologies to reduce and/or recover any improper benefit payments.	Ongoing. SSA will begin a pilot for verifying claimant identity by picture ID in early 2003, and is exploring the possibility of using matching agreements.
Initiate pilot reviews to assess the cost-efficiency of matching data with other States that have employed biometrics in their social service programs.	Ongoing. SSA continues to discuss its privacy concerns with such matches with the OIG.

Scorecard on Inspector General Recommendations to Tighten Controls on Issuing Social Security Numbers	
RECOMMENDATION	STATUS
Review of Controls over Nonwork SSNs A-08-97-41003 September, 1999	
Conduct periodic quality reviews of processed SSN applications and provide timely feedback to field office (FO) personnel.	Completed. SSA's Office of Quality Assurance (OQA) conducts periodic reviews of processed SSN applications and timely feedback is provided based on their findings. SSA has expanded our performance indicators for enumeration for Fiscal Year (FY) 2003 and beyond.
Propose legislation to prohibit the crediting of nonwork earnings and related quarters of coverage for purposes of benefit entitlement.	Unable to implement. We are unable to implement this recommendation because INS does not have historical information on when an individual was or was not authorized to work.
SSA should perform its own actuarial calculations of the effects of nonwork quarters of coverage on benefit payments, if deemed necessary to support changes in legislation.	Unable to implement. Because it is not feasible to accomplish this recommendation, SSA has not pursued this analysis.
Review the 452 unrestricted SSNs processed by the California FO's temporary SR to identify other coding errors that resulted in the incorrect issuance of SSN cards containing work authorization.	Completed. It was established that the employee misunderstood operating instructions, resulting in the employee making the same error on all of the incorrectly processed applications. The situation has been corrected.
Using Social Security Numbers to Commit Fraud A-08-99-42002 May 28, 1999	
Incorporate preventive controls in Modernized Enumeration System (MES) that address 1) multiple SSNs to a common address, 2) parents claiming an improbably large number of children, 3) known fraudulent documentation used as evidence in support of SSN applications.	Ongoing. SSA continues its efforts to implement enhancements to the Modernized Enumeration System (MES). 1) There is an end-of-line integrity review for too many cards to the same address, 2) software changes in 2003 will interrupt the assignment of the SSN to parents claiming an improbably large numbers of children, and 3) currently in place is software which interrupts the issuance of a card where there is a fraud indicator on a prior application.
Continue efforts to have INS and the State Department collect and certify enumeration information for aliens.	Partially Completed. SSA implemented the first phase of its Enumeration at Entry (EaE) program with the State Department in October 2002, and is working with INS on identification of the next phases.
SSA should require verification from the issuing state when an out-of-state birth certificate is presented as evidence for an SSN application.	Completed. Effective June 2002, we started collateral verification of birth records for all U.S. born SSN applicants age one and older.
SSA should require that the field offices obtain independent verification of the alien's evidentiary documentation from the issuing agency (e.g., State Department, INS) before approving the SSN application, if an alien chooses to visit a SSA office to apply for his or her SSN.	Completed. SSA now obtains independent verification for all alien evidentiary documents.

2. During the hearing, Mr. Johnson, who represents the Dallas area in Texas, mentioned that illegal aliens in an 18-wheeler had been appre-

hended. Approximately 26 of the individuals were released and told by the local Immigration and Naturalization Service (INS) office that they could get a Social Security number from SSA and go to work. Can you provide more details on this situation?

Our understanding is that approximately two dozen Mexican immigrants survived a harrowing journey that began in El Paso and ended in North Texas aboard an unventilated tractor trailer rig. Two men died of heat exhaustion and nearly a dozen others were hospitalized briefly for heat stress. Because of the need for witnesses against the smugglers when the cases come to trial, the INS granted the immigrants permission to work.

The Attorney General pursuant to § 212(d) [8 U.S.C. § 1182(d)] of the Immigration and Nationality Act has the authority to parole individuals into the United States for reasons specified in the Act and provide them with work authorization. Inquiries should be directed to the Department of Justice because once the Attorney General exercises his discretion and issues work authorization, SSA has no discretion. Section 205 (c)(2)(B)(i) of the Social Security Act requires that the Commissioner of Social Security issue a work Social Security Number if an individual has a valid INS work authorization.

3. The Earnings Suspense File (ESF) has increased more than fourfold in the last 10 years. The SSA's Office of Inspector General (OIG) found there are patterns of reporting errors among certain employers, including identical Social Security numbers (SSNs) used for more than one employee, non-issued SSNs, and consecutively numbered SSNs—all of which end up in the Earnings Suspense File. There are also many instances of employers and industries that continually submit erroneous wage reports—one study of 20 agriculture employers in which 60% of their wage reports had inaccurate names or SSNs and who submitted almost \$250 million in mismatched wages between 1996 and 1998—and that three industries (agriculture, food and beverage and services) account for almost half of wage items in the suspense file. What is the agency doing to address this growing file? Is SSA making any special endeavor to refer these employers to the Immigration and Naturalization Service (INS) or the Internal Revenue Service (IRS) or to otherwise target them for corrective action in submitting erroneous wage reports? What else can be done? Please also provide information requested by Mr. Becerra regarding the administrative costs associated with the ESF (sending out letters responding to workers/employers' questions, and so forth).

The ESF contains approximately 238.2 million items (name/SSN mismatches). This covers items submitted for tax years (TY) 1937 through 2000. Approximately 25 percent or 61.6 million items were added to the ESF for TYs 1991–2000, which is an increase of about one-third.

SSA developed a tactical plan to address the growth and management of the ESF. As a result SSA:

- Has instituted multiple computer-matching routines to increase SSA's ability to match a reported name/SSN that does not match SSA's record with the correct record.
- Is building a new process that would electronically find millions of additional matches and post them to the correct earnings record. The new process would compare earnings items to the Master Earnings File (which includes the Employer Identification Number), the benefit record, and the Numident (the record of SSNs assigned to individual names). (The current matching process compares earnings items only to the Numident.) The new process would also employ new techniques with earnings record patterns to match the earnings to the correct individual. It is estimated that at least 30 million items would be removed from the suspense file and credited to the records of individual workers. If so, benefits for several hundred thousand beneficiaries would be increased.
- Provides regional office assistance to employers with a high volume of mismatches to assist them in improving the accuracy of their records.
- Is discussing with IRS its existing authorities to penalize employers who contribute a large number of or a high percentage of name/SSN mismatches to the ESF. (The penalties for submitting erroneous records are in the Internal Revenue Code.) We understand that the IRS has begun to pilot a process to penalize these employers.
- Currently piloting with a small group of employers the Social Security Number Verification Service (SSNVS), an Internet option to verify the accuracy of

employees' names and Social Security Numbers (SSN) by matching the employee-provided information to SSA's records. SSA's current system provided to the employer community through SSA's 800 number and through electronic (magnetic tape, diskettes) and paper processing is time consuming for employers. An Internet option will be more efficient and encourage more employers to use SSA's name/SSN verification program for new employees, thereby reducing items posted to the suspense file.

- Developed and conducted outreach programs to the employer and payroll communities to address the issue of correctly matching names and SSNs. SSA staff have spoken to numerous employers and payroll groups on this and related issues. SSA has made changes to our publications to help employers better understand the issues. In our quarterly publication, the "SSA/IRS Reporter," which is sent to over 6.5 million businesses, we have had numerous articles on the importance of providing correct name/SSN information on the Form W-2. SSA has built a website that is designed specifically for employers to address their payroll reporting issues and provide guidance.
- Has worked with both the INS and IRS on the mismatch issue. Both agencies have incorporated training on the importance of name/SSN information into their training programs for businesses.
- Has revised the letters sent to the employer to provide more detailed information about name/SSN mismatches. SSA also provides detailed step-by-step instructions of what the employer should do to resolve the discrepancy. The letters highlight the responsibilities of employers and the rights of employees when there are name/SSN mismatches.
- Worked with the IRS to revise the Form W-2 and its magnetic and electronic formats to provide separate first and last name fields to facilitate capturing the proper last name. This separation of the last name better assures that the information reported can be properly matched to SSA's records, especially in cases where a person has a multiple or hyphenated last name. Similar name presentation changes have also been made to the Form W-4.
- Modified the Spanish version of the Form SS-5 (Application for a Social Security Card) to separate the first name from the last name. There are plans to make similar changes to the English version of the Form SS-5.
- Improved the timeliness of the notices sent to every employee whose name and SSN do not match requesting correction information.
- Has engaged Price Waterhouse Coopers to review the Agency's management practices of the ESF and make recommendations as appropriate for improvement.

You asked if SSA is making any special endeavor to refer these employers to the INS or the IRS or to otherwise target them for corrective action in submitting erroneous wage reports. SSA shares name and SSN mismatch data reported on the Form W-2 with the IRS since SSA processes these forms on behalf of the IRS. SSA is working with IRS cooperatively in the development of its penalty program.

SSA is precluded from making referrals of name/SSN mismatch information to the INS due to section 6103 of the Internal Revenue Code, which prevents SSA from sharing tax information with other agencies.

In response to your question concerning what else can be done, SSA is now piloting an Internet based SSNVS. This is a free service where employers can verify that the name and SSN on their payroll records matches SSA's records. Expanding this limited pilot to the entire employer community will offer an inexpensive and easy way for all employers to verify their employee's names and SSNs.

As far as the administrative costs associated with the earnings suspense file, SSA sends a notice to every individual whose name and SSN does not match SSA's records. For TY 2001 (calendar year 2002), it costs SSA approximately \$5.4 million to send these notices.

SSA also sends notices to employers. For TY 2001, SSA sent notices to all employers that had an item go into the ESF at a cost of \$600,000 for the 944,000 notices sent.

There are additional costs associated with both types of notices:

- Over \$200,000 for system maintenance and cyclical changes; and
- An average of \$9.00 for each call to our National 800 number generated by the notices. We estimate that we received about 100,000 inquiries about the TY 2001 letters.

4. SSA shares information on work credited to non-work SSNs with INS annually (worker name, address, employer, wages). What does INS tell you they do with the information? In 2000, about 9.6 million wage items rep-

resenting \$49 billion in wages did not match SSA's records. The SSA IG recommended that SSA share information on wage records that do not match SSA files. The IG also recommended that SSA match Office of Child Support Enforcement files with non-work SSNs and share that data with INS. What are your views and do you plan to take action on these recommendations?

With regard to the INS' use of information on work credited to non-work SSNs, we defer to the INS for an explanation of what they do with the information and its usefulness.

Concerning IG's recommendation that SSA share information with INS on wage records that do not match SSA files, SSA does not have the legal authority to share such records with INS. Whether or not the wage records submitted to SSA match SSA records, they constitute tax return information subject to the disclosure restrictions in the Internal Revenue Code (IRC) (26 U.S.C. 6103). section 6103 of the IRC prohibits sharing of wage records when SSNs on those records do not match information in SSA records.

With respect to the IG recommendation that SSA match Office of Child Support Enforcement files with non-work SSNs and share that data with INS, SSA cannot act on this recommendation for reasons similar to those cited above regarding sharing wage data with INS. SSA's access to and use of OCSE data is subject to limitations specified in section 453 of the Social Security Act (the Act) (42 U.S.C. 653). Section 453(l)(1) of the Act prohibits SSA from sharing this information with INS.

5. Do you believe it would make it easier for employers to identify illegal workers if the SSN number itself was changed to indicate whether the person is not authorized to work? If so, are you planning to implement this change and if yes, when?

It is not clear if the SSN itself were changed to indicate whether the person is not authorized to work whether it would significantly help employers identify "illegal" workers. Most illegal workers use made up numbers. The best way for employers to identify them is to use one of SSA's matching systems.

6. An article published by The Deseret News, of Phoenix, Arizona, on Tuesday, October 01, 2002 entitled "Thefts of Social Security ID rising fast," by Pat Reavy, Deseret News staff writer, described the substantial problems of a retired woman named Frances Stone, aged 70. According to the article:

"... in 1992, Stone noticed her Social Security checks were getting smaller. After some investigating, Stone discovered that the woman who allegedly took her wallet, an illegal immigrant, had gotten a job and was earning wages using her Social Security number. The government thought Stone was earning more money than she really was. Now, 10 years later, the problem still hasn't been settled. Each year Stone's Social Security checks are cut, and each year she has to go through a lot of red tape to prove somebody else is using her Social Security number. And each year it takes three to four months' worth of phone calls and letter writing to get the matter cleared up."

The SSA sent some eight million letters to people identified with "mismatched SSNs." How many of these were to people who are using someone else's SSN? Has the SSA compiled any reports as to how many people receiving SSA benefits are experiencing the same kind of fraud experienced by Frances Stone? How many citizens and lawful residents are now subject to erroneous records of SSA benefits and don't recognize the problem? If SSA receives a report from an employer that indicates someone else is working using another's SSN, would SSA contact the true owner to let him or her know? Doesn't the SSA have a responsibility to the person to whom the SSN was lawfully issued? Why not?

SSA is committed to achieving the results our citizens expect. We regret the difficulties that Frances Stone experienced resulting from the theft of her wallet. Her earnings record is now correct.

SSA/OIG does not have enough information to determine how many no-match letters went to people who are using someone else's SSN. For Tax Year 1999, SSA has over 8.3 million wage items in suspense because the name/SSN on the employer wage reports failed to match SSA's records. SSA produced no-match letters in an attempt to resolve these suspended items. About 2.6 million wage reports could not be matched due to zero SSNs, invalid SSNs, no names, and so forth. About 5.7 million wage reports contained SSNs that matched SSA's records; however, the names did not match. SSA/OIG does not know how many of the 5.7 million letters were

mailed to individuals who used someone else's valid SSN. Without a valid name/SSN match, these earnings could not be posted to an individual's master earnings record.

Although 5.7 million of the wage items could have led to letters going to people who are using someone else's SSN, they could have also gone to the owner of the SSN who used an incorrect name (i.e. married name, improperly hyphenated name, and so forth.) Since these items are still in need of resolution, SSA/OIG cannot determine the actual number of people who are using someone else's SSN.

You asked, if SSA receives a report from an employer that indicates someone is working using another's SSN, would SSA contact the true owner to let him or her know? SSA does not notify the actual SSN holder if someone is using his or her SSN. SSA has a number of ongoing processes to obtain the correct name and SSN associated with the wages, including manual and automated edits. Due to these internal efforts, notifying the actual number holder of this situation may be premature and create unnecessary alarm. In addition, the earnings history of the SSN owner, as well as their status with SSA's programs, has not been impacted since the wages earned by the other user (who may or may not have fraudulently used the number) remain in suspense.

SSA does not have reports as to how many people receiving SS benefits are experiencing the same kind of fraud experienced by Frances Stone. SSA's IG is currently completing an audit of Internal Revenue Service referrals to SSA where a taxpayer has claimed that someone else is working under their name and SSN. IRS refers such cases to SSA so that their earnings history within SSA's records can also be corrected. SSA/OIG's audit work has found numerous instances of potential and actual identity theft. While SSA/OIG does not know how many other citizens and lawful residents do not recognize this problem, SSA does send annual Social Security statements to the public which allow the individuals to identify anomalies in their earnings records.

SSA has a responsibility to ensure that the earnings recorded on all wage reports with names/SSNs that match SSA's records are properly posted to employees' earnings records. In addition, should the SSN owner request a correction to their earnings history, SSA has the ability to do so.

SSA also has the ability to assign a new SSN if this is the only means of resolving an identity theft situation. SSA allows a second SSN to be issued when: (1) attempts to locate the individual using the number holder's SSN have been unsuccessful; (2) the number holder has earnings posted to his/her account in the last 2 years which belong to someone else; (3) the number holder requests or agrees to accept a new SSN; and (4) the number holder has cooperated with SSA.

7. What is the timeframe for merging your data systems so that employers who verify SSNs will be notified that an SSN is a non-work SSN or that the individual assigned the SSN is deceased?

Modifications to include additional verification information are planned for the Internet based SSNVS (Social Security Number Verification Service) now in an initial pilot phase. The next step in that process is to expand the pilot to include additional employers.

8. The Privacy Act says an agency can share information with another agency for purposes of civil or criminal law enforcement activity if the head of that agency makes a written request. However, your regulations limit disclosure to law enforcement activities related to serious crimes (e.g., murder, kidnapping) where the person has been indicted or convicted and to criminal activity involving the Social Security program or similar programs, correct? Does this mean that employers can request verification of basic information, but law enforcement agencies cannot?

SSA's authority for verifying SSNs for employers and law enforcement entities is separate and distinct. SSA verifies SSNs for employers under the Privacy Act's routine use provision (5 U.S.C. 552a(b)(3)). For law enforcement, the disclosure authority is 5 U.S.C. 552a(b)(7).

SSA's verification of SSNs for employers is for a compatible purpose, i.e., routine use, because employers' submittal of wage reports to SSA is a part of SSA's business process. It is in SSA's interest that employers submit wage reports with correct SSNs so that the Agency can post wages to the correct individual's record. These verifications enable the Agency to maintain correct wage records on which to base individuals' future retirement, survivors or disability benefits.

Unlike verifying SSNs for employers, the disclosures SSA makes for law enforcement purposes generally are for non-program related purposes; thus are more limited. These disclosures are based on a balanced policy that provides service to the

law enforcement community while maintaining the confidentiality and integrity of personal information in SSA's records. We provide information to law enforcement organizations in connection with an individual who has been indicted or convicted of a violent crime. We also provide information if an individual is suspected of committing fraud against the Social Security program or any other government health or income program.

SSA has ad hoc authority (under the ad hoc provision in Regulation 20 CFR 401.195) allowing the Commissioner to make one-time disclosures to law enforcement authorities upon written requests from law enforcement agencies in special situations of national emergency or security.

On September 13, 2001 the Commissioner exercised this ad hoc authority to law enforcement requests concerning the events of September 11. SSA's Inspector General and our then Office of Disclosure Policy established a streamlined process to handle law enforcement requests pertaining to these tragic events.

9. The SSA Inspector General mentioned in his testimony that a person is able to receive credit toward Social Security benefits based on illegal work. Does current statute explicitly say SSA may credit work toward Social Security eligibility and benefits, regardless of whether the person is a citizen or authorized to work in the U.S.? Would you describe how SSA would process this application for benefits? What proof would SSA request, and would SSA use the illegal work to determine his eligibility and benefit amount? Would SSA refer him INS for the illegal work?

Section 210 of the Social Security Act states that all work performed in the United States is considered employment under the Social Security program with specific, but limited, exceptions. The Act does not specifically address "employment" of persons who lack INS authorization to work and, therefore, these aliens working without authorization are not specifically "excepted" from engaging in covered employment. The Act concerns itself with the kind of work done, rather than who is performing the work.

As long as the individual has worked in employment covered by the Act, and once they meet all the other factors of entitlement including lawful presence in this country, and submit the required proofs, they can receive benefits. If the individual had worked under an assumed or invalid SSN, we would request evidence of this and develop to determine which earnings belong to him/her.

Thus, the receipt of benefits hinges on work in covered employment rather than immigration status at the point of employment. However, lawful presence in this country at the point of entitlement is required.

10. Under current law, a non-citizen applying for benefits today cannot collect Social Security benefits if he is not legally residing in the United States, but he can get credit toward Social Security for illegal work. Also, a person can earn credit toward Social Security while breaking immigration law. Should these inconsistencies be rectified in your view?

Under present law, a non-citizen living in the United States will only receive benefits if he is legally residing in this country. If Congress wished to reconsider the issue, a key concern would be whether a change would drive more employees into the non-tax-paying underground.

11. The Inspector General has recommended that legislation be enacted preventing Social Security from using wages from unauthorized work to determine eligibility and benefit amounts. A previous administration did not agree with the recommendation—where does the current Administration stand? What would be the policy arguments for and against the SSA OIG's proposal to prohibit crediting wages earned from illegal work toward Social Security benefits and eligibility? Could you also elaborate on whether INS has sufficiently complete data on immigrants' work authorization status over time to enable SSA to pursue this recommendation?

A proposal to deny credit for covered earnings on which the employee and employer paid the required Social Security taxes would be a major shift in public policy. The Administration has not reviewed this proposal.

Current law already provides that individuals can be paid benefits within the United States only if they are lawfully present. Thus, this proposal would reduce benefits primarily for individuals who are, at the time they apply for benefits, either U.S. citizens or otherwise legally within the country.

To administer such a change, it would be necessary to know exactly which periods in the past that a person was authorized to work and not authorized to work. However, it is our understanding that INS does not maintain an electronic historical record of the alien status of each noncitizen in this country. Without this informa-

tion it would be impossible to implement this change. We defer to INS for a more thorough explanation of their databases.

12. This year, SSA began mailing letters to all employers who submit information in which the name or SSN of the employee does not match SSA's records. Could you explain what the purpose of this letter is, since some employers may mistakenly believe they should no longer employ a worker because of the letter?

The Internal Revenue Code provides that employers are responsible for providing correct name/SSN information on the Form W-2. When an employee's reported name and SSN do not match SSA's records, SSA may send a "no match" letter informing the employer of the discrepancy and requesting the employer's assistance in resolving the error. Our purpose in sending these letters is to obtain the necessary information to clean up our suspense file and ensure that number holders receive proper credit for their earnings.

These letters are intended to remind employers about the importance of providing SSA with correct names and SSNs of employees. They also encourage employers to correct their records and to use SSA's Employee Verification Service.

We are concerned that some employers may use SSA's letters to take inappropriate adverse action against affected employees. We therefore specifically advise employers not to take adverse action against an employee because of the "no-match" letter, as indicated in the following paragraph from the letter used for tax year 2001:

"This letter does not imply that you or your employee intentionally provided incorrect information about the employee's name or SSN. It is not a basis, in and of itself, for you to take any adverse action against the employee, such as laying off, suspending, firing, or discriminating against an individual who appears on the list. Any employer that uses the information in this letter to justify taking adverse action against an employee may violate state or Federal law and be subject to legal consequences. Moreover, this letter makes no statement about your employee's immigration status."

13. It appears that many employers do not understand what they need to do to fix the record mismatch, and may inadvertently violate other laws. What guidance does SSA give to employers to help them fix the problems identified?

SSA provides detailed, step-by-step guidance with every "no-match" letter in order to help employers resolve the reported records discrepancy. Instructions are provided for correcting SSNs and Filing Tips for accurate annual wage reporting are automatically included when "no-match" letters are mailed.

Is this guidance consistent with that provided by INS, IRS, and the Department of Justice (DOJ) regarding hiring practices and documentation of an individual's work authorization status?

Yes.

Have you had discussions with these agencies to develop clear, consistent guidelines for employers so that they do not violate other laws in their efforts to comply with SSA's letters or out of fear of IRS penalties associated with non-matching wage reports?

INS, IRS, and DOJ have been consistently involved in the development of the no-match policy guidelines. SSA has met with various agencies to discuss the Earnings Suspense File, "no-match" letters and related policies to assure that the guidance SSA provides to employers is consistent with INS, IRS and the DOJ policies.

14. Did SSA consult with business groups and others before implementing the new policy of sending out no-match letters to all employers with mismatched information? If not, why?

SSA discussed changes to the "no-match" letter process with both the employer and payroll communities. We meet with groups such as American Payroll Association, the American Society of Payroll Management and the Payroll Service Bureau Consortium at our annual National Payroll Reporting Conference. "No Match" was a major topic at the Payroll Conference held in August, 2002. At this as well as other meetings, employers consistently indicate willingness to actively cooperate with SSA in order to resolve wage reporting discrepancies.

15. What has SSA heard back from employers and others since the mass mailing of no-match letters began?

There has been an increased interest by employers in verifying SSN's for their employees. Representatives of labor unions, immigrant advocacy groups, and employer associations have expressed concerns about possible misinterpretation and misuse of the mismatch information. SSA has worked to address the issues identified by these groups to try to alleviate their concerns.

16. How many employers have contacted SSA attempting to verify their employee's SSNs?

Employers can verify their employees' SSNs in a variety of ways:

- Approximately 7,400 employers are registered to use the batch verification system. In calendar year 2001, there were 218 employers who used the batch verification system.
- Employers can visit a local SSA field office or call a teleservice center. We have no data on the verification requests to SSA field offices and teleservice centers, but we believe they probably receive thousands of SSN verification requests from employers.
- They can use the Employer Reporting Services Center (an 800 number). SSA has very recently begun tracking the numbers of SSN verification requests received here. For September, October and November 2002 the average monthly volume of verification requests received through the 800 number at the Employer Reporting Service Center is about 60,000. No breakout on the numbers of employers involved is available.
- In addition, there are a select number of participants using the pilot Social Security Number Verification (online) Service (SSNVS). There are six companies participating in the SSNVS pilot.

17. The INS is responsible for assisting State and Federal agencies to train employees of those agencies in examining immigration documents such as visas. Isn't it true that the SSA only reversed its policy on checking INS records before issuing Social Security cards to aliens after September 11, 2001?

SSA has had longstanding policies to verify documents with INS. However, until recently we could not electronically confirm the legitimacy of documents with the INS until the person had been in this country for at least 30 days. Therefore we relied on visual inspection, pursuant to security guidelines provided by INS, to verify documents. In every case in which our own scrutiny led to any doubts about the authenticity of the documents, we held up assignment of the SSN until INS verified the documents, no matter how recent the entry.

The events of September 11, 2001, caused SSA's new management to reexamine many of our internal processes and our interactions with other agencies, including INS. INS has made improvements in the timeliness of their data entry, and earlier this year gave SSA expanded access to non-immigrant data. Based on a decision by Commissioner Barnhart, no alien's SSN application is processed until SSA receives verification of the alien's INS documents from INS. Full implementation of this procedure was rolled out from July 15, 2002 through September 2002. Where the verification still cannot be done electronically, we will request verification from INS, which could be for as many as a half million of the 1.5 million non-citizens we enumerate each year.

18. More than 6 months after the initial request by the SSA, the INS still has not completed any arrangements to provide automated record checking against INS records, despite public statements that this was a "top priority." Is the problem with INS or is the SSA request more complicated than the press releases suggest?

SSA is now able to verify most INS documents online, using INS' Systematic Alien Verification for Entitlements (SAVE) system. Online access was provided by INS on May 25, 2002. The system was piloted in SSA field offices in June 2002, and implemented in all SSA field offices on September 1, 2002. For documents that cannot be verified online, SSA sends a manual request to INS for verification.

19. Beginning in June 2002, SSA started contacting the State bureau of vital statistics to verify a birth certificate presented for a SSN application. Starting in July 2002 and nationwide by September 2002, SSA started verifying immigration documents with INS. Before these changes, SSA generally examined the documents and accepted them if they appeared genuine. Did SSA consult with employers before changing its verification procedures?

As indicated above, SSA's general policy prior to September 11 was to verify documents with INS, except for certain new arrivals whose records were scrutinized by our employees. The events of September 11 made it necessary for SSA to aggressively move forward in instituting additional verification measures to further ensure the integrity and security of the enumeration process. While we are working with the employer community and others to make them aware of the additional verification, we did not consult with them before changing our procedures.

20. What feedback has SSA heard from employers, particularly those employing seasonal workers, about the new verification procedures? Does SSA plan to make any exceptions or accommodations for temporary/seasonal workers? Under the new verification procedures, how long does it take a non-citizen to obtain an original SSN?

We recognize that our efforts to enhance the integrity of the enumeration process may result in a delay in receipt of an SSN or replacement card and therefore could hamper employment of temporary or seasonal workers. However, our procedural changes are designed to assure that only those who meet the enumeration requirements receive an SSN or replacement card. SSA is making no exceptions to its rules for any applicant.

Some employers have contacted SSA expressing their concern about the length of time it may take for us to verify records manually with INS if the documents cannot be verified electronically. Any delays affect how quickly their newly hired employees obtain SSN cards. SSA's commitment is to assign an SSN within no more than a few days after receiving verification from the INS. Paper verification from INS may require as little as about a week or some number of weeks. SSA is working with INS to minimize these delays. Generally, employers are attempting to adjust their operations accordingly. Under IRS regulations 26 CFR Ch.1 §31.6011(b)-2 employers may hire an individual before he or she receives his/her SSN card.

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

21. Is it true that State benefit agencies, via your data matches with them, receive confirmation of their data or correct information from SSA's databases if their data is incorrect, for purposes of preventing fraud? State Departments of Motor Vehicles (DMVs) and employers only receive information on whether their data matches SSA's data or a note saying which piece of information did not match (without the correct information from SSA), even though they are also trying to prevent fraud, correct? In addition, is it also correct that the match with State DMVs may not provide information on whether the person on whom information was submitted shows up as deceased in SSA's records, depending on the system the State is using (online vs. batch file)? Why does SSA provide different levels of information to State DMVs than to State benefit agencies when they request matches with SSA data? Why don't the matches with Departments of Motor Vehicles or employers consistently include notification that a SSN belongs to a deceased individual? When do you expect SSA will provide information to employers and DMVs on whether a SSN is for a deceased person in these data matches?

It is true that SSA provides different levels of information to State benefit paying agencies, DMVs and employers. We are working to enhance our verification systems as part of SSNVS. The next step in that process is to expand the pilot to additional employers.

22. Why doesn't SSA require a photo ID with SSN and benefit applications? Do you plan to change your procedures to require a picture ID when anyone does business with you? If not, why? If so, what is your time frame?

SSA requires convincing evidence of identity (evaluated on a case-by-case basis) from all applicants for original or replacement SSN cards. Most people can provide some reliable evidence of identity, such as a drivers license, passport, or school ID, that is acceptable for SSA purposes.

In determining what identity documents to accept, SSA is mindful of the public burden, considering:

- Not all SSN card applicants are adults;
- Not every applicant, even if age 16 and older, has a picture identity document; and

- Not every applicant has more than one identity document that meets SSA's criteria.

It must be noted that there are many commercial organizations that sell identity cards with photographs. Anyone can easily purchase a photo ID card on the Internet. SSA does not accept these because they are generally issued based solely upon the person's allegations and the issuing agents cannot verify them. A photo ID is only as good as the documentation used to obtain it.

However, SSA has a pilot in certain SSA offices that will test and gather photographic identification to address the issue of complicit impersonation in the disability claims process. The pilot is expected to start in mid 2003, once necessary actions resulting from the publication of the Federal Register notice on November 15, 2002 are completed.

23. The SSA IG suggested in a September 2001 report that SSA limit the number of replacement cards to 3 in a year and 10 over a lifetime, except in extraordinary circumstances. Does SSA agree with the recommendation? If so, when will SSA implement it? If not, what other actions will SSA undertake to prevent misuse of replacement SSN cards? Also is SSA planning to take any action to restrict replacement cards issued to persons with non-work SSNs who report earnings?

We are currently considering various options for limiting the number of replacement cards an individual can receive.

24. I understand that the Federal statute does not specifically prohibit somebody from selling his or her own validly issued SSN with intent to deceive. Is this correct? If so, do you think Congress should consider changing the law to make this illegal?

Section 208 of the Social Security Act (42 U.S.C. 408) does prohibit a person from selling a Social Security card that is, or purports to be, a card issued by SSA. This provision also prohibits a person from possessing a Social Security card with the intent to sell it, for the purpose of obtaining anything of value "or for any other purpose." See 42 U.S.C. 408(a)(7). However, the section does not prohibit selling an SSN.

Nonetheless, that section does prohibit unlawful use of another person's SSN. If the number holder (NH) conspired with another person to unlawfully use the SSN, including selling it, knowing that it would be used unlawfully, then the NH could be charged with conspiracy and, perhaps other offenses (e.g., aiding and abetting).

