

**THE ROLE OF SOCIAL SECURITY NUMBERS
IN IDENTITY THEFT AND OPTIONS
TO GUARD THEIR PRIVACY**

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

APRIL 13, 2011

Serial No. 112-SS2

Printed for the use of the Committee on Ways and Means



U.S. GOVERNMENT PRINTING OFFICE

70-880

WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

**COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY**

SAM JOHNSON, Texas, *Chairman*

KEVIN BRADY, Texas

PAT TIBERI, Ohio

AARON SCHOCK, Illinois

ERIK PAULSEN, Minnesota

RICK BERG, North Dakota

ADRIAN SMITH, Nebraska

XAVIER BECERRA, California

LLOYD DOGGETT, Texas

SHELLEY BERKLEY, Nevada

FORTNEY PETE STARK, California

CONTENTS

	Page
Advisory of April 13, 2011, announcing the hearing	2
WITNESSES	
The Honorable Patrick P. O'Carroll Jr., Inspector General, Social Security Administration	7
Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection, Federal Trade Commission	17
Theresa L. Gruber, Assistant Deputy Commissioner, Office of Operations, Social Security Administration	34
SUBMISSIONS FOR THE RECORD	
Juan J. Martinez, Ph.D.	54
Helene Perry	56
LifeLock	57
Patrick P. O'Carroll Jr.	62
Maneesha Mithal	72
Theresa L. Gruber	78

**THE ROLE OF SOCIAL SECURITY NUMBERS
IN IDENTITY THEFT AND OPTIONS
TO GUARD THEIR PRIVACY**

WEDNESDAY, APRIL 13, 2011

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

The subcommittee met, pursuant to notice, at 2:02 p.m., in Room B-318, Rayburn House Office Building, the Honorable Sam Johnson [chairman of the subcommittee] presiding.
[The advisory of the hearing follows:]

HEARING ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

Chairman Johnson Announces Hearing on the Role of Social Security Numbers in Identity Theft and Options to Guard Their Privacy

April 06, 2011

Congressman Sam Johnson (R-TX), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing to examine the role of Social Security numbers in identity theft and options to guard their privacy. **The hearing will take place on Wednesday, April 13, 2011, in room B-318 Rayburn House Office Building, beginning at 2:00 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:

Identity theft is the fastest growing type of fraud in the United States, affecting 11.1 million victims in 2009, up 12 percent since 2008. The Federal Trade Commission (FTC) estimates that identity theft costs consumers about \$50 billion annually. Further, identity theft is often used to facilitate other crimes, including credit card, document, or employment fraud. The Social Security number (SSN) is especially valuable to identity thieves as it serves as the key to authenticating an individual's identity in order to open accounts or obtain other benefits in the victim's name.

Although created in 1936 solely to track workers' earnings for Social Security benefit purposes, use of the SSN has become widespread. Largely because the SSN is permanent and unique to an individual, SSNs are used by many industries, including financial institutions, insurers, universities, health care providers, and government agencies. While many SSN uses are beneficial and required by law, such as for purposes of employment and taxation, other uses may not be necessary, such as displaying it on an identification card.

Despite its important role, there is no Federal law that requires comprehensive confidentiality protection for the SSN. However, there are laws that provide limited SSN confidentiality. For example, the Gramm-Leach-Bliley Act (P.L. 106-102) restricts the reuse and redisclosure of certain personal information, including SSNs, by financial institutions. Also, many States have enacted legislation to restrict the use, disclosure, or display of SSNs.

In 2006, the President established an Identity Theft Task Force to coordinate Federal agencies' efforts against identity theft. One of many recommendations in its 2007 report was to decrease the unnecessary use of SSNs in the public sector. In response to the Task Force's mandate for the study of private sector uses of SSNs, the FTC developed recommendations to reduce the availability of SSNs to identity thieves while preserving legitimate uses.

In announcing the hearing, Chairman Sam Johnson (R-TX) stated, **"Americans are rightly worried about the security of their personal information, including their Social Security number. We must stop overuse and abuse of Social Security numbers in order to help prevent ID theft and further protect Americans' privacy."**

FOCUS OF THE HEARING:

The Subcommittee will examine the impacts of identity theft, the role of SSNs in abetting identity theft, and options to restrict its use. In addition, the role of the SSN in administering Social Security programs and how the Social Security Administration protects SSNs will be considered, along with legislative proposals to limit the use of SSNs.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, <http://waysandmeans.house.gov>, select "Hearings." Select the hearing for which you would like to submit, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, **by the close of business on Wednesday, May 4, 2011**. Finally, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225-1721 or (202) 225-3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word or WordPerfect format and **MUST NOT** exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.
2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.
3. All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission listing the name, company, address, telephone, and fax numbers of each witness.

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.

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

Chairman JOHNSON. The subcommittee will come to order. Welcome, everyone.

Identity theft is a lasting and devastating crime. Victims spend years having to prove who they are, while monitoring credit reports, fending off collection agencies or the IRS for charges they

never made or wages they never earned. Some are picked up by law enforcement by crimes committed by the ID theft using their name. Americans have every reason to be concerned.

According to the Congressional Research Service, in 2009 ID theft claimed over 11 million victims and cost consumers about \$50 billion annually. The Privacy Rights Clearinghouse reports the total number of known records that have been compromised due to security breaches beginning in January 2005 through last week topped 500 million. Just yesterday, in my own state of Texas, the comptroller's office announced the largest security breach in state history: some 3.5 million personal files were mistakenly left on a computer file available to the public, putting current and retired state employees at risk.

Even though Social Security numbers were created to track earnings for determining eligibility and benefit amounts under Social Security, the numbers are widely used as personal identifiers. Some of the uses of these numbers in preventing fraud are vital to many commercial and government operations. Examples include enforcing child support, aiding law enforcement, and compiling information from many sources to help ensure the accuracy of credit reports.

Unfortunately, as pointed out by GAO in testimony before this subcommittee, Social Security numbers have become the identifier of choice, and are used for everyday business transactions. In fact, in their April 2007 report, the President's Identity Theft Task Force identified the Social Security number as the most valuable commodity for an identity thief.

Even worse, identity theft continues to threaten our national security. As said in the 9/11 Commission report, fraud and identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding airplanes, sources of identification are the last opportunity to ensure that people are who they say they are, and to check whether or not they are terrorists.

Congress needs to get to work on identity theft and limiting access to Social Security numbers is an excellent place to start. For years, Ways and Means Subcommittee on Social Security has been working on this problem in a bipartisan way. In fact, Mr. Doggett and I have been on a bill year after year to try to do this. We have approved bills to protect the privacy of Social Security numbers and prevent identity theft since the 106th Congress, when it first approved the Social Security Number, Privacy, and Identity Theft Prevention Act.

The legislation was first introduced on a bipartisan basis by then-subcommittee chairman Clay Shaw, and then-ranking member, the late Bob Matsui. Despite numerous attempts, Congress has not been able to close the deal. Sadly, Social Security number use is so widespread across so many industries that the committees of jurisdiction have yet to reach agreement on the right approach to limiting their use.

Still, I believe this committee can make progress. To that end, today I am reintroducing, with Mr. Doggett, the Medicare Identity Theft Prevention Act, a bill to remove the Social Security number from the Medicare card. It makes no sense that people are told,

“Don’t carry your Social Security card in order to protect your identity,” but then every senior citizen is told, “Carry your Medicare card,” which displays prominently the Social Security number.

The risk of ID theft goes far beyond the card being stolen. Every medical record at nursing homes, hospitals, and doctor offices has a Social Security number written on it. The wholesale amount of Social Security numbers that are available to identity thieves is staggering and completely unnecessary.

You know, just last night I was dealing with the TV guys on cable. Guess what they asked for?—my Social Security number to prove it was me. Can you believe that? Well, I didn’t know what to say.

The Centers for Medicare and Medicaid Services have refused to act. If they won’t do what is right for America’s seniors, we will. I thank my colleague from Texas for his work on this issue, and I urge my other colleagues to support this issue, as well.

The problem of identity theft is not going to be addressed with one single piece of legislation. But protecting Medicare cards carried by 47 million Americans is a good place to start. I will say that if the military can remove Social Security numbers, CMS ought to be able to do the same.

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

And I now yield to my friend, Xavier Becerra, our ranking member.