Moreover, selling the SSN might violate State laws concerning fraud, consumer protection, and so forth., depending on how the SSN is used.

We note that the Subcommittees' bill, H. R. 2036, would remedy this. SSA would be glad to continue to work with you on such legislation.

25. When do you expect to have the first Enumeration at Entry Center running? What has been the reason for delay? Will only persons admitted for lawful permanent residence be processed through these centers? Does SSA have any near-term plans to expand these centers to persons temporarily admitted to the United States who are authorized to work?

Enumeration at Entry (EAE) is a process that enables aliens applying for immigrant visas at DoS's Foreign Service posts to apply for SSNs at the same time. The process started in October 2002. DoS passes the SSN application data to INS along with the visa application data. INS, in turn, passes the SSN application data on to SSA for issuance of the SSN. Significant programming and systems modifications on the part of all three agencies were necessary to make EAE a reality. Furthermore, EAE implementation requires that DoS staff physically install software containing the EAE changes at each post.

EAE is already operational in the posts in Manila, Philippines; London, England; and Ciudad Juarez, Mexico. As of December 18, 2002, we have issued 1,943 SSNs using this process.

Beginning January 2003, DoS will begin to install EAE software at other Foreign Service posts around the world. When this phase is fully implemented, more than 90 per cent of the people applying for immigrant visas at DoS posts will be able to apply for SSNs at the same time.

SSA, INS and DoS will soon begin discussions on expanding the process to other groups of aliens.

26. The IG has urged SSA to implement additional protections against issuance of multiple SSNs to children and to help State bureau of vital statistics to ensure records of hospital birth units and registered births match. For example, it can take a couple of months to get a SSN through

enumeration at birth, and parents may come into the Social Security office to request a SSN at the same time it is processing the information from the State BVS, sometimes causing infants to be issued multiple SSNs. Also, some hospitals do not separate the duties of clerks gathering birth information from parents and clerks entering information into the hospital database, making it easier for someone to enter births for children who do not exist. Is SSA implementing any of the SSA IG's suggestions?

The current Enumeration at Birth (EAB) contract expires on December 31, 2002. SSA is pursuing OIG's recommendation for the Bureaus of Vital Statistics to perform periodic independent reconciliation of registered births with statistics obtained from the hospitals to verify the legitimacy of sample birth records by building it into its negotiations for the new EAB contracts, which will be effective January 1, 2003.

27. Fingerprints and photos have been accepted biometric identification for government documents for more than fifty years. Why does the Social Security Administration not employ any sort of biometric identification to confirm identity? Doesn't the absence of biometric identity confirmation put at risk innocent citizens with regard to their bank accounts, their credit, sometimes even their mortgage loans?

From the inception of the program, the Social Security number (SSN) card was never intended for use as an identity document. If the Social Security Administration were to use biometrics to link the SSN card to the bearer to allow identity confirmation, the agency would become the trusted authority and authenticator of individual identity in the U.S. We believe this task would have an adverse impact on our ability to fulfill our mission. In addition, the use of biometrics would require the re-enumeration of every Social Security number holder at considerable cost.

We provided a report to Congress in 1997 on replacing the Social Security card with a plastic card that could include identifying information, such as a picture or biometric identifiers. Several of the prototypes developed in this study are still valid examples of the kind of identity document in question. The report found that issuing new Social Security cards with biometric information would cost from about \$4 billion to \$9 billion (in 1996 dollars), depending on the form of the card, and would require about 70,000 work years.

SSA's Office of Inspector General and other SSA components continue to actively pursue information about potential technologies that we could use to support more accurate earnings reporting and to reduce benefit and SSN fraud.

28. The Social Security card is generally accepted to be very easily counterfeited. Has the SSA looked into the processes used by the State Department for passports or visas or by the INS for the "Permanent Resident Card (green card)" or the Border Crossing Card?

We do not agree that the SSN card is "very easily" counterfeited. It has numerous sophisticated security features that help to prevent counterfeiting. These include:

- The front contains a marbled light blue security tint, with the words "Social Security" in white.
- Intaglio printing is used in some areas on the front of the card. (Intaglio printing can be done only by certain security printing companies, on registered machinery.)
- The front and back contain yellow, pink, and blue planchettes (small discs). These can appear anywhere on the card, including the area on the card that contains the Department of Health and Human Services or Social Security Administration seal and the number holder's name and SSN.

Further, there are additional security features that we do not make a matter of public record.

While we have confidence in the current security features of the card, we are open to considering options that would make it even less subject to counterfeiting and use by identity thieves.

29. Should the Social Security Administration, or another federal agency such as the INS start issuing a number that can be used for identification, so that the SSN can be reserved only for payroll tax withholding and benefit awards?

SSA does not have a position on whether it or another Federal agency should issue numbers that could be used for identification. We believe that this is an issue for the new Department of Homeland Security, and we will be happy to work with them and provide any support needed.

30. How many individuals have been issued more than one SSN? How does this happen? What measures exist to prevent this from happening?

Before SSA implemented the Systems controls explained below, there were occasional rare instances where more than one SSN was erroneously assigned to a single individual. We also know that there are limited cases where SSA has purposefully assigned a new SSN for domestic violence victims, those suffering continued harm due to identity theft, and so forth.

In July 1990, SSA implemented the Modernized Enumeration System (MES), which gave FO personnel the capability to take an SSN application using online screens rather than on a paper application form. As part of the application process, MES searches the SSN database and returns possible matches when an application for a new SSN is entered. This helps the field office identify a previously assigned SSN, and prevents assignment of a new one.

31. We know that non-citizens who are authorized to work are able to legitimately obtain SSNs for work purposes. However, if they no longer are working in this country or have left the country, the SSN issued to them remains on record as being assigned to them. Should some notation on SSA's record be placed to indicate that the individual is no longer working and/or residing in this country? Should that number be valid for all times?

It should remain an INS responsibility to determine who is authorized to work, and to keep track of entry/exit from the U.S. Employers, as part of the hiring process, can determine current status and work authorization by following INS' I-9 rules. We do not think SSA should duplicate this function.

Regarding the validity of the SSN for all times, the SSN needs to remain valid in case the number holder returns to the United States and is once again authorized to work. The number is used to keep an accurate record of each individual's earnings and to pay and monitor benefits, including those paid under a Totalization agreement.

Chairman GEKAS. Thank you, Sam.

Yes, we invite the second panel to begin to take their places at the witness table. We call upon Charisse Phillips, Director of Fraud Prevention Programs, Bureau of Consular Affairs, U.S. Department of State; Robert Bond, Deputy Special Agent in Charge, Financial Crimes Division, U.S. Secret Service; Grant D. Ashley, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation; Hon. James G. Huse Jr., Inspector General, Social Security Administration in Baltimore; Matthew Reindl, Operator of Stylecraft Interiors Inc. of Great Neck, New York; and, Chris Hoofnagle, Legislative Counsel, Electronic Privacy Information Center.

We state to the witnesses that their written statements will be accorded a place in the record, without objection. We will ask them each to try to limit their remarks, their reviews of their written testimony, to about 5 minutes. We will begin in the manner in which we introduced the panel, starting with Charisse Phillips.

You may proceed.

STATEMENT OF CHARISSE M. PHILLIPS, DIRECTOR, OFFICE OF FRAUD PREVENTION PROGRAMS, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE

Ms. PHILLIPS. Mr. Chairman, thank you very much. I am very pleased to be here to testify before the Subcommittee this afternoon.

I have had the privilege of serving as the Director of Fraud Prevention Programs in the Bureau of Consular Affairs for 2 years now. Previously, I served in a number of consular sections abroad, where I had frontline experience with document fraud, and with attempts by criminals, terrorists, and hostile governments to obtain

U.S. travel documents. I have been a consular officer for almost 17 years now.

The State Department has an integral interest in the quality of identity documents and vital records produced in the United States because those documents form the basis of U.S. passport issuance. The U.S. passport is perhaps the most highly valued document in the world, because of the many benefits and privileges it confers. It is not “just a document,” it is the passkey into our country.

Let me tell you about the methadone moms. As these low-income women leave their drug-rehab clinics, they are targeted by alien smugglers. They are offered money, maybe a couple hundred dollars, to apply for passports for their own kids, but here’s the catch. They will substitute photos of different kids, photos supplied by the alien smugglers.

Who are these substitute kids? In the majority of cases, they are the children of people who cannot bring those kids to the United States legally immediately. Those parents pay thousands of dollars for these fraudulent passports.

How do we know about this? Well, the proverbial alert passport employee. We are fortunate to have a cadre of trained, experienced, and loyal personnel who detect these attempts to obtain our passports through fraud.

The Bureau of Consular Affairs is in the business of preventing this kind of abuse of children and of travel documents. We have developed an extremely tamper-resistant passport. In fact, just last week, Members of the Five Nations Conference told me what we have noticed ourselves, that our passports are now so good that alien smugglers have stopped trying to alter them.

Instead, now they are trying to get hold of them by other means. They are using look-alike travelers to match passports stolen from American tourists overseas. They are helping imposters apply for U.S. passports, using identities stolen from U.S. citizens in the United States. They are selling counterfeit documents—birth certificates, drivers’ licenses, Social Security cards—to aliens for use in applying for passports. All these documents are available cheap on the Internet.

We are pretty good at detecting these false documents. We have done studies of our passport issuances, and we provide training and information to our passport staff to keep them alert. As home computers, the Web, and high-tech scanners, and photocopiers become more accessible, we need more and better tools for our people.

We need to be able to confirm Social Security numbers easily and routinely. Right now, our people put a lot of energy into developing informal contacts to help them confirm Social Security numbers and work histories. They rely on this information in suspect cases to help them quickly identify Americans who are just taking an innocent trip from the aliens, sometimes criminal aliens, who are seeking U.S. passports to evade the scrutiny of immigration officials around the world.

Our people also need help in confirming the bone fides of U.S. birth certificates. This country has more than 8,000 authorities issuing birth certificates and more than 50,000 different versions issued by States, counties, and municipalities.

We also need an easy way to verify drivers' licenses, the usual proof of ID submitted with passport applications. High-quality duplicates of State drivers' licenses are available on the Internet with only a removable sticker warning "novelty item" to deter criminals. Our passport workers have no way of verifying drivers' licenses either online or through routine access.

We call these kinds of documents "breeder documents" because they can all be used to obtain more identity documents. My office has, therefore, purchased the Social Security CD-ROM with death records of Social Security recipients going back to 1936. We have made this available to our passport and our visa personnel online.

We have begun to brief Social Security fraud investigators. We are trying to work with Social Security on a way to identify Social Security numbers online.

[The prepared statement of Ms. Phillips follows:]

Statement of Charisse M. Phillips, Director, Office of Fraud Prevention Programs, Bureau of Consular Affairs, U.S. Department of State

Mr. Chairman and Members of the Committees:

Thank you for the opportunity to appear at this hearing on *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists*.

I have had the privilege of serving as the Director of Fraud Prevention Programs, in the Bureau of Consular Affairs, for two years now. Previously I served in a number of consular sections abroad where I had front-line experience with document fraud, and with attempts by criminals, terrorists, and hostile governments to gain U.S. travel documents. I have been a consular officer for almost 17 years.

The Bureau of Consular Affairs is in the business of preventing travel document fraud. We have an integral interest in the quality of identity documents and vital records produced in the United States, because those documents form the basis of U.S. passport issuance. The U.S. passport is perhaps the most highly valued document in the world, because of the many benefits and privileges it confers. It is not "just a document"—it is the pass-key into our country.

We have developed an extremely tamper-resistant passport. In fact, passport and immigration authorities in other countries have told us what we have found ourselves—the U.S. passports now being issued are now so difficult to alter or counterfeit that alien smugglers have stopped trying to alter them.

Instead they are acquiring authentic passports that have been lost or stolen and then using "look-alike" travelers to match passports stolen from American tourists overseas. They are helping impostors apply for U.S. passports using identities stolen from U.S. citizens in the USA. They are also producing and selling counterfeit documents—birth certificates, driver's licenses, Social Security cards—to aliens to use in applying for passports. All these documents are available—cheap—on the Internet.

Personnel of the Bureau of Consular Affairs are experienced at detecting these false documents. We have done studies of our passport issuances, and we provide training and information to our passport staff to keep them alert. But as home computers, the Web, and high tech scanners and copiers become more accessible, we need more and better tools for our people.

One tool that will help our officers is on-line access to Social Security Administration records. Comparing the documents submitted in support of passport and visa applications against the official databases of the issuing authorities will greatly improve the accuracy and integrity of the citizenship and identity confirmation process. We are currently working closely with the Social Security Administration and state vital records offices toward this goal.

I will begin by giving some examples of document fraud cases.

Alien Smuggling Ring Exposed

Let me tell you about the methadone moms. As these low-income women leave their drug-rehab clinics, they are targeted by alien smugglers. They are offered money—several hundred dollars, maybe—to apply for passports for their own kids. But, here's the catch. They will submit photos of different kids, supplied by the alien smugglers. Who are these substitute kids? In the majority of cases, they are the children of people in the U.S. either illegally, or as permanent residents, but who cannot bring their kids to the U.S. immediately through any legal means. Their parents pay thousands of dollars for those fraudulent passports. How do we know about

this? An alert passport employee. We are fortunate to have a cadre of trained, experienced and loyal personnel who detect these attempts to obtain our passports through fraud.

Operation Oak Park: Passport Agency Uncovers Criminal Document Ring

Late in 2000, the Chicago Passport Agency's Fraud Program Manager (FPM) linked 25 passport applications to a document fraud ring involving Nigerian nationals. A subsequent investigation conducted by the State Department's Diplomatic Security Field Office in Chicago revealed the fraud ring involved one document broker, who was already under investigation by the U.S. Postal Inspector's Office, the Social Security Administration's Inspector General's Office, the Immigration and Naturalization Service (INS), and the Drug Enforcement Agency. With Diplomatic Security as the catalyst, the agencies and others formed a task force, "Operation Oak Park," under the direction of the U.S. Attorney.

The ringleader and his associates provided young women with computer-generated counterfeit birth certificates and immunization records that named the women as the mothers of non-existent newborn babies. They used those documents to apply for Social Security cards, which they passed on to the ringleader. He then created other counterfeit birth certificates, using the name on the Social Security card but with the date of birth of the ultimate recipient or purchaser of the documents. The recipients could then use the birth certificates and Social Security cards to obtain driver's licenses and apply for passports. The ringleader charged about \$5,000 for each fraudulent identity.

The investigation developed leads into Jamaican and Nigerian community-based criminal activities and implicated two Illinois State Bureau of Vital Statistics employees and one Federal employee, who actively participated in the broader fraudulent documents scheme.

Operation Blind Date

When Federal investigators arrested the ringleader, he agreed to cooperate, spawning a subsidiary investigation, Operation Blind Date. Under guidance from the task force he arranged for his network of brokers to fly to Chicago to pick up their documents and meet a supposedly corrupt Social Security supervisor, who was in reality an undercover Secret Service agent. The Chicago Police Department was included in the operation and arrested eight of the ringleader's associates ostensibly in routine traffic stops as they left his office so they wouldn't suspect him of turning them in. Those arrested included six Nigerian nationals, a Kenyan and a Jamaican posse street gang leader who was sought at the time by U.S. Customs and the DEA for narcotics trafficking.

As part of a plea agreement, the ringleader took responsibility for preparing more than 100 sets of false documents. He was charged with fraudulently obtaining and selling passports and Social Security cards and counterfeiting birth certificates. He faced a possible sentence of 10 years imprisonment and a \$250,000 fine. However, he did not give up as easily as it appeared at the time. In December 2001, his family informed Federal agents that the individual, who was at home on electronic detention while awaiting sentencing, had passed away. However, when a Secret Service agent went to the morgue to identify the body he discovered that the corpse was not the ringleader's. The family and their doctor allegedly conspired to kidnap and murder a homeless man, pass him off as the convicted individual and planned to have the body cremated as soon as the morgue released it. A manhunt for the ringleader ensued, and Federal agents were able to track him to Massachusetts. He was apparently planning to flee the country to Poland where he had ties. He is still awaiting sentencing. The U.S. Attorney in Chicago has added capital murder charges to the document fraud charges.

West African Fraud in Texas

Interagency cooperation is also active in other parts of the country to combat document fraud. The Houston Passport Agency's region has two of the country's largest enclaves of West African nationals in the U.S. The majority resides in Dallas and Houston, which has over 50,000 Nigerian residents. The number of scams involving West African nationals in this region grew so great that a Federal task force comprised of various Federal and local law enforcement agencies convened several years ago in an effort to share case information and develop joint strategies. The majority of passport fraud cases by West Africans detected involved additional crimes, such as marriage fraud, narcotics trafficking, credit card fraud, insurance fraud and Social Security fraud.

Falsified Visas Also Used for Social Security Fraud

Another type of fraud we have seen involves altered visas used by people who are already in the U.S. to obtain a benefit. Copies of fraudulent visas have been submitted to the Social Security Administration and the INS. The SSA applications are most commonly submitted by citizens of the Former Soviet Union who have legitimately issued visitor visas. The visas are altered, however, to show work classification so that the person will appear eligible for a Social Security number.

Why Social Security Number Checking is Critical to Passport and Visa Processing

Passport Applications

As state and local vital statistics offices improve the security features of their birth certificates to deter counterfeiters, deceased identity fraud will become an increasingly popular mode of fraud. Confirming a deceased identity is often difficult for Passport Agency Fraud Program Managers (FPMs) since many states have not cross-matched out-of-state birth and death records. Social Security data can be very useful in exposing attempts at passport fraud.

FPMs have learned to recognize potential fraud cases by spotting anomalies in passport applications. Among the most frequent indicators of passport fraud are:

- **The breeder document phenomenon**

In this scenario, a birth certificate is used to generate a series of new documents, culminating in an application for a passport. One hallmark of such activity is a readily identifiable timeline sequence of the respective transactions. First, a birth certificate appears, then a Social Security card or a document such as a state ID or driver's license, and finally, the passport application is executed.

- **Little evidence to support the deposed facts**

Often, a passport application shows omissions and references to third parties (e.g., a friend as the person-to-be-notified in the event of an emergency). In person, the applicant is generally unfamiliar with the assumed identity, thus tending to respond evasively and making claims that are generally inconsistent with his appearance.

- **Unusual signatures**

Signatures on the applications may appear labored or obviously forged. FPMs are trained to detect handwriting that is not American in style.

Passport agency personnel frequently check whether a previously issued passport was issued in error. The most useful method to do so is to obtain a copy of the previous application and verify the subject's Social Security number and check birth/death records and the FBI's National Crime Information Center files.

If the passport was issued in a deceased identity a possible indicator would be a recently issued SSN or a record of two SSN's issued in that identity. There will also be minimal personal data on the original application. If the passport was obtained based on a counterfeit or falsely filed delayed birth certificate, a new SSN in the applicant's identity may have been issued weeks after the first passport was issued. The previous application may show a different SSN.

Immigrant Visa Utility

Consular sections at U.S. Embassies and Consulates also rely on Social Security records when handling immigrant visa cases. Consular Sections overseas are sometimes hard pressed to determine whether an elderly petitioner in an immigrant visa case is still alive, particularly in cases where the petition was filed many years before. In other cases, the follow-to-join beneficiaries may claim the original petitioner is deceased in order to avoid a likely visa refusal resulting from ineligibility under the public charge section of the Immigration and Nationality Act. Sometimes there are also fraud problems when employment-based immigrant visa cases filed many years before for beneficiaries to care for elderly or seriously ill individuals raise questions whether the individuals still need such assistance. A check of the SSA database will in some cases provide definitive evidence of misrepresentation.

How the Department of State Combats the Fraud

Purchasing SSA Database

My office has purchased from Social Security a CD ROM with death records of Social Security recipients dating back to 1936. We have made this available to our passport and visa personnel on-line. Fraud Prevention Managers in consular sections and passport agencies now have access to over 77 million U.S. death records via the Office of Fraud Prevention Programs' Intranet Web page. Over 98% of the death records in the database are for individuals who died after 1962. However, the

database only includes death records of individuals for whom a death benefit claim was made to SSA. It may therefore not provide a positive response if the decedent never worked or never had a Social Security number, even if that person is indeed deceased.

Multiple Passport Issuance Verification Helps Detect Fraudulent Passport Applications

Passport Services' Multiple Passport Issuance Verification (MIV) feature of the new Photodigitized Passport Issuance System is a quantum leap forward in fraud prevention technology that is already paying handsome dividends.

Acting much like a name-check system, MIV automatically searches the passport files database for records of passport issuance during the past ten years and notifies the adjudicating officer if an applicant was issued a previous passport. It tells the officer how many passports were issued and for each issuance provides the name, date and place of birth, passport number, issuance and expiration dates. Some records also provide the Social Security number. This is proving to be a powerful tool for passport agency FPMs. A recent survey of ten passport agencies revealed that the MIV system detected an average of 25 additional fraud cases per month.

Liaison with Vital Records Offices

When questions arise concerning the authenticity of a U.S. birth certificate submitted with a passport application, FPMs often seek to verify the questioned document with appropriate local authorities. Over the years, FPMs have established informal working relationships with most of the state registrars in their regions.

Consular personnel also work with the National Association for Public Health Statistics and Information Systems (NAPHSIS). At their annual conference in 2001 NAPHSIS members approved a Consular Affairs-drafted resolution recommending cooperation with the Department of State's anti-fraud program. In the resolution, NAPHSIS recognized that cooperation with the State Department is essential to the integrity of the passport issuance process and the states' vital records operations. The resolution encouraged all vital statistics offices to establish and maintain liaison with the FPM whose passport agency is responsible for their state.

• What the Problem Needs Now

We need to be able to confirm Social Security numbers easily and routinely. Right now our people put a lot of energy into developing informal contacts to help them confirm Social Security numbers and work histories. They rely on this information in suspect cases to help them quickly identify the bona fide Americans taking an innocent trip from the aliens, sometimes criminal aliens, who are seeking U.S. passports to evade the scrutiny of immigration officials around the world.

Our people also need help with confirming the bona fides of U.S. birth certificates and driver's licenses. This country has more than 8,000 authorities issuing birth certificates, and more than 50,000 different versions issued by states, counties and municipalities. One commonly accepted proof of identity is the driver's license. It is not commonly known, however, that high-quality duplicates of state licenses are available on the Internet, with only a removable sticker warning "novelty item" to deter criminals. Our passport workers have no way of verifying driver's licenses, either on-line or through routine access. We call these documents "breeder documents" because they can all be used to obtain more identity documents. Over the past several years we have been working with other agencies to combat fraudulent use of these documents and detect counterfeits and other fraud.

We have begun to brief Social Security fraud investigators in identifying foreign passports presented with Social Security number applications. We are also working closely with the Social Security Administration to identify a way for us to routinely verify Social Security numbers on-line.

We are working with the National Association of Public Health Statistics and Information Systems and the Social Security Administration to encourage states to automate their birth and death records. My office is also building a database of lost-or-stolen blank documents, such as birth certificates. We are also part of an inter-agency working group, headed by INS, on developing standards for U.S. birth certificates, to make it easier to identify counterfeits.

In addition, we are talking to the American Association of Motor Vehicle Administrators on standardizing driver's license features. My office recently sponsored a pilot program at one passport agency to purchase readers to verify that the information on the front of driver's licenses at least matches that on the barcodes or magnetic strips on the back—police departments use these same devices to detect underage drinkers. We are also developing a pilot program with one state Department of

Motor Vehicles to construct a train-the-trainers program on foreign passports, and share information on trends in document fraud.

If we have this much difficulty with fraudulent documents in the United States, it is easy to imagine the problem encountered in our consular sections overseas. Some countries have automated, centralized records that are verified before passports are issued, and their documents are therefore easy to accept. In others, wars and natural disasters have destroyed vital local records, where they even existed. Poorly paid civil registry workers are also subject to pressure to fraudulently issue legitimate documents.

To counter this problem, my office maintains information on lost-or-stolen blank foreign travel documents. Every consular section has a designated Fraud Prevention Manager who is responsible for helping new officers learn the local documents, and for maintaining exemplars for reference. We have on-line country fraud summaries available for visa adjudicators to refer to. We train consular officers to detect altered or counterfeit documents, even when they have never seen such documents before. In addition, the U.S. Government has several programs to encourage countries to centralize and automate their vital records.

As much progress as we believe we have made, we continue to explore possibilities for improving our fraud detection. For instance, we would like to explore the use of commercial databases to help identify fraudulent applications. We will work with INS to obtain additional information from its records that would be helpful.

We in the State Department are proud of our fraud prevention programs and the technological improvements we are making. We will continue to work with the Social Security Administration, other Federal agencies, and the states to aggressively combat document fraud.

Chairman GEKAS. We thank the lady for the testimony. I take it she is not completed with all that she wants to render, but perhaps during the question and answer period, some commentary will be forthcoming.

We will go to the second witness. You may proceed.

STATEMENT OF ROBERT BOND, DEPUTY SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, U.S. SECRET SERVICE

Mr. BOND. Mr. Chairman, thank you. Members of both Subcommittees, thank you for the opportunity to address the subject of identity theft and the Secret Service's efforts to combat this problem. I am particularly pleased to be here with my colleagues and partners in fighting identity theft from the Federal Bureau of Investigation, the State Department, and the Social Security Administration.

With the passage of new Federal laws in 1982 and 1984, the Secret Service was given primary jurisdiction for the investigation of access device fraud and parallel authority with other law enforcement agencies in identification fraud cases. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes.

While advances in technology and the burgeoning use of the Internet has provided numerous benefits to the consumer through readily available credit and consumer-oriented financial services, it has also created a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Identity theft is almost always a component of one or more crimes, such as financial crimes, violent crimes, or, possibly, the facilitation of terrorist activities.

Identity theft can affect all Americans, regardless of age, gender, nationality, or race.

The events of September 11 have focused the priorities and actions of law enforcement throughout the world, including the Secret Service. Immediately following the attacks, the Secret Service assisted the FBI and the joint terrorism task forces with their investigations through the leveraging of our established relationships, especially within the financial sector, in an attempt to gather information as expeditiously as possible.

The Secret Service is also involved in a collaborative effort to analyze the potential for identity theft to be used in conjunction with terrorist activities through our liaison efforts with Operation Green Quest, Operation Direct Action, FinCEN, and the Terrorist Financing Operations section of the FBI.

Since our inception in 1865, the twin pillars of the Secret Service have been prevention and partnership building.

We simply could not fulfill our dual missions of protecting our Nation's elected leaders and safeguarding our financial infrastructure without two essential elements, incorporating preventative strategies and training, and building cooperative, trusted relationships with our local and Federal law enforcement partners.

A central component of the Secret Service's preventive and investigative efforts with regard to identity theft has been educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives, including our 37 financial and cybercrime task forces the Secret Service has developed throughout the country.

The Secret Service has already undertaken a number of unique initiatives aimed at increasing awareness and providing the training necessary to combat identity theft and assist victims in rectifying damage done to their credit. This includes the development of a number of training tools designed to assist local law enforcement partners.

Ultimately, most identity theft cases are reported to and investigated at the local level, but too often, local law enforcement agencies lack the expertise, experience, and resources to sufficiently investigate electronic-based crimes such as identity theft.

In partnership with the International Association of Chiefs of Police, the Secret Service produced the "Best Practices for Seizing Electronic Evidence Manual." This pocket-size guide instructs law enforcement officers in seizure of evidence from personal computers to wireless telephones to digital cameras. To date, the Secret Service has distributed over 315,000 copies of this guide free of charge to local law enforcement officials.

We have also worked with this group and our private sector partners to produce the interactive and computer-based training program known as "Forward Edge," and this is "Forward Edge." It is a computer-based training program that takes the next step in training officers to conduct electronic crimes investigations. "Forward Edge" incorporates virtual reality features as it presents different investigative scenarios to the trainee.

Copies of State computer crime laws for each of the 50 States, as well as corresponding sample affidavits, are also part of the

training program and are immediately accessible for instant implementation.

In short, any police department in the country, regardless of the size and the resources that they may have, now has access to state-of-the-art training on the seizure and preservation of electronic forensics evidence, which can be central to an identity theft investigation. To date, we have distributed over 35,000 of these training CDs, again, free of charge, to our local law enforcement partners.

Finally, the Secret Service and the International Association of Chiefs of Police are developing an "Identity Theft Roll-Call Video" geared toward local police officers throughout the Nation. This video will emphasize the need for police to document a citizen's complaint of identity theft, regardless of the location of the suspects. The video will also provide officers with instructions to assist victims who are seeking their reputations and credit worthiness.

In addition to preventive measures, legislation currently pending in Congress can further enhance law enforcement efforts to combat identity theft. Stronger penalties, increased enforcement, and continued focus on prevention and training are the ingredients to successfully combating identity theft in the future.

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

[The prepared statement of Mr. Bond follows:]

Statement of Robert Bond, Deputy Special Agent in Charge, Financial Crimes Division, U.S. Secret Service

Mr. Chairman, I would like to thank you for the opportunity to address both Subcommittees on the issue of identity theft and the Secret Service's efforts to combat this problem. I am particularly pleased to be here with my colleagues and partners in fighting identity theft from the Federal Bureau of Investigation, the Department of State, and the Social Security Administration.

The Secret Service was originally established within the Department of the Treasury in 1865 to combat the counterfeiting of U.S. currency. Since that time, this agency has been tasked with the investigation of other Treasury related crimes, as well as the protection of our Nation's leaders, visiting foreign dignitaries and events of national significance. With the passage of new Federal laws in 1982 and 1984, the Secret Service was given primary authority for the investigation of access device fraud and parallel authority with other law enforcement agencies in identification fraud cases. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes.

The burgeoning use of the Internet and advanced technology coupled with increased investment and expansion has led to fierce competition within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer oriented financial services, it also creates a target rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Information collection has become a common byproduct of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. This has led to an entirely new business sector being created which promotes the buying and selling of personal information. Consumers routinely provide personal, financial and health information to companies engaged in business on the Internet. They may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize are valuable commodities in this new age of information trading. With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing, and brokering of this information. These companies collect a wealth of information about consumers, including information as confidential as their medical histories. Like all businesses, data collection companies are profit motivated,

and as such, may be more concerned with generating potential customers rather than safeguarding their information to prevent its misuse by unscrupulous individuals. The private sector represents the first line of defense in identity theft and has a responsibility to safeguard the data that it has collected. The greater the protections that industry provides to the public, the fewer the opportunities for identity theft.

Based upon this wealth of available personal information, the crime of identity theft can be perpetrated with minimal effort on the part of even relatively unsophisticated criminals.

There is no area today that is more relevant or topical than that of identity theft. Simply stated, identity theft is the use of another person's identity to commit fraudulent activity.

Identity theft is not typically a "stand alone" crime. It is almost always a component of one or more crimes, such as financial crimes, violent crimes, or possibly, the facilitation of terrorist activities. In many instances, an identity theft case encompasses multiple types of fraud. According to statistics compiled by the FTC for the year 2001, 20% of the 86,168 victim complaints reported involved more than one type of fraud. The major complaints compiled by the FTC, which include multiple types of fraud reported in multiple categories, were:

- **42%** of complaints involved credit card fraud—i.e. someone either opened up a credit card account in the victim's name or "took over" their existing credit card account;
- **20%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;
- **13%** of complaints involved bank accounts that had been opened in the victim's name, and/or fraudulent checks had been negotiated in the victim's name;
- **7%** of complaints involved consumer loans or mortgages that were obtained in the victim's name;
- **9%** of complaints involved employment-related fraud;
- **6%** of complaints involved government documents/benefits fraud; and
- **17%** of miscellaneous fraud, such as medical, bankruptcy and securities fraud.

IMPACT

Identity theft, unlike many types of crime, affects all types of Americans, regardless of age, gender, nationality, or race. Victims include everyone from restaurant workers, telephone repair technicians, and police officers, to corporate and government executives, celebrities and high-ranking military officers. What victims do have in common is the difficult, time consuming, and potentially expensive task of repairing the damage that has been done to their credit, their savings, and their reputation. Obviously, the impact is magnified when it affects one of America's most valued assets, our senior citizens, as they represent a generation with a trusting nature that is easy to exploit. This group is particularly dependent on other caregivers for assistance, such as relatives, medical staff, service personnel, and oftentimes, complete strangers. This dependency increases their vulnerability to certain schemes involving identity theft.

LEGISLATION

In past years, victims of financial crimes such as bank fraud or credit card fraud were identified by statute as the person, business, or financial institution that incurred a financial loss. All too often the individuals whose credit was ruined through identity theft were not even recognized as victims. This is no longer the case. The Identity Theft and Assumption Deterrence Act was passed by Congress in 1998. This represented the first comprehensive effort to re-write the Federal criminal code to address the insidious effects of identity theft on private citizens. This new law amended Section 1028 of title 18 of the United States Code to provide enhanced investigative authority to battle the growing problem of identity theft. These protections included:

- Expanding the scope of the statute to include as victims those individuals whose identity information was stolen and whose primary loss is creditworthiness and reputation rather than financial loss;
- The establishment of the Federal Trade Commission (FTC) as the central clearinghouse for victims to report incidents of identity theft. This centralization of all identity theft cases allows for the identification of systemic weaknesses and provides law enforcement with the ability to retrieve investigative data at one central location. It further allows the FTC to provide victims with

the information and assistance they need in order to take the steps necessary to correct their credit records;

- Asset forfeiture provisions were enhanced to allow for the repatriation of funds to victims; and
- The closing of a significant gap in existing statutes. Previously, only the production or possession of false identity documents was unlawful. With advances in technology such as e-commerce and the Internet, criminals did not need actual, physical identity documents to assume an identity. This legislative change made it illegal to steal another person's personal identification *information* with the intent to commit a violation, regardless of actual possession of identity *documents*.

We believe that the passage of this legislation was the catalyst needed to bring together both Federal and state government resources in a focused and unified response to the identity theft problem. Today, law enforcement, regulatory and community assistance organizations have joined forces through a variety of working groups, task forces, and information sharing initiatives to assist victims of identity theft.

The United States Sentencing Guidelines have also been amended since the passage of the 1998 Act to better address identity theft. Section 2B1.1 now provides an offense level of 12 in cases involving the possession of device-making equipment, the production of or trafficking in an unauthorized or counterfeit access device, the unauthorized transfer or use of any means of identification to unlawfully produce or obtain any other means of identification, or the possession of five or more means of identification that were lawfully produced from, or obtained by the use of, another means of identification.

The guidelines amendments also provide a revised minimum loss rule for offenses involving counterfeit or unauthorized access devices. Specifically, a minimum loss amount of \$500 per access device is to be used when calculating the loss involved in the offense, with the exception of the possession, not the use of, telecommunications access devices, in which case the minimum loss per unused device is \$100.

Finally, the guidelines now include grounds for an upward departure in identity theft cases in which the penalty range, which is largely based on financial loss, does not adequately reflect the seriousness of the offense. Specifically, courts may now consider whether the offense conduct harmed the victim's reputation or credit record, whether the victim suffered substantial inconvenience related to repairing that reputation or credit record, whether the victim was erroneously arrested or denied a job due to the theft, and whether the defendant produced or obtained numerous means of identification such that he or she essentially assumed the victim's identity.

Violations of the Act are investigated by Federal law enforcement agencies, including the Secret Service, the U.S. Postal Inspection Service, the Social Security Administration (Office of the Inspector General), and the Federal Bureau of Investigation. Schemes to commit identity theft or fraud may also involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud, as well as violations of state law. Because identity theft is often connected to criminal activity that falls under the jurisdiction of the Secret Service, we have taken an aggressive stance and continue to be a leading agency for the investigation and prosecution of such criminal activity.

Given the relative ease with which criminals can steal the identities of others and the allure of enormous profits with few, if any, repercussions, relying on the current sentencing structure to deter the victimization of our citizens, is shortsighted. Recently, S. 2541, the Identity Theft Penalty Enhancement Act of 2002 was introduced in the Senate with the intent to establish increased penalties for aggravated identity theft, that is, identity theft committed during and in relation to certain specified felonies. This Act, in part, would provide for two (2) years imprisonment for aggravated offenses, in addition to the punishment associated with the related felony; committing the crime of identity theft in relation to specified felony violations, in addition to the punishment provided for such felony; and five (5) years imprisonment for the same related felonies associated with terrorism. Additionally, the Act prohibits the imposition of probation for those convicted of such violations and allows for consecutive sentences. While this particular legislation cannot be expected to completely suppress identity theft, it does recognize the impact identity theft has on society and the need to punish those engaging in criminal activity for personal or financial gain. The Administration strongly supports this bill.

SECRET SERVICE INVESTIGATIONS

Although financial crimes are often referred to as “white collar” by some, this characterization can be misleading. The perpetrators of such crimes are increasingly diverse and today include organized criminal groups, street gangs and convicted felons. This can be attributed to many factors including:

- The probability of high financial gain versus low sentencing exposure;
- The increased availability of goods or services which can be obtained on credit; and
- The proliferation of computer technology in our society that provides easy access to the information needed to commit many financial crimes, as well as a means for committing them remotely.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily Social Security numbers, names, and dates of birth.

The methods of identity theft vary. It has been determined that many “low tech” identity thieves obtain personal identifiers by going through commercial and residential trash, a practice known as “dumpster diving.” The theft of both incoming and outgoing mail from mailboxes is a practice used equally as often by individuals and organized groups, along with thefts of wallets and purses.

With the proliferation of computers and increased use of the Internet, many identity thieves have used information obtained from company databases and web sites. A case investigated by the Secret Services that illustrates this method involved an identity thief accessing public documents to obtain the Social Security numbers of military officers. In some cases, the information obtained is in the public domain, and in others, it is proprietary, and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. The Secret Service has discovered that individuals or groups who wish to obtain personal identifiers or account information for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

In most of the cases our agency has investigated involving identity theft, criminals have used another individual’s personal identifiers to apply for credit cards or consumer loans. Less commonly, they are used to establish bank accounts, leading to the laundering of stolen or counterfeit checks, or are used in a check-kiting scheme.

The majority of identity theft cases investigated by the Secret Service are initiated on the local law enforcement level. In most cases, the local police department is the first responder to the victims once they become aware that their personal information is being used unlawfully. Credit card issuers as well as financial institutions will also contact a local Secret Service field office to report possible criminal activity.

It is quite probable that older Americans will become an increasingly attractive target by criminal elements given the fact that 70% of our Nation’s wealth is controlled by those 50 years of age and older. Additionally, the common perception is that it is difficult for elderly victims to repair the effects of identity theft due to a lack of technical knowledge and uncertainty on how to protect themselves. Often, the level of diligence in monitoring personal finances decreases among the elderly or, after discovering the fraudulent activity, some are embarrassed and unsure of the steps necessary to report the compromise.

TERRORISM

The events of September 11, 2001 have altered the priorities and actions of law enforcement throughout the world, including the Secret Service. Immediately following the attacks, Secret Service assisted the FBI with their terrorism investigation through the leveraging of our established relationships, especially within the financial sector, in an attempt to gather information as expeditiously as possible.

The Secret Service has become involved in several collaborative efforts with respect to the investigation of terrorist activities through our liaison efforts with Operation Green Quest, Operation Direct Action, FinCEN, and the Terrorist Financing Operations Section of the FBI. As part of these collaborative efforts, the Federal law enforcement community is analyzing the potential for identity theft to be used in conjunction with terrorist activities.

COORDINATION

The Secret Service continues to attack identity theft by aggressively pursuing our core Title 18 investigative violations, including access and telecommunications device fraud, financial institution fraud, computer fraud and counterfeiting. Many of these schemes would not be possible without compromising the personal financial information of an innocent victim.

Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal information to further their financial crime activity.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working closely with other Federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country, pursuant to our section 1030 computer crime authority. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that falls within the investigative jurisdiction of the Secret Service. Members of these task forces, who include representatives from local and state law enforcement, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes.

While our task forces do not focus exclusively on identity theft, we recognize that a stolen identity is often a central component of other electronic or financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity theft.

OUTREACH EFFORTS

Another important component of the Secret Service's preventative and investigative efforts has been to increase awareness of issues related to financial crime investigations in general, and of identity theft specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity theft, now routinely involves the seizure and analysis of electronic evidence. In response to this trend, the Secret Service developed, in conjunction with the International Association of Chiefs of Police (IACP), the "Best Practices for Seizing Electronic Evidence Manual," to assist law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

As a follow-up to this guide, the Secret Service and the IACP developed "Forward Edge," a computer-based training application designed to allow officers to "virtually" seize different types of evidence, including electronic evidence, at various crime scenes.

Further, the Secret Service, in conjunction with the U.S. Postal Inspection Service and the Federal Reserve Bank System, produced an identity theft awareness video. The video, which explains how easily one can become a victim and what steps should be taken to minimize damage, has been made available to Secret Service offices for use in public education efforts.

In April of 2001, the Secret Service assisted the FTC in the design of an identity theft brochure, containing information to assist victims on how to restore their "good name," as well as how to prevent their information and identities from becoming compromised.

Finally, the IACP and the Secret Service have partnered to produce an "Identity Theft Roll-Call Video" geared toward local police officers throughout the Nation. The purpose of this video is to emphasize the need for police to document a citizen's complaint of identity theft, regardless of the location of the suspects. In addition, the video and its companion reference card will provide officers with information that can assist victims desperate to restore their reputations and creditworthiness.

The Secret Service is also actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice. This group, which is comprised of Federal, state, and local law enforcement agencies, regulatory agencies, and professional agencies, meets regularly to discuss and coordinate investigative and prosecutive strategies as well as consumer education programs.

Last spring, the Secret Service's Financial Crimes Division assigned a full-time special agent to the Federal Trade Commission (FTC) to support all aspects of their program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The Identity Theft and Assumption Deterrence Act established the FTC as the central point of contact for identity theft victims to report all instances of identity theft. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft. To date, the Secret Service representative at the FTC has:

- Met with and made presentations to Federal, state and local law enforcement about the FTC's Identity Theft Data Clearinghouse and its victim assistance program;
- Worked closely with agents in the field to ensure that they have access to the Consumer Sentinel system and are comfortable using the Identity Theft Data Clearinghouse database;
- Used the Identity Theft Data Clearinghouse to identify possible case leads, and developed a protocol for selecting which victim complaints are most likely to be successful case leads for criminal law enforcement agencies;
- Developed points of contact at the local, state and Federal levels of government to receive case lead referrals from the Identity Theft Data Clearinghouse database, and also identified routines and procedures to be followed when referring such cases; and
- Served as both a presenter and an instructor at 11 law enforcement training conferences hosted by various law enforcement agencies or organizations, such as the International Association of Financial Crimes Investigators (IAFCI) and the U.S. Marshal's Investigators Conference.

It is important to recognize that public education efforts can only go so far in combating the growth of identity theft. Because Social Security numbers, in conjunction with other personal identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

PRECAUTIONS AND REMEDIES

The Secret Service recommends that consumers take the following steps to protect themselves from credit card fraud and identity theft:

- Maintain a list of all credit card accounts that is not carried in a wallet or purse so that immediate notification can occur if any cards are lost or stolen;
- Avoid carrying any more credit cards in a wallet or purse than is actually needed;
- Cancel any accounts that are not in use;
- Be conscious of when billing statements should be received, and if they are not received during that window, contact the sender;
- Check credit card bills against receipts before paying them;
- Avoid using a date of birth, Social Security number, name or similar information as a password or PIN code, and change passwords at least once a year;
- Shred or burn pre-approved credit card applications, credit card receipts, bills and other financial information that you do not want to save;
- Order a credit report once a year from each of the three major credit bureaus to check for inaccuracies and fraudulent use of accounts; and
- Avoid providing any personal information over the telephone unless you initiated the call, and be aware that individuals and business contacted via the Internet may misrepresent themselves.

Should an individual become the victim of identity theft, the Secret Service recommends the following steps:

- Report the crime to the police immediately and get a copy of the police report;
- Immediately notify your credit card issuers and request replacement cards with new account numbers. Also request that the old account be processed as

“account closed at consumers’ request” for credit record purposes. Ask that a password be used before any inquiries or changes can be made on the new account. Follow up the telephone conversation with a letter summarizing your requests;

- Call the fraud units of the three credit reporting bureaus, and report the theft of your credit cards and/or numbers. Ask that your accounts be flagged, and add a victim’s statement to your report that requests that they contact you to verify future credit applications. Order copies of your credit reports so you can review them to make sure no additional fraudulent accounts have been opened in your name;
- Notify the Social Security Administration’s Office of Inspector General if your Social Security number has been used fraudulently;
- File a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT or writing to them at Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580. Their web site can also be accessed at www.ftc.gov/ftc/complaint.htm; and
- Follow up with the credit bureaus every three months for at least a year and order new copies of your reports so that you can verify that corrections have been made, and to make sure that no new fraudulent accounts have been established.

CONCLUSION

For law enforcement to properly prevent and combat identity theft, steps must be taken to ensure that local, state and Federal agencies are addressing victim concerns in a consistent manner. All levels of law enforcement should be familiar with the resources available to combat identity theft and to assist victims in rectifying damage done to their credit. It is essential that law enforcement recognize that identity theft must be combated on all fronts, from the officer who receives a victim’s complaint, to the detective or Special Agent investigating an organized identity theft ring. The Secret Service has already undertaken a number of initiatives aimed at increasing awareness and providing the training necessary to address these issues, but those of us in the law enforcement and consumer protection communities need to continue to reach out to an even larger audience. We need to continue to approach these investigations with a coordinated effort—this is central to providing a consistent level of vigilance and addressing investigations that are multi-jurisdictional while avoiding duplication of effort. The Secret Service is prepared to assist this committee in protecting and assisting the Nation’s largest growing population segment, with respect to the prevention, identification and prosecution of identity theft criminals.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions that you or other Members of the Committee may have.

Chairman GEKAS. We thank the gentleman, we turn to the next witness, Mr. Ashley.

STATEMENT OF GRANT D. ASHLEY, ASSISTANT DIRECTOR, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. ASHLEY. Thank you, Mr. Chairman and Members of the Subcommittee. The FBI, along with Federal, State, and other agencies investigates persons who assume the identities of others to carry out violations of Federal law. These crimes include bank fraud, credit card fraud, violent crimes, mail fraud, money laundering, drug trafficking, bankruptcy fraud, computer crimes, terrorism, organized crime, and fugitive cases.

These crimes, as has been previously mentioned, include the use of false identity, both at the planning of as well as carrying out and continuation of the crime.

The false identity is providing a cloak of anonymity for the offender to prepare their crime, obtaining things such as covert mail drops, residence, office space, vehicles, and such, and then, finally,

to carry on with the deception. This theft of identity or assumption of identity is not new to law enforcement. What is new is the pervasiveness through all the crimes. We are seeing it throughout most of our investigative programs in the FBI.

We do not see it as a separate and distinct crime in the FBI, but it is a component of the various investigative programs.

As has been previously mentioned, possession of a Social Security number is key to laying the groundwork for the process of taking over someone's identification and then obtaining other false documents, which can lead to drivers' licenses, loans, credit cards, and so on. It is also a crucial step in actually taking over a person's existing identity and then possibly, as has been mentioned before, depleting people's financial accounts, destroying their credit, and so on.

The FBI works very closely with other law enforcement agencies at the Federal, State, and local level to address crimes which are carried out through the use of stolen identities, as well as with the Inspector General of the Social Security Administration.

The FBI has participated in a recent identity theft sweep, which the Attorney General discussed earlier in May, as well as efforts to strengthen existing Federal laws and penalties with respect to identity theft. I believe that is in Senate bill 2541.

I was asked to provide an example of a case. Our New York division investigated the identity theft of six corporate executives, whose names were drawn from "Who's Who in America." Three of them were deceased. This case has been adjudicated. The victims were executives from Hilton, Coca-Cola, other major corporations. Essentially through an online information-broker, the offender obtained Social Security numbers and then other identification, and then made online purchases and others, using these persons' names. The total attempted amount was almost \$1 million, and I think about \$340,000 was obtained before this was shut down.

We are also seeing where people in positions of trust, both inside government and outside, are abusing their positions to access information about people that they can subsequently use for obtaining false identification. Our cyberdivision, which was recently created in our reorganization, will have a component of it that will address online identity theft issues, which will support our other investigative programs.

That concludes my remarks.

[The prepared statement of Mr. Ashley follows:]

Statement of Grant D. Ashley, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation

Good afternoon Chairmen and Members of the Subcommittees. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to the Subcommittees for affording us the opportunity to participate in this forum and to provide comment regarding preserving the integrity of Social Security numbers and preventing their misuse by terrorists and identity thieves.

As the Subcommittees are well aware, the FBI, along with other Federal law enforcement agencies, investigates individuals who use the identities of others to carry out violations of Federal criminal law. These crimes include bank fraud, credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, computer crimes, terrorism, organized crime, and fugitive cases. These crimes, carried out using a stolen identity, make the investigation of the offenses much more complicated. The use of a stolen identity enhances the chances of success in the commission of almost all financial crimes. The stolen identity provides a cloak of anonymity

for the subject while the groundwork is laid to carry out the crime. This includes the rental of mail drops, post office boxes, apartments, office space, vehicles, and storage lockers as well as the activation of pagers, cellular telephones, and various utility services.

Identity theft is not new to law enforcement. For decades fugitives have changed identities to avoid capture, and check forgers have assumed the identity of others to negotiate stolen or counterfeit checks. What is new today is the pervasiveness of the problem. The FBI does not view identity theft as a separate and distinct crime problem. Rather, it sees identity theft as a component of many types of crimes which we investigate.

The recent "sweep" of identity theft prosecutions that the Attorney General announced on May 2, 2002, reflects how widespread identity theft has become and how it is associated with a wide range of criminal activities. The sweep involved 73 criminal prosecutions against 135 individuals in 24 districts. The crimes charged in these cases involving identity theft ranged from traditional fraud to murder. In one indictment in the Northern District of Illinois, for example, the defendant, who was facing Federal counterfeiting charges, allegedly murdered a homeless man and tried to fake his own death by making it look as though the deceased victim was the defendant. Other cases involved defendants who allegedly located houses owned by elderly citizens and assumed their identities in order to fraudulently sell or refinance the properties; a defendant charged with selling Social Security numbers on eBay; and a hospital employee allegedly stole the identities of 393 hospital patients to obtain credit cards using the false identities.

This sweep, it should be noted, was the first part of a two-pronged strategy by Federal law enforcement to combat identity theft. The second prong involves efforts to strengthen existing Federal identity theft criminal statutes. Under S. 2541, which the Administration strongly supports, sentencing in a wide range of cases involving identification document fraud would be subject to a mandatory two-year enhanced penalty (over and above the sentence that would otherwise apply in a particular case). S. 2541 also would amend 18 U.S.C. 1028(b)(2) to increase the maximum imprisonment for a section 1028(a)(3) offense from three to five years, and would otherwise broaden the reach of the identity theft offense. In addition, S. 2541 specifically would allow judges the discretion to impose consecutive sentences in cases involving multiple counts of aggravated identity theft, and it authorizes the Sentencing Commission to issue guidelines and policy statements governing the exercise of such discretion. We believe that these changes, if enacted, would go a long way to strengthening the penalties that could apply when defendants are dealing in multiple identification documents.

Possession of someone else's Social Security number is key to laying the groundwork to take over someone's identity and obtain a driver's license, loans, credit cards, cars, and merchandise. It is also key to taking over an individual's existing account and wiring money from the account, charging expenses to an existing credit line, writing checks on the account or simply withdrawing money.

The FBI works closely with other law enforcement agencies at the Federal, state and local level to address crimes which are carried out through the use of stolen identities. This includes working closely with the Social Security Administration's (SSA) Office of Inspector General to confirm the authenticity (*i.e.*, the existence or non existence, of Social Security numbers being utilized by criminals).¹ Our Detroit and St. Louis offices participate in official task forces established specifically to investigate crimes involving identity theft. In Memphis and Mobile, official task forces are being created and our offices will be participating in these task forces which will specifically investigate crimes involving identity theft. Numerous field offices have task forces that investigate various financial crimes which include an element of identity theft. Other offices simply address the crimes the FBI has always investigated, but now include an element of identity theft.

A number of identity theft related problems are being seen by law enforcement that are caused by people in trusted positions within a business or government office that misuse the personal identifying information to which they have access. Additionally, people are improperly obtaining Social Security numbers without any legitimate access. Increases in security features on Social Security cards, alone, would not solve this problem as an actual card is seldom required for verifying someone's Social Security number. However, additional security and safeguards of the actual Social Security numbers could have a substantial impact.

¹In addition to the SSA's Office of Inspector General, the Federal Trade Commission and the United States Secret Service, among others, do important work in combatting identity fraud at the Federal level.

One case under investigation by one of our offices in conjunction with the U.S. Postal Inspection Service involves an individual who obtained personal identifying information such as the names, and dates of birth of attorneys in the Boston area from the Martindale-Hubbell directory of attorneys. Using this information, his co-conspirator visited the Massachusetts Bureau of Vital Records which has an open records policy and was able to obtain copies of birth certificates of his victims. According to interviews with the defendants, using the combined information, they were able to contact the Social Security Administration and obtain the victims' Social Security numbers. Once they obtained the Social Security numbers, they were able to order credit reports and look at the credit scores for these victims to determine their creditworthiness and where accounts already existed. Using this information they were able to make pretext calls to at least one bank and obtain the account number. This enabled them to wire transfer \$96,000 from one of the victim's bank accounts, half of which went to a casino and the remainder went to one of the subject's personal accounts. One of these suspects also added authorized users to the victims' credit card accounts and ordered emergency replacement cards which were sent to them by overnight delivery. At the time of arrest, this individual was found to be in possession of at least 12 different license or identification cards from three states and at least four or five credit cards, all in the names of the victims whose identity he had stolen. Although there are a number of enabling flaws in the system, including open records policies in some states, there was also an apparent lack of verification by the Social Security Administration as to whether or not the person armed with the information and requesting the Social Security number was truly the person to whom the Social Security number belonged.

One of our field offices is currently investigating a case whereby Social Security numbers for children of various ages have been sold to individuals with bad credit for future use in obtaining credit. It is unknown at this time as to how these numbers were obtained. However, individuals who obtained these numbers acted as middlemen. As part of the sale of the Social Security numbers to the actual users, they formed companies which they used to falsely report positive credit information on these Social Security numbers to the credit reporting agencies. Such information included loan payoffs and information on other fictitious credit accounts which were paid off. This information boosted the user of the number's credit history and thereby the user's credit score. Next the users applied to legitimate credit issuers, including mortgage companies and were able to obtain credit. The users were instructed they could use their true names with these Social Security numbers, but not to use any previous addresses or other information similar to their previous credit record that could cause the credit reporting agencies to possibly merge their old and new credit files. Since the victims are children and are not applying for any credit, they are not aware their Social Security numbers were used in this way. As a result, these victims are not filing any complaints with law enforcement, the credit reporting agencies or any of the defrauded creditors. When these victims later become old enough to attempt to establish credit, they will learn about this activity.

A case our New York office investigated included the use of the personal identifying information of six prominent executives, three of whom were deceased. Although this information was not received directly from the Social Security Administration, using the names of these deceased executives, this individual, who was later convicted, paid Internet information brokers to obtain these executives' Social Security numbers. After obtaining their Social Security numbers, he fraudulently obtained bank account and credit card numbers as well as other personal identifying information for these executives. He then impersonated these executives and purchased diamonds and Rolex watches over the Internet, and either wire transferred money from one of his victim's bank accounts or used one of his victim's credit card numbers. This individual had ordered approximately \$730,000 in diamonds and Rolex watches but was only able to take delivery on just over half of this merchandise. There needs to be some serious review of the availability of personal identifying information, including the Social Security number, over the Internet, especially through these types of information brokers who can provide this information for a fee.

Like some other States, Hawaii utilizes the drivers' Social Security number as its drivers license number. One significant case in our Honolulu field office, operation CARD SHARKS, was a financial institution fraud investigation that also targeted businesses dealing in the production of false identifications. Several of the subjects identified during the investigation utilized stolen Hawaii driver's licenses, including real identities and Social Security numbers to make their false identifications. These individuals then opened bank accounts under their assumed names to commit financial institution fraud. Other aspects of this investigation included subjects who utilized real names and addresses, but would make up Social Security numbers to

commit their crimes. This was a joint investigation with Federal and local law enforcement that resulted in seventeen indictments. Search warrants were executed on six different locations and all six sites had evidence of violations of Title 18, United States Code, Section 1028.

As far as terrorism matters are concerned, since December 2001, the Social Security Administration has provided prompt support to the FBI's Terrorist Financing Operations Section's initiative of identifying misuse of Social Security numbers. The FBI has been taking Social Security numbers identified through past or ongoing terrorist investigations and providing them to the Social Security Administration for verification. This multi-phase project seeks to identify potential terrorist related individuals through Social Security number misuse analysis.

Once the validity or non-validity of a Social Security number has been established, investigators look for misuse of Social Security numbers by checking immigration records, Department of Motor Vehicle records, and other military, government, and fee-based data sources. Incidents of Social Security number misuse are separated according to type and forwarded to the appropriate investigative and prospective entity for follow-up.

With assistance from the Social Security Administration, approximately 150 instances of potential Social Security number misuse have been identified. Each identified instance of potential Social Security number misuse must be resolved through field investigation. This process is continuing with ongoing investigations.

The Social Security Administration's information should have very stringent limitations placed on its access and availability to the general public. However, we must be careful not to make it more difficult for law enforcement to conduct their investigations and access this information. There appears to be a need for various businesses, including the banking community, as well as government agencies to run verifications of the legitimacy of Social Security numbers used by individuals when conducting business. However, this could be accomplished without providing broad access to the universe of Social Security numbers.

In addition to these general concerns, there are some other, more specific potential issues involving access to Social Security Administration information that I would prefer not to discuss in open session so as not inadvertently to aid potential criminals.

Mr. Chairmen and Members of the Subcommittees, that concludes my prepared remarks. I would be happy to attempt to answer your questions at this time.

Chairman GEKAS. Thank you, Mr. Ashley. We now turn to Mr. Huse, the Inspector General of Social Security.

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

Mr. HUSE. Good afternoon, Mr. Chairman, Mr. Johnson, and Members of both Subcommittees. I am pleased to be back here for the seventh time to talk about Social Security number integrity issues this year. So, I guess this is a pretty important topic.

Chairman GEKAS. You have to get it right this time.

[Laughter.]

Mr. HUSE. I will get it right this time.

[Laughter.]

Mr. HUSE. I am going to dispense with most of these oral comments because I think they've been made by others and just try to sum my testimony up into some key points.

One, I think as you heard from our Deputy Commissioner, the Social Security Administration has made an awful lot of progress since September 11 in dealing with the enumeration business process and trying to strengthen it. I have to acknowledge that.

However, there are still some things that have to be done. One of the most critical areas is the need for some legislation, and I know Chairman Shaw has his bill introduced, and that would be a big help.

The legislation we need would limit the use and display of the Social Security number already in circulation in the public and private sectors; enhance the present arsenal of criminal, civil, and administrative penalties to deter and/or punish identity thieves; and require cross-verification of Social Security numbers through both governmental and private sector systems of records to identify and address those anomalies that will come out of that process.

This is the most common-sense way and readily available way to bring back some integrity into the Social Security number without a lot of new bureaucracy. I can't urge anything more. That is what I really came to say this afternoon.

I think that there has been a significant amount of focus on these issues, but we come to a point where there is a natural dilemma that is present between the legitimate interests of law enforcement and the legitimate interests of social insurance and privacy. These all collide, and we need the Congress's help in determining how we go forward from here, while we preserve the best intentions of each of those pieces of legislative action in the past.

There is a tension there, and it can't be ignored. Some of the problems that we speak to here today come from those issues that need to be addressed.

That is the substance of why I came here this afternoon, and I would be glad to answer any questions during the question period.

[The prepared statement of Mr. Huse follows:]

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

Introduction

Good afternoon, Chairman Shaw, Chairman Gekas, Ranking Member Matsui, Ranking Member Jackson Lee, and Members of the Subcommittees on Social Security and Immigration, Border Security, and Claims. I welcome the opportunity to be here today to discuss homeland security as it relates to the integrity of the Social Security number (SSN). This is my seventh appearance before a congressional hearing this year to discuss the importance of extending protections for SSN integrity, and I cannot bring this message to Congress too often.

My testimony today follows up my June 25th testimony before Chairman Gekas, Ranking Member Jackson Lee, and Members of the Subcommittee on Immigration, Border Security, and Claims. Today I would like to examine further the role SSN fraud plays in crime and terrorist activity, and some methods by which criminal fraud is executed utilizing stolen or fraudulently-obtained SSNs.

The problem of SSN fraud as it applies to terrorist activities can be very different from using the SSN for illicit gain. Let me focus on the challenge of homeland security, because while the financial crimes involving SSN misuse are also serious, they are perhaps less deadly and yet better known to Congress. Both aspects are part of the growing phenomenon of false identity, and both call for protecting the integrity of the SSN.

Let me say at the outset that the Social Security Administration (SSA) has worked very hard in recent years and made significant progress in strengthening the defenses of the SSN, implementing important suggestions our office has made and working with us to find solutions. There is more to be done, and it includes legislative action.

Our audit and investigative work identifies three distinct approaches to SSN integrity for which legislation is critically needed. The first area is limiting the use and display of the SSN already in circulation in the public and private sectors. Second, the present arsenal of criminal, civil, and administrative penalties is clearly insufficient to deter and/or punish identity thieves. The third approach is requiring the cross-verification of SSNs through both governmental and private sector systems of records to identify and address anomalies in SSA's files, and in data bases at various levels of government and the financial sector. I will discuss these further below.

The Risk to Homeland Security

In calendar year 2000 alone, SSA issued approximately 1.2 million SSNs to non-citizens, out of some 5.5 million SSNs issued in all. A recently conducted Office of Inspector General (OIG) study indicates that 8 percent (about 96,000) of those 1.2 million SSNs were based on invalid immigration documents, which SSA processes did not detect. We have no way of determining how many SSNs have been improperly assigned to non-citizens.

The issuance of SSNs based on invalid documentation creates a homeland security risk. My office has participated in 24 airport security operations across the country with the Department of Justice (DOJ) and its Joint Terrorism Task Forces and other Federal agencies since the 9/11 terrorist attacks a year ago. The aim is to ensure that no airport employee who has misrepresented his or her SSN and identity has access to secure areas of the Nation's airports. OIG's focus in airport security operations has been SSN misuse and false statements. Hundreds of people have been arrested to date, and more importantly, have been denied access to the secure areas that represent a significant vulnerability to terrorism.

Immediately after the terrorist attack of September 11, 2001, we sought to determine if and how the hijackers might have obtained SSNs. We may never know with absolute certainty how many of the 19 hijackers of September 11th used improperly obtained SSNs, or how they obtained them. The investigation into the events of that day, and related work, revealed the importance of the SSN in any attempt at assimilation into American society. Today, it is unrealistic to believe that the SSN is simply a number for tracking workers' earnings and the payment of social insurance benefits. The SSN has become the *de facto* national identifier. Protecting the integrity of that identifier is as important to our homeland security as any border patrol or airport screening.