Mr. BECERRA. Mr. Chairman, thank you very much for calling this hearing. As you just said, millions of Americans are harmed each year, due to the misappropriation of their identities. This subcommittee is deeply concerned about this particular problem. In fact, we have held 17 previous hearings on this subject since 2000, the year 2000.

Let me urge this subcommittee to show the same diligence and thoroughness in examining some other critical issues that we will be confronting soon surrounding Social Security, such as the impact of cuts to the Social Security Administration’s (SSA) operating budget proposed for this year, and the consequences for people, for example, who are waiting for their disability benefits. Also, the impact of cuts to the Social Security Administration’s operating budget on the ability of the SSA to prevent waste, fraud, and abuse, and certainly in regards to the impact on senior’s retirement security from the kinds of Social Security benefit cuts that budget Chairman Paul Ryan has proposed and praised.

While we may have different views on the importance of Social Security benefits for today’s seniors and future retirees, we are united in our concern about identity theft. Identity theft ruins individuals’ good names, and destroys their credit ratings. It has even ruined the future credit ratings of young children. This subcommittee has heard from many victims of identity theft, and have described the extensive harm that they have suffered, as a result of identity fraud, harm which continues long after the fraud is discovered. Identity theft crimes carry a total cost to Americans of over \$17 billion.

I welcome the testimony of the Social Security Administration and its inspector general. I also welcome the testimony of the Federal Trade Commission, which plays a critical role in protecting consumers from identity theft.

Chairman Johnson, I look forward to joining you and others in reintroducing identity theft legislation for this new Congress, and I am hoping that we can make significant progress as we work together in that regard.

Before I yield back my time, Mr. Chairman, if I could yield one minute to the gentleman from Texas, Mr. Doggett.

Mr. DOGGETT. Thank you. While I shared the broader concerns that Mr. Becerra has just outlined, I just want to applaud your leadership on this, Mr. Chairman. I agree with every word you said about the subject that is up today, identity theft.

This is at least the third Congress in which you and I have been in partnership, trying to solve this problem. We actually passed it through the House in 2008, despite a lot of bureaucratic obstacles that were thrown up, and then the bureaucracy managed to kill it over in the Senate Finance Committee, or it would already be law.

I think one of the most effective ways for the bureaucracy to stand in the way of something that they don't want to move quickly on is to throw up a big cost estimate. And that is what has happened here. And we have been trying to get the specifics for months, if not years, from CMS about their claim that it will be too costly for them to protect the Identity of our seniors. They need to come forward with their study, and it needs to be well-founded. And we should not let their objections stand in the way, again, of doing what is right by our seniors and, as you said, at least doing for folks who rely on Medicare what the military has already been able to do for our military men and women and for our veterans. I thank you, Mr. Chairman. Thank you, Mr. Becerra.

Chairman JOHNSON. The gentleman from California, you are recognized.

Mr. STARK. Mr. Chairman, I am pleased that you called this markup, and proud to be a cosponsor of your bill, and I would ask you if you would consider, and if the committee would not object, we introduced legislation that would address the problem of identity theft for foster children. The foster children's Social Security numbers often pass through many hands, and we have encountered problems when the children age out of foster care, they have found that their identity has already been stolen, and people have opened credit cards, and so forth. And we have some language that I hope you would consider adding to your legislation that would protect these very vulnerable children.

I know that Mr. Delay worked with us years ago on doing this, and I look forward to seeing if we can include this in your—

Chairman JOHNSON. Yes, I am sure Mr. Doggett would agree.

Mr. DOGGETT. Absolutely.

Chairman JOHNSON. We will certainly look at it.

Mr. STARK. Thank you, Mr. Chairman.

Mr. BECERRA. Chairman, we are pleased that you have called this hearing, and I would yield back the balance of my time.

Chairman JOHNSON. Thank you, Mr. Becerra. Let me tell you we are getting a vote in about 10 or 15 minutes, maybe 20. There

will be four votes and three of them are five minutes. So we will break when that occurs and come back after the votes, which will be about a half-hour.

Today we are joined by three witnesses. Our first witness is the honorable Patrick O'Carroll, Jr. He is the Social Security Administration Inspector General. Next is Maneesha Mithal, who is the Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission. And lastly we will hear from Theresa Gruber, who is the Assistant Deputy Commissioner, Office of Operations at the Social Security Administration.

So, all I would ask you is stop dragging your feet and let us get these things done.

[Laughter.]

Chairman JOHNSON. Mr. O'Carroll, you are recognized. I welcome all of you, and thank you for being here.

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

Mr. O'CARROLL. Good afternoon, Chairman Johnson, Congressman Becerra, and Members of the Subcommittee. Thank you for the invitation to testify today.

We all understand the serious threat and damaging effects of identity theft. But to better illustrate the issue, I would like to present one victim's story. Dr. Juan Martinez, born and raised in Chicago, was thrilled to accept a teaching position at the University of Chicago in 2005. Soon after he began working in his hometown, however, Dr. Martinez received a letter from the IRS that stated he failed to pay his taxes on wages earned the previous year in Colorado. The letter arrived with a substantial bill.

Someone had stolen his identity, and Dr. Martinez was left to prove his case to the IRS. Dr. Martinez and his wife struggled for several years, as they disputed charges with the IRS, and attempted to track down the person who was fraudulently using Dr. Martinez's name, Social Security number, and birth date.

In 2010, Dr. Martinez learned that a bank account was opened in his name in Missouri. Authorities in Chicago referred the case to one of our special agents in St. Louis. Working with the bank where the account was opened, our agent quickly identified and located the man who illegally used Dr. Martinez's information for five years. The man admitted to purchasing false identity documents, and using Dr. Martinez's name to get a job, rent an apartment, and open a bank account. Last month he was sentenced to seven months in prison and ordered to pay restitution of more than \$5,000 to Dr. Martinez.

Now, Dr. Martinez and his family may finally breath a sigh of relief. We in OIG are very pleased to have helped Dr. Martinez. And while he could not be here today, he has prepared a written statement about his ordeal, and we would like to enter that into the record.

[Dr. Martinez statement for the record follows:]

**Victim Impact Statement of Juan J. Martinez, Ph.D.
Submitted for the Record
Committee on Ways and Means, Subcommittee on Social Security
Hearing on the Role of Social Security Numbers in Identity Theft and Options to
Guard Their Privacy**

April 13, 2011

The following is a statement that I would like to be read into the hearing record before the Ways and Means Subcommittee on Social Security:

Chairman Sam Johnson, Ranking Member Xavier Becerra and members of Congress,

One often associates theft as a violent crime where something is physically taken from an individual usually by force. This may be in the form of armed robbery, a forced break-in, a car jacking or a "hold-up." I, fortunately, was not subjected to any of these ordeals, but I am a victim. Something significantly more valuable than material goods was taken from me and for 5 years (and possibly more years to come) I have been working to regain that which was stolen from me. I am speaking of my identity that in 2005, Mr. Roberto Ramos-Carvente willfully, knowingly and unlawfully took from me.

It is possible that the defendant came to this country to gain a better life for himself and his family. It is also possible that in taking my name, my social security number, my birth date and other information, Mr. Ramos-Carvente thought that he wasn't hurting anyone. The problem is that in taking this information, the defendant initiated a cascade of events that has made certain aspects of my life rather unpleasant.

Mr. Ramos-Carvente, starting in 2005 and continuing into 2010, utilized my identity (including, but not limited to the use of my name, social security number, and date of birth) to unlawfully gain employment and establish savings and checking accounts in various states of the USA including Colorado and Missouri. During this time, the defendant did not pay the required federal or state income taxes on the wages he earned. Since he had utilized my personal information to gain employment, his reported income on W2 forms were linked to federal and Illinois state tax returns that my wife and I filed as required by law. Suffice it to say, I have spent more time than I would like to admit trying to regain something that is rightfully mine: my identity, what I feel makes me, me. I have spent numerous work days, weekends and any available free time gathering information for audits, contacting credit bureaus, contacting the IRS, contacting the Social Security Administration, contacting banks, contacting telephone companies, contacting various local and federal law enforcement authorities to report the defendant's actions as identity theft. Meanwhile, the defendant led his life not caring about the wake of a mess that he left behind as he made his way from town to town, employer to employer.