Let me give you an example of this threat from a case that is just completing the sentencing phase. The Anti-Terrorist Task Force arrested a naturalized American citizen who had trained with Palestinian guerrilla groups in Lebanon since he was 12 years old. He was carrying a loaded semi-automatic pistol and an assault rifle in the back seat of his car, along with four loaded 30-round magazines for the rifle and hundreds of rounds of additional ammunition. In his home were a calendar with September 11th circled in red, three different Social Security cards in his name, a false Alien Registration Card, evidence of credit card fraud and \$20,000 in cash, as well as a wood carved plaque with the name of the terrorist group " Hamas " on it. We determined he had obtained the three different SSNs from SSA by falsifying two of his three SSN applications. He had used them to get jobs as a security guard and as an employee with the multi-billion-dollar Intel Corporation, when a criminal history check would have kept him from getting either job under his true identity.

Failure to protect the integrity of the SSN has enormous financial consequences for the Government, the people, and the business community. We must protect the number that has become our national identifier and the key to social, legal, and financial assimilation in our country.

It is becoming more and more apparent that those connected with terrorism will at some point obtain SSNs. They may buy them, they may create them, or they may obtain them from SSA directly through the use of falsified immigration records. But to operate in the United States, they need those numbers, and we must take those steps necessary to ensure that those numbers do *not* come from SSA.

While SSA alone cannot solve the complicated problem of homeland security, no government agency, system or policy should be ignored. Congress and SSA, as public stewards, must continue their efforts to strengthen the systems and processes that minimize the use of SSNs for illegal purposes. SSN integrity is a link in our homeland security that must be strengthened and sustained.

Federal Interagency Coordination and Cooperation

You have asked that I comment on Federal interagency coordination and cooperation to verify identification documents and to detect and prevent fraud. We recently issued a Management Advisory Report entitled *Social Security Number Integrity: An Important Link in Homeland Security*. This report said it is critical that SSA independently verify the authenticity of the birth records with States, immigration records with Immigration and Naturalization Service (INS), as well as other identification documents presented by an applicant for an SSN.

Additionally, in other reports, we have urged full and expedited implementation of a joint Enumeration at Entry program in which the Agency would issue SSNs to non-citizens upon their entry into the United States, based on information obtained from INS and the Department of State. Until September 11th, SSA had limited success encouraging INS to move quickly on these planned initiatives.

We continue to work with other Federal officials to ensure that we are doing all that we can to assist the DOJ and others to use SSN information in the homeland security context. We are in constant contact with these Federal officials and agencies and with other committees of both houses of Congress to provide expertise and assistance in the analysis of data and the creation of legislation aimed at protecting the SSN and preventing it from being used improperly. We appreciate your interest in these issues, and your support of increasing cooperation, coordination, and information sharing between SSA and the Departments of Justice, State, and Treasury.

Legislative Proposals to Combat SSN Misuse and Protect Privacy

Let me take this opportunity to recommend some legislative proposals aimed at combating SSN misuse and protecting privacy. While no legislation can eradicate SSN misuse and identity theft altogether, the criminal penalties that exist today are clearly insufficient to either deter or punish identity thieves. Members of both houses of Congress have introduced legislation over the past several years to deal with the national dilemma presented by SSN misuse and identity theft.

The felony provisions of the Social Security Act have no civil or administrative counterparts. Federal prosecutors cannot pursue every SSN violation criminally, or even civilly. We have found the Civil Monetary Penalty program to be an effective tool in the similar area of program fraud, and could have a useful impact in the area of SSN misuse if Congress would grant us such authority. We have asked before, and I ask again—vest in us the authority to impose penalties against those who misuse SSNs.

We also believe it is time to consider enhancing the penalties for identity theft violations. Congress should also move beyond the penalties for the improper use of another person's identity to address the problem of selling SSNs and other Social Security information. We should strengthen the laws on sales and enhance the sentencing guidelines to allow us to better address this aspect of identity theft today. Congress might consider something on the order of escalating penalties, perhaps parallel to the treatment of drug cases.

Controlling SSNs in Circulation

Another area in which legislation is sorely needed is in limiting the use and display of the SSN in the public and private sectors. Although we cannot return the SSN to its simple status of a half-century ago, we must take steps to limit its use and to limit the *expansion* of its use. First and foremost, it is time to make the difficult determinations as to those uses that are appropriate and necessary, and those that are merely convenient.

One easy decision can be made now. The public display of SSNs—on identification cards, motor vehicle records, court documents, and the like—must be curtailed immediately. Those who use the SSN must share the responsibility for ensuring its integrity. We can prevent identity thieves and other criminals from walking out of a municipal courthouse with the means of committing state-facilitated identity theft. The cost to the victims of identity theft, and to all of us, is too great. And the potential for using SSNs to support acts of violence and terrorism is unthinkable.

Congress should consider requiring the cross-verification of SSNs through both governmental and private sector systems of records to identify and address anomalies in SSA's files, and in data bases at various levels of government and the financial sector. Only in such a way can we combat and limit the spread of false identification and SSN misuse. In this way can we correct errors on a timely basis that might otherwise keep workers from receiving full credit for years of labor, credit that can be nullified by simple typographical errors in submitting their data. Similarly, all law enforcement agencies should be provided the same SSN cross-verification capabilities currently granted to employers. The rewards of cross-verification can be great, and it does not require major expenditures of money or the creation of new offices or agencies. It would use data the Federal, State and local governments and the financial sector already have.

I have come before you today not only to report on what has been done so far, but also to ask that Congress instruct us on the path to follow in resolving conflicts of law and policy. We face contradictions among serious and legitimate interests regarding the sharing of information between agencies—and, indeed, often within a single agency—and privacy, and between Federal laws pertaining to immigration and our Nation's economic interests.

In this vein, I would urge Congress to examine whether sufficient authority—and, indeed, requirement—for data-sharing exists in current law. In recent months, SSA has sent about 800,000 letters to employers and some 7 million letters to workers in an attempt to clean up discrepancies created when employers submit employee names and SSNs which do not match information in SSA files. SSA provides the

Internal Revenue Service (IRS) with information on the employers with the highest volume of discrepancies, because only the IRS can levy penalties. SSA has no authority to levy penalties when employers submit invalid name and SSN combinations. SSA does not have a similar process in place to share this mismatched data with the INS. As we have learned since September 11 of last year, agencies must be able to share information that can make linkages that will help head off threats and enforce our laws. That authority must be made clear in statute.

We still need legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. If we are to head off the many crimes identity theft breeds—the fraud against public and private institutions, the ruin of people’s security, possibly even the disguising of terrorists as ordinary people—we need legislation with provisions such as:

- Restrictions on the private and governmental use of SSNs. This should include restrictions on the sale of SSNs by governmental agencies, prohibition of the display of SSNs on government checks and driver’s licenses or motor vehicle registrations, and some prohibitions of the sale, purchase, or display of the SSN in the private sector.
- Prohibitions of prison inmate access to SSNs.
- Restrictions on unfair or deceptive acts or practices, such as refusals to do business without receipt of an SSN.
- Confidential treatment of credit header information.

Two Small Changes in Existing Law Would Strengthen SSN Integrity

We have recently had several cases in which an individual with a legitimate SSN sells that SSN to a third person. The seller may or may not then go to SSA and request a replacement Social Security card. This furthers the phenomenon of false identity.

The issue is this: how can we charge the individual who sells his SSN? The identity theft statute forbids the use of *another person’s* means of identification without lawful authority. Likewise, the Social Security Act prohibits a person from presenting another person’s SSN as his or her own. It does not appear to address the situation of a person selling his or her own SSN to a third person.

We are currently researching whether there is a criminal statute such as conspiracy or aiding and abetting that may be applicable. We are also looking at whether such people may be prosecuted for making false statements if they return to SSA and request a replacement card.

Legislative action should resolve this problem. A suggested solution may be to amend section 208 of the Social Security Act, 42 U.S.C. 408, to add a subsection prohibiting the sale of an individual’s SSN by that individual. SSA assigns an individual a unique SSN to accurately track the wages and earnings of the individual. SSA regulations state that “Social Security number cards are the property of SSA and must be returned upon request.” Such language should also apply to the number itself. The SSN was not meant to be the property of the individual it identifies, and its sale by any person, including the persons identified by the number, should be made illegal.

I would mention one other problem that could be easily remedied with minor changes in the law. Current language in 18 U.S.C. § 1028 primarily addresses fraud in connection with identification documents. It has been a problem to proceed under the statute when we arrest someone with a sheet or printout of, say, 50 to 100 SSNs as these SSNs are not technically on a Social Security card. Therefore, in any amendment or new legislation put forth, I would urge you to address both the Social Security card and SSN.

SSNs, Immigrants, and the Earnings Suspense File

SSA’s Earnings Suspense File (ESF) is an indicator of the problem. The ESF is the Agency’s record of annual wage reports submitted by employers for which employee names and SSNs fail to match SSA’s records.

Most immigrants—about 75 percent—come to the United States legally, many to join close family members. However, INS estimated the illegal immigrant population reached about 5 million in 1996, not including the 3 million who were given amnesty under the Immigration Reform and Control Act of 1986. INS estimates the number of undocumented (i.e., illegal) immigrants continues to grow by about 275,000 each year.

To acquire an SSN improperly, undocumented immigrants either apply for a “legitimate” SSN using false documents, or they create or purchase a counterfeit Social Security card. Since an undocumented immigrant is not required to show a Social Security card prior to hiring, he or she may simply invent a nine-digit number.

These are all criminal acts. This SSN may be one the Agency has already assigned to another individual (stolen SSN) or one never assigned (fake SSN).

SSA acknowledges that illegal immigrants account for a significant portion of items in the ESF. Three industries—agriculture, food and beverage, and services—account for almost half the wage items in the ESF. Agriculture is the largest contributor, representing about 17 percent of all ESF items. In one study of 20 agriculture employers, we determined that 6 of every 10 wage reports submitted by these employers had incorrect names or SSNs. From 1996 through 1998, these 20 employers submitted over 150,000 wage items for which the employee's name and/or SSN did not match SSA records, representing almost \$250 million in suspended wages over the 3-year period.

A moment ago, I discussed SSA's letters to employers and workers aimed at clearing up discrepancies in the ESF. As I noted, SSA has no legal authority to levy fines and penalties against employers or employees who submit incorrect SSN information on wage reports. As provided by law, SSA must rely on the IRS to enforce penalties for inaccurate wage reporting and upon the INS to enforce immigration laws. IRS has been reluctant to apply penalties, and SSA and the INS have had limited collaboration on the issue.

Applying penalties would have a ripple effect on employers who consistently submit wage reports for employees whose names and SSNs do not match SSA's records. Although SSA is primarily interested in penalizing the most egregious employers, IRS staff expressed concern with the application of even these penalties. IRS senior staff members believe they and SSA would have a difficult time determining whether an employer exercised appropriate diligence in obtaining the necessary information from employees. We believe SSA could provide the IRS with sufficient evidence to show an employer knew or should have known its employees' SSNs were incorrect. Despite the concerns of IRS, the two agencies held discussions to explore the enforcement of an existing penalty provision (\$50 per incorrect wage report) for employers who repeatedly submit erroneous name and/or SSN information.

In calendar year 2000, based on this agreement, SSA provided a list of 100 of the most egregious employers to the IRS. These employers submitted the largest number of name/SSN match failures in consecutive years. The IRS expressed interest in the listing but, to date, has not assessed penalties.

SSA's coordination with the INS has been minimal. For example, SSA does not provide the INS a list of employers who repeatedly submit erroneous name and/or SSN information. In a previous audit report, we recommended that SSA:

- (1) collaborate with INS to develop a better understanding of the extent that immigration issues contribute to SSN misuse and growth of the ESF, and
- (2) re-evaluate its application of existing disclosure laws or seek legislative authority to remove barriers and allow SSA to share with the INS information regarding employers who chronically submitted incorrect wage reports. SSA disagreed with our recommendations and stated that its interpretation of the privacy and disclosure issues is accurately applied and continues to provide appropriate disclosure guidance within existing authority.

The intent of our recommendations was to suggest that the Agency look for avenues under current law and regulations first before seeking legislative authority. We acknowledge SSA's efforts to combat SSN misuse and reduce the ESF's growth. However, given the magnitude of SSN misuse by unauthorized non-citizens, we continue to believe SSA should take preemptive and preventive measures to ensure the SSN's integrity. We continue to believe that the sharing of such information in certain situations would stem the growth of SSN misuse for employment purposes.

The Fruits of Illegal Labors

SSA allows an individual to present evidence of a work history on a non-work SSN or as an illegal alien, and to receive credit for the work towards Old-Age, Survivors and Disability Insurance (OASDI) benefits. SSA provides these benefits to people based upon their lifetime earnings reported under a valid SSN. The number of quarters of earnings maintained on the ESF determines whether an individual has enough credits for insured status. SSA creates a work history for all individuals with a valid SSN, even when:

- those earnings are based on a non-work SSN, or
- those earnings are added later for an individual who was in the country illegally at the time of earnings but who subsequently becomes eligible for a valid SSN.

As long as an individual can prove that earnings belong to him or her, SSA will provide earnings credits to that individual. Once these earnings are recorded, these

individuals are essentially treated as any other individual applying for OASDI benefits.

One problem is the widespread use of non-work SSNs by people who work in the economy illegally. The earnings from illegal work from these people is recorded directly in the SSA claims systems for their future credit. In our September 1999 report, *Review of Controls Over Non-work Social Security Numbers (A-08-97-1002)*, we estimated that unauthorized earnings associated with non-work SSNs may have already cost SSA's trust funds \$287 million, and could cost the trust funds as much as \$63 million annually. In our report, we recommended that SSA propose legislation to prohibit the crediting of non-work earnings and related quarters of coverage for purposes of benefit entitlement.

In addition, people who are in the country illegally and working under a created SSN, or misusing someone else's SSN, can later rebuild their earnings record from wage items posted to the ESF. In such a case, an individual could work illegally in the United States for 25 years, later request and receive a valid SSN, and then ask SSA to locate those suspended earnings that SSA could not post due to an invalid name/SSN combination. Once found, SSA can reinstate these earnings to this individual's earnings record. The individual claiming the wages would only need to provide corroborating documents, such as relevant wage reports, for the period of claimed earnings. These newly posted earnings can then be used to make the individual eligible for OASDI benefits.

Our reviews of the suspended wages in the ESF suggest that illegal work is the primary cause of suspended wages. These claims represent a future obligation to the SSA that is growing at a rapid rate. Under current SSA procedures, workers who are subsequently issued a legal residency card under an amnesty or other INS procedures can subsequently recover most of these wage claims.

In addition, we do not have a good number for illegal aliens receiving work credits. We routinely identify some of them through our audits and investigations, but these are not all-encompassing. For example, in a recent report, we projected that almost 100,000 non-citizens obtained SSNs in calendar year 2000 with false documents. Approximately 42 percent of those had earnings posted to their accounts, thereby receiving work credits. Nonetheless, this figure does not take into account any future wages these 100,000 may earn. Furthermore, the 100,000 figure does not include illegal aliens using other people's SSNs for work purposes and whose earnings either end up in the ESF or incorrectly posted to the legitimate number-holders' accounts.

SSA has recently changed its policies governing the issuance of non-work SSNs so that it is likely that fewer than 30,000 non-work SSNs will be issued in 2002. However, many non-work SSNs remain in circulation. Prior to the recent curtailment, SSA had issued roughly 7.3 million non-work SSNs since 1974.

Viewed another way, although such aliens may be residing and working illegally in our country, they are doing work for pay, they are paying taxes, and they are accumulating earnings records with SSA in the same manner as legal workers. SSA's policy of allowing such workers who subsequently obtain *bona fide* SSNs to recreate their files so as to capture the fruits of their labors are drawn from the agency's mission, history, and understanding of the Social Security Act, rather than from a lack of concern for immigration law.

Here, once again, I submit that we are in need of this body's guidance to resolve a dilemma of legitimate interests. We find ourselves stuck in a quagmire of contradictory interests that has resulted in the absence of clear, controlling laws and regulations, or in the ignoring of those laws and regulations that do exist.

Conclusion

We believe SSA has a clear and important role in homeland security. We appreciate your interest in these issues, and your support of increasing cooperation, coordination, and information sharing between SSA and the Departments of Justice, State, and Treasury. We believe our earlier recommendations and legislative proposals should be considered in any future discussion on homeland security. It is also important that we be able to reduce the growth of the ESF, and I commend SSA for the efforts it has made. More needs to be done, even though the ESF problem is more a symptom of the undermining of SSN integrity rather than a cause of it. Finally, we need to change the current laws which allow illegal work to be used in obtaining Federal benefits. Ours is a Nation of laws, and those laws originate here. I ask for your help in clarifying and strengthening the laws, and toughening the penalties that are designed to improve the integrity of the SSN, which is a key component of homeland security.

Thank you.



Chairman GEKAS. We thank you, and now we turn to Mr. Reindl from New York.

**STATEMENT OF MATTHEW JAMES REINDL, OPERATOR,
STYLECRAFT INTERIORS INC., GREAT NECK, NEW YORK**

Mr. REINDL. Chairman Gekas and Members, thank you for the privilege to testify today. My name is Matthew Reindl. I operate of a small family owned woodworking factory. I am here to speak for the tens of thousands of law-abiding small-businessowners who are being adversely affected, many forced to close, because of the illegal hiring practices of some of our competitors. These unlawful employers are able to operate because of the lack of enforcement by some Federal agencies, such as INS and IRS.

On behalf of the majority of businesses who carefully comply with Federal tax and wage reporting requirements, I want applaud Commissioner Barnhart for directing the Social Security Administration to send out the much-publicized letters to employers and employees with mismatched W-2 wage items.

If a mismatch of Social Security numbers is not a typo, it means that the person has false identification. The government has no idea who this person is, where this person came from, or what the person is doing in the country. We have no way of knowing if this undocumented person is a terrorist here with the intent to harm our Nation.

In the wake of the September 11 murders, no American can oppose the Social Security Administration's need to share information with the INS. The INS needs to investigate those companies which knowingly employ illegal workers and penalize them.

I hope that President Bush will require the other Federal agencies to enforce wage and labor laws so that my company will no longer have to compete from a disadvantage. Our company is a family business formed by my grandfather in 1951. It took him 20 years from when he entered the country legally to open a wood-working factory with the money he saved.

With other legal immigrants at his side, he made the American dream happen. The factory was passed on to my father and now on to me, the third generation.

Our company has employed Turks, Armenians, Haitians, Italians, Yugoslavians, and also a Jewish Holocaust survivor from Holland. The diversity of our shop makes our conversations lively.

Many of my employees waited 5 to 7 years to enter our country legally. They did the right thing. They obeyed our laws. Now people who broke the law are keeping down their wages. They wonder why both the Federal and State governments refuse to enforce any laws when it comes to illegal immigrants.

Our company pays withholding taxes and fair wages to our workers. We pay the entire cost of health insurance. However, with increasing competition from employers using illegal aliens, I fear we will not be able to provide health insurance to our employees. In fact, I may even be forced out of business. Unfortunately, my company has to compete with employers who are paying off the books and committing workers' compensation fraud, unemployment fraud, Federal and State tax fraud, and Social Security fraud.

In my written testimony, I have created a simple illustration that compares the cost of a legitimate employer to that of a lawbreaking employer who pays \$500 per week off the books. My example shows that the labor costs for the honest, law-abiding employer are roughly 80 percent higher than for the employers hiring illegal workers.

Chairman and Members of the Subcommittee, Federal law prohibits anyone from hiring illegal aliens. Local governments, private and church organizations, are setting up so-called hiring sites so that legal and illegal immigrants can work off the books and disregard Federal and State laws. Long Island towns, such as Farmingville, Glen Cove, Freeport, Huntington, and Farmingdale, have these unorganized and organized hiring sites and many more are emerging.

Without employment or the hope of employment, illegal aliens would not be tempted to enter our country in violation of our laws. Employers need to be prosecuted for hiring illegal workers, and legal immigrant workers need to believe that all employers respect our laws.

I honestly believe that there are a growing number of businesses that hire illegal aliens. If there is no enforcement, that number will grow and grow and grow.

The Federal Government cannot allow a criminal minority of employers to profit from illegal labor practices. It undermines the founding principles of our Nation. When employers ignore immigration law, it tends to lead to other laws being broken, such as Social Security fraud, workers' compensation fraud, and income tax fraud. Because of the lax enforcement from other agencies of government, honest, law-abiding employers are being punished.

That concludes my testimony, and I look forward to your questions. Thank you.

[The prepared statement of Mr. Reindl follows:]

**Statement of Matthew James Reindl, Operator, Stylecraft Interiors Inc.,
Great Neck, New York**

Mr. Chairman and Members of the Subcommittee: I am extremely honored, and I thank you for the privilege to testify at today's hearing. My name is Matthew Reindl and I am an operator of a small family owned woodworking factory. I am not a paid lobbyist, and I do not draw a salary from any political or social advocacy group. I believe I am speaking for the tens of thousands of law abiding small business owners, who are being adversely affected, many forced to close, because of illegal hiring practices of employers.

I am thankful that President Bush has appointed someone to the Social Security Administration who has taken steps to have businesses comply with the law. On behalf of those tens of thousands of small businesses who carefully comply with Federal tax and wage reporting requirements, I want to applaud Commissioner Barnhart for directing the agency to send out the much publicized letters to employers and employees with mismatched W-2 wage items.

A mismatch of Social Security numbers could mean two things. In many cases it could be a simple typographical error. Our company is familiar with this type of error. The correct number can be resubmitted to the Social Security Administration, and the problem will be solved.

However, if it is not the case of a simple mix-up, it means that the person supplying the documents has falsified his or her identification, and neither the employer nor the government has any idea who this person is, or where this person came from or what this person is doing here in this country. We have no way of knowing if this unknown undocumented person is a terrorist here with the intent to destroy this Nation. If verifying Social Security numbers can prevent terrorism it is a necessity. In the wake of the 9/11 murders, no American can be opposed to

the Social Security Administrations need to share this information with INS. INS needs to investigate those companies which knowingly employ illegal workers and penalize them.

Our country has maintained rational laws for legal immigrants. Our immigration laws provide an organized procedure for people to enter our country legally and obtain legal employment. Our company has been employing legal immigrants with for more than fifty years. Seven of our ten current employees were legal immigrants when they joined us. In fact, our company's skilled workforce has been built by the positive effects of our immigration laws.

The Reindl Family Business

Many Americans emigrated from another country. Parents, grandparents, great grandparents made a journey for America and came for the opportunities America had to offer. My grandfather, who was a trained cabinetmaker, made that journey from Europe in 1930. Back in those days an immigrant had to be sponsored in order to enter our Nation legally, and thus he did so. He was a man that always obeyed the law and taught his family to respect the rules and laws of the country.

In 1951, 20 years after he entered this country, he was bold enough to open a woodworking factory with the money he saved through the years. With other legal immigrants at his side he made the American dream happen. Hand in hand different cultures working together to fulfill many dreams. The factory was passed onto my father and now onto me, the 3rd generation. Today as it was 50 years ago I work with American citizens and legal immigrants. Our company has employed Turks and Armenians, Jamaicans and Haitians, Italians and French, Polish and Germans, Yugoslavians and Dutch, El Salvadorians and also a Jewish holocaust survivor from Holland. The diversity of our shop makes our conversations lively. It seems like a UN assembly meeting. Our employee with the longest longevity (25 years) is a Muslim immigrant from Turkey. The company went through all the legal channels to sponsor him. In addition to him, our company has sponsored other employees throughout the years. We work hard. And no job is too demeaning for anyone, including myself. I normally work at least 60 hours a week. This is what is required to run a small business. This is the strength of America.

One thing I am grateful for is the fact that my grandfather instilled in my father excellent morals and taught him to always abide by the law. This philosophy too, was passed on to me. Our company has always paid its fair share of taxes and its fair share of salary. We do everything ethically and by the book. We also have always paid the entire cost for the employee's health benefits, years before others in our industry did. However, if illegal immigration continues to drive our selling price down, I fear we will not be able to provide health insurance to our employees in the future. In fact, I may even be forced out of business.

The following is the diversified representation of the current employees in my shop.

Ahmet	Legal immigrant now American citizen born in Turkey
Luis	Legal immigrant from Colombia
Alrick	Legal immigrant from Jamaica
Chaplin	Legal immigrant from Jamaica
John	American born citizen
Roberto	American born citizen from Puerto Rico
Borgdan	Legal immigrant from Croatia
Krzystof	Polish legal alien under 1986 amnesty
Mark Reindl	American born family member
Fred Reindl	American born father of family

Employer's Responsibility

The INS has placed the responsibility of immigration enforcement on American employers. Every employer receives a handbook for completing form I-9, and in this handbook it states:

"Employment is often the magnet that attracts persons to come to or stay in the United States illegally. The purpose of the law is to remove the magnet by requiring employers to hire only citizens and aliens who are authorized to work here."

This law requires that every newly hired employee and employer to fill out an I-9 and proper documentation must be verified by the employer. As a small business, we certainly know the requirements of the law and how to pick one from col-

umn A—OR—one from column B and one from column C. It is hard to believe that a big corporation with a professional staff cannot figure out how to fill this I-9 out.

Stylecraft Interiors Inc. complies with these Federal laws:

- Verify immigration status and complete Federal form I-9.
- Deduct Federal income tax and process W-4 forms.
- Deduct Social Security and Medicare contributions.
- Match Social Security and Medicare contributions.
- Pay Federal Unemployment Tax.

Stylecraft Interiors Inc. also complies with these New York State Laws:

- Deduct state income tax.
- Deduct Disability Insurance.
- Pay New York State Workers Compensation Insurance.
- Pay New York State Unemployment insurance tax.
- Pay New York State disability insurance.
- Fill out State form N-96-2. And send that and a copy of W-4 or equivalent to the State.

These are the labor laws that every New York State employer is required to obey. However, from the newspapers articles it is clear that a growing percentage of businesses are not complying. If laws are not enforced, even a greater number of businesses will not comply with these labor laws thus driving wages down.

If the laws, which I just mentioned, were enforced and obeyed, I believe that there **WOULD BE MUCH LESS ILLEGAL IMMIGRATION**. I know people in my community are well aware that many day workers who are illegal aliens work for employers who are paying off the books and committing workers compensation fraud, unemployment fraud, Federal and State tax fraud, and Social Security fraud.

Several years ago a hiring site emerged in Glen Cove, NY. In 1995 we lost two legal immigrant employees to this Glen Cove site. They both left our company because they made more money standing at the Glen Cove site, or street corner working off the books and not paying taxes. They told me they were clearing between \$75 to \$100 a day off the books, much more than what I could pay them after taxes. They were very happy that the local government set up a site where they would be hired illegally, and not pay into the tax system. When I asked about health insurance for their family they replied if I get sick, I go to the hospital and it is free. Organized and unorganized hiring sites are popping up on Long Island. Towns such as Farmingville, Farmingdale, Freeport and Huntington have these sites and many more are emerging. Bishop Murphy of the Roman Catholic Church has gone on record saying the Catholic Church will do everything it can to help establish day laborer sites. Local governments and Catholic Charity organizations seem eager to build them. Illegitimate contractors are not getting audited at these sites. Business owners and we the taxpayers foot the bill for our ex-employees health care. Also, the employers who hire illegal aliens are not paying into workers compensation insurance. When they get hurt, guess who pays the bill?—The law abiding business owner and taxpayer. I believe that the sole purpose of hiring sites is to try to indoctrinate the American people into believing that it is somehow legal for illegal aliens to be here and to be hired at these sites.

I believe that the endorsement of any hiring of illegal aliens is an attack on our laws and on every single law abiding employer. All it is doing is undermining the labor laws of this great country.

Economics of Illegal Labor Practices

The contractors and factory owners that disregard immigration laws and disregard labor and insurance laws result in a profitable but illegal advantage over legitimate business owners who play by the rules. I am not an accountant but I do pay bills, and our company has prepared the following breakdown for a single person with himself as a dependent. It compares the cost of a legitimate employer to that of a lawbreaking employer who pays \$500 per week off the books.

Gross pay on the books would have to be \$670 to net \$500 because:

Social Security & Medicare	\$51.26
Federal withholding	\$83.63
N.Y. State withholding	\$35.62
N.Y. State disability	\$00.60

This equals \$499 net pay.

Now the legitimate employer also has additional costs. He has to match Social Security, Medicare and pay New York State workers compensation and New York State unemployment insurance.

Social Security & Medicare	\$51.26
Workers Comp (+/-)	\$50.25
N.Y. State unemployment (+/-)	\$5.06

The legitimate employer is now paying \$776.57 a week compared to \$500 net pay "off the books." This represents a 55% higher cost to the honest law-abiding employer.

Add health insurance, which is \$77.86 a week.

And 1 week vacation and 5 holidays averages out to \$35.00 a week.

The total cost a legitimate employer would be paying to equal that \$500 net pay a week now adds up to \$889.43. This represents a 78% higher cost to the honest law-abiding employer.

The Federal Government loses \$83.63 in Federal withholding when employers pay "off the books." However, in view of the fact that current Federal accounting standards comingle Social Security & Medicare contributions into the Federal budget (not into a separate trust fund) we must add the \$51.26 employee contribution plus the \$51.26 employer contribution, totaling \$102.52 for the total Social Security & Medicare contribution. Add \$83.63 plus \$102.52 and the total cost to the Federal Government becomes \$186.15—37% of the \$500 net pay a law-abiding worker would receive.

Please note unemployment and workers compensation rates are variable. Low rates were used, and Federal unemployment contributions were not included. Also note that only 1 week vacation and 5 holidays create a very low comparison. The actual cost to a legitimate employer would probably be higher.

Due to the unscrupulous employers that hire illegal aliens I do not know if Stylecraft Interiors can continue to survive. Illegal immigration lowers my wage and that of my employees too. The legal immigrants in my shop are very aware of this. Many of my employees waited 5 to 7 years to enter our country legally. They did the right thing. They obeyed our laws, and now people who broke the law are keeping down their wages. They wonder why both our Federal and State governments refuse to enforce any laws when it comes to illegal immigrants. They ask me why people who did not wait their turn are being rewarded.

Conclusion

Without employment or the hope of employment, illegal aliens would not be tempted to enter our country in violation of our immigration laws. Employers need to be actively penalized for hiring illegal workers, and legal immigrant workers need to believe that all employers respect our laws. I honestly believe that there are a growing number of businesses that hire illegal aliens. If there is no enforcement, that number will grow and grow and grow. The Federal Government can't allow a criminal minority of employers to profit from illegal labor practices, because it undermines the founding principles of this country.

As an employer, I am pleased to know that the Social Security Administration is finally cracking down on workplace fraud.

When employers ignore immigration laws it tends to lead to other laws being broken, such as Social Security fraud, workers compensation fraud, and income tax fraud. Because of the lax enforcement from all other agencies of the government, honest employers are being punished.

Lax enforcement of immigration and labor laws penalizes all those employers that comply with Federal and State laws. Our company obeys the law and we refuse to hire illegal aliens. If my competitors are allowed to break the law, and hire low-wage illegal immigrant workers, they gain an unfair and illegal advantage over my company. My competitors will undercut my prices, and take away my business and could possibly cause me to be put out of business.

Chairman GEKAS. Thank you. We turn to the final witness, Mr. Hoofnagle.

**STATEMENT OF CHRIS JAY HOOFNAGLE, LEGISLATIVE
COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER**

Mr. HOOFNAGLE. Good afternoon. Mr. Chairman and Members of the Subcommittee, my name is Chris Hoofnagle, and I am Legislative Counsel with the Electronic Privacy Information Center (EPIC). The EPIC is a not-for-profit research center that focuses on privacy and civil liberties.

Since our founding in 1994, we have been extensively involved in the privacy of the Social Security number. Most recently, we submitted an amicus brief in *Remsburg v. Docusearch*, the Amy Boyer case.

As many of you probably remember, in that case, a young woman was stalked and killed based on information provided by a commercial Social Security number lookup company.

We believe that good privacy can make good security, and that in this area, we need to protect the Social Security number so that criminals and terrorists do not use it to attack us and our country.

The Social Security number plays an unparalleled role in the identification, authentication, and tracking of all Americans. Identity thieves know the value of a Social Security number, and that is why we believe that limiting the collection and the use of the Social Security number is critical to stemming the growing tide of identity theft.

My colleagues on this panel have outlined the extreme harm that identity theft causes. According to the Privacy Rights Clearinghouse, somewhere between 500,000 and 700,000 Americans are victimized by this crime every year. Victims often do not discover the crime has occurred until many months after their identity has been stolen. They spend many hours of their time and substantial sums of their money to fix their credit report and to expunge criminal records that might have been created in their name.

Since September 11, 2001, there has been a renewed focus on this crime, as identity theft could be used both to raise funds for and to actually commit acts of incredible destruction.

The majority of identity thieves still use low-tech methods to acquire our personal data. While there are general fears of transmitting credit card numbers and other personal information over the Internet, the biggest risk from identity theft still comes from criminals who steal our mail or sorts through our trash in order to get our personal identifiers.

Other low-tech methods to steal identifiers are also common. Employees of businesses that collect the Social Security numbers are in a unique position to obtain many personal identifiers. In my written testimony, I cite to a recent case involving a branch of Bally's Health Spa in Cambridge, Massachusetts. There an employee was caught stealing Social Security numbers to open bank accounts, possibly for the commission of terrorism.

The Bally's case raises an important point about private sector use of the Social Security number. In most cases, it is wholly unnecessary for a business to even collect the Social Security number. Collecting the Social Security number creates risk for the individual. Businesses should be encouraged to use alternative identifiers.

Discouraging the use of the Social Security number should be a primary concern of Congress, especially when one considers how the business community uses the identifier. Some businesses use the Social Security number to identify individuals while other businesses use it as a password. This means that the Social Security number is used widely as both an identifier and as an authenticator.

From a security perspective, this doesn't make sense. It is the equivalent of using the same user name and password to access your e-mail, for instance, but identity theft risks are not only created by bad business practices. Public records are increasingly playing an increasing role identity theft. As Americans have more interaction with our growing government, we leave trails of our activities in the form of public records. Court case files, marriage license, and other public records are creating a trail of our personal identifiers from cradle to grave.

It is important that Congress act now to remove the Social Security number from public records.

Two States, California and Georgia, have both recently enacted common-sense Social Security number legislation that will likely stem the tide of some identity theft.

In California, Senate bill 168 was signed into law last year. The bill prohibits public posting of the Social Security number. It also prohibits the printing of the Social Security number on an identity card. Most importantly, it prevents the mailing of an invoice or a bill to a consumer with an Social Security number on it.

In Georgia, Senate bill 475 now requires businesses to safely dispose of documents that might contain personal identifiers on it. They have to shred records, or they have to actually erase computer hard drives.

Despite these significant steps forward, we still lack comprehensive protections. We believe that H.R. 2036, the Social Security Number Privacy and Identity Theft Protection Act of 2001, which enjoys strong bipartisan support, would create a framework of protection to reduce identity theft and to protect privacy.

With that, let me conclude my remarks, as I have run out of time. Thank you.

[The prepared statement of Mr. Hoofnagle follows:]

Statement of Chris Jay Hoofnagle, Legislative Counsel, Electronic Privacy Information Center

My name is Chris Hoofnagle and I am legislative counsel with the Electronic Privacy Information Center (EPIC), a not-for-profit research organization based in Washington, D.C.

Founded in 1994, EPIC has participated in cases involving the privacy of the Social Security number (SSN) before Federal courts and, most recently, before the Supreme Court of New Hampshire.¹ EPIC has also taken a leading role in campaigns against the use of globally unique identifiers (GUIDs) involving the Intel Processor Serial Number and the Microsoft Corporation's Passport identification and authentication system.

¹*Estate of Helen Remsburg v. Docusearch, Inc., et al*, C-00-211-B (N.H. 2002). In *Remsburg*, the "Amy Boyer" case, Liam Youens was able to locate and eventually murder Amy Boyer through hiring private investigators who tracked her by her date of birth, Social Security number, and by pretexting. EPIC maintains information about the Amy Boyer case online at <http://www.epic.org/privacy/boyer/>.

I appreciate the opportunity to testify this afternoon. I will briefly summarize identity theft developments, review historical and recent attempts to regulate the use of the SSN, and make recommendations.²

The states have taken effective, common sense steps to reduce private and public-sector reliance on use of the SSN. Congress should take action now to implement these protections on a national level. Long-term approaches to the problem of privacy and identity theft need a comprehensive legislative framework of protections for individuals. Accordingly, it will be necessary for Congress to pass legislation limiting the collection and use of the SSN to mitigate risks of identity theft and the risk that terrorists will use credit or identity fraud to harm the Nation. H.R. 2036, the Social Security Number Privacy and Identity Theft Protection Act of 2001, which enjoys bipartisan support, would establish much of the framework needed to address these risks.

I. The Problem of Identity Theft is Far Reaching

Identity theft accounts for over 80 percent of Social Security number misuses reported to the Social Security Administration.³ The cost of identity theft is expected to reach eight billion dollars by the year 2005.⁴ However, this represents one tenth of a percent of the credit industry's income and only a small fraction of the amount of loss due to fraud and stolen credit cards. The average loss to the financial industry is \$17,000 per identity loss, but the loss to the victim is potentially much greater, especially because most victims do not discover the crime until many months after its occurrence.⁵

Most victims of identity theft face significant credit bills and the destruction of their credit history. The immediate consequence could be the loss of securing a job or purchasing a home, or worse.⁶ Other victims face arrest for crimes that an impersonator has committed in their name. If the arrest occurs, it may be impossible to expunge the criminal record. Identity theft has been used to obtain employment, drivers' licenses, receive government benefits, and evade criminal prosecution. Identity theft indirectly affects everyone because it causes interest rates to increase to cover the industry's losses.

Identity thieves have proven themselves to be crafty criminals. Earlier this year, Experian, one of the principal credit reporting agencies, experienced an unprecedented breach of security involving individuals' personal information. In that case, identity thieves posed as Ford Motor Credit employees to gain access to almost 13,000 credit files of wealthy individuals.⁷ In another case this year, identity thieves used stolen SSNs to engage in a series of fraudulent sales designed to strip equity from elderly homeowners in the Detroit area.⁸

But criminals do not necessarily have to be resourceful to obtain credit or identification in another person's name. The problem of identity theft has been exacerbated by the financial service industry's hunger to issue credit. Aggressive marketing of credit, including unsolicited direct mail credit advertising, gives "dumpster divers" and people with access to mailboxes opportunity to obtain credit in another's name.

Since September 11, 2001, public attention has also focused on how identity theft can facilitate terrorism or raise funds for terrorist activities. For instance, a terrorist suspect reportedly connected to the Al Qaeda network was recently charged with selling the SSNs of twenty-one people who were members of the Bally's Health Club in Cambridge, Massachusetts. The SSNs were sold in order to create false passports and credit lines for bank accounts.⁹ The situation could be avoided by not collecting the SSN and by issuing health club members alternative identifiers. If the SSN was collected in order to run a credit check, the health club could have purged the SSN after the check was complete.

² EPIC maintains an archive of information about the SSN online at <http://www.epic.org/privacy/ssn/>.

³ Analysis of Social Security Number Misuse Allegations Made to the Social Security Administration's Fraud Hotline, Management Advisory Report, SSA (Aug. 1999).

⁴ Identity Theft Complaint Data, Identity Theft Data Clearinghouse, Federal Trade Commission (2001).

⁵ Statewide Grand Jury Report: Identity Theft in Florida, Case No. SC 01-1095 (Jan. 10, 2002).

⁶ *Id.*

⁷ *Security: Hackers pose as Ford Motor Credit workers to take confidential data about wealthy individuals*, Los Angeles Times, May 17, 2002.

⁸ *Thieves Steal Homeowners' Identities and Their Equity*, New York Times, May 28, 2002.

⁹ Robert Ellis Smith, *Privacy Protects Against Terror*, Privacy Journal, Mar. 2002.

Several times this year, news reports have been published outlining theft of blank identity cards, equipment, and personal information.¹⁰ Most recently, burglars entered a Colorado DMV office, and stole all the equipment and information necessary to manufacture identity cards that include a biometric identifier.¹¹ It is clear that the burglars involved are sophisticated criminals who disabled alarms and performed two different break-ins in one week. It is unclear how the criminals will use the identification cards and equipment.

II. Congress and the Courts Have Regulated the Collection and Use of the SSN

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 risks with the use and misuse of the Social Security number. 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."¹²

In response to growing risks over the accumulation of massive amounts of personal information and the recommendations contained in the 1973 report, Congress passed the Privacy Act of 1974.¹³ Among other things, this Act makes it unlawful for a governmental agency to deny a right, benefit, or privilege merely because the individual refuses to disclose his SSN. This is a critical principle to keep in mind today because consumers in the commercial sphere often face the choice of giving up their privacy, their SSN, to obtain a service or product. The drafters of the 1974 law tried to prevent citizens from facing such unfair choices, particularly in the context of government services. But there is no reason that this principle could not apply equally to the private sector, and that was clearly the intent of the authors of the 1973 report.

Section 7 of the Privacy Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." 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 concerns in the Nation." Short of prohibiting the use of the SSN outright, the provision in the Privacy Act attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed where the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

It is certainly true that the use of the SSN has expanded significantly since the provision was adopted in 1974. This is particularly clear in the financial services sector. In an effort to learn and share financial information about Americans, companies trading in financial information are the largest private-sector users of SSNs, and it is these companies that are among the strongest opponents of SSN restrictions. For example, credit bureaus maintain over 400 million files, with information

¹⁰A series of these reports are online at <http://www.aamva.org/weekinreview/branchtheftnotices.asp>.

¹¹*A major identity crisis: Info stolen from motor vehicles offices has residents worried*, Rocky Mountain News, August 20, 2002, at http://www.rockymountainnews.com/drmn/state/article/0,1299,DRMN_21_1336085,00.html.

¹²Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens 108-35 (MIT 1973) (Social Security Number as a Standard Universal Identifier and Recommendations Regarding Use of Social Security Number).

¹³5 U.S.C. 552a. Marc Rotenberg, Privacy Law Sourcebook: United States Law, International Law, and Recent Developments (EPIC 2001).

on almost ninety percent of the American adult population. These credit bureau records are keyed to the individual SSN. Such information is freely sold and traded, virtually without legal limitations.

Outside the financial services sector, many companies require the SSN instead of assigning an alternative identifier. These requirements appear in a myriad of commercial interchanges, many of which absolutely do not require the SSN. For instance, Golden Tee, a popular golf video game, requires players to enter their SSN in order to engage in “tournament play.”¹⁴ The company could assign its own identifier for players, but instead relies upon the SSN, which puts players at risk by requiring them to further circulate personal information.

It is critical to understand that the legal protection to limit the collection and use of the SSN is still present in the Privacy Act and can be found also in recent court decisions that recognize that there is a constitutional basis to limit the collection and use of the SSN. When a Federal Appeals court was asked to consider whether the State of Virginia could compel a voter to disclose an SSN that would subsequently be published in the public voting rolls, the Court noted the growing concern about the use and misuse of the SSN, particularly with regard to financial services.¹⁵ The Fourth Circuit said:

Since the passage of the Privacy Act, an individual’s concern over his SSN’s confidentiality and misuse has become significantly more compelling. For example, armed with one’s SSN, an unscrupulous individual could obtain a person’s welfare benefits or Social Security benefits, order new checks at a new address on that person’s checking account, obtain credit cards, or even obtain the person’s paycheck. . . . Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous.¹⁶

The Court said that:

The statutes at issue compel a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote. As illustrated by the examples of the potential harm that the dissemination of an individual’s SSN can inflict, Greidinger’s decision not to provide his SSN is eminently reasonable. In other words, Greidinger’s fundamental right to vote is substantially burdened to the extent the statutes at issue permit the public disclosure of his SSN.¹⁷

The Court concluded that to the extent the Virginia voting laws, “permit the public disclosure of Greidinger’s SSN as a condition of his right to vote, it creates an intolerable burden on that right as protected by the First and Fourteenth Amendments.”¹⁸

In a second case, testing whether a state could be required to disclose the SSNs of state employees under a state open record law where there was a strong presumption in favor of disclosure, the Ohio Supreme Court held that there were privacy limitations in the Federal Constitution that weighed against disclosure of the SSN.¹⁹ The court concluded that:

We find today that the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs. Our holding is not intended to interfere with meritorious investigations conducted by the press, but instead is intended to preserve one of the fundamental principles of American constitutional law—ours is a government of limited power. We conclude that the United States Constitution forbids disclosure under the circumstances of this case. Therefore, reconciling Federal constitutional law with Ohio’s Public Records Act, we conclude that [the provision] does not mandate that the city of Akron discloses the SSNs of all of its employees upon demand.²⁰

¹⁴ Official ITS Rules, at http://www.itsgames.com/ITS/its_rules.htm.

¹⁵ *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) and brief amicus curiae for CPSR (Marc Rotenberg and David Sobel) (SSN requirement for voter registration) (lead case on privacy of Social Security number).

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Beacon Journal v. City of Akron*, 70 Ohio St. 3d 605 (Ohio 1994) and brief amicus curiae for CPSR (Marc Rotenberg and David Sobel) (SSN disclosure of city employees).

²⁰ *Id.*

In an important recent case from the U.S. Court of Appeals for the D.C. Circuit, a Court upheld the Federal Trade Commission's determination that SSNs are non-public personal information under the Gramm-Leach-Bliley Act.²¹ The Court rejected First and Fifth Amendment challenges to regulations that restricted the use of the SSN without giving the individual notice and opportunity to opt-out. Additionally, the Court upheld regulations that prohibited the reuse of SSNs that are furnished to credit reporting agencies.²²

While it is true that many companies and government agencies today use the Social Security number indiscriminately as a form of identification and authentication, it is also clear from the 1936 Act, the 1974 Privacy Act, and these three cases—*Greidinger v. Davis*, *Beacon Journal v. City of Akron*, and *Trans Union v. FTC*—that there is plenty of legislative and judicial support for limitations on the collection and use of the SSN. The question is therefore squarely presented whether the Congress will at this point in time follow in this tradition, respond to growing public concern, and establish the safeguards that are necessary to ensure that the problems associated with the use of the SSN do not increase.

III. States Have Acted to Address Privacy and Identity Theft

California and Georgia have both recently enacted legislation that will increase protections against identity theft. Recognizing that most identity theft occurs when malicious actors steal personal identifiers from invoices and solicitations from mail or waste bins, California and Georgia have enacted legislation to limit the reproduction of the SSN in the private sector. Both states have incorporated common sense protections that could be adopted at the Federal level to reduce identity theft.

In California, Senate Bill 168 was signed into law in October 2001.²³ The bill gives individuals the ability to request that a “security alert” be placed on their credit record via a toll-free phone number. The bill also enables Californians to request a “security freeze” that prevents credit agencies from releasing personal information from an individual's credit report. The bill places important restrictions on use of the SSN—public posting of a SSN and printing the SSN on an identity card or document used to obtain a product or service is prohibited. Businesses that use the SSN to identify customers, such as utility companies, will no longer be permitted to print the SSN on invoices or bills sent through the mail.

In Georgia, businesses are now required to safely dispose of records that contain personal identifiers.²⁴ Business records—including data stored on computer hard drives—must be shredded or in the case of electronic records, completely wiped clean where they contain SSNs, driver's license numbers, dates of birth, medical information, account balances, or credit limit information. The Georgia law carries penalties up to \$10,000.

IV. H.R. 2036, The Social Security Number Privacy and Identity Theft Protection Act of 2001, Is a Good Proposal

The Social Security Number Privacy and Identity Theft Protection Act of 2001, sponsored by Chairman Shaw, contains a comprehensive set of rights to protect individuals from identity theft. As of this writing, the bill enjoys the bipartisan support of 77 Representatives.

Title I establishes important protections against public-sector sale or display of SSNs. We commend the Chairman for including language in the Act that would stem the unnecessary publication of the SSN. These provisions will prohibit the display of the SSN on checks and government-issued employment cards. We also commend the Chairman for including a prohibition on disclosure of the SSN to inmates. Perhaps most importantly, the language sweeps broadly enough to prohibit the display of SSNs in public records. Increasingly, public records are a source for the collection of personal identifiers that then can be reused for any purpose. It is important now more than ever to limit the appearance of SSNs in publicly-available case files and other public records, such as marriage licenses.

Title II places needed restrictions on private sector sale of the SSN. I believe it especially important that Section 202 of the bill prohibits “coercive disclosure”—the

²¹ *Trans Union L.L.C. v. Fed. Trade Comm'n*, No. 01-5202, 2002 U.S. App. LEXIS 14321 (D.C. Cir. July 16, 2002), at <http://pacer.cadc.uscourts.gov/common/opinions/200207/01-5202a.txt>.

²² *Id.* In another recent case, the D.C. Circuit rejected a First Amendment challenge to the use of credit reports for marketing purposes. *Trans Union v. FTC*, No. 00-1141 (D.C. Cir. 2001), *cert. denied*, 536 U.S. _____ (2002).

²³ California Senate Bill 168, at http://info.sen.ca.gov/pub/bill/sen/sb_0151-0200/sb_168_bill_20010914_enrolled.html.

²⁴ Georgia Senate Bill 475, at http://www.legis.state.ga.us/Legis/2001_02/fulltext/sb475.htm; *New law takes effect to fight identity theft; Businesses face fines of up to \$10,000 for not protecting data*, Atlanta Journal-Constitution, July 4, 2002.

practice of denying a product or service when an individual refuses to give a SSN. Additionally, Section 203 would place the SSN “below the line” on credit reports. This is an important and much needed protection that would stem unregulated trafficking in SSNs.

Title II, however, suffers a weakness that needs attention: the rulemaking authority of the Department of Justice must be guided by the principle that the private sector should minimize the use of SSNs. This could be accomplished by adding another factor to the balancing test in Section 201(c) that requires the Department of Justice to consider whether an alternate identifier could be used in place of the SSN. In many circumstances, private entities could use an alternate identifier, and reduce privacy risk to individuals by stemming the circulation of the SSN.

Title III creates a framework of accountability of civil and criminal penalties for misuse of the SSN. We recommend that this provision be expanded to include a private right of action for the misuse of SSNs that provides for actual, liquidated, and punitive damages and that provides for the awarding of attorneys fees and costs to a plaintiff who has substantially prevailed in litigation. Additionally, provisions allowing attorneys general to enforce these protections should also be included. In recent years, state attorneys general have zealously pursued privacy violators; the application of their resources to identity theft prevention and privacy protection should be expressly encouraged.

I believe it is important that individuals do not assume civil or criminal liability for inadvertent disclosure of a false SSN, or for intentional disclosure of a false SSN when the individual is attempting to protect her privacy. Individuals often provide false information to businesses when attempting to protect their privacy. Section 302 would prohibit this form of “privacy self-defense.” That section prohibits the false representation of one’s Social Security number to any individual. We recommend that this section be amended to only prohibit individuals from falsifying a SSN when there is intent to commit fraud or a crime.

V. Conclusion

Without a framework of restrictions on the collection and use of the SSN and other personal identifiers, identity theft will continue to increase, endangering individuals’ privacy and perhaps the security of the Nation. 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 particularly important that such legislation not force consumers to make unfair or unreasonable choices that essentially require trading the privacy interest in the SSN for some benefit or opportunity.

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, its 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 afternoon and would be pleased to answer your questions.

Chairman GEKAS. I think we all have.

[Laughter.]

Chairman GEKAS. The Chair, in consultation with the Co-Chair here, we have decided that we will pose whatever questions we can with the remaining Members, and then ask the panel to acquiesce to written interrogatories that we my submit to them pertinent to their testimony.

Very quickly, I would like to ask Mr. Reindl if he believes that there is more to this than the failure of the INS to crack down on illegal aliens. Is the Social Security Administration also at fault, in your view?

Mr. REINDL. I think it is good that they are putting out those letters and putting people on notice if there is a mismatch. So, in a way, it is kind of helping the illegal immigration situation. So it is beneficial.

Chairman GEKAS. It is beneficial that the Social Security Administration is using that procedure.

Mr. REINDL. Right, with the INS. I think so.

Chairman GEKAS. The sharing the information.

Mr. REINDL. The sharing information is good, yes.

Chairman GEKAS. The first three witnesses, I would like to ask this question, having to do with the tamper-resistant passport, which was mentioned, and also the fact that the passport is the universal key to entry into the United States.

I remember an incident—in fact, we were briefed on it—where, in Afghanistan, our personnel found in a cave many, many different passports fraudulently produced that could have ostensibly been used for the passkey to the United States.

How would we have stopped the use of such a passport, if it were expertly, fraudulently produced? Would that have allowed a terrorist to come in and do his worst?

Ms. PHILLIPS. Well, I can say that, for instance, my office has created a database of blank foreign travel documents that are reported missing, so that they cannot be used. We share this information with INS. In fact, we put them out in the form of intelligence alerts that goes to a number of Federal agencies and State law enforcement offices, even to the military.

We also train our personnel to detect counterfeit or altered passports that people are presenting in the course of a visa application.

Chairman GEKAS. So, you are saying that the routine conduct of checking the passport would probably yield the fact that this was fraudulently produced?

Ms. PHILLIPS. Most of the foreign passports that are altered are something that we can train people to detect.

Chairman GEKAS. Do you have any comment on that?

Mr. BOND. From the Secret Service's perspective, we have noticed in the cases where we are working identity theft, where we seize an electronic piece of equipment—be it a computer, Palm Pilot, whatever; in most cases, computers—that they will have all different kinds of identities on those computers that are being counterfeited. Some of the identity is changed or altered off of originals that are stolen, and then they use those base plates, I guess, for a passport or a driver's license or a Social Security number, to then change different numbers and identification pieces of information on that document to make it look like an original document.

So, we are training our investigators in the field to take a close look at computers when they are seized. It is a partnership with law enforcement, be it at the State level, the local level, or the Federal level, to ensure that we are getting those guys that are in the process of making identification out there.

Chairman GEKAS. From the FBI, how would you assess this batch of passports found in a cave?

Mr. ASHLEY. Well, they do present a risk, obviously. It is another means for somebody to try and get into our country. We are fortunate with our joint task forces that there is presence of INS and State Department on many of them.

In my previous experience, before I reported earlier this year, I was assigned to Las Vegas as the agent in charge. We had some

issues, and the State Department personnel were very helpful in resolving those on the scene.

So, I think that while it is a problem, the agencies are working well together.

Chairman GEKAS. I begin to get the theme of what we are all hoping will be the case, a complete sharing of information, and helping one another find the culprit and produce investigations and convictions and expulsions, and so forth.

I yield back the balance of my time.

Chairman SHAW. [Presiding.] Mr. Chairman, I would yield, since we have only about 2 minutes before we are going to have to go over the Capitol in order to cast our votes.

Are there any Members who wish for me to yield to them? Mr. Hayworth?

Mr. HAYWORTH. Thank you, Mr. Chairman.

Ms. Phillips, hearing the testimony of the Deputy Commissioner who proceeded you on panel one, I have real questions about student visas and the issuance of same. Do you have any documentation on the numbers of Iraqi students who have come into this country to study?

Ms. PHILLIPS. We can tell how many visas we have issued to people who are Iraqi citizens, but we are unable to say if they have actually entered the United States or if they have entered the United States in some other manner and then gained permission from INS for student status. We could say how many people of Iraqi heritage have gotten student visas.

Mr. HAYWORTH. So, again, for the student status, we would look to the Immigration and Naturalization Service?

Ms. PHILLIPS. Right.

Mr. HAYWORTH. Okay, I thank you.

Chairman SHAW. I yield to anyone on the minority side. Mr. Becerra?

Mr. BECERRA. Quick question. Thank you, Mr. Chairman.

To Mr. Hoofnagle, the laws that you mentioned, the State laws in Georgia and California, since they have been implemented, can you tell us how they have worked? Any results yet? Have they worked well?

Mr. HOOFNAGLE. It is still too early to tell. The California law takes effect partially in 2003, and then it will take full effect in 2005. The Georgia law took effect in July of this year, and many businesses are now coming into compliance with it.

If I could use this opportunity to address Social Security number use, Representative Hayworth earlier mentioned during the previous panel that there is a problem with universities requesting Social Security numbers perhaps fraudulently. That practice could be limited. The problem we have is that many universities and other places are requiring the Social Security number as an identifier. If we can cut down on that practice, we can cut down on circulation of Social Security numbers, just how Georgia and California have.

Mr. BECERRA. Good point. Thank you very much, all of you, for your testimony.

Chairman SHAW. Ms. Jackson Lee?

Ms. JACKSON LEE. Let me thank both Chairmen for this very important hearing, and I just want to restate something—Chair-

man Shaw, I don't think you were in the room. It is that the task force is working, the combination of the State Department and I believe the FBI and others along with the INS. I want to state for the record that false passports are still being made, but the technology and the expertise is more enhanced, Mr. Chairman, inasmuch as I viewed firsthand the connection between the State Department and the INS by Chinese smugglers smuggling people into an international airport. Because of a list that was given, the passports were checked and scanned, determined to be false, and the individuals were immediately intercepted as they got off the plane.

Systems are working. We just need to improve them and, as well, to be able to provide the resources necessary.

Thank you, Mr. Chairman.

Chairman SHAW. I want to thank this very distinguished panel. I have particularly a very long question, which I will submit in writing, regarding seaport security, which is something I am very concerned about, representing two very active deepwater ports, Port of Everglades and the Port of Palm Beach, which I will submit, together with some other questions.

I want to thank you all for being here. You have added tremendously to our knowledge in trying to work through this whole situation of the fraudulent use of Social Security numbers. Both in the area of crime as well as we are finding in the area of terrorism. It is becoming a big, big problem, and it is something the Congress needs to address, and it something the administration needs to address.

We will be very busy doing so for the balance of this Congress and well into next year.

Thank you all very much for being here, and we are now adjourned.

[Whereupon, at 2:57 p.m., the hearing was adjourned.]

[Questions submitted from Chairman Shaw to the panel, and their responses follow:]

U.S. Department of State
Washington, DC 20502

1. *Mrs. Phillips' testimony stated, "One tool that will help our officers is online access to Social Security Administration records." To what degree does the Department of State's Bureau of Consular Affairs require information or other assistance from the Social Security Administration (SSA)? For example, does the Bureau of Consular Affairs currently have any automated data exchange with the SSA to facilitate confirmation of valid Social Security numbers (SSNs) and the associated identity of the person to whom the SSN was originally issued included in U.S. Passport applications? Is there information you currently need that you are not receiving or are not receiving timely from the Social Security Administration? If so, what information, and do you know the reasons for the non-receipt or the delay in receipt? What results would receiving such information or receiving such information more timely produce?*

The Department needs access to the Social Security Administration's (SSA) compilation of Social Security Numbers (SSNs), including year and state of issuance, and death records. The death records consist of 70 million names of individuals whose estates have filed for death benefits under their social security numbers. We could use these databases to verify that SSNs provided by passport applicants are valid and refer to the respective applicant, and were not issued to an individual who is deceased.

Passport Services currently has very limited electronic verification of SSNs. Our Passport Specialists use a static table populated with SSN data, including the year and State of issuance, covering the period 1951 through 1999. The Department is working with the SSA to establish an electronic link that will give us more complete access to current SSN data and to death records.

2. *Operation Tarmac has just scratched the surface of the potentially tens of thousands of illegal aliens and smaller number of U.S. citizens using false identities who hold security clearances issued by private companies under contract to municipal and government agencies. If such people represent an unacceptable risk at airports, aren't they also a risk for buildings and facilities operated by the U.S. Department of State within the United States and worldwide? What is the Department of State doing, going forward, to "clear out" these high-risk workers?"*

Perhaps the term "security clearances" used in this context, is a misnomer. "Access authorization" may be a more fitting term. It should be noted that private companies do not issue security clearances. It is standard procedure to require all contract employees be put through a vetting process, prior to granting access to the Department's facilities. This is designed to mitigate the threat of "high-risk" employees in the workplace. The vetting process is similar to the one used for determining eligibility for a secret level clearance. This includes a national Agency Name Check to verify identity, conduct criminal records inquiries, and determine hiring eligibility. Upon successful completion of the vetting process, the contract employee is granted authorization to access the Department's facilities *under escort by a direct-hire employee with Top Secret clearance*. We note that contract employees are not permitted to escort others.

Access to national security information carries further restrictions, limited on a case-by-case basis; granted only to those having a "need to know." Authorization is rescinded when the employee's duties no longer require such access. Looking to the future, the Department is proceeding with a revitalized security updating program for all employees, and recently implemented a "smart card" identification card system to provide tighter access controls.

3. *We know that identity theft is pervasive and is increasing at an exponential rate. The U.S. Passport is the only equivalent to a national identity document issued by an agency of the Federal Government. Has the State Department any initiatives under consideration to provide a "wallet sized, tamper proof" U.S. Passport equivalent to U.S. Passport holders who would be willing to pay for such an identity card?*

The Department is researching the possibility of issuing an advanced memory card to be used as a travel document that attests to U.S. citizenship and identity. Eventual implementation requires bilateral agreements with other governments willing to accept such documents. An important first step has been taken by the international community (through the International Civil Aviation Organization (ICAO)) by defining a basic "passport card" standard. However, we in the United States are focusing on technical capacity to produce such a document. We are not yet ready to engage in formal discussions with other governments as to acceptability.

The concept of a passport card has been discussed for at least 10 years, and early models of passport cards date back to the 1960's. With recent technological advances, and advances in specifications that enable the technology to be standardized, the concept of an interoperable passport card is now closer to reality.

4. *A March 2002 GAO study described a 40% increase in identity thefts reported to the Social Security hotline during a 7-month period in 2001, over the same period in 2000. Mrs. Phillips' testimony described the assistance provided by the Consular Affairs' Office of Fraud Prevention Programs to the SSA's fraud investigators. She also described assistance to the National Association of Public Health Statistics and Information Systems and Social Security Administration to automate their birth and death records. What additional resources are required from Federal Government agencies to stop the increasing levels of identity theft?*

First: Standardization of birth records and electronic access to state birth and death records. These are most important—the birth certificate is the primary document used to establish entitlement to U.S. citizenship and is easy to obtain.

Also, access to the INS' naturalization database is a resource that would benefit us immensely. Access to this database would help our passport adjudication and identity confirmation process, prevent citizenship fraud and avoid duplication of data entry and adjudicative effort by both agencies. The Bureau of Consular Affairs has opened discussions with INS on this.

Recently introduced bills in the Congress would mandate a common national format and security features for driver's licenses. The Department supports enactment of legislation to standardize U.S. driver's licenses. The driver's license is a principal form of identification that passport applicants present and is critical to our adjudication process.