One of the major headaches that resulted from the defendant's criminal activity was that my family's tax returns to the IRS were consistently "flagged" and subjected to re-examination by auditors. This was due to our filing tax returns that contained un-reported wages that were unknown to me (those unlawfully earned by the defendant posing as me) year after year. I have

had to prove to the IRS that the wages reported by the defendant in each fiscal year were in fact unlawfully earned by him and not by me. For example, the burden of proof was placed on me to prove that wages earned in the state of Colorado were not earned by me as I have never resided in Colorado nor worked in that state. As one can imagine, trying to prove one's own identity when another has documentation in the same name, with the same social security number and same date of birth can be a rather trying and difficult task. Trying to do this to federal agencies such as the IRS and the Social Security Administration has not been in any way easy as the wheels of bureaucracy do not always turn at a reasonable rate.

I am proof that ID theft is not a victim-less crime. Mr. Ramos-Carvente stole from me and whether or not he did this knowingly is not my concern. I want him to know that he hurt my family and at this time, I have very little sympathy for him. He deserves the punishment that he has received and I am grateful to the various local and federal law enforcement agencies across the country whose collective efforts resulted in his arrest. I take solace knowing that has been incarcerated and that the nightmare that he put us through is now hopefully over.

Respectfully,

/s/

Juan J. Martinez, Ph.D.
Assistant Professor
The University of Chicago
Department of Microbiology

As the case illustrates, identity theft places a huge burden on the victims. Use of the SSN is still widespread throughout government programs and financial transactions. And with technology constantly evolving, stealing SSNs and entire identities has become even easier. As we pursue investigations similar to the case of Dr. Martinez, our agents participate in SSN misuse task forces across the country, investigating identity theft, as well as mortgage, bankruptcy, and benefit fraud.

My office has done work that led to the removal of the SSN from the selective service mailings. We have also recommended its removal from other government documents and IDs, such as the Medicare card. The Department of Defense recently announced it will remove the SSN from military IDs, and we agree that this is a step in the right direction to protect valuable personal information.

SSA, though, still cannot prohibit the collection and use of SSNs. Our investigative and audit work has taught us that the more SSNs are used, the higher the probability that these numbers can be used to commit crimes. Our recent recommendations to SSA include: supporting legislation to limit public and private entities' use of the SSN; continuing efforts to safeguard and protect personal information; and ensuring the highest level of online security before offering replacement Social Security cards over the internet.

We have recently completed audits that question the collection of students' SSNs in kindergarten through 12th grade, as well as state and local governments' collection and use of SSNs. We have also completed reviews on assigning SSNs to non-citizens with fiancée visas and exchange visitor visas. Although temporary residents may be authorized to work in the United States, we question whether they should receive SSNs which will remain valid for life.

We are currently reviewing SSA's controls over how the Agency issues SSN print-outs, which are often used as a substitute for replacement Social Security cards. We plan to issue that report this summer.

In conclusion, we must continue to ensure the integrity of the enumeration process, limit the use and public display of the SSN, encourage SSN protection, and provide meaningful penalties for those who misuse the SSN or fail to protect it. My office will continue to work with you and SSA to maintain and improve the integrity of the Social Security number.

Thank you again for this invitation to testify today, and I will be happy to answer any questions.

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

U.S. House of Representatives

**Committee on Ways and Means
Subcommittee on Social Security**



Statement for the Record

**Hearing on the Role of Social Security Numbers in Identity Theft
and Options to Guard Their Privacy**

**The Honorable Patrick P. O'Carroll, Jr.
Inspector General
Social Security Administration**

April 13, 2011

Good afternoon, Chairman Johnson, Mr. Becerra, and members of the Subcommittee. As always, it's a pleasure to appear before you, and I thank you for the invitation to testify today. I have appeared before this Subcommittee many times to discuss issues critical to the Social Security Administration (SSA) and the services the Agency provides to American citizens. Today, we are discussing the Social Security number (SSN) and ways to improve SSN protection and guard against misuse and identity theft.

I last spoke to the Subcommittee about this issue in June 2007, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft lingers. We in the Office of the Inspector General (OIG) are well aware of the central role that the SSN plays in American society, and part of our mission is to protect its integrity along with the other personally identifiable information (PII) within Social Security Administration (SSA) records. To provide some context on the issue, in Fiscal Year (FY) 2009, SSA processed about 6 million original SSN cards and 12 million replacement SSN cards; and received about \$671 billion in employment taxes related to earnings under assigned SSNs. Protecting the SSN and properly posting wages under SSNs is paramount to ensuring SSN integrity and protecting our citizens' PII.

As the Subcommittee is well aware, the SSN was created in 1935 to keep an accurate record of each person's Social Security earnings, but over the years, Federal and State governments have relied on the SSN as the identifier of choice for a variety of government programs. Financial institutions are also required to obtain the SSNs of their customers. With each new use, the SSN has more value, and when you create something of value, someone will try to steal it. In May 2006, President Bush ordered the establishment of the National Identity Theft Task Force, which created directives for Federal agencies to strengthen efforts to protect against identity theft. Our reviews have found that SSA has followed these directives for years and strives to improve SSN integrity.

SSA has implemented numerous improvements in its SSN assignment, or enumeration, process. We believe SSA's improved procedures have reduced its risk of improperly assigning these important numbers. Some of the Agency's more notable improvements include:

- establishing enumeration centers that focus exclusively on assigning and issuing SSN cards;
- requiring that field office personnel who process SSN applications use a standardized Web-based, intranet process known as SSNAP, which reinforces Agency enumeration policies and standardizes data collection; and
- strengthening the requirements for identity documents presented with SSN applications to ensure that the correct individual obtains the correct SSN.

In addition, to prevent misuse of personal information, SSA has reported the following actions:

- SSA removed SSNs from the Social Security Statement, displaying only the last four digits.
- The Department of the Treasury removed the SSN and other types of numeric identifiers from Federal checks.
- SSA no longer releases SSNs or any PII to a caller who cannot provide his or her SSN. SSA now refers such callers to field offices for further verification of their identity before releasing any information.
- When SSA assigns a new SSN because a person has recently been disadvantaged by the misuse of his or her SSN, a special indicator is placed on the old SSN record to block issuance of replacement SSN cards and SSN printouts.

Several years ago, to keep track of OIG's many efforts to protect the SSN, we formed the Social Security Number Integrity Protection Team, or SSNIPT. That group, comprised of attorneys, auditors, and investigators, led to the eradication of displays of SSNs on Selective Service mailings and the Thrift Savings Plan Website—two practices by which the Federal government was itself putting the SSN at risk. We are very pleased to learn that the Department of Defense is replacing the SSN with a DOD identification number on all agency identification cards, to protect the privacy and personal information of our military personnel.

We applaud these and other efforts, but even now, SSA has no authority to prohibit the legitimate collection and use of SSNs. Moreover, our audit and investigative work has taught us that the more SSNs are unnecessarily used, the higher the probability that these numbers can be used to facilitate the commission of crimes throughout society. We believe SSA should support legislation to limit public and private entities' collection and use of SSNs, and improve the protection of the information when obtained; continue its efforts to safeguard and protect PII; and develop appropriate authentication measures to ensure the highest level of security and identity assurance before offering replacement SSN cards over the Internet.

Our ongoing and recently completed audit work has highlighted vulnerabilities and suggested some ways in which SSA can persuade public and private organizations to limit the collection, use, and disclosure of SSNs. We are working on or have completed the following related reviews:

- We are currently conducting an audit to assess State Departments of Health use of SSNs in their newborn screening process. Our focus will be to determine whether States have adequate controls in place to safeguard SSNs.
- *Kindergarten Through 12th Grade Schools' Collection and Use of SSNs*, released in July 2010, determined that many K-12 schools used SSNs as the primary identifier for students or for other purposes, even when another identifier would have sufficed. We believe that while some schools use SSNs as a matter of convenience, administrative convenience should never be more important than safeguarding children's personal information.
- *Prisoners' Access to SSNs*, released in March 2010, was a follow-up to a 2006 review that found that prisons in 13 States allowed inmates access to SSNs through various work programs. We determined that eight of the 13 States identified in our 2006 report continued this practice. However, in December 2010, the President signed the *Social Security Number Protection Act of 2010*, which prohibited prison work programs from granting prisoners access to SSNs.
- *State and Local Governments' Collection and Use of SSNs*, released in September 2007, identified instances in which some State and local governments posted public documents that contained SSNs on the Internet. We recommended that SSA seek legislation to limit SSN collection by State and local governments.