5. *What should Congress consider to stop the wholesale document fraud that has made it very difficult to distinguish illegal aliens from U.S. citizens and made it easy for terrorists to obtain counterfeit documents?*

Determining an individual's identity and citizenship, whether in the context of an application for a U.S. passport or otherwise, is certainly complicated by the lack of uniformity between local governments in the creation and maintenance of vital records, and in the issuance of drivers licenses or state ID's. Nevertheless, the Department of State believes that our passport process is quite secure and that our process serves to both deter and to detect attempts to commit citizenship fraud.

Local governments should not be in the position of adjudicating an individual's citizenship. Nationality law cases can be both legally and factually complex. In a small minority of cases, even individuals born in the US may not have acquired US citizenship, or may have lost citizenship at some point in time. At present, a US passport, a Certificate of Naturalization, or a Consular report of Birth Abroad are the principal documents establishing an individual's citizenship. Because only twenty percent of US citizens have a passport, the majority of citizens never apply for any official document attesting to their citizenship.

6. *It sounds like the INS has been the only agency that has actively pursued organized criminals who manufacture counterfeit Social Security cards for "wholesale distribution." What programs has your agency initiated to combat the widespread use of counterfeit Social Security cards and false or stolen SSNs?"*

Statutory authority limits the Department's involvement, through the Bureau of Diplomatic Security (DSS), to violations pertaining to passports and visas. Fraudulent social security cards, however, can and indeed frequently do provide a nexus. Accordingly, DSS has conducted, and continues to conduct undercover operations with a view toward dismantling organizations, and apprehending individuals engaged in the production or procurement of fraudulent documentation. Indeed, the bulk of recently implemented DSS undercover operations are being conducted with the active participation of INS, USCS, DEA, state and local law enforcement entities. Recent DSS undercover operations have been successful in closing down organizations engaged in the full-scale production of fraudulent identity packages, which included birth certificates, driver's licenses, and Social Security cards, used in application for U.S. passports. Additionally, our undercover operations successfully targeted organizations that had obtained genuine U.S. passports, which were later altered for use by individuals who were not entitled to them. Further, standard procedure calls for referring developed case information to the appropriate authority whenever DSS investigations uncover criminal activity outside of its core statutes. It should be noted that fraudulently obtained Social Security cards are often used as a means of identification, along with driver's licenses, when submitting bogus passport applications (DSP-11). In block 6 of the DSP-11, the applicant is requested to write or type his/her Social Security number. Use of a fraudulent Social Security card for identification purposes or providing a false Social Security number on the DSP-11 constitutes a violation of 42 USC 408, a 5-year felony. For this reason, DS agents in the field often conduct joint investigations with Special Agents assigned to the Social Security Administration OIG.

7. *The SSA IG has emphasized the need to quickly implement the Enumeration at Entry (EAE) initiative, which will assign SSNs to certain immigrants who need one at the point they are legally admitted to the United States. Could you explain the Department of State's role in EAE? Do you think it will help prevent fraud in assigning SSNs to non-citizens? What other benefits do you think will result from EAE? SSA has been working on this initiative since 1999; what has caused the delay in implementation? What has the State Department been doing to help get this initiative under way?*

The Bureau of Consular Affairs welcomes the Social Security Administration's efforts to obtain immigrant visa records electronically to support its enumeration of newly arrived immigrants admitted for permanent residence. We have updated the software in our modernized immigrant visa system to accommodate Social Security's data needs. We just deployed a beta test of this system to Manila. After Manila, several other posts will also test it. This datasharing has three partners, the Bureau of Consular Affairs at State, the Immigration and Naturalization Service and Social Security. All parties are working together very closely. The initiative will reduce fraud in enumeration and encourage interagency cooperation in providing benefits to immigrants.

8. *We understand that the EAE initiative will assign numbers to persons legally admitted for permanent residence. Will this initiative be expanded to persons temporarily admitted to the U.S. for work purposes (e.g. seasonal workers, au pairs, and*

so forth)? If not, what would you suggest to help ensure SSNs are properly assigned to these individuals in a timely manner?

The Social Security Administration has contacted the Bureau of Consular Affairs about extending this initiative beyond immigrants to nonimmigrants, such as temporary workers or exchange visitors, who need Social Security numbers. The Bureau of Consular Affairs welcomes the idea and our Bureau and Social Security are planning to hold an interagency meeting, hosted by Social Security, on this topic before the end of October.

9. *In light of troubling reports from law enforcement at both the Federal and State level that counterfeit birth certificates and loose local control of birth and death certificates exist, what can Congress do legislatively to tighten up such lax controls and make it more difficult to counterfeit a birth certificate? What revisions and/or new laws would provide law enforcement the necessary tools needed to stop these types of crimes? What further recommendations can you provide to Congress in this area?*

The Department supports implementation of the provisions of IRAIRA '96 which established the interagency Task Force, chaired by INS, to define and publish as regulations security standards for State birth certificates. The Task Force has been slow to act.

The Department also supports the enactment of legislation that would mandate that only birth certificates issued by State authorities (as opposed to local authorities) are valid for Federal uses. We also believe that unrestricted public access to birth records via the Internet should be prohibited.

More and more local governments across the nation are establishing websites on the Internet that permit direct, unrestricted, on-line access to actual birth records.

Since the Department generally accepts certified copies of state and local U.S. birth records as primary evidence of U.S. citizenship for passport application purposes, we are very concerned about the vulnerability of vital records accessible over the Internet.

Records posted to the Internet can be accessed, downloaded, altered and/or printed out by anyone with a home computer. Individuals can match their age, gender or other facts of birth and request certified copies of genuine records from the county or state.

The National Association of Public Health Statistics and Information Systems (NAPHSIS), a locally based national association of State vital records and public health offices, has contracted with the Social Security Administration (SSA) to design the Electronic Verification of Vital Events system (EVVE), an online verification process. Short-term pilots began in August 2002. While we are enthusiastic about the EVVE process, we recognize that this is a long-term project involving non-government organizations and the fifty states, each of which has different rules as to document availability, systems development and funding. We anticipate that the project could take 10 or more years to complete, but we believe that the project could be expedited through increased Federal Government emphasis on the initiative.

10. *Terrorists exploited the weak procedures for document issuance of several States to obtain valid, but improperly issued, identity cards, which allowed them to engage in their terrorist activities on September 11, 2001. Virginia has made reforms to drivers' license procedures since then. Mrs. Phillips' testimony suggests it is still a problem in many States. How do we get other States to reform their practices to make it more difficult for terrorists to get State issued identification?*

Recent bills introduced in the Congress would mandate a common national format and security features for driver's licenses. The Department supports enactment of legislation to standardize U.S. driver's licenses. The driver's license is a principal form of identification that passport applicants present and is critical to our adjudication process.

The American Association of Motor Vehicle Administrators (AAMVA) is a voluntary, non-profit, tax exempt, educational organization. AAMVA represents the state and provincial driver license and law enforcement officials in the United States and Canada, who are responsible for administration and enforcement of laws pertaining to the motor vehicle and its use, including licensing. AAMVA encourages uniformity and reciprocity among the States and provinces, and liaison with other levels of government and the private sector. The States are generally willing to accept standardization and AAMVA is developing uniform standards, but we believe that implementation of a common national format for U.S. driver's licenses could be expedited through a Federal mandate.

11. *Federal law enforcement has informed the Congress and the public of a continuing threat from terrorists using false identities. The practices of some Federal*

agencies and many State agencies have made it relatively easy to obtain valid identity documents using counterfeit source documents. Should there be Federal laws setting minimum standards for confirming identity before issuing identity documents to reduce this vulnerability?

The Federal law defining a passport states that it is a document showing the bearer's origin, identity and nationality. The Department may not issue a passport until it is satisfied with an applicant's identity. See 8 USC 1101 (a) (30) and the supporting passport regulations, 22 CFR, Part 51. We believe at this point that the present broad cooperation among the states and Federal agencies creates the right environment for achieving the national goal of secure basic identity documents.

12. Mrs. Phillip's testimony indicated that on-line access to Social Security records will enable your agency to compare documents submitted against official data bases, and will improve the accuracy and integrity of the citizenship and identity confirmation processes. She also said that your Agency has done preliminary work with SSA and State Vital Statistics Offices toward this goal. Can you describe specifically what work has been done? Will this goal be achieved? What is your timeframe?

The Department has discussed with the Social Security Administration (SSA), the feasibility of establishing a data link that would provide the Department with access to current SSN data and death records. Both agencies have identified the fields that are available that might be used in the data exchange process to confirm identities. The next step will be to determine the feasibility of establishing a communications network between the two organizations. Systems groups from both organizations would need to be heavily involved in the development process to ensure that the final goal is achieved.

Until the data link can be established, passport specialists continue to have access to static SSN reference tables that assist in determining that SSN data provided by passport applicants is accurate. In addition, the Department recently upgraded its Photodig Travel Document Issuance System to include a new Social Security matrix that provides information that can be used to validate a Social Security number and the state and date of birth provided by the applicant.

The Department has held discussions with SSA and NAPHSIS regarding getting access to EVVE database that is currently being designed and tested to bring all State-level records of births and deaths together. Access to this database will enhance the integrity of the passport issuance process by significantly inhibiting the use of false or misappropriated supporting documents.

This is a long-term project that could take 10 or more years to complete, but we believe that the project could be expedited through increased Federal Government emphasis on the initiative.

U.S. Secret Service
Washington, DC 20223
October 31, 2002

The Honorable Clay Shaw
Chairman
Subcommittee on Social Security
House Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am writing to respond to a series of questions the Subcommittee has submitted for the record, pursuant to my testimony before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration on September 19, 2002. The subject of the hearing was "Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves". I hope the information below is useful to the Subcommittee as it further examines this important issue.

1. Sheik Mohamed Abdirahman Kariye is currently being held without bail in Portland, Oregon under charges that include false information while applying for and receiving three different Social Security cards between 1983 and 1995. Does the Secret Service request information from the Social Security Administration that would identify people who have received multiple Social Security numbers and/or who have requested/received multiple Social Security cards?

Answer: The Secret Service requests information from the Social Security Administration when there is a specific investigative need in a case involving a Secret Service core violation.

Does the Secret Service utilize "data mining" techniques to identify investigative leads for professional identity thieves and terrorists?

Answer: As part of our efforts to investigate identity theft and other financial crimes, the Secret Service does apply such techniques to data our agency receives from other sources.

Is there information you currently need that you are not receiving or are not receiving in a timely manner from the Social Security Administration?

Answer: No. The Secret Service consistently receives sufficient information in a timely manner from the Social Security Administration.

2. Operation Tarmac has just scratched the surface of the potentially tens of thousands of illegal aliens and smaller numbers of U.S. citizens using false identities who hold security clearances issued by private companies under contract to municipal and government agencies. The Secret Service is an important security element for Federal Government buildings and for key government officials. Has the Secret Service sought the assistance from Immigration and Naturalization Service (INS) and/or the Social Security Office of the Inspector General to initiate similar reviews of security clearance documents for contract employees with access to Federal buildings? If not, why?

Answer: The Secret Service is responsible for the security of the White House Complex—which includes the White House itself, the Eisenhower Executive Office Building and the Department of the Treasury—and the Naval Observatory, which serves as the residence of the Vice President. The Secret Service follows a number of well-established procedures to ensure that only appropriate individuals have access to those buildings and sites under our control.

If people who have obtained security clearances using false identity documents represent an unacceptable risk at airports, aren't they also a risk for subway systems, railroads, Federal Government offices, hazardous material sites, and government weapons laboratories and nuclear power plants?

Answer: Individuals who obtain security clearances by any type of deception are always of concern, especially when such individuals access sensitive venues. However, security clearances are typically provided by the government agency with oversight authority for a specific location. The Secret Service has no jurisdiction to implement security programs at subway systems, railroads, most Federal Government offices, hazardous material sites, weapons laboratories and nuclear plants.

Doesn't the Secret Service have a responsibility to initiate actions to "clear out" these high risk workers?

Answer: The Secret Service does not have statutory authority to initiate investigations of "high risk" workers other than those employees or contractors who may be working at Federal buildings secured by the Secret Service.

3. We know that identity theft is pervasive and is increasing at an exponential rate. In your testimony, you noted that the Administration strongly supports the provisions of S. 2541, the "Identity Theft Enhancement Act of 2002" introduced in the Senate. Will the increased penalties for identity thieves proposed in the bill be sufficient to curb this kind of crime?

Answer: The Secret Service strongly supports the enhanced penalties set forth in S. 2541. These increased penalties will not only provide the appropriate level of punishment, but also serve as an effective deterrent for those considering engaging in this form of fraud.

Are there other changes in law you would recommend?

Answer: The Secret Service supports any initiatives that will make identity theft more difficult and our personal information more secure. Specifically, we note that while section 1028 of Title 18 criminalizes the use of another individual's information to commit a crime, it does not address the sale of personal data. Currently, there are no Federal criminal statutes to address such sales by brokers who are often found in computer "chat rooms" and other similar forums.

4. What do you see as the next frontier for identity thieves, as far as emerging sources of personal information? What changes in current law could be made to cut off new avenues of information that identity thieves would use?

Answer: The continued growth of the Internet, e-commerce, and the increased connectivity between individuals, businesses, and government will only increase the

availability of personal information. We should expect that as technology continues to evolve, so will its criminal abuses. In order to preserve the security of confidential personal information, there must be incentives for private industry to take steps necessary to safeguard it.

5. A March, 2002 GAO study described a 40% increase in identity thefts reported to the Social Security hotline during a 7-month period in 2001, over the same period in 2000. Should we expect a continuation of this rate increase?

Answer: The number of cases reported is likely to continue to increase as the public becomes better educated about identity theft, and greater efforts are made to statistically document the various forms of identity theft.

6. What should Congress consider to stop wholesale document fraud that has made it very difficult to distinguish illegal aliens from U.S. citizens and made it easy for terrorists to obtain counterfeit documents?

Answer: The issue of counterfeit documents, particularly “breeder” documents such as drivers’ licenses and birth certificates, has been a growing problem within the United States. Of particular concern is the dependency of terrorist organizations on counterfeit documents, particularly travel-related documents, which are used to facilitate unimpeded travel between countries. Congress may wish to further examine potential remedies to this problem, and include in that discussion any interested law enforcement and government agencies, as well as private sector representatives, who could provide valuable insight and expertise with respect to this issue.

7. It sounds like the INS has been the only agency that has actively pursued organized criminals who manufacture counterfeit Social Security cards “wholesale.” What programs has the Secret Service initiated to combat widespread use of counterfeit Social Security cards and false or stolen SSNs?

Answer: As part of our investigative mission, the Secret Service actively investigates the manufacturing of counterfeit Social Security cards, birth certificates, driver’s licenses, employment identification cards and other counterfeit government documents. The Secret Service, both individually and with task forces throughout the country, is focused on the suppression of counterfeit identification plants.

8. Are operations similar to “Operation Tarmac: (i.e., ID checks conducted at airports) being considered at other entry points, such as seaports? To what degree are full background checks being conducted? Can you provide any particular details regarding recent arrests or investigations relative to entry points into our country? What suggestions do you have relative to the issues we are discussing today, particularly preventing SSN fraud, to help secure our seaports?

Answer: The Secret Service does not have jurisdictional authority over security at entry points and does not conduct background checks for entry points.

I hope this information is helpful to the Subcommittees. If I can answer any additional questions, or provide any further information, please do not hesitate to contact me.

Sincerely,

Robert Bond
Deputy Special Agent in Charge

Federal Bureau of Investigation
Washington, DC 20535

Question #1: Is there information you currently need that you are not receiving or are not receiving timely from the Social Security Administration? If so, what information, and do you know the reasons for the non-receipt or the delay in receipt? What results would receiving such information or receiving such information more timely produce?

Response #1

As a whole, there does not appear to be a problem for the FBI in receiving necessary information from the Social Security Administration (SSA). However, there is no way to identify whether or not on a case-by-case basis there is an existing problem. The FBI does not routinely receive fraud referrals from the SSA.

Question #2: Operation Tarmac has just scratched the surface of the potentially tens of thousands of illegal aliens and smaller numbers of U.S. citizens using false identities who hold security clearances issued by private companies under contract

to municipal and government agencies. If such people represent an unacceptable risk at airports, aren't they also a risk for subway systems, railroads, Federal Government offices, hazardous materials sites, and so on? Is the Federal Government going to take further initiatives beyond the airport investigations? Shouldn't such agencies "clear out" these high-risk workers?

Response #2

A number of FBI field offices participated in Operation Tarmac, which was an Immigration and Naturalization Service (INS) initiative mainly through government fraud task forces. Some offices have also been active in similar type operations, with the Department of Transportation and the U.S. Customs Service targeting individuals employed in the same type of capacity. In cities such as Miami, Dallas, Houston, Salt Lake City, and New York there have in the past few months been hundreds of arrests in such sweeps. History has shown the vulnerability of our airports. These sweeps were priorities due to the vast number of workers and the fact that they were either in, had unfettered access to, or controlled secured areas of the airport.

Any other immigration initiatives of this type would typically be initiated by the INS, since these matters are primarily under their jurisdiction. Such people targeted in Operation Tarmac would also be a risk if employed in subway systems, railroads, Federal Government offices, hazardous materials sites, and other such locations.

Question #3: We know that identity theft is pervasive and is increasing at an exponential rate. The Attorney General has endorsed S. 2541, introduced in the Senate. Will the increased penalties in that bill be sufficient to curb this kind of crime?

Response #3

S. 2541 would substantially increase the criminal penalties applicable to the most serious forms of identity theft, and would streamline the requirements for prosecuting Federal identity theft offenses. The actual deterrent effect of such measures can only be determined over time, but we believe that these important reforms, together with other measures designed to combat identity theft, will strengthen the ability of federal law enforcement to address this growing and serious problem.

Question #4: A March 2002 GAO study described a 40% increase in identity thefts reported to the Social Security hotline during a 7-month period in 2001, over the same period in 2000. Should we expect a continuation of this rate of increase?

Response #4

It is difficult for the FBI to predict future increases in identity theft reported to the SSA Hotline. However, without changes being made to the availability of personal identifying information and without any standardization of documents used to take over someone's identity such as birth certificates, state issued identification cards, and state issued driver's licenses, further identity theft increases are probable.

Question #5: What should the Congress consider to stop the wholesale document fraud that has made it very difficult to distinguish illegal aliens from U.S. citizens and made it easy for terrorists to obtain counterfeit documents?

Response #5

The safeguarding of personal identifying information, including Social Security Numbers, appears to be a key component in protecting one's identity from fraud. Safeguarding includes security features on actual documents as well as limitations on the sale and distribution of personal account information.

Question #6: It sounds like the INS has been the only agency that has actively pursued organized criminals who manufacture counterfeit Social Security cards for "wholesale". What programs has the FBI initiated to combat the widespread use of counterfeit Social Security cards and false or stolen SSNs?

Response #6

The FBI typically investigates fraudulent Social Security cards and the use of false or stolen Social Security Numbers in conjunction with other criminal matters, such as check fraud, credit card fraud, loan fraud, mail fraud, wire fraud, computer crimes, and terrorism matters. The FBI typically investigates organized groups involved in identity theft activities including the misuse of someone's Social Security Number.

An example of one of these cases investigated by the Detroit Division relates to five subjects who used the identity of their victims to obtain mortgages on the vic-

tims' homes, which had no liens. Over \$1.2 million was obtained by the subjects through this scheme. They used the victims' identities, including their Social Security Numbers, to complete documentation to receive these loans. At the closings, they presented counterfeit Social Security cards and fake driver's licenses to the title company representatives as identification.

Another example of an FBI investigation involved 15 subjects and over one half million dollars in fraud. These subjects used sources inside businesses, such as car rental companies and hospitals, to provide forms that had personal identifying information regarding their customers. These forms were used to extract such information, as well as to obtain the credit card number used as payment. The subjects then contacted the credit card issuer purporting to be this person. They used the information from the form to provide the Social Security Number, date of birth, and home address of their victims to confirm they were the accountholders. Then they requested to add authorized users to the accounts and get additional cards issued. The subjects then intercepted these cards, which were going to be delivered to the various victims' homes, and used them to obtain merchandise as well as cash advances.

Question #7: Are operations similar to "Operation Tarmac" (i.e., ID checks conducted at airports) being conducted at airports being considered at other entry points such as our seaports? To what degree are full background checks being conducted? Can you provide any particular details regarding recent arrests or investigations relative to entry points into our country, particularly our seaports? What suggestions do you have relative to the issues we are discussing today, particularly preventing SSN fraud, to help secure our seaports?

Response #7

As stated in question number 2, the FBI participated in Operation Tarmac, which was an INS operation as well as being actively involved in other operations regarding airport workers. However, this question would be better directed to the INS, the U.S. Customs Service, and any other agency that has jurisdiction regarding matters occurring at entry points into the United States. The FBI does not typically investigate point of entry matters but may get involved in such matters where the criminal violation is also under the FBI's jurisdiction. The U.S. Coast Guard has also played a traditional role inside the international waters contiguous to the United States.

Full background checks at the airports are conducted by the employing companies, and spot checks of these background checks have been made by FAA in past years. With the entrance of Homeland Security, and through the Transportation Security Administration, oversight of these background checks may indeed intensify. Such an intensification would appear to be in line with their regulatory oversight of transportation and transportation facilities.

Social Security Administration
Baltimore, Maryland 21235-0001
November 8, 2002

The Honorable E. Clay Shaw, Jr.
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives
Washington, D.C. 20515-0922

Dear Mr. Shaw:

In response to your letter of October 10, 2002, we submit the following answers to your questions for the record to supplement my testimony at your Subcommittees' joint hearing on Preserving the Integrity of Social Security Numbers (SSN) and Preventing Their Misuse by Terrorists and Identity Thieves held on September 19, 2002.

1. Expanding from the Operation Tarmac investigations by the Immigration and Naturalization Service (INS) with the support of other Federal agencies, there are potentially tens of thousands of illegal aliens and smaller numbers of U.S. citizens using false identities who hold security clearances issued by private companies under contract to municipal and government agencies.

a. If such people represent an unacceptable risk at airports, aren't they also a risk for subway systems, railroads, Federal Government offices, hazardous materials sites, and so on?

Yes. Such people could present risks to facilities deemed part of our nation's critical infrastructure. We recommend that the workload required to address these vulnerabilities be prioritized in accordance with the harm potential of each individual site. It is important to stratify our priorities in order to meet these challenges in a cogent manner.

b. Is the Federal Government going to take further initiatives beyond the airport investigations?

Yes. Under the auspices of many United States Attorney's Offices across the nation, we are reviewing nuclear plants, and informal discussions are underway to expand our efforts to include sites such as dams, bridges and seaports. Additionally, SSA/OIG has begun to review Federal sites which employ contract guards under the purview of the Federal Protective Service (FPS) and GSA.

c. Shouldn't it be made incumbent on such agencies to "clear out" such high-risk workers?

SSA/OIG believes that agencies should periodically review their work force to identify high-risk workers. It is the responsibility of each individual agency that employs high-risk workers at such sites to review their own personnel files and take such steps as necessary to properly screen their work force. SSA/OIG stands ready to assist these agencies in matching files and records as allowed by law.

2. We know that identity theft is pervasive and is increasing at an exponential rate. The Attorney General has endorsed legislation introduced in the Senate to increase the penalties for identity theft. Will that bill be sufficient to curb this kind of crime?

While SSA/OIG cannot state that S. 2541, the "Identity Theft Penalty Enhancement Act of 2002" will, in and of itself, be sufficient to curb identity theft, we are supportive of the legislation. In our view it builds upon and strengthens the identity theft legislation enacted in 1998 and codified at 18 U.S.C. § 1028(a)(7). We have reviewed and compared the felonies listed in the legislation with felonies which Special Agents from our Office of Investigations have used, or could use, in SSN misuse cases. Based on this review, we suggest the addition of the following four felony violations to section 1028A(c), created by S. 2541. The four sections are: (1) 18 U.S.C. § 371 (Conspiracy to commit offense or to defraud the United States); (2) 18 U.S.C. § 641 (Public money, property or records); (3) section 811 of the Social Security Act (42 U.S.C. § 1011); and, (4) section 1632 of the Social Security Act (42 U.S.C. § 1683a). We believe the addition of these four felony violations will strengthen S. 2541.

As discussed in more detail in response to the last part of question 7 and to question 9, we also recommend additional legislative initiatives we believe will help address SSN misuse and identity theft.

3. A March 2002 GAO study described a 40% increase in identity thefts reported to the Social Security hotline during a seven-month period in 2001, over the same period in 2000. Should we expect a continuation of this rate of increase?

While SSA/OIG expects the calls reporting identity theft to increase, SSA/OIG is currently taking steps to forward a significant portion of these reports directly to the Federal Trade Commission (FTC), which has been designated the national clearinghouse, in accordance with Congress' wishes. Many of these are allegations involving issues such as credit card misuse or obtaining loans, goods, and/or services not directly related to SSA's programs and operations. In this way, the callers information will be immediately available to Federal, State and local law enforcement who have access to FTC's Identity Theft database. SSA/OIG is also updating its brochure and website information to direct victims of SSN misuse to the FTC. Consequently, SSA/OIG will focus its resources on SSN misuse allegations related to SSA programs and operations.

4. What should Congress consider to stop the wholesale document fraud that has made it very difficult to distinguish illegal aliens from U.S. citizens, and made it easy for terrorists to obtain counterfeit documents?

SSA/OIG audit and investigative work has identified three distinct approaches to SSN integrity for which legislation is critically needed. The first area is limiting the use and display of the SSN already in circulation in the public and private sectors. Second, the present arsenal of criminal, civil, and administrative penalties is clearly insufficient to deter and/or punish identity thieves. The third approach is requiring the cross-verification of SSNs through both governmental and private sector systems of records to identify and address anomalies in SSA's files, and in data bases at var-

ious levels of government and the financial sector (we discuss SSN verification later in this document).

Specific needs for legislation to curtail the use of counterfeit documents include:

- Applying the Civil Money Penalty to the felony provisions of the Social Security Act in the area of SSN misuse;
- Enhancing the penalties for identity theft violations, to include selling SSNs and other Social Security information;
- Immediately curtailing the public display of SSNs on identification cards, motor vehicle records, court documents, and the like;
- Restricting private and governmental use of SSNs, including the display of SSNs on government checks and driver's licenses or motor vehicle registrations, and some prohibitions of the sale, purchase, or display of the SSN in the private sector;
- Prohibiting prison inmate access to SSNs;
- Restricting unfair or deceptive acts or practices, such as refusals to do business without receipt of an SSN; and
- Treating credit header information as confidential.

5. What programs has your office initiated to combat the widespread use of counterfeit Social Security cards and false or stolen SSNs?

SSA/OIG actively pursues cases involving the trafficking of SSNs. SSA/OIG's Office of Investigations (OI) Field Divisions regularly investigate allegations of SSN misuse related to program fraud. Furthermore, five OI Field Divisions are active Members of identity theft task forces, focusing on counterfeit documents and the trafficking of documents.

Immediately after the tragic events of September 11, 2001, we intensified our efforts to combat the enumeration of individuals who use false evidentiary documents to suborn the enumeration process. As part of these efforts, we continue our close liaison with Anti-Terrorism Task Forces around the nation. With other Federal, State and local law enforcement agencies, we continue to investigate allegations of SSN misuse that affect the Nation's critical infrastructure, such as airports.

SSA/OIG/OI personnel have been trained in the identification of fraudulent documents. We are in the process of expanding and upgrading our training efforts in the detection and identification of fraudulent documents during the enumeration process. In conjunction with regional antifraud initiatives, SSA/OIG/OI Field Divisions conduct training in an effort to assist SSA Field Office personnel in detecting false documentation.

Additionally, SSA/OIG, in partnership with SSA, has been heavily involved in several pilot projects designed to detect fraudulent documents. SSA/OIG continues to meet with SSA to enhance the Modernized Enumeration System and subsequently reduce the enumeration of individuals presenting false documents. SSA/OIG has also been instrumental in effecting a policy change mandating that all INS evidentiary documents be verified by INS, as discussed below.

Recognizing the SSN's importance in non-citizens' assimilation in U.S. society, SSA established an Enumeration Task Force in November 2001 to examine and establish policy that would strengthen SSA's procedures. As a Member of this Task Force, SSA/OIG has shared many insights and ideas with SSA, which we believe will help increase integrity of the enumeration process.

SSA/OIG's Office of Audit (OA) has issued numerous reports addressing SSN integrity. These reports included recommendations that addressed vulnerabilities in several SSA processes including assignment and issuance, employer wage reporting, and death master file reporting and issuance. SSA elected to implement many of these recommendations. Additionally, after the events of September 11, 2001, SSA revisited its position on many of our prior recommendations that it had either not yet disagreed with or implemented. In several cases, SSA decided to escalate the implementation of some recommendations, and reversed its position on others.

In our May 2002 Management Advisory Report, *Social Security Number Integrity: An Important Link in Homeland Security*, we provided insight into what more needs to be done to ensure SSN integrity in a post-September 11th environment. Our audit and investigative work has shown that there are three stages at which protections for the SSN must be put in place: upon issuance, during the life of the number holder, and upon that individual's death. To address vulnerabilities at each of these three stages, we suggested that SSA and Congress pursue the following actions: (1) independently verify birth and immigration records; (2) limit the SSN's public availability; (3) prohibit the sale and limit the display of SSNs; (4) enact strong enforcement mechanisms and stiff penalties; and (5) do more to protect the SSN after the number holder's death.

We have also reviewed SSA programs that assist employers in recognizing incorrect name and SSN combinations on their wage reports, which could include false or stolen SSNs. Our September 2002 audit *The Social Security Administration's Employee Verification Service for Registered Employers (A-03-02-22008)* evaluated the policies and procedures SSA had in place to provide information to registered users of the Employee Verification Service (EVS). The purpose of the EVS program is to ensure that employees' names and SSNs are valid before employers' wage reports are submitted to SSA. The use of EVS is voluntary, and can assist employers in eliminating common SSN reporting errors. Employers who wish to verify 51 or more SSNs at one time are encouraged to register for the EVS program. There are approximately 7,400 registered employers in the EVS program—including about 260 third-party users who submit requests on behalf of their clients.

However, while the number of employers registering with EVS has increased since 1997, less than 1 percent of all U.S. employers are registered to use the service. Furthermore, only 392 employers (5 percent of those registered) submitted data to SSA since 1999. Finally, EVS did not disclose pertinent information that could have assisted registered employers to detect potential SSN problems. Specifically, SSA did not inform employers when a submitted SSN belonged to a deceased individual. In response to our report, SSA states it planned to review the information shared with employers. In addition, SSA is piloting an online version of EVS, the Social Security Number Verification Service, which SSA hopes will increase employer usage of the SSA verification program.

6. Your office has issued several reports related to the Earnings Suspense File and cited many instances of employers and industries that continually submit erroneous wage reports.

a. Has your office initiated any investigations based on these findings?

SSA/OIG's Offices of Investigation and Audit reviewed the instances of employers and industries that submit erroneous wage reports. It is our view that under the current statutory scheme, the IRS was best equipped to address this situation and issue penalties. Therefore, we have met with IRS auditors and shared this information, while encouraging them to review IRS enforcement actions related to erroneous wage reports. In addition, it is our understanding that SSA has also shared specific problem employer information with the IRS.

b. Will your office utilize "data mining" techniques to identify employers that consistently make questionable mistakes in large numbers of wage reports?

Yes. SSA/OIG's September 1999 audit report, *Patterns of Reporting Errors and Irregularities by 100 Employers with the Most Suspended Wage Items (A-03-98-31009)*, identified those employers with the most suspended wage items from Tax Years (TY) 1993-1996. In the report, we concluded that a relatively small number of employers account for a disproportionate share of the suspended items and dollars in the ESF, which is the repository for wage items that fail to match name and SSN to SSA records. The types of reporting errors and irregularities by the Top 100 employers for the 4-year period included large numbers of: unassigned SSNs, e.g., one employer had over 6,500 unassigned SSNs; zero SSNs, e.g., one employer had 663 SSNs in which all 9 digits were '0'; consecutively numbered SSNs in which the first 6 digits were identical; and duplicate mailing addresses for 3 or more employees.

In this report, we stated that many of the wage reporting problems warranted follow-up action by SSA. Therefore, we recommended that SSA:

- develop and implement a corrective action plan for the 100 employers and continue its efforts to contact those employers responsible for large numbers of suspended wage items;
- establish preventive controls to detect wage reporting errors and irregularities;
- identify those employers who continually submit annual wage reports with large numbers and/or percentages of unassigned, identical, and/or consecutively numbered SSNs; and
- run address standardization software as soon as practical after employers submit their annual wage reports to identify employers who report the same address for many employees.

In addition, OA has recently started an audit to revisit the issues highlighted in the 1999 report. Our review will assess SSA's implementation of the recommendations made in the top 100 employers' report as well as other actions or initiatives related to employers with large numbers of suspended earnings. In addition, later

this fiscal year we plan to initiate another “data mining” audit to identify the top 100 employers with reporting irregularities during Tax Years 1997 through 2000. We also understand that the Internal Revenue Service will be reviewing employer reporting for this same 4-year period to identify non-compliant employers and determine what corrective actions are necessary—to include penalties.

c. Are there legal or policy barriers to making the names of such “scoff law” employers public?

Wage and earnings information provided by employers that is placed in SSA’s Earnings Suspense File is taxpayer return information and its disclosure is subject to 26 U.S.C. § 6103, which controls the disclosure of Internal Revenue Service data.

7. In your testimony, you ask for civil monetary penalty authority to impose penalties against those who misuse SSNs. Can you provide more details as to what authorities you are specifically looking for?

SSA/OIG is seeking authority to impose civil monetary penalties for those criminal provisions of section 208 of the Social Security Act (42 U.S.C. 408). This would include those who:

- Use a SSN obtained by false information;
- Falsely represent a SSN to be theirs;
- Knowingly alter a SSN, or intend to alter it;
- Knowingly buy or sell a card that is or purports to be a card issued by the Commissioner of Social Security;
- Counterfeit a Social Security card, or possess a counterfeit Social Security card with intent to buy or sell it;
- Disclose, use or compel the disclosure of, or knowingly purchase the SSN of any person in violation of any law of the United States; and
- Furnishes false information to the Commissioner in connection with the establishment and maintenance of the records provided for in section 205(c)(2) of the Social Security Act.

In addition, SSA/OIG is requesting civil monetary penalty authority for (1) the circumstance of an individual offering, for a fee, to assist in acquiring for another individual, an additional SSN or a number that purports to be a SSN; and, (2) violations of certain provisions of H.R. 2036.

These proposals are designed to supplement the current criminal penalties in section 208 of the Social Security Act as well as the criminal provisions in H.R. 2036.

Based on our OA audit reports regarding SSA’s Earnings Suspense File, we would also request authority to impose civil monetary penalties on employers who knowingly submit incorrect SSNs.

Since the submission of these proposals, another circumstance has arisen that we feel merits inclusion for both criminal and civil penalties. SSA/OIG Special Agents have encountered instances of individuals selling or otherwise allowing another person to use their identity for fraudulent purposes. As discussed in more detail in the last part to this question, we believe this should be prohibited.

Do such authorities lie with other agencies now?

The SSN is required by Federal law for the administration of several Federal programs, including Medicaid, Temporary Assistance for Needy Families and food stamps. It is our understanding that each of these programs provides for criminal and civil penalties for improperly receiving benefits. We would defer to the appropriate oversight agency for a complete list of applicable statutes.

In addition, from our reading of the Internal Revenue Code, it appears the IRS may impose a civil monetary penalty against an employer that files an incorrect W-2.

How would you coordinate?

In those instances where the SSN misuse occurred in the program or operation of another agency, we anticipate that we would defer to that agency. We would conduct a joint investigation with that agency should we be requested or if the circumstances warranted. This would also apply to the imposition of civil monetary penalties.

SSN misuse that ends up in SSA’s Earnings Suspense File has a direct impact on the programs and operations of SSA. We believe that we should be able to impose civil monetary penalties in these cases. We recognize the IRS has a civil penalty for employers providing incorrect information. We believe that coordination, through a Memorandum of Understanding as to who would initially proceed in these types of cases, could be entered into. However, we would defer to the direction of Congress as to which agency should have the lead.

Don't available resources limit your ability to pursue SSN misuse today?

Available resources do limit the number of SSN misuse cases SSA/OIG Special Agents can investigate and the number of audits that can be performed on SSN misuse. However, from a civil monetary penalty standpoint, currently, the biggest limitation to pursuing SSN misuse is the lack of statutory ability to impose a civil monetary penalty, not necessarily resources. Imposition of a civil monetary penalty under section 1129 of the Social Security Act is by the Office of the Chief Counsel to the Inspector General.

What additional resources would you need?

SSA/OIG is acutely aware of the problem of SSN misuse and related crimes, such as identity theft, where the SSN is a key component. We believe we have a duty to the American public to safeguard the integrity of SSN. Additionally, we, as SSA's investigative arm, have a duty to detect, investigate, and seek prosecution of crimes involving SSN misuse. Equally important is the responsibility for finding methods of preventing these crimes from occurring, through process and systems enhancements.

To address this issue, we propose establishing a core SSN Misuse Response Team. This integrated model combines the talents of our auditors, investigators, and attorneys. This team will focus its efforts on identifying patterns and trends to better target our audit work, refer cases for investigation, and liaison with other relevant public and private sector entities. Using the combined skills of its Members, the team will manage incoming allegations, and using established protocols, evaluate the investigative merit of each allegation and determine whether it should be referred to an SSA/OIG Field Division. This team will also work with the SSA/OIG Office of Audit to conduct official audits based on leads developed as a result of the team's analysis and investigations.

Additional audit resources would enable SSA/OIG to target more reviews at determining how SSA might prevent SSN misuse fraud. Reducing crimes involving SSN misuse would help SSA meet the expectations of the American public and improve the public's confidence in SSA's ability to ensure the privacy of sensitive and personal information.

The team would also act as liaison on projects and initiatives with task forces involving SSN misuse, credit bureaus, motor vehicle administrations, the Federal Trade Commission, credit card companies, and other entities. This is a comprehensive approach, yet focused enough to allow us to more effectively address this issue and provide assistance to SSA, Congress, the public, and other law enforcement.

To staff this initiative we would request the following personnel over the next 5 years. Twenty-two staff for Fiscal Years (FY) 2004, 2205 and 2006. Twenty-four staff for FYs 2007 and 2008. This would be utilized by the hiring of 88 investigative staff, 14 forensic auditors, 10 attorneys, and 2 computer specialists.

From a civil monetary penalty standpoint, we anticipate that the recommended legislation would, if enacted, generate a substantial new civil monetary penalty workload. Significant attorney resources will be required to process and evaluate such cases.

Are there provisions you would change or add in H.R. 2036?

SSA/OIG would recommend the following additions to H.R. 2036 that we believe will enhance our ability to combat SSN misuse.

- Current legislation requires that an individual needs to be in possession of five or more false identification documents before being subject to prosecution. We recommend that legislation be amended to eliminate the specific number of documents an individual needs to have in his possession before being charged.
- Current legislation does not prohibit an individual from selling his/her own identity documents. We recommend that a legislative enhancement be introduced to prohibit the sale of one's own identifiers or identification documents to another. In addition to a criminal penalty, there should also be a corresponding civil monetary penalty.
- The ability of SSA or the OIG to verify the SSN of a felony subject for Federal, State and local law enforcement officials, similar to the current process whereby SSA verifies the SSN of individuals for employers.
- Enhance penalties for violations of section 208 of the Social Security Act, 42 U.S.C. § 408. Potential structured enhancement of the punishment could be:
 - If the SSN is used to facilitate an act of terrorism—up to 25 years.
 - If the SSN is used to facilitate drug trafficking or in connection with a crime of violence—up to 20 years.

- After a prior offense under section 208, a conviction could result in up to 10 years in prison, double the current sentence.
- Leave the rest of the violations at the current punishment—up to 5 years. This would apply to those individuals who improperly receive benefits from SSA using a false SSN.
- Amend 18 U.S.C. § 641 to provide for the aggregation of individual Social Security payments improperly made to individuals.
- Law Enforcement Authority for SSA/OIG Special Agents, codifying the current Memorandum of Understanding between the Department of Justice and the SSA/OIG, with the additional ability for the Inspector General to cross-designate State and local law enforcement officials on a case by case basis.
- Authority to impose civil monetary penalties on employers who knowingly submit false SSN information on the submitted wage and earnings statements.
- Enhanced sentencing guidelines for SSA employees convicted of improperly providing SSA information or SSNs.
- Authority to disclose SSA information to law enforcement to assist in an investigation involving a serious crime.

8. In light of the widespread use of fraudulent Social Security documents, the fact they assisted the 9/11 terrorists in committing the attacks, and the exponential increase of 40% in identity theft reported to the SSA, should Congress consider giving the SSA/OIG statutory law enforcement authority?

Yes, Congress should consider giving SSA/OIG statutory law enforcement. Due to its uniqueness and prevalence in society, the SSN has become our de facto national identifier, used as a key means of identification in both the public and private sectors. Today approximately 300 million people have SSNs. Since the program began in 1936, SSA has issued approximately 390 million SSNs. Since it is so heavily relied upon as an identifier, it is a valuable commodity for criminals. It can be obtained in many ways: presenting false documentation to SSA; stealing another person's SSN; purchasing an SSN on the black market; and, simply making one up. Congress recognized the importance of the SSN in enacting the Identity Theft and Assumption Deterrence Act 1998, P.L. 105–318, by specifically listing the SSN as a “means of identification.”

From organized crime to illegal aliens, there is an ever-increasing market for SSNs. More and more, the SSN is being used for identification purposes. Based on our experience, the SSN is a prime “breeder document,” used to obtain other documents including credit cards, driver's licenses, and so forth. This can be the first step to committing crimes involving financial transactions, banking, false identities, and benefit programs. This could also allow the individual to improperly obtain benefits, items of value, conceal bad debt, avoid arrest, and if the individual is an alien, to work. Private businesses, including credit-reporting agencies, cite the value of the SSN in tracking individuals.

Because of its use as a breeder document, ensuring the integrity of the SSN has taken on added significance since September 11, 2001. SSA/OIG Special Agents have been active participants in the Department of Justice's Anti-Terrorism Task Forces throughout the country, providing valuable investigative assistance. We have played a key role in 37 airport operations around the country, targeting airport employees who misrepresent their SSN's to gain access to secure areas. To date, these operations have resulted in 741 arrests and numerous deportations. A number of other Homeland Security operations are pending.

With the importance of the SSN in identifying and eliminating potential threats to our Nation's airports, nuclear power plants and other critical sites, SSA/OIG has become a vital participant in our Nation's Homeland Security efforts. With SSA/OIG's role in identity theft and SSN misuse, as well as its interrelationship to Homeland Security efforts, it is imperative that SSA/OIG be afforded full statutory law enforcement authority.

How would your office use these new powers to combat the widespread use of counterfeit Social Security cards and false or stolen SS numbers?

Statutory law enforcement authority would reduce SSA/OIG's administrative burden and provide the most effective use of our resources. This authority would allow the Inspector General to cross-designate State and local law enforcement agents to assist OIG Special Agents in the investigation of Social Security cases, including SSN misuse. This would provide greater opportunity for additional undercover operations, identity theft task force involvement and expanded Homeland Security operations.

9. Are there additional law enforcement tools that you need in order to address document trafficking, such as increased penalties or increased information sharing?

We would recommend the enactment of the legislation listed in the last part of question 7, where we responded as to what additions we would make to H.R. 2036.

10a. Are operations similar to “Operation Tarmac” (i.e., conducting ID checks at airports) being considered at other entry points such as our seaports?

Please refer to our answers to question 1.

b. What degree is a full background check being conducted?

Since each agency conducts security background checks to the level they deem appropriate, this office does not know whether a full background check is being utilized. However, we are available to assist each agency in matching SSA records under the auspices of the DOJ or otherwise as allowed by law.

c. Can you provide any particular details regarding recent arrests or investigations relative to entry points into our country, particularly our seaports?

There have been no arrests at seaports. However, to date there have been 741 criminal arrests by SSA/OIG personnel at 37 airports. Other Federal, State and local law enforcement agencies participating in airport operations effected many more arrests, as well as INS administrative detentions.

What suggestions do you have relative to the issues we are discussing today, particularly preventing SSN fraud, to help secure our seaports?

It is our belief that the same focus and methodology used in airport operations throughout the country can also be employed at other points of entry, including seaports.

11. What are your views regarding SSA “deactivating” SSNs of certain individuals?

a. Is it possible?

b. Would it work?

Although “deactivating” SSNs is possible, it may be difficult to share this information with those who encounter these SSNs throughout the economy. SSA could place an indicator on the record of an individual with a deactivated record. For example, SSA already places indicators on an individual’s records when they have died or were issued an SSN for nonwork purposes. In addition, SSA has already established a special indicator when the Agency believes an SSN was issued based on fraudulent documents. Nonetheless, we have seen instances where this information is not being shared with the users of this information.

As discussed above, EVS allows employers to verify employees’ names and SSNs before they submit wage reports to SSA. However, very few employers actually utilize this service. For this reason, we have recommended that certain employers be mandated to use this service. In addition, EVS does not disclose pertinent information that could assist employers in detecting potential SSN problems. For example, although SSA knows an SSN belongs to a deceased individual or knows the Agency issued the number based on fraudulent documents, EVS does not provide such information to employers. As a result, employers have no way of knowing that an employee is not entitled to use the SSN.

SSA also shares the SSNs of deceased individuals in a publicly available Death Master File. Other indicators, such as deactivated SSNs, could also be shared with the public in a similar way. However, this information is sold for a fee, which could limit the number of interested users, and we do not know the full extent of its usage throughout the economy. We have also found that the Death Master File has disclosed SSN information when the SSN owner was improperly listed as deceased. As a result, SSA would need to ensure the integrity of any data shared in any similar file.

To ensure SSN integrity, we believe SSA has the responsibility to be the sole source for verifying SSN information and alerting external entities when they have information that indicates an individual may be improperly using an SSN. This responsibility supports the need for SSA to cross verify its data with other Federal, State and local authorities. However, SSA is not appropriately sharing current indicators with the public, so a new special indicator to deactivate an SSN would have to overcome these existing shortcomings. We believe SSA could improve public notification by modifying and expanding EVS and its other SSN verification services, including the online SSN Verification System pilot, the Employer 800-Number, and local field offices.

12. As discussed in the hearing, have you confirmed whether there are universities promoting the fact that they will help foreign students obtain SSNs?

No. Although we have not conducted an audit for the sole purpose of verifying this situation, previous audit work has identified situations where SSN applicants have claimed to be students authorized to work, but INS later confirmed that these individuals were not students and not authorized to work. In addition, we received an inquiry regarding a Web site instructing foreign students to go to a certain SSA field office in New York in order to be enumerated. We advised the SSA Regional Commissioner of this inquiry. In general, the schemes alluded to on the subject Web site were known to SSA. In addition, in OA's 2000 audit report on the *The Social Security Administration's Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications*, we described a large case in California in which several students of one University used false documents to obtain SSNs. The case was investigated by our Office of Investigations and it was determined that store-front ethnic language schools were involved, not legitimate universities. It was further determined that an SSA employee was involved in the improper issuance of SSNs in this case, which were then sold by a middleman. The employee in this case resigned during the investigation and the middleman has been indicted. Further judicial action is still pending in this case. Currently, we have no ongoing audit work in this area. However, we are willing to work with DOJ OIG as well as SSA and INS to determine if there is sufficient information available to conduct additional audit work in this area.

An identical letter has also been sent to George W. Gekas, Chairman, Subcommittee on Immigration, Border Security and Claims. We are also including a copy of this response on an IBM compatible 3.5-inch diskette in Microsoft Word format per your directions. If you have any questions regarding these answers, or need additional information, please contact H. Douglass Cunningham of my staff at 202-358-6319.

Sincerely,

James G. Huse, Jr.
Inspector General

Electronic Privacy Information Center
Washington, DC 20009
October 25, 2002

The Honorable E. Clay Shaw
Chairman
Subcommittee on Social Security
U.S. House of Representatives
B-316 Rayburn House Office Building
Washington, DC 20515

The Honorable George W. Gekas
Chairman
Subcommittee on Immigration, Border Security, and Claims
U.S. House of Representatives

Dear Chairmen Shaw and Gekas:

Thank you for soliciting additional information from the Electronic Privacy Information Center (EPIC) following the September 19, 2002 Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists. I am honored to have been called upon to assist the Committee on these issues.

In order to complete the hearing record, I have reprinted the questions posed below along with answers.

1. What limitations on sale, purchase, and display of SSNs do you think Congress should consider? What exceptions, if any, do you think are necessary to ensure the public can still conduct business in a reasonably efficient way, but without sacrificing their privacy and protecting their identity?

Individuals would be best protected from identity theft if serious limitations were placed on both governmental and commercial use of the SSN. It is critical that we craft legislation that encourages these entities to use alternative identifiers. Some

entities already have created alternative identifiers that are not based on the SSN for customer identification.¹

Exceptions may be made for situations where other Federal laws require the disclosure of the SSN, for instance, for the reporting of taxable income. However, there should not be blanket exemptions to protections for personal information.

If a substantial interest exists in creating an exemption for a particular use of the SSN, statutory protections for the collection and use of the SSN should be established. Under section 7 of the Privacy Act, entities that collect the SSN must give notice to the individual stating whether collection of the information is mandatory or voluntary, the statutory authority for the collection of the SSN, and the uses for which it will be employed.² A similar set of protections should be created for entities that are allowed to collect and use SSNs. This set of protections should include the ability of individuals to gain access to all records keyed by the SSN, an obligation on the data collector to securely store the SSN, limits on the use and disclosure of the SSN, and a cause of action for the individual if any of these provisions are violated.

Additionally, we recommend that where possible, exemptions for continued sale, purchase, or display of the SSN should sunset. We believe that the guiding principle of SSN protection should be one that encourages use of alternative identifiers. Sunset provisions will allow business to be conducted in a reasonably efficient way, and motivate data holders to migrate to more privacy-friendly practices.

Congress should also explore technical measures to ensure secure storage and transmission of the SSN. When the SSN must be collected and used, it should be stored in an encrypted format. In doing so, the data collector can still use the encrypted result for matching without exposing the full SSN to employees or others.

2. You mentioned the pervasiveness of use of SSNs in conducting business and the need to curb use of the SSNs. To what extent would you carryover the same concerns to use of derivatives of SSNs?

The problem with the use of “derivative” or partial SSNs is that the individual pieces may be obtained and the complete SSN then reconstructed.

Derivative use of the SSN, when done properly, presents less risk than using the entire identifier. It is important that derivative users only employ the last four digits of the SSN. Proper derivative use will reduce risk of identity theft.

I hope these answers adequately address your concerns. If I can be of further help, please do not hesitate to contact me.

Sincerely,

Chris Hoofnagle
Legislative Counsel

[Submissions for the record follow:]

Statement of the Hon. Hal Daub, Chairman, Social Security Advisory Board, and Former Member of Congress

Chairman Shaw, Chairman Gekas, Ranking Member Matsui, Ranking Member Jackson Lee, and Members of the Subcommittees. I welcome the opportunity today to share with you, for the record, the views of the Social Security Advisory Board on the importance of protecting the integrity of Social Security numbers.

Since its inception, the Advisory Board has actively examined both the authorized and unauthorized uses of Social Security numbers, weaknesses in SSA’s enumeration processes and systems, and SSA’s role in deterring identity-related crimes, illegal immigration and other security issues related to Social Security numbers. In addition, we have been keeping abreast of developments in the Congress, public sentiments, and SSA’s progress in responding to the ever-changing needs of the system.

The Board has grown increasingly concerned about rapidly growing incidences of Social Security number misuse, other identity-related crimes, fraud, and acts of terrorism that are often facilitated by the misappropriation or misuse of Social Security numbers. According to SSA’s Inspector General, the vast majority of identity crimes—most of which are financial in nature—involve the misuse of an individual’s Social Security number. But despite the seriousness with which these concerns were being debated both inside and outside of government circles *before* September 11th,

¹ Robert Ellis Smith, *Alternatives to Using Social Security Numbers in Large Organizations*, Privacy Journal, at http://www.epic.org/privacy/ssn/alternatives__ssn.html.

² 5 U.S.C. § 552a(7)(b).

2001, it was not until the recent terrorist attacks against the United States that we have seen such widespread awareness of the vulnerabilities and the weaknesses inherent in the current systems. This awareness is accompanied by an equally strong commitment to resolve unanswered questions about the appropriate roles each agency must fill in protecting the integrity of individual identity systems and safeguarding our citizens and our nation against crime and acts of terrorism.

As I indicated earlier, these debates are not new. But in light of the new urgency they have taken on since September 11th, 2001, we find ourselves at a pivotal time in our nation's history. Our civic leaders, our business leaders, our social and religious organizations, and our citizens need to join forces, share information, and come to agreement on three very important questions regarding the use of Social Security numbers as a key to validating identity. What role, if any, should the Social Security number play in terms of identity validation for purposes both inside and outside the scope of Social Security programs? What procedures and systems are needed at all levels of our society to prevent the continued misuse of identity information to facilitate acts of terror, violence, mayhem, and abuse? And what safeguards are needed to achieve our security and integrity goals, without unduly compromising individual privacy and freedom?

On many occasions over recent years, the Board has heard SSA Inspector General Jim Huse urge the agency, the Congress, the business community, and the public to come to grips with the reality that the Social Security number has become a *de facto* national identifier. Many times, we have heard Inspector General Huse say that it is too late to "put this runaway horse back in the barn". But perhaps we should not be looking to put the horse back in the barn. Perhaps, instead, we should be thinking about building a stronger fence to keep the horse from escaping the farm as well.

Slowing the Runaway Horse

The Federal Bureau of Investigation (FBI) recently recognized identity fraud as the fastest growing white-collar crime in America, making it a significant public policy issue. And, according to other recent reports from SSA's Inspector General and the FBI, improperly obtained Social Security numbers present a significant vehicle for would-be terrorists to infiltrate themselves into our society—making Social Security number abuse a national security concern as well. Likewise, the Board has heard from SSA officials and the agency's Inspector General that improper attainment or theft of Social Security numbers, including counterfeit Social Security cards, plays a major role in unauthorized work and the growing inaccuracies in wage reporting that have resulted in huge increases in SSA's earnings suspense file.

In preparation for its reports on improving service to the public and on SSA's responsibilities to safeguard the responsible collection and expenditure of the public's funds, the Board has met with SSA executives, managers and staff all over the nation. We have met with managers and staff in both headquarters and in the agency's field structure, including more than a thousand SSA field office employees who work on the front lines each day, delivering important services to the American people. We have met with representatives and staff from SSA's Office of Inspector General, the agency's Enumeration Task Force, Regional Security and Integrity Centers in both New York City and Denver, and with the new Enumeration Center established in Denver to begin developing specialized expertise on these issues within the service delivery structure. We have held public hearings all over the nation and have spoken to victims of identity theft, migrant worker groups, employers, and even the Consul General of Mexico, in our attempt to grasp the vast dimensions of these problems.

Throughout our work, we have heard one message overwhelmingly—SSA, *alone*, cannot do all that is necessary to protect our society from identity-related crimes and the other crimes that they enable. SSA must also rely on the expertise, efficiency and effectiveness of the Immigration and Naturalization Service (INS), the Department of State, the Internal Revenue Service (IRS), and law enforcement, as they carry out their own important responsibilities. We have heard, loud and clear, that it is imperative for these other agencies to do their part by delivering prompt and effective identity validation and effective enforcement of statutory work requirements—including the use of appropriate penalties and prosecution in cases where individuals, groups or employers are found to be abusing the system or perpetrating criminal acts.

Building Stronger Fences

The importance of the Social Security number and the Social Security card to the government and to any individual who wants to work or transact some other kind of business in the United States cannot be overstated. Employers are required to

ask for an individual's Social Security number before hiring, and the number is the identifier used in all claims for Social Security or SSI benefits, as well as for many other Federal and State programs, such as Medicare, Medicaid, and public assistance benefits. The IRS uses the SSN as an identifier for individual taxpayers, for identifying taxpayer dependents, and for tracking income and payroll tax contributions. Many States use it in their individual driver's license systems. Many businesses and organizations in the private sector, including banks and credit card companies, also depend on the Social Security number as an identifier for maintaining their records. The law specifically authorizes many of these uses. Additional uses have developed over time. While these additional uses may not be specifically authorized by statute, the law does not prohibit them either.

In recent testimony before the House Committee on Ways and Means, officials from the General Accounting Office (GAO) reported that many federal agencies are not taking the necessary precautions to safeguard personal information, including the Social Security number, from improper display and disclosure. GAO officials have also urged agencies to look at alternatives to using Social Security numbers as identifiers wherever this is a possibility. It is imperative that government agencies, at *all* levels of government—federal, state, and local—take the necessary steps to protect the privacy and integrity of individual identifying information. What is lacking here—according to GAO and other observers—is a uniform system of safeguards and policies about how an individual's personal information can be used, displayed or disclosed. Some agencies, businesses, organizations and even State governments have responded to these concerns responsibly—but far too many have failed to understand the importance of keeping identity information safe and ensuring the integrity of the data they maintain and disclose.

To illustrate this point, I would like to tell you about a recent interaction that the Board had with the Selective Service System. As Chairman of the Advisory Board, I contacted the Director of Selective Service to voice my concerns about the manner in which his agency captures personal information from the young men who are required by law to register. Registration forms are distributed in U.S. Postal Service offices throughout the nation. They are double-sided, tear-away "postcards" that registrants must fill out and mail back to an agency processing center. The form collects such personal identifiers as the young man's name, address, date-of-birth, Social Security number and signature. While I fully understand the need for the system to collect and maintain personal identifying information on the young men who register, the open format for supplying this information does not adequately protect its privacy. The sum total of personal data elements that are reported on this form, if misappropriated, could easily be used by unscrupulous individuals to facilitate crime, immigration fraud, and terrorism. The Office of Management and Budget approved this form for use in September 2001.

In response to the issues that I raised, the Board was told that, while the Selective Service System prefers to have men register using electronic methods, they are also given the option to register by mail. Mail-back postcards are used instead of a more secure option because it minimizes postage costs. For those young men who are concerned about the privacy of their information, the throw-away part of the form contains a suggestion that they place the registration card in an envelope before they mail it back. To me, this approach seems pennywise and pound foolish—to save a few cents on postage, are we truly willing to expect and trust that the average eighteen-year-old will recognize the importance of keeping his data secure? While the Selective Service System has agreed to move their "privacy concern" instruction to a more prominent location on the registration card itself, the Board believes that this remains an insufficient effort to protect the privacy, integrity and security of the vital information contained on this document. We believe that more responsible measures are needed to address this situation, and countless similar situations in other agencies and organizations.

For many years, Committees and Members of Congress have emphasized the importance of maintaining the integrity of the Social Security number and the Social Security card. Hearings have been held and bills have been introduced. In 1996, the Congress passed legislation requiring SSA to study the feasibility of issuing a secure Social Security card. The agency issued a report in 1997, but no action was taken. During the last session of Congress, the Chairman and Ranking Minority Member of the House Social Security Subcommittee, along with other members of Congress, introduced a bill to limit the display of the Social Security number by public and private entities, including on motor vehicle licenses and registration. It provided for making refusal to do business without receipt of an SSN an unfair or deceptive act or practice, and provided new criminal penalties for misuse of SSNs. A similar bill was reintroduced during the current session of Congress to even wider support. This

bill establishes important parameters and safeguards that apply to both government agencies and the private sector. We believe that it is a step in the right direction.

Strengthening SSA to Meet the Challenge

While SSA cannot do the job alone, and while we applaud the progress made by the agency since September 11th, 2001, further improvements in SSA's enumeration processes and systems are needed.

As the Board has documented elsewhere, many of those individuals who present themselves daily at one of SSA's over-crowded field office waiting rooms around the country have come to apply for a new or—more often—a replacement Social Security card. In fact, handling applications for new and replacement cards is the largest category of work that field offices perform. In fiscal year 2001, the agency issued 18.1 million cards, a 16 percent increase since 1997. Currently, about 32 percent of all Social Security number-related requests are for new numbers and about 68 percent are for replacement cards for people with existing numbers.

SSA's performance standards for issuing cards reflect a concern for both speed of issuance and quality. With regard to speed, the agency's statistics show that in fiscal year 2001, 96.8 percent of Social Security number applicants were advised of their assigned number within 24 hours of initial processing. Agency statistics for 2000 show that 99.8 percent of numbers were issued accurately. Nonetheless, SSA's Office of the Inspector General has expressed a high level of concern about the integrity of the agency's enumeration process and the validity of the agency's performance measurement system. It points out that given the importance of the Social Security number, many unscrupulous individuals have a strong motive for fraudulently acquiring a number and using it for illegal purposes. Problems that the OIG has identified include using an illegally obtained number to receive government services or benefits, obtain employment, or enter the country, and using another individual's number to steal their identity and commit crimes, usually financial crimes, in that person's name.

Among other concerns, the OIG has criticized the agency's procedures for validating identity documents that are used by individuals to illegally obtain cards. In 1999, PriceWaterhouseCoopers conducted an independent study that also found that SSA's front-end controls for enumeration were deficient. In one recent review the OIG conducted, it found that significant numbers of cards had been issued based on invalid or inappropriate evidentiary documents presented as evidence of age, identity, citizenship, or legal alien status. These included INS forms that were never issued, and forms that INS had issued to individuals other than the Social Security number applicants, or had issued with a different alien classification. SSA had also assigned many numbers to applicants whose U.S. birth certificates were counterfeit.

The OIG has also concluded that SSA employees in the field do not have adequate training or the tools they need to determine the validity of evidentiary documents. Some within SSA have observed, however, that SSA employees are not and should not be expected to become experts on the latest counterfeiting technologies, capable of identifying the highly sophisticated false documents that are now commonly available. The Board also has heard repeated complaints about the integrity of the enumeration process from SSA managers and employees. They believe that many of the documents they are seeing are not valid, but as one field office employee noted, the policy is that "Unless you have a specific reason to suspect the validity of a document, you should go ahead and process." A field office manager told the Board that false identity documents are easily gotten. For example, a false driver's license "can be bought down the street," and there is no cross check with the Department of Motor Vehicles. Employees in one office the Board visited observed that every office follows its own processing procedures. Some are stricter than others, and the result is that people shop around for the office that is most likely to issue a card. One SSA executive told the Board that in his area the selling of Social Security numbers is one of the agency's biggest stewardship problems. There are gangs who routinely approach SSA employees who might be vulnerable. These gangs are sophisticated in finding out about employees' personal situations and they use this information as leverage to coerce or entice employees to steal numbers or provide them with sufficient personal information from SSA's databases, information that can then be used to establish fraudulent identities. Another problem that concerns many employees is that, without a photo ID or some form of biometric identification, neither of which is required, there is no way they can be sure that individuals who come into the office are who they say they are. This is an issue that goes beyond the issuance of a number and includes individuals who claim benefits as well.