Although temporary residents may have authorization to work in the United States for the limited time they are here, we question the propriety of assigning an SSN, which is valid for life, to these individuals, because the SSN may be a key to a temporary resident's ability to overstay his or her visa. We are working on or have completed the following related reviews:

- Because of numerous instances of fraud and abuse in the H1-B (non-immigrant) worker program, we are currently conducting an audit to assess these workers' use of SSNs. An individual in the H1-B visa program is allowed to work for only one specific employer that has been approved by the Departments of Labor and Homeland Security. Our focus will be to determine whether these non-immigrants are working for their approved employers.
- *Assignment of SSNs to Noncitizens with Fiancé Visas*, released in May 2008, questioned the approval of an SSN to someone for as long as three months before they marry, because SSA might be giving those who have no intention to marry a tool for overstaying their visas. We recommended that SSA discuss with the Department of Homeland Security the feasibility of not granting work authorization to K-1 visa holders until they marry, but SSA and DHS determined it was not feasible.
- *Assignment of SSNs to J-1 Exchange Visitors*, released in July 2007, recommended that SSA work with the IRS to develop alternatives to assigning SSNs to certain types of exchange visitors, including the IRS' issuing Individual Taxpayer Identification Numbers. SSA declined to do so, stating that changing the way individuals are enumerated under the two J-1 categories we reviewed would create inconsistencies with policies regulating the other 11 categories.

Another issue to consider is SSA's procedures for issuing SSN Verification Printouts. Under the *Privacy Act*, individuals are allowed to obtain their SSN information from SSA, and the printout is among the items available. The printout is a limited version of the Numident record, but it still contains the same basic information as the Social Security card. The printout, however, has no security features.

SSA's current disclosure regulations that implement the *Privacy Act* allow an individual to provide less probative identity documents to obtain an SSN Printout. In certain circumstances, an individual can obtain the SSN printout from a field office without any identity documents. In a December 2007 report, *Controls for Issuing Social Security Number Verification Printouts*, we said procedures for issuing the printouts should follow SSA's improved replacement card procedures.

In response to the *Intelligence Reform and Terrorism Prevention Act of 2004*, SSA revised its policies and procedures for issuing Social Security replacement cards. Some of SSA's actions included increasing the identity requirements, such as presenting valid photo identification documents for obtaining a replacement SSN card; and limiting the number of replacement Social Security cards an individual can receive to no more than three in a year and 10 in a lifetime.

However, SSA did not implement similar procedures in the SSN printout issuance process. Our ongoing audit on SSA's controls over the issuance of SSN printouts determined the Agency issued about 7 million printouts in FY 2009, up from about 4.6 million in FY 2003, the first full year SSA issued the printouts. That audit is almost complete, and we anticipate issuing a report early this summer.

Turning to the issue of identity theft, the Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. The victim and their families often suffer mentally and emotionally as they attempt to repair the cracks in their financial foundation. The Martinez family, unfortunately, has coped with the effects of identity theft for several years, as I will explain.

Dr. Juan Martinez is a 37-year-old assistant professor of microbiology. Dr. Martinez was born and raised in southwest Chicago, so he was thrilled to accept a position teaching at the University of Chicago

in 2005. Shortly thereafter, Dr. Martinez received a letter from the IRS that stated he failed to pay taxes on wages earned the previous year in Colorado; the letter arrived with a substantial bill. Although Dr. Martinez had never worked in Colorado, someone using his name, SSN, and date of birth had received wages there from a facilities management company. Dr. Martinez then had to go about proving his case to the IRS, tracking down credit reports, bank records, and cell phone accounts, all while searching for a person who was working under a common Hispanic name.

Local law enforcement authorities eventually referred the case to one of our investigators, Special Agent Thomas Brady, who has investigated many identity theft cases. Brady worked with Dr. Martinez and Bank of America, where the other "Juan Martinez" had opened an account. Bank of America provided Agent Brady with account records, including a Missouri address and a photo taken at an ATM.

Agent Brady went to the address in Missouri, and the man who answered the door was the man in the ATM photo. He identified himself as Roberto Ramos-Carvente, and he admitted to obtaining false documents and using Dr. Martinez's identity to gain employment at a restaurant, rent his apartment, and open a bank account in Missouri.

Our investigation resulted in criminal charges of SSN misuse and identity theft against Mr. Ramos-Carvente, who was sentenced in March 2011 to seven months in prison and two years' supervised release. He was also ordered to pay restitution of \$5,650 to Dr. Martinez. Finally, Ramos-Carvente was ordered to participate in deportation proceedings and remain outside the United States, if deported.

Dr. Martinez is grateful for our efforts in resolving this issue, but a huge amount of credit goes to the victim himself for working tirelessly to track down the person who had stolen his identity. Nevertheless, we are very pleased to have helped Dr. Martinez, and while he could not be here today, he has prepared a written statement for the record. He has said he wants to help others protect themselves so they can avoid the trauma of identity theft.

As we pursue investigations similar to the case of Dr. Martinez, our agents also participate on about 45 SSN misuse task forces throughout the country, which cover mortgage fraud, bankruptcy fraud, and document and benefit fraud, as well as identity theft. In FY 2010, we opened 309 cases related to SSN misuse, which accounted for about 5 percent of all cases we opened during that period. In addition, in FY 2010, we had 441 SSN misuse cases that resulted in a criminal conviction, as a result of either a sentencing or a pre-trial diversion.

We support the prior bipartisan legislative efforts of this Subcommittee to limit the use, access, and display of the SSN in the public and private sectors; and to increase penalties against those who fraudulently misuse the SSN. Most recently, the Subcommittee introduced the *Social Security Number Privacy and Identity Theft Prevention Act of 2009*. This legislation included new criminal penalties for the misuse of SSNs; criminal penalties for SSA employees who knowingly and fraudulently issue Social Security cards or SSNs; and enhanced penalties in cases of terrorism, drug trafficking, crimes of violence, or prior offenses.

The legislation would also expand the types of activities that are subject to civil monetary penalties (CMP) and assessments under Section 1129 of the *Social Security Act*. Currently, an individual who misuses an SSN is not subject to a CMP, except in cases related to the receipt of Social Security benefits or Supplement Security Income. The legislation would authorize the imposition of CMPs and

assessments for activities such as providing false information to obtain an SSN, using an SSN obtained through false information, or counterfeiting an SSN.

The expanded use of the SSN in today's society has made it a valuable commodity for criminals. In addition to being a lynchpin for identity theft crimes, it also assists an individual to assimilate into our society, in some instances to avoid detection. The importance of SSN integrity to prevent identity theft and ensure homeland security is universally recognized. Providing enhanced, structured penalties is appropriate to reflect the vital importance of the SSN.

As we saw with Dr. Martinez, identity theft can take many forms, as an individual used his SSN to gain employment, rent an apartment, and open bank accounts. Identity theft is serious, and while OIG and SSA have controls in place to protect the SSN, we should all be aware of the dangers of being careless with our personal information. We urge people to keep their Social Security cards in a secure place, to shred personal documents, and to be aware of phishing scams, because no reputable financial institution or company will ask for personal information like an SSN via the Internet. It is also important to protect personal computers with a firewall and updated anti-virus protection.

Additionally, we should all be judicious in giving out an SSN in business transactions, because while it is required for financial transactions, an SSN is not necessary for everyday transactions like applying for a gym membership. It is also critically important that we all monitor our financial information regularly by checking credits report from one of the three major credit bureaus. By knowing how to protect ourselves, we can make life much more difficult for identity thieves.

In conclusion, SSA has a long history of protecting PII, and while current conditions may be the most challenging yet, we are confident SSA will rise to the occasion and address the challenges of today and tomorrow. Identity theft will undoubtedly persist for years to come, because of the reliance on the SSN as a national identifier and advances in technology and communication, but we are committed to ensuring that the information in SSA's records remains safe and secure. The SSN was never intended to do more than track a worker's earnings and to pay that worker benefits, but as the use of the SSN has expanded over the decades, its value has increased as a tool for criminals. Therefore, we must continue to ensure the integrity of the enumeration process; limit the collection, use, and public display of the SSN; encourage the protection of the SSN by those who use it legitimately; and provide meaningful sanctions for those who fail to protect the SSN or misuse it.

The OIG has done, and continues to do, significant audit and investigative work related to SSN misuse and identity theft. We will continue to provide information to Agency decision-makers and this Subcommittee about this critically important issue. I thank you again for the invitation to speak with you today, and I'd be happy to answer any questions.

Chairman JOHNSON. Thank you. I am told that most of the stolen numbers are from young people who have not yet begun to work. Is that your information?