Employees in field offices have told the Board that interviews with individuals who are applying for Social Security numbers—and who want them right away—are the most contentious that they must face. There is also a concern within the

agency that more careful checking of documentation or developing a more secure card would require additional resources, which the agency does not currently have.

In March of 2002, the Board issued its report on the agency's responsibility to ensure program integrity, outlining many of the same issues addressed here today. In that report, we recommended that SSA work more aggressively with the INS and with the Department of State to resolve any outstanding loopholes or gaps in data sharing and in the identity verification process. In addition, we have recommended that SSA work more aggressively to encourage the IRS to exercise its statutory authority and begin sanctioning chronic abusers of work authorization requirements. We applaud the progress that has been made by SSA since that time. The agency has taken giant steps forward in closing many of the loopholes that we have discussed in our stewardship report and elsewhere. But, as outlined above, and as is apparent from the testimony of others here today, further efforts are needed.

SSA *does not* and *should not* work in a vacuum. The agency depends upon the support of the Administration and the Congress to provide the resources necessary for the agency to do its job and uphold its responsibilities. As we have learned from recent events in our country, it is imperative that those critical functions of the agency—including the protection of the Social Security number from misuse and abuse—be fully staffed, fully funded and provided the same level of serious consideration as other agencies that have a responsibility for protecting our security and national well-being. The Board intends to continue monitoring these critical stewardship and security issues. We look forward to working with the Congress and the Administration on these very important matters.

Statement of Witold Skwierczynski, National Council of SSA Field Operations Locals, American Federation of Government Employees, AFL-CIO, Baltimore, Maryland

Chairman Shaw, Chairman George W. Gekas, Ranking Member Matsui, Ranking Member Jackson Lee and members of the Subcommittees, I thank you for the opportunity to present this statement regarding Social Security's ability to preserve the integrity of Social Security numbers and preventing their misuse by terrorists and identity thieves.

As a representative of the AFGE Social Security General Committee and President of the National Council of SSA Field Operations Locals, I speak on behalf of approximately 50,000 Social Security Administration (SSA) employees in over 1400 facilities. These employees work in Field Offices, Offices of Hearings & Appeals, Program Service Centers, Teleservice Centers, Regional Offices of Quality Assurance, and other facilities throughout the country where retirement and disability benefit applications and appeal requests are received, processed, and reviewed.

AFGE is committed to serve, as we always have in the past, as not only the employees' advocate, but also as a watchdog for clients, taxpayers, and their elected representatives.

Let me begin by stating we agree with Chairman Gekas' comments that the privacy of the Social Security numbers of every American is under attack and that the Social Security Administration can do more to tighten up its procedures for issuing Social Security Cards to prevent fraud.

Accuracy on the part of the SSA employees processing requests for Social Security numbers is greater than those of the agency charged with safeguarding immigration records. In SSA, we process 6 million Social Security Number requests annually. According to SSA's OIG, less than 1.6% of Social Security Number requests have been issued with false INS documents. That figure was based on FY2000 statistics. However, since FY2000, SSA has implemented new systems enhancements and policies that require all INS documents of foreign-born applicants to be verified by INS before the issuance of a Social Security number. The Union believes that these measures have further safeguarded the privacy and integrity of the SSN records.

Unfortunately, SSA has also implemented initiatives that we believe are harmful to the integrity of all SSA records leaving every American vulnerable to attack by terrorists, international criminals, and an increasing number of identity thieves.

Employer Access

In May 2002, the Union became aware that the Agency implemented a program that allowed employers to gain access to SSN records of their newly hired employees via the Internet. This program has been approved by OMB for 630 major employers and may be soon expanding. According to approved procedures, SSA business partners and companies are nominated by SSA's Senior Financial Executive under the

Deputy Commissioner Finance Assessment and Management, then approved by SSA's Commissioner.

The Union believes that employer access to SSN records will result in misuse, fraud and abuse of individual privacy. On the issue of privacy, if the employer can obtain this information about an individual, anyone with an EIN may gain access to personal information. The gatekeeper of SSN records thus becomes the employer and its employees authorized access to "verify" Social Security records.

SSA has notified the Union that audits were not conducted by any private or governmental entity, i.e. SSA, OIG, or GAO, of the initial "Employer Access" pilot, prior to implementing expansion. SSA went forward with full implementation without assurances that:

- Information sought on individuals were actual employees hired by their companies,
- Employee verifications were conducted by approved employers only,
- The public's privacy was not compromised, and to determine if the integrity of SSA programs had been compromised by inappropriate or unauthorized use of this program,
- Employers accessed SSN records only for new hires rather than access to discriminate and/or violate individual privacy.
- Information obtained through this program was not relied upon to justify adverse action against a worker, which would violate State or Federal law.
- Signed statements were obtained, acknowledging there are criminal penalties for making a knowing and willful request for access to records concerning another individual under false pretences. Such abuses are considered criminal and punishable by law and carry penalties.

Additionally, the Union has learned that details needed to determine an individual's identity are not being required by SSA for these employers to obtain information about SSN records. This would include the date of birth, place of birth, mother's maiden name. Therefore, SSN records of someone with a similar or same name may be provided to the employer, making it easier for someone to use another person's SSN. Therefore, the employer would further compromise the integrity of SSN records.

SSA has developed an alert system to determine if employers may be verifying an excess of SSN records. If an employer requests verification on more than 200 percent of the number of W-2s processed in the preceding tax year, an alert will be issued. The Union strongly believes that this "alert" system is a façade to provide concerned parties with a false sense of security of individual privacy. This "system" provides a means for employers to abuse their privilege and allow the abuse to go undetected and unexposed. For example, a corporation with 100,000 employees would be able to access 200,000 SSN records of individuals for family, friends and colleagues without detection. Although SSA's own reports indicate that one employer has already exceeded its number of employees by more than 500%, SSA has failed to conduct an audit.

Furthermore, SSA has not developed or communicated a written policy to hold companies legally liable for misuse of employer access of SSN records.

It is the Union's understanding that SSA plans to expand other services and/or records to employers in the future. OMB must give approval to SSA to expand the number of employers who can gain access to SSN records. We strongly believe that Congress should urge the OMB to rescind this program to insure integrity of SSN records and individual privacy.

INS Involvement—Enumeration Centers and Enumeration at Entry

In January 2002, SSA signed an agreement with the Immigration and Naturalization Service (INS) to implement the Enumeration at Entry project. This allows INS, during the initial phase, to electronically forward to SSA enumeration data from certain aliens lawfully admitted for permanent residence. SSA will then electronically assign an SSN and issue a Social Security card to the alien.

As members of the Judiciary Committee are painfully aware, the INS has a lengthy history of being severely mismanaged. Its workers are faced with tremendous backlogs approaching 2 million applications. In January 2002, the GAO made Congress aware that immigration benefit fraud at the INS is a significant problem that threatens the integrity of the legal immigration system. INS officials believe that the problem is pervasive and serious and they also believe that some aliens are using the benefit application process to enable them to carry out illegal activities, such as crimes of violence, narcotics trafficking, and terrorism.

Until the INS and Congress can successfully address these problems, how can SSA consider allowing the INS to provide SSA with accurate, legal information to

“electronically” assign a Social Security number when the integrity of INS records cannot be maintained?

SSA now intends to implement an Enumeration Center as a pilot in the Brooklyn, NY area. This Enumeration Center will be staffed by SSA field office employees, SSA’s OIG and INS employees. SSA intends to rotate field office employees in/out of the Enumeration Center. All requests for Social Security cards will be handled at the Enumeration Center, rather than an SSA field office. This means that if someone walks into a SSA field office to apply for a SSN, the SSA employee who normally would help the applicant will have to refer him or her to the Enumeration Center for assistance. This would include referring clients who have other business at an SSA field office.

AFGE opposes Enumeration Centers. SSA’s field offices have always been full-service facilities. The taxpayer deserves full-service and one stop shopping. To refer SSN applicants to an Enumeration Center that may be miles away, will create barriers and greatly inconvenience folks who rely on public transportation or have physical disabilities. Foreign-born applicants should not have to be subjected to the intimidation of SSA–OIG and INS workers when applying for a Social Security card.

The security issues raised by SSA are unfounded. SSA employees are highly trained. Systems enhancements and new policies have virtually eliminated the unknowing acceptance of fraudulent INS documents.

To prevent highly qualified SSA employees from providing the services they were trained to do, at the convenience of the public, is a disservice. This Congress is already aware of the human capital crisis at SSA, particularly in its field offices. Detailing employees to enumeration centers is needless and not a good use of our precious resources.

Integrity of SSA Internet Services

Two months after SSA gave employers access to SSA records via the “Employer Access” program, SSA discovered weaknesses in the Internet firewalls, which compromises SSN records to hackers.

Rather than inform the public or Congress of this possible breach of privacy and possibility of identity theft, SSA posted a message that misled the public to believe that routine maintenance was the cause for SSA Internet access to be down for 3 days.

This was not a surprise to AFGE. Computer specialists had previously advised SSA that its database would be difficult, if not impossible, to protect from hackers. In spite of warnings and protests, SSA decided to move forward with its “E–Gov” goals. AFGE informed Congress of its objections to SSA’s plans to expand online services. The American public trusts SSA to guard and protect the very source of their livelihood, their Social Security numbers. AFGE strongly believes that the protection all SSA records against identity theft, fraud and misuse should be guaranteed and never compromised. Now, when identity theft poses its greatest threat to our nation in the way of terrorism and criminal acts, SSA’s records need to be more secure than ever. Instead, SSA is taking actions that we strongly believe will ultimately be harmful to the integrity of all SSA records.

We urge your Committees to consider the following:

- At a minimum, request GAO to audit SSA Employer Access initiative to insure the proper access of SSA records.
- Urge SSA to cease and desist giving access of SSA records to third party entities (governmental and private).
- Request GAO to assess and/or audit the SSA Internet firewall protections of all SSA records.
- Urge SSA to rescind it plans to create SSA/INS Enumeration Centers and direct SSA to seek Congressional approval for the creation of such a flawed bureaucracy, which will only serve to undermine SSA’s public service and the integrity of its records.

I thank you for your time and your consideration of our concerns.

American Immigration Lawyers Association
Washington, DC 20004

The Honorable E. Clay Shaw, Jr.
Chairman, House Social Security Subcommittee
B-316 Rayburn House Office Building
Washington, DC 20515-6353

The Honorable George Gekas
Chairman, House Immigration, Border Control and Claims Subcommittee
B-370B Rayburn House Office Building
Washington, DC 20515-6353

The American Immigration Lawyers Association (AILA) thanks the committees for the opportunity to submit our comments on the September 19, 2002 joint hearing on Preserving the Integrity of the Social Security Number and Preventing Misuse by Terrorists and Identity Thieves. AILA supports taking constructive steps to ensure that identifying documents, such as the social security card, are not subject to fraud and misuse. AILA urges the committees to consider how positive reforms to our immigration laws can help achieve this goal.

The testimony seemed to indicate that a large number of the employees who were the subject of the 800,000 no-match letters the Social Security Administration (SSA) sent to employers this year are undocumented workers. This, if true, underscores that there are millions of undocumented workers in the United States who are here to fill "essential worker" positions, those unskilled and semi-skilled jobs vital to all sectors of our economy. These essential workers fill jobs that U.S. workers are unwilling to take, despite the general downturn in the economy.

Reports from the Bureau of Labor Statistics reinforce the need for essential workers and the fact that this need is rising. During the labor force expansion that took place from 1996-2000, foreign labor filled the lesser skilled positions native-born workers left. As a result, over 55% of the foreign-born work force is concentrated in service and labor occupations. Projections for the next ten years indicate that the need for workers in these occupations will continue to rise as new jobs are created: the service-producing sector alone is expected to create over 12 million new positions. 57 percent of all job openings will be for essential worker positions and will only require modest or on the job training. In order to keep our economy strong, the U.S. needs these essential workers to fill these positions.

This nation has long benefited from the large number of undocumented worker who fill unskilled and semi skilled positions essential to our economy. It is long past due that we change our immigration laws to provide legalization for the hard-working, taxpaying workers in this country and create a legal means for workers we will need in the future.

That these workers are here illegally is a symptom of an immigration system that is out of touch with the needs of our economy. Simply put, there is no way for workers currently here to legalize their status and there is no visa category through which semi-skilled and unskilled workers can legally enter the United States in order to perform full-time, year-round work. These workers do not want to be undocumented. Many are paying taxes and social security, the same as legal workers. However, the lack of any legal means to regularize the status of those who are here and the absence of any temporary immigration program through which people can legally enter and leave the country is not good for our communities, our economy, or our security.

In fact, both a legalization program and an essential worker temporary visa program will help us to enhance our security. A legalization program that rewards work would bring hardworking, well meaning individuals out of the shadows and would allow us to properly identify and document them. We would know who they are and why they are here. A temporary program that designates legal channels for entry would allow us to focus our resources at the border on those who mean to do us harm, not those who fill our labor needs, and reduce the number of tragic deaths associated with border crossings. Both these initiatives would further enhance our security by permanently reducing the demand for counterfeit documents and other related acts associated with unauthorized work. These positive changes would allow free up our agencies' time and resources and allow them to concentrate their efforts on achieving security goals that actually enhance our security.

The legalization of these workers also would provide a second benefit to the SSA through the reduction of the Earnings Suspense Fund (ESF). When the SSA announced its no-match letter program for this year, reduction of this file was touted as one of the goals. A legalization program will help reduce the ESF, and the agency

will be able to reduce administrative costs associated with maintaining such a large fund.

AILA strongly opposes initiatives that would prohibit foreign nationals who legalize their status from receiving credit for the social security contributions they made while they were in an undocumented status. America needed the contributions these workers made in the labor force when they were undocumented. We should recognize their contribution by allowing them to access their social security benefits once they are legalized.

In this time of heightened security, we must foster an environment that that will encourage individuals to emerge from the shadows and participate as productive members of our society in order to separate them from those that are here to do us harm. Positive immigration reform in conjunction with constructive reforms to protect the integrity of the social security numbers and prevent identity theft will greatly improve our nation's efforts to provide effective security.

Sincerely,

Statement of ERISA Industry Committee (ERIC), National Association of State Retirement Administrators (NASRA), National Council on Teacher Retirement (NCTR), National Rural Electric Cooperative Association (NRECA), Profit Sharing/401(k) Council of America (PSCA)

The undersigned organizations urge you to carefully consider the unintended consequences of legislation being currently pending before the House Ways and Means, Energy and Commerce, and Financial Services committees. Without amendment, the Social Security Number Privacy and Identity Theft Prevention Act of 2001 (H.R.2036) could unintentionally hinder the delivery of benefits from, and the efficient administration of, public and private employee benefit plans.

We strongly support the bill's purpose of ensuring the integrity of the social security number (SSN). We are extremely concerned about the proliferation of identity theft and other financial crimes that exploit individual SSNs, and believe strong legislation should be enacted to combat such nefarious acts. As currently drafted, however, H.R.2036 could make it more difficult to deliver comprehensive health and retirement benefits to public and private employees alike.

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

Public and private sector defined benefit and defined contribution pension and savings plans, like 401(k), 403(b), and 457 plans, use SSNs to identify plan participants, account for employee contributions, implement the employee's investment directions, track "rollovers" from other plans, and allow employees to view their account activity or benefit accrual online (typically in conjunction with a secure "PIN"). H.R.2036's broad prohibitions could impede, for example, an individual's ability to stay current on the accumulation of benefits for his or her retirement.

SSNs are also used as the primary identifier in many medical and health benefit and prescription drug plans to coordinate communications between the doctor, the medical service provider, and the plan. H.R.2036's broad prohibitions could, for example, put at risk the delivery of appropriate medications to the individual.

The application of H.R.2036's broad prohibitions could:

- **Unintentionally restrict access to employee benefit plans.** Section 202 of H.R.2036 makes it a violation of the Federal Trade Commission Act for "any person" to refuse to "do business" with an individual because the individual refuses to give his or her social security number to the person. While the commonly understood definition of "business" would not include employee benefit plan administration, we are concerned the broad prohibition unintentionally would restrict plan operation. *We recommend making it clear that section 202 applies only to commercial transactions, and not in the context of employment of an individual, including the provision of compensation or benefits.*
- **Unnecessarily limit the legitimate and beneficial use of SSNs.** Section 201 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 making legitimate and beneficial uses of social security numbers a violation of Federal criminal law.

For example, many benefit plan sponsors require participants to submit their social security number to the plan in order to be enrolled in and receive benefits from the plan. While such a transaction would not meet the commonly understood definition of “sale,” the definition of “sale” in section 201 encompasses an exchange of “anything of value” for a social security number.

Expressly excluded from the definition is the application of “any type of Government benefits or program” (which would cover government assistance programs, not necessarily the employment benefits governments offer their employees). The limited exclusion from the definition of “sale” for the application of social security benefits creates a risk that a court will read the exchange-for-value formulation to encompass everything not expressly excluded, including employee benefits. *We recommend that the bill’s exclusions be modified to encompass the administration and provision of employee benefit plans.*

Section 201 also prohibits the intentional placing of a social security number, or derivative thereof, “in a viewable manner on an Internet site that is available to the general public or in any other manner intended to provide access to such number or derivative to the general public.” This definition, too, may sweep in routine benefit plan administration. For example, individual social security numbers may appear on correspondence between the plan, the plan administrator, the individual, and an outside third party, like a medical care provider. We are unclear if such “displays” are to the “general public.” *We recommend the bill be amended to include a more precise definition of “general public” to ensure that secured and private displays of social security numbers typical in benefit plan administration are not construed to be to the “general public.”*

Section 201 provides an exception to the prohibition if “voluntary and affirmative written consent” of each affected individual is obtained. Our plans may cover tens of thousands of individuals. Thus, obtaining affirmative written consent would be wholly impracticable and extremely costly. Moreover, if an individual not consenting to the use of his or her social security number is dropped from the benefit plan, the plan sponsor would be exposed to a significant risk of litigation, enforcement actions, civil penalties, excise tax penalties, and plan disqualification for violation of the federal laws that govern pension and other benefit plans. *Thus, we recommend that relief for employee benefit plans be provided by narrowing the bill’s definition of “sale” and “general public” as discussed above.*

- **Unwisely subject public and private employee benefit plans to regulations promulgated by a federal agency with no expertise in employee benefit plans.** Section 201 also gives authority to the U.S. Attorney General to promulgate regulations to ensure, among other things, that the prohibitions contained in section 201 are “no broader than necessary” to accomplish its purpose. If the bill is not amended, as we have recommended, to exclude routine benefit plan administration from the definitions of “sale” and “purchase,” *we strongly recommend that the rulemaking authority granted to the Attorney General be done in consultation with a federal agency familiar with the workings of employer-sponsored benefit plans with the clear direction that regulations accommodate legitimate uses of social security numbers in employee benefit plans.*

Please do not hesitate to contact Janice Gregory (202-789-1400) at ERIC, Jeanine Markoe Raymond (202-624-1417) at the NASRA, Cynthia Moore (703-243-1667) at the NCTR, Chris Stephen at the NRECA (703-907-6026) or Edward Ferrigno at PSCA (202-626-3634) to discuss this matter in more detail.

Federation for American Immigration Reform
Washington, DC 20011
September 18, 2002

The Honorable E. Clay Shaw, Jr.
Chairman, House Social Security Subcommittee
B-316 Rayburn House Office Building
Washington, DC 20515-6353

The Honorable George Gekas
Chairman, House Immigration, Border Control and Claims Subcommittee
B-370B Rayburn House Office Building
Washington, DC 20515-6217

In connection with the hearing that you jointly are holding on September 19, 2002 on Protecting Integrity of Social Security Numbers, I would appreciate your consideration of the views of the Federation for American Immigration Reform (FAIR).

Shortly after the tragic terrorist attacks last year FAIR issued a blueprint outlining several urgently needed measures to protect homeland security. Recently, on the anniversary of the attacks, we issued a report card on the progress towards adopting these earlier recommended measures. In that report card, we singled out the significance of the actions taken by the Social Security Administration (SSA) toward improving our national security.

In particular, two actions merit the recognition and strong support of Congress and the American public. First, the decision by SSA to stop issuing social security cards to aliens in order to satisfy the requirements of some state departments of motor vehicles for Social Security Numbers (SSNs). The prior practice meant that the SSA was issuing SSNs to aliens who were illegally in the country to facilitate their applications for state-issued driver's licenses. The tragic effects of that policy were revealed when it became clear that all 19 of the 9/11 terrorists had state-issued driver's licenses, some of them from multiple states. Under the circumstances, we strongly urge each of the subcommittees to underscore your support for sustaining the current practice of SSA in this regard.

Second, the SSA has finally begun to insist on the need to reestablish the integrity of the SSN as an identifier for payroll purposes. It is a well-documented fact that counterfeit document operations have proliferated in the period since adoption in 1986 of the Immigration Reform and Control Act (IRCA) prohibition against hiring illegal aliens. One of the most frequently counterfeited documents has been the Social Security card. This abundance of fraudulent documentation has made it difficult for employers—even the vast majority who have no intention of hiring illegal aliens—to discern the authenticity of the work eligibility documents presented by prospective employees.

The SSA's failure in the past to compare the SSNs on payroll documents with the SSNs they have issued has actually encouraged growth in the numbers of employers willing to hire illegal aliens. Beginning with agriculture and meatpacking industries and spreading throughout the hospitality industry, employers have been so motivated by the spread of illegal alien hiring by their competitors and the by the lack of enforcement against illegal employment that many have looked the other way and become fully dependent on cheap illegal employees. As a consequence, illegal immigration has been further encouraged, and qualified American and legal resident workers have been displaced as once prevailing wages have been dramatically depressed.

While the SSA has offered a free online service to employers to verify the work eligibility of potential employees, there has been no real incentive to use the service. That may change now as a result of the SSA's recent actions systematically to notify employers of mismatches between SSNs listed on payroll documents and the SSNs issued.

Complaints that this program of advising employers of no-matches may cost legal workers their jobs is unfounded, because the notification process specifically advises employers that they should allow the employee to reconcile with the SSA any possible data error that has led to a false no-match notification before a no-match notification leads to the termination of employment.

Once again, we applaud the Administration and the SSA for taking these steps. Our concern, however, is that if they could be accomplished as policy changes, they similarly could be discontinued by a new policy decision. We urge you to assure that this program of issuing no-match letters to employers becomes a permanent requirement.

There remain, however, two outstanding actions that would help to buttress the new SSA program. The first of these would apply the law sanctioning employers

who continue to ignore the SSA alerts that employees do not have valid SSNs. The Internal Revenue Service (IRS) should be required to begin immediately fining businesses that flagrantly continue to ignore the SSA notifications.

Secondly, the SSA has long maintained a policy of non-cooperation with the INS in identifying workplaces with potential illegal alien employees. This has changed somewhat in the Basic Pilot employment verification system mandated by the Illegal Immigrant Reform and Immigrant Responsibility Act of 1996. In that program, the SSA was required to verify SSN data and forward employment data on foreign-born workers to the INS for verification of work eligibility status. Although that program is still ongoing, its trial period has been completed and successfully evaluated by an outside contractor.

Until such time as Congress enacts the Basic Pilot program as a permanent fixture in the nation's efforts to regain control over its borders, the SSA should require that no-match notifications to employers be retained by the employer for potential audit by the INS at the time that it may investigate whether employers are in compliance with the requirements of the IRCA prohibition against hiring illegal alien workers.

The nation must never again return to the luxury of ignorance about the threat of international terrorism, and it can never relax in a hope that all foreigners will respect our sovereign right to have our nation's immigration policy respected. Instead, we must take the necessary steps to deter both threatening terrorists and illegal immigration by gaining control over our borders and denying safe haven to those who enter or stay in the United States illegally. Assuring the integrity of the SSN system, because it is the universal identifier for many purposes in our society, is critical to achievement of this objective.

We trust the members of the House Social Security Subcommittee and the House Immigration, Border Control and Claims Subcommittee will agree that the recent advances in restoring integrity to the SSN system must be locked in place so that they are not subject to erosion as a result of pressures from whoever has the attention of any given Administration at the moment.

Sincerely,

Dan Stein
Executive Director

National Council of La Raza, and National Immigration Law Center
Washington, DC 20036
October 3, 2002

The Honorable E. Clay Shaw, Jr.
Chairman, House Social Security Subcommittee
B-316 Rayburn House Office Building
Washington, DC 20515-6353

The Honorable George Gekas
Chairman, House Immigration, Border Security and Claims Subcommittee
B-370B Rayburn House Office Building
Washington, DC 20515-6353

RE: Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists, Hearing held before the U.S. House of Representatives Subcommittee on Social Security and Subcommittee on Immigration, Border Security, and Claims, September 19, 2002

Dear Chairmen and Members of the U.S. House of Representatives Subcommittee on Social Security and Subcommittee on Immigration, Border Security, and Claims:

The National Council of La Raza and the National Immigration Law Center appreciate the opportunity to submit comments on the issue of the Social Security Administration's no-match letters.

Sent by the Social Security Administration (SSA) to certain employers, no-match letters have had a devastating impact on immigrant worker communities throughout the country. For the last several years, advocates have been expressing deep concern about the continued use of these no-match letters by employers to discourage immigrant workers from asserting their workplace rights. Advocates have also been working hard to educate employers who, due to the confusion caused by these letters, feel pressured to take some action against employees listed in the no-match letters. The recent hearing before the Subcommittee on Social Security and the Subcommittee on Immigration, Border Security, and Claims of the U.S. House of Rep-

representatives highlighted many of our concerns regarding the no-match letters. The hearing also clearly demonstrated the need for a balanced and thoughtful approach to immigration policy that recognizes the contributions that immigrant workers make to the U.S. economy as well as our nation's economic and security needs.

In an effort to update its database, the SSA sends no-match letters to employers when the names or Social Security Numbers listed on an employer's W-2 forms do not agree with SSA records. Attached to each no-match letter is a list of employees for whom the SSA database could not find a match. The no-match letter is intended to be an educational correspondence that informs companies that their employees' wages are not being properly credited to their Social Security accounts. The SSA aims to correct its records so that employees' earnings are accurately tracked and can be used to calculate benefit levels when applications for retirement or disability benefits are made with SSA. Correcting the SSA database is certainly a commendable goal. However, the effectiveness of these no-match letters is unproven, and the resulting consequences on immigrant worker communities have been devastating.

The SSA's use of the no-match letters has increased dramatically over the past year. While fewer than 100,000 letters were sent in 2000, 110,00 were issued in 2001 and 870,000 were reportedly sent to employers in 2002. However, despite this increase in letters, the Earnings Suspense Fund (ESF) has not decreased. Rather than identify a more effective means to decrease the suspense file, the SSA has increased substantially the use of the ineffective no-match letters. During Mr. Lockhart's testimony, the Social Security Administration itself admitted that it must review the effectiveness of this policy.

However, the system's ineffectiveness is not its gravest consequence. The impact of the no-match letters on the immigrant community has been profound and widespread. The failure of the no-match letters to safeguard workers effectively against unfair and illegal practices on the part of employers has had devastating effects on the workers and their families.

As the SSA admits, there are many reasons for computer no-matches, and the no-match letters themselves do not prove any wrongdoing by either employer or employee. For example, a large proportion of the names on the no-match letters are Latino, Asian, or other names frequently misspelled by employers resulting in computer no-matches. These honest data-entry mistakes disproportionately affect immigrant workers. However, employer misuse of the no-match letters has caused great harm to workers nationwide. While the letter explicitly warns employers not to take adverse action against workers listed on the letter, layoffs, suspensions, firings, retaliations, and discrimination against these workers are widespread and well-documented. Some employers have simply fired all workers on the list; others have incorrectly reverified the work authorization of workers on the list. In many cases, only Latino or other "immigrant" workers, or workers involved in union organizing campaigns, have been fired or harassed (*See Aaron Nathans, UW and Janitors Settle; Tentative Deal: \$24,000 for Latinos, Capital Times, Dec. 8, 2001 at A1*). And since a disproportionate number of names on the no-match lists are "foreign-sounding" names, many employers fear that they will face sanctions if they hire additional workers who look or sound "foreign" resulting in increased citizenship or national origin discrimination in the hiring process.

Low-wage immigrant workers are the most likely to be affected by all of these illegal practices. In fact, our communities have reported widespread abuse of the SSA no-match letters resulting in greatly increased anxiety within the immigrant community. Many legal permanent residents and even U.S. citizens have been affected, and the undocumented worker community has been pushed even further underground. Because many immigrants live in mixed-status families and close-knit communities, when one worker is fired entire families including U.S. citizen children suffer.

Thus the SSA's no-match letter policy has not resulted in reducing the suspense file, has not eliminated computer no-matches, and has not diminished unfair hiring practices. In fact, the consequences have been quite the contrary. Particularly in this time of heightened security, we must foster an environment that that will encourage individuals to emerge from the shadows and participate as productive members of our society in order to separate them from those who are here to do us harm. Rather than pour the SSA's resources and energies into an ineffective and harmful policy, we must be prepared to step back and look at the larger picture.

The testimony of Mr. Matthew James Reindl highlighted the advantage that unscrupulous employers who hire undocumented workers have over law-abiding employers. For years, immigrant advocates have argued that unlawful hiring practices harm both immigrant workers and U.S. workers. The recent Supreme Court decision in the *Hoffman Plastic Compounds Inc. vs. NLRB*, ___ U.S. ___, 122 S. Ct. 1275 (2002),—further exacerbates that advantage and gives added incentive to employers

to hire unauthorized workers. In that decision the Court found that undocumented workers who are illegally fired are not eligible for certain backpay remedies under the NLRA. This decision means that employers can continue to hire unauthorized workers and subject them to exploitative conditions and even fire them for union organizing activities—all of which are illegal regardless of a worker's immigration status—with no out-of-pocket costs. The Social Security Administration's no-match policy will not punish these employers nor resolve the underlying problems associated with the hiring of undocumented labor. Instead, it provides added incentives for employers to take unlawful action against the workers whom they have knowingly hired with no legal ramifications. The answer to the problem raised by Mr. Reindl is to enact legislation reversing *Hoffman*, thus leveling the playing field by removing the incentive to hire undocumented workers to whom they will never owe backpay.

The problems highlighted during the hearing clearly demonstrate the need for comprehensive immigration reform. The existence of the SSA suspense file shows that immigrant workers, regardless of their immigration status, are paying Social Security taxes and are not receiving the benefits of those taxes. The evidence presented also demonstrates that immigrant workers are essential to the U.S. economy and that U.S. employers have knowingly and unknowingly hired many undocumented workers needed to fill jobs in key sectors of the economy. These hard-working, taxpaying immigrants should be rewarded for their contributions by getting the opportunity to legalize their immigration status and obtain permanent residence in the U.S. Only in this way can these workers come out from the shadows, be known to U.S. authorities, properly pay all of their taxes, and be compensated appropriately. Such a legalization program would also greatly reduce document fraud by virtually eliminating the market for falsified Social Security Numbers and other identifying documents, and the Social Security Administration could continue its primary mission of administering the Social Security program.

We urge you to reflect upon the ineffectiveness of the no-match letter policy and work towards effective and comprehensive solutions to the problems associated with unauthorized labor in the U.S. We look forward to working with you in the future.

Sincerely,