Mr. O'CARROLL. I would qualify that by saying that a lot of them belong to children that haven't begun to work. And when people are vacuuming up numbers that are out there, often times they are targeting children's numbers. But I cannot say it is exclusive.

Chairman JOHNSON. That is because they have not ever recorded them anywhere.

Mr. O'CARROLL. Agreed.

Chairman JOHNSON. Yes. Thank you.
Ms. Mithal, you are recognized for five minutes.

**STATEMENT OF MANEESHA MITHAL, ASSOCIATE DIRECTOR
OF THE DIVISION OF PRIVACY AND IDENTITY PROTECTION,
FEDERAL TRADE COMMISSION**

Ms. MITHAL. Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, I am Maneesha Mithal from the Federal Trade Commission. I appreciate the opportunity to present the FTC's views on the role of Social Security numbers and identity theft.

Protecting consumers against identity theft is a critical component of our consumer protection mission. The Commission's written testimony describes the widespread use of SSNs in our economy, as well as its role in facilitating identity theft. In my oral statement I would like to focus on the FTC's activities to implement the recommendations of the President's 2007 identity theft task force, which the FTC's chairman co-chaired, along with the attorney general. I would like to highlight our implementation of four recommendations, in particular.

First, we have tried to find ways to reduce the use of SSNs in the public and private sectors. As to the public sector, federal agencies have taken a lot of steps to eliminate or restrict the use of SSNs. Most recently, as we have heard, the Department of Defense announced that it would stop using SSNs on military ID cards as of June 2011.

As to the private sector use of SSNs, we hosted a workshop and issued a report recommending federal legislation in a variety of areas. Among other things, we recommended legislation to reduce the public display of SSNs, and to improve consumer authentication.

Second, a key component of our efforts to combat identity theft is to make sure that consumers' sensitive data, including SSNs, don't fall into the hands of identity thieves. To that end, we enforce laws requiring companies to maintain reasonable security of consumers' information. Since 2001, the Commission has brought over 30 law enforcement actions challenging businesses that failed to reasonably protect sensitive consumer information.

Several of these cases have involved breaches of SSNs. One example is Choice Point. We sued Choice Point and alleged that it sold sensitive information about more than 160,000 consumers to identity thieves. We obtained \$15 million in monetary relief against the company.

More recently, we settled actions against three sellers of credit reports. These sellers allowed hackers to access sensitive credit report information, including SSNs. The settlements require each company to have comprehensive information security programs in place.

We also brought a case against a company called LifeLock, which deceptively advertised its identity theft protection services. Now, you may recall LifeLock's ads, in which the CEO displayed his own real Social Security number, stating that he guaranteed protection against identity theft. Of course, he later became a victim of identity theft. We worked with 36 state attorneys general to bring a

case against the company for deceptive practices, and we obtained \$12 million in monetary relief.

Third, in addition to bringing cases, we provide consumer assistance and education. We manage a toll-free Identity theft hotline, along with a dedicated website through which we receive 15,000 to 20,000 contacts each week. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft.

We also make available a wide variety of consumer education materials, including many in Spanish, to help consumers deter, detect, and defend against identity theft. I am now holding some examples of our consumer education materials, and I would be happy to provide additional copies to your staff after the hearing.

One successful strategy in disseminating our materials has been to provide them to first responders. For example, because victims often report identity theft to local law enforcement agencies, we inform these agencies on how to talk to victims. The FTC and its partners have provided identity theft training to over 5,400 law enforcement officers from over 1,700 agencies. Similarly, we have created a comprehensive guide to pro bono attorneys and legal services clinics who assist low-income identity theft victims.

Finally, we serve as a clearinghouse for information about identity theft. We make information in our complaint database available to over 2,000 law enforcement partners. To assist law enforcement and policy makers, we also routinely issue reports on the number and nature of identity theft complaints we receive. Most recently we announced that in 2010 we received 250,000 identity theft complaints, which represents 19 percent of the total number of complaints we received. Identity theft has remained a top complaint category for more than a decade.

Fighting identity theft continues to be a top priority for the FTC, and we look forward to working with the subcommittee on this important issue.

[The prepared statement of Ms. Mithal follows:]

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

on

Protecting Social Security Numbers from Identity Theft

Washington, DC

April 13, 2011

I. INTRODUCTION

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, I am Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s views on how Social Security numbers (“SSNs”) are used in identity theft. Protecting consumers against identity theft and its consequences is a critical component of the Commission’s consumer protection mission.²

This testimony begins by describing the nature of identity theft and the role SSNs play in facilitating it. It then summarizes the work that federal and state agencies have done to prevent the misuse of SSNs in the public sector, as well as the recommendations of the Commission’s 2008 Report on preventing the misuse of SSNs in the private sector.³ Finally, the testimony describes the Commission’s law enforcement, data collection and analysis, and education and outreach efforts on identity theft. In particular, it describes some of the 32 actions the

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any individual Commissioner.

² See Identity Theft and Assumption Deterrence Act, Pub. L. 105-318, 112 Stat. 3007 (1998). Among other things, this Act directs the FTC to establish the federal government’s central repository for identity theft complaints and to provide victim assistance and consumer education. The repository of identity theft complaints, known as the “Identity Theft Clearinghouse,” is discussed in greater detail below in Section IV.

³ FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008) (“SSN Report”), available at www.ftc.gov/os/2008/12/P075414ssnreport.pdf.

Commission has brought since 2001 challenging businesses that failed to reasonably protect sensitive consumer information that they maintained, including SSNs.

II. THE ROLE OF SOCIAL SECURITY NUMBERS IN IDENTITY THEFT

Millions of consumers are victimized by identity thieves each year,⁴ collectively costing consumers and businesses billions of dollars⁵ and countless hours to repair the damage. There are two predominant varieties of financial identity theft: the takeover or misuse of existing credit card, debit card, or other accounts (“existing account fraud”), and the use of stolen information to open new accounts in the consumer’s name (“new account fraud”).⁶ SSNs are valuable to identity thieves in committing both of these types of identity theft.

SSNs are widely used throughout our economy. With 300 million American consumers, many of whom share the same name, the unique nine-digit SSN provides a key tool to identify individual consumers.⁷ Financial institutions, insurers, businesses, universities, health care providers, government, and others use SSNs to ensure accurate matching of consumers with their information within organizations, to match consumers with information held by other organizations, and to avoid the costs and burdens of establishing different identification systems

⁴ See Bureau of Justice Statistics, *National Crime Victimization Survey Supplement, Victims of Identity Theft, 2008* (Dec. 2010) (“BJS Supplement”) at 1-2 (finding 11.7 million persons, representing 5% of all Americans age 16 or older, were victims of identity theft during a two-year period).

⁵ *Id.* at 4 (finding the total financial cost of identity theft was 17.3 billion dollars over a two-year period).

⁶ Although less prevalent, new account fraud typically causes considerably more harm to consumers.

⁷ See generally General Accounting Office, *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information* (GAO 04-01) (2004), available at <http://www.gao.gov/new.items/d0411.pdf>.

for each set of consumer records. For example, financial institutions generally require SSNs to open new accounts, either by law or because SSNs enable them to obtain creditworthiness information from consumer reporting agencies. In addition, SSNs often are used to control access to existing accounts by serving as internal identifiers to match consumers with their records, and for authentication purposes. Consumer reporting agencies use SSNs to ensure that data furnished to them is placed in the correct consumer file and that they are providing a credit report on the correct consumer. Businesses and other entities use these reports in making eligibility and pricing decisions for a variety of products and services, including credit, insurance, home rentals, or employment. At the same time, SSN databases also are used to fight identity fraud – for example, to confirm that a SSN provided by a loan applicant does not, in fact, belong to someone who is deceased.

Additionally, federal, state, and local governments rely extensively on SSNs in administering programs and providing services to consumers.⁸ For example, the Internal Revenue Service (“IRS”) requires private sector entities, including banks, insurance companies, and employers, to collect SSNs for income and tax-related purposes. The federal government also uses SSNs to administer the federal jury system, as well as federal welfare and worker’s compensation programs. SSNs are also used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments.

The widespread use of SSNs to identify individuals in both the private and public sectors makes them readily available and valuable to identity thieves. Thieves gather SSNs in many

⁸ See Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), Chapter II, available at www.ssa.gov/history/reports/ssnreportc2.html.

ways, from the high-tech (e.g., hacking, phishing, malware, spyware, and keystroke loggers) to the low-tech (e.g., dumpster diving, stealing workplace records, stealing mail or wallets, and accessing public records containing SSNs).⁹ The challenge in combating the misuse of SSNs is to find the proper balance between the need to keep SSNs out of the hands of identity thieves and the need to give businesses and government entities sufficient means to attribute information to the correct person.

III. ACTIONS AND RECOMMENDATIONS TO PREVENT MISUSE OF SOCIAL SECURITY NUMBERS

Over the past several years, the federal government has taken numerous steps to prevent the misuse of SSNs in the public sector.¹⁰ For example, the Office of Personnel Management (“OPM”) has been reviewing its use of SSNs in collecting human resource data from federal agencies and on OPM forms, and taking steps to eliminate, restrict, or conceal their use whenever possible.¹¹ Further, OPM issued guidance to federal agencies on the appropriate and

⁹ SSN Report, *supra* note 3, at 3.

¹⁰ In May 2006, President Bush established an Identity Theft Task Force, comprised of 17 federal agencies, and co-chaired by the FTC’s Chairman. The Task Force’s mission was to develop a comprehensive national strategy to combat identity theft. See The President’s Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (April 2007), available at www.identitytheft.gov/reports/StrategicPlan.pdf. In September 2008, the Task Force published its recommendations. See The President’s Identity Theft Task Force, *Task Force Report* (Sept. 2008) (“Task Force Report”), available at www.idtheft.gov/reports/IDTReport2008.pdf. A number of the activities described in this section are the result of these recommendations. Federal agencies continue to implement the Task Force recommendations. For example, the Department of Defense recently announced the discontinuance of SSNs on identification cards beginning June 1, 2011. A news release explaining this policy is available at www.defense.gov/news/newsarticle.aspx?id=63409.

¹¹ Task Force Report, *supra* note 10, at 6-7.

inappropriate use of SSNs in federal employee records.¹² Additionally, the FTC, Social Security Administration (“SSA”), and IRS have coordinated with states and local governments to encourage: (1) a reduction in the need for, and display of, SSNs on public documents, especially online documents, (2) the improvement of data security, and (3) the protection of tax payer information.¹³

With respect to private sector uses of SSNs, the FTC hosted a two-day workshop in December 2007 to examine ways to make SSNs less valuable and less accessible to identity thieves. In December 2008, the Commission issued a report, containing four legislative recommendations in this area.¹⁴ The Commission continues to believe that these recommendations are still needed.

First, the Commission recognized that because there has been widespread use and availability of SSNs, any solution to the misuse of SSNs must include reducing their value to identity thieves through improved consumer authentication.¹⁵ As detailed in the report, this can be achieved by encouraging or requiring all private sector businesses and organizations that have

¹² Task Force Report, *supra* note 10, at 7. On June 18, 2007, OPM issued “Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft” to the Chief Human Capital Officers of all federal departments and agencies, *available at* www.chcoc.gov/Transmittals/Attachments/trans847.pdf. That Guidance has two goals: (1) to eliminate the unnecessary use of SSNs in federal personnel records; and (2) to strengthen the protection of employees’ sensitive information from theft or loss.

¹³ Task Force Report, *supra* note 10, at 9-10.

¹⁴ *See generally* SSN Report, *supra* note 3.

¹⁵ *Id.* at 6-7. “Authentication” is the process of verifying that someone is who he or she claims to be. Financial institutions, government agencies, and countless other organizations that enter into transactions with consumers authenticate individuals on a regular basis. It is when authentication fails – when an imposter successfully presents himself as someone else – that identity theft occurs. Good authentication reduces the likelihood that identity thieves can use stolen data to assume another’s identity.

consumer accounts to adopt appropriate, risk-based consumer authentication programs that do not rely on SSNs alone to authenticate consumers. This approach would make it more difficult for thieves to use SSNs to open new accounts or access existing accounts.¹⁶ To that end, the Commission recommended that Congress consider establishing national consumer authentication standards to verify that consumers are who they purport to be.¹⁷

Second, the Commission recommended that Congress consider creating national standards to reduce the public display and transmission of SSNs, such as by eliminating their unnecessary display on publicly-available documents and identification cards and limiting how they can be transmitted.¹⁸ Such steps would reduce the availability of SSNs to thieves, without hindering the use of SSNs for legitimate identification and data-matching purposes.

Third, the Commission recognized that an important step in limiting identity thieves' access to SSNs is for entities that collect and store them to maintain reasonable safeguards against unauthorized access. Thus, the Commission expressed support for national data security standards that would cover SSNs in the possession of any private sector entity.

Finally, the Commission supported national data breach notification standards requiring private sector entities to provide public notice when they suffer a breach of consumers' personal

¹⁶ Congress directed the Commission and banking regulatory agencies to promulgate a rule requiring certain covered entities to be on guard against "red flags" of possible identity theft in their day-to-day operations. The resulting Red Flags Rule suggests that one way to detect the red flags of identity theft is to have in place procedures for authenticating customers. *See* 16 C.F.R. Part 681.

¹⁷ The SSN report recommended that an authentication requirement cover all private sector entities that maintain consumer accounts, other than financial institutions already subject to authentication requirements promulgated by bank regulatory agencies. SSN Report, *supra* note 3, at 6.

¹⁸ *Id.* at 8-9.

information.¹⁹ In addition to alerting affected consumers to protect themselves, such a law would have the indirect benefit of motivating companies to weigh their need to collect SSNs against the potential cost and liability that may ensue if collected SSNs are compromised.²⁰

IV. COMMISSION ACTIVITIES TO COMBAT IDENTITY THEFT

In addition to making these recommendations, the Commission has used its existing authority and resources to implement a longstanding and comprehensive program to combat identity theft, acting aggressively on three fronts: law enforcement, data collection, and consumer and business education.

A. Law Enforcement

The Commission enforces a variety of specific statutes and regulations that restrict disclosure of SSNs in particular contexts. For example, the Fair Credit Reporting Act (“FCRA”) requires consumer reporting agencies to truncate the SSN on consumer reports at the consumer’s request when providing the reports to the consumer.²¹ Eliminating the unnecessary display of this information could lessen the risk of it getting into the wrong hands.

¹⁹ Congress enacted a federal breach notification law in the health area, enforced by the Department of Health and Human Services and the FTC. *See* American Recovery and Reinvestment Act of 2008, Pub. L. 111-5, 123 Stat. 155 (2009). To implement this law, the Commission promulgated the Health Breach Notification Rule, 16 C.F.R. Part 318, which requires certain entities within the Commission’s jurisdiction that offer personal health records and related services to provide consumers with notification in the event of a security breach.

²⁰ *See also* FTC Staff, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at www.ftc.gov/os/2010/12/101201privacyreport.pdf (recommending that companies should protect consumers by not collecting information they do not need, securing information they do collect, and not retaining information they no longer need).

²¹ 15 U.S.C. § 1681(g).

In addition, the Commission enforces a variety of laws requiring entities, in some circumstances, to have reasonable procedures in place to secure consumer information, such as SSNs. For example, the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act contains data security requirements for financial institutions.²² The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,²³ and imposes safe disposal obligations on entities that maintain consumer report information.²⁴ In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices²⁵ in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.

Since 2001, the Commission has brought 32 law enforcement actions challenging businesses that failed to reasonably protect sensitive consumer information that they maintained. Several Commission cases have involved breaches of SSNs. One of the best-known FTC data security cases is the 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including SSNs in some instances) concerning more than 160,000

²² 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

²³ 15 U.S.C. § 1681e.

²⁴ *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

²⁵ 15 U.S.C. § 45(a).

consumers to data thieves posing as ChoicePoint clients.²⁶ In many instances, the thieves used that information to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of its information and ignored obvious security red flags. For example, the FTC alleged that the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for violations of the FCRA and \$5 million in consumer redress for identity theft victims, and agreed to undertake new data security measures.²⁷

More recently, the Commission reached settlements with two pharmacy chains – CVS Caremark²⁸ and Rite Aid²⁹ – alleging that both companies failed to take reasonable and appropriate security measures to protect sensitive financial and medical information concerning customers and employees. As a result, information such as employment records and pharmacy labels were found in open trash dumpsters. Settlements with the two companies require them to establish comprehensive information security programs.

²⁶ *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006).

²⁷ In 2009, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay monetary relief in the amount of \$275,000. *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. (settlement entered on Oct. 14, 2009). In bringing cases under section 5, Commission staff routinely collaborate with state Attorneys General and other federal and state authorities, as it did in *Choicepoint*.

²⁸ *CVS Caremark Corp.*, FTC No. C-4259 (June 18, 2009).

²⁹ *Rite Aid Corporation.*, FTC No. C-4308 (Nov. 12, 2010).

Finally, earlier this year, the Commission settled actions against three credit report resellers,³⁰ alleging violations of the FCRA, the FTC Act, and the Safeguards Rule. Due to their lack of information security policies and procedures, these companies allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access sensitive consumer reports through an online portal. By failing to ensure that their clients maintained basic security protections when accessing the portal, the companies enabled hackers to access more than 1,800 credit reports without authorization. The settlements require each company, among other things, to have comprehensive information security programs in place to protect the security, confidentiality, and integrity of consumers' personal information.

B. Data Collection and Analysis

In addition to law enforcement, the Commission collects and analyzes identity theft complaint data in order to target its education efforts and assist criminal law enforcement authorities. The Commission manages the Identity Theft Clearinghouse, a secure online database of identity theft-related complaints. Identity theft victims can enter complaint information directly into the database via an online complaint form or by calling a toll-free identity theft hotline and speaking with a trained counselor. The Commission makes the Clearinghouse data available to over 2,000 American and Canadian federal, state, and local law enforcement agencies who have signed confidentiality and data security agreements.³¹ Through

³⁰ *SettlementOne Credit Corp.*, FTC File No. 082 3208; *ACRAnet, Inc.*, FTC File No. 092 3088; *Fajilan and Assoc., Inc.*, FTC File No. 092 3089 (Feb. 3, 2011) (consent orders accepted for public comment). A news release and links to these cases is available at <http://www.ftc.gov/opa/2011/02/settlement.shtm>.

³¹ For example, each of the 50 Offices of the Attorney General have access to the Clearinghouse data.

the Clearinghouse, law enforcers can search identity theft complaints submitted by victims, law enforcement organizations, and the Identity Theft Assistance Center, a not-for-profit coalition of financial services companies. To assist law enforcement and policy makers, the FTC also routinely issues reports on the number and nature of identity theft complaints received by the FTC.³²

C. Consumer and Business Education

Consumer and business education is another important part of the Commission's mission. The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives about 15,000 to 20,000 contacts each week through its toll-free hotline and dedicated website. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft.

Further, the FTC makes available a wide variety of consumer educational materials, including many in Spanish, to help consumers deter, detect, and defend against identity theft. For example, the FTC publishes a victim recovery guide – *Take Charge: Fighting Back Against Identity Theft*³³ – that explains the immediate steps identity theft victims should take to address the crime; how to obtain a credit report and correct fraudulent information in credit reports; how

³² See, e.g., FTC, *Consumer Sentinel Network Data Book for January - December, 2010* (Feb. 2011), available at <http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf>. The 2010 Data Book shows that over 250,000 consumers reported some form of identity theft, which represents 19% of the total number of complaints submitted to the Commission. This makes identity theft the most frequently reported category of consumer complaints, continuing a pattern that started over a decade ago.

³³ Available at www.ftc.gov/bcp/ed/pubs/consumers/idtheft/idth04.pdf.

to file a police report;³⁴ and how to protect personal information. The Commission has distributed over 3.8 million copies of the recovery guide and has recorded over 3.5 million visits to the Web version.

The Commission also sponsors a multimedia website, OnGuard Online,³⁵ designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudulent operators. OnGuard Online was developed in partnership with other government agencies and technology companies. Visitors to the site can download educational games and videos, learn more about specific topics, including phishing and social networking, and obtain useful tips and information in an interactive format.

The Commission directs its outreach to businesses as well.³⁶ It has developed a brochure and an online tutorial³⁷ that set out the key components of a sound data security plan. These materials alert businesses to the importance of data security and give them a solid foundation on how to address those issues. In addition, the FTC creates business educational materials to

³⁴ The FCRA also provides identity theft victims with additional tools to recover from identity theft. For example, identity theft victims who provide police reports to a consumer reporting agency may obtain a seven-year fraud alert on their credit files, alerting potential users of their reports to exercise special vigilance in opening accounts in the consumers' names. In addition, victims may block fraudulent information on their credit files, obtain from creditors the underlying documentation associated with transactions that may have been fraudulent, and prohibit creditors from reporting fraudulent information to the consumer reporting agencies. See FCRA, 15 U.S.C. §§ 605A, 605B, 609(e), and 611.

³⁵ Available at www.onguardonline.gov. A Spanish-language counterpart, Alerta En Línea, is available at www.alertaenlinea.gov.

³⁶ See FTC, *Protecting Personal Information: A Guide for Business*; and FTC, *Information Compromise and Risk of Identity Theft: Guidance for Your Business*. Both publications are available at <http://business.ftc.gov>.

³⁷ The tutorial is available at www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html.

address particular risks. For example, the Commission developed a new business education brochure – *Peer-to-Peer File Sharing: A Guide for Business*³⁸ – to educate businesses about the risks associated with P2P file sharing programs and advise them about ways to address these risks.

Finally, the Commission leverages its resources by providing educational and training materials to “first responders.” For example, because victims often report identity theft to state and local law enforcement agencies, the FTC informs law enforcers on how to talk to victims about identity theft.³⁹ The Commission also distributes a law enforcement resource CD Rom that includes information about how to assist victims, how to partner with other law enforcement agencies, how to work with businesses, and how to access the Identity Theft Clearinghouse. In addition, the FTC and its partners have provided identity theft training to over 5,400 state and local law enforcement officers from over 1,770 agencies.

Similarly, the FTC has encouraged the development of a nationwide network of *pro bono* clinics to assist low-income identity theft victims. As part of this initiative, the FTC has created a comprehensive guide for advocates providing legal assistance to identity theft victims. The Guide for Assisting Identity Theft Victims (*Pro Bono Guide*)⁴⁰ describes how advocates can intervene with creditors, credit reporting agencies, debt collectors, and others, and it provides self-help measures that victims can take to address their problems. Step-by-step instructions

³⁸ Available at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm. Peer-to-Peer (P2P) technology enables companies to form a network in order to share documents and to facilitate online telephone conversations.

³⁹ Resources for law enforcement are available at www.ftc.gov/idtheft.

⁴⁰ The *Pro Bono Guide* is available at www.idtheft.gov/probono.

provide best practices for recovering from identity theft.

V. CONCLUSION

Identity theft remains a serious problem in this country, causing enormous harm to consumers, businesses, and ultimately our economy. The Commission will continue to play a central role in the battle against identity theft and looks forward to working with this Subcommittee on this important issue.

Chairman JOHNSON. Ms. Gruber, you are recognized for five minutes.

STATEMENT OF THERESA L. GRUBER, ASSISTANT DEPUTY COMMISSIONER, OFFICE OF OPERATIONS, SOCIAL SECURITY ADMINISTRATION

Ms. GRUBER. Thank you. Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, my name is Theresa Gruber, and I am the Assistant Deputy Commissioner for Operations at the Social Security Administration. I have worked for the Agency for nearly 20 years, starting in one of our field offices in Minnesota. In my current role I oversee the operation of more than 1,200 Social Security offices, 8 card centers, 33 1-800-number tele-service centers, and 8 processing centers.

Thank you for the opportunity to discuss how we assign Social Security numbers, and the role that the Social Security number, or SSN, can play in identity theft. My written statement provides details on the history of the SSN, and I will focus today on what we have done to improve and strengthen our enumeration and card issuance processes.

Originally, the only purpose of the Social Security number was to keep an accurate record of earnings under Social Security, and to pay benefits based on those earnings. We provided the SSN card to show what SSN we assigned to a particular individual, with the idea that, when shown to an employer, that employer would be able to properly report that individual's earnings. The card was never intended, and does not serve, as a personal identification document.

Assigning SSNs has been one of our most important and significant workloads. Since the inception of the program, we have assigned about 465 million Social Security numbers. Last fiscal year we assigned 5.5 million original Social Security numbers, completed 11.5 million requests for replacement cards, and processed over 1 billion verifications of SSNs.

Although the card is not an identification document, unscrupulous individuals use the SSN to steal identities and obtain false identification documents.

I would like to thank you for helping us to strengthen our SSN assignment process, for example, through the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004. As a result of this legislation, we have implemented numerous changes to our assignment process. We added new security features to the card to help prevent counterfeiting. We also limited the number of replacement cards we issue to any one individual, and established new, rigorous standards for evidence.

As an agency, we are always looking for ways to improve the security and efficiency of our records. For example, we know that we have to expand the pool of nine-digit numbers available for assignment. To that end, we plan to implement this summer a new assignment methodology called "SSN randomization." Randomization will help protect the Social Security number by eliminating any geographic significance in the number, and making it more difficult to reconstruct an SSN using public information. As a result, the new process will also extend the pool of SSNs available for assignment nationwide.

We have also taken a number of steps to improve the way we assign Social Security numbers. First, we opened two new Social Se-

curity card centers, bringing our total now to eight. These specialized centers process all applications for original SSNs and replacement cards in specific metropolitan areas.

In coordination with the Department of State and the Department of Homeland Security, we expanded the Enumeration at Entry program, permitting all individuals applying for an immigrant visa to elect to receive an SSN at the time of initial admission. This program allows us to use information collected and verified by both agencies to assign an SSN automatically.

We have implemented and are continuing to enhance our new Social Security Number Application Process, which our field offices use to process SSN applications. This automated system ensures uniform compliance with our enumeration policies and evidence requirements.

In conclusion, we must remember that with all the improvements in the way we assign SSNs, the Social Security card is still just a record of an SSN assigned to an individual, and not an identity document. We understand the use of the SSN for other purposes has grown exponentially over the years. The challenge we face is to balance our commitment to assigning SSN numbers quickly and accurately, with the equally important need to maintain the integrity of the enumeration system, and to prevent SSN fraud.

I want to thank the Chairman and the Members of the Subcommittee for inviting me here today, and look forward to your continued support for our Agency and our mission. I will be happy to answer any questions.

[The prepared statement of Ms. Gruber follows:]



HEARING BEFORE
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

THE ROLE OF SOCIAL SECURITY NUMBERS IN IDENTITY THEFT

APRIL 13, 2011

STATEMENT OF
THERESA L. GRUBER
ASSISTANT DEPUTY COMMISSIONER
OFFICE OF OPERATIONS

Introduction

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, thank you for inviting us to participate in these important oversight hearings about Social Security numbers (SSNs), how and for whom we verify SSNs, and the relationship between SSNs and identity theft. My testimony today will focus on how we assign SSNs and the role SSNs can play in identity theft.

As you know, Social Security touches the lives of every American, often during difficult times of personal hardship, transition, and uncertainty. We serve the public through a network of 85,000 Federal and State employees who work in offices across the country and even the world. Each day almost 200,000 people visit our field offices. Many people come to our offices for scheduled appointments made weeks in advance, and some visitors must travel a significant distance. Over 450,000 people call us every day for a variety of services such as filing claims, asking questions, and changing direct deposit information.

Our annual numbers are even more staggering. During Fiscal Year 2010, we paid 58 million Americans over \$740 billion in benefits. Specifically, we paid \$572.5 billion in Old-Age and Survivor Insurance benefits, \$129.9 billion in Disability Insurance benefits, and \$47.2 billion in Supplemental Security Income payments. During this same time, we received 45 million visitors to our field offices, conducted almost 68 million transactions over our toll-free 800 number telephone system, and held over 737,000 disability hearings.

We have a long-standing and well-deserved reputation as a “can-do” agency. Our hard-working dedicated employees have done their utmost to maintain the level of service that the American people expect and deserve. We have been innovative and proactive in adopting strategies to allow us to meet the challenges we face. To the extent resources allowed, we hired and trained staff to handle our increased workloads, and used technology to complement our traditional work processes and make them more efficient.

History of the Social Security Number

Following the passage of the Social Security Act in 1935, the SSN was devised as a way to keep track of the earnings of people who worked in jobs covered under the new program. The Department of Treasury published regulations in 1936 that require workers covered by Social Security to apply for an SSN.

The purpose of the SSN is to keep an accurate record of earnings covered under Social Security and to pay benefits based on those earnings. Names alone cannot ensure accurate reporting, but the combination of a name and an SSN provides a system for accurately reporting and recording wage information. Properly crediting earnings to the correct SSN ensures that we can determine eligibility for retirement, survivors, and disability benefits and pay the correct benefit amount. If we cannot properly record a worker's earnings, he or she may not qualify for Social Security benefits or the amount of benefits paid may be wrong.

The SSN card shows the SSN we assigned to a particular individual. When shown to an employer, the card assists the employer in properly reporting earnings. The SSN card was never intended, nor does it serve, as a personal identification document. Although we have made many changes over the years to make the card counterfeit-resistant and continue to work to strengthen its security, the card does not contain personal information that proves a person's identity.

Assigning SSNs and issuing SSN cards has always been one of our most significant workloads. We have assigned about 465 million SSNs since the inception of the program. In FY 2010, we assigned 5.5 million original SSNs, issued 11.2 million replacement SSN cards, and processed over 1 billion SSN verifications.

How We Assign SSNs and Cards

We issue the vast majority of original Social Security cards to United States citizens or to noncitizens who are permanently authorized to work in the United States. These cards show only the name and SSN of the individual.

Originally, we assigned SSNs and issued cards based solely on the applicants' allegations of name, date of birth, and other personal information. We required no documentation to verify that information. Today, applicants for an SSN and SSN card must submit evidence of age, identity, and United States citizenship or current work-authorized immigration status. In most cases, individuals (other than newborn babies) must come into a Social Security field office or Card Center to apply for an SSN and SSN card. We require an in-person interview of all applicants age 12 or older. During the interview, we attempt to locate a prior SSN to help ensure that we do not assign an SSN to an individual assuming a false identity. We verify the birth records for United States citizens requesting an original card and the immigration documents presented by noncitizens requesting original or replacement cards.

Enumeration at Birth Process (EAB)

Most newborn babies get their Social Security numbers through the EAB process. EAB allows parents to indicate on the birth registration form whether they want an SSN assigned to their newborn child. When a parent requests an SSN for a child, the State vital statistics office receives the request with the birth registration data from the hospital and then forwards this information to us. Based on the information the State forwards to us, we assign an SSN and issue a card for the child.

Hospitals, States, and other jurisdictions participate in EAB voluntarily. We administer the program pursuant to a contract between us and each State. We reimburse States for their participation on a per item basis (currently \$2.40 for each birth record). EAB is a secure and convenient service option for parents to request an SSN. The program also provides significant savings to the Federal Government.

All fifty States, the District of Columbia, and Puerto Rico participate in EAB. We assign SSNs to about 98 percent of newborns through EAB. In FY 2010, we issued approximately four million SSNs through this process.

Enumeration at Entry (EAE)

In 2002, we established the EAE program in coordination with the Department of State (DOS) and the Department of Homeland Security (DHS). This program allows us to use information collected and verified by these agencies to assign SSNs automatically to lawful permanent residents upon their initial admission to the United States in that status.

Intending lawful permanent residents can apply for both an immigrant visa and an SSN by filing an immigrant visa application at a DOS office in his or her home country. When an individual gets a visa, State transmits the identifying information from the visa application to DHS. When the immigrant enters the United States, DHS notifies us and we issue the card. In FY 2010, we issued over 144,000 SSNs using EAE.

SSNs and Cards for Individuals with Temporary or No Work Authorization

We also assign a small number of SSNs and issue cards to aliens legally in the United States but to whom DHS has not granted work authorization. We refer to these SSNs as “non-work” SSNs. In FY 2010, we issued about 28,000 non-work SSNs.

A non-work SSN card bears the legend "Not Valid for Employment." We issue such an SSN only when: (1) a Federal statute or regulation requires an SSN to receive a particular benefit or service (for example, Temporary Assistance to Needy Families, or TANF), for which a noncitizen has otherwise established entitlement; or (2) a State or local law requires an SSN to get public assistance benefits, for which the noncitizen has otherwise established entitlement and for which all other requirements have been met.

We also issue SSNs and cards to noncitizens lawfully in the United States with temporary authorization to work. The legend on these cards reads "Valid for Work Only with DHS Authorization." In these cases, employers must look at the noncitizen's DHS documents to determine if the individual has current work authorization.

While a person's basis for work authorization may change, if he or she does not report the change to us (the law does not require cardholders to do so), then we cannot update our records. As a result, we may credit earnings to what appears to be a non-work number on our records. This does not necessarily mean that the person performed unauthorized work. We have been discussing with DHS the feasibility of using DHS work authorization records to update our records as necessary.

Integrity of Social Security Cards

When Social Security began, there was little incentive to counterfeit Social Security cards. However, as the card's use expanded and technology improved, counterfeiting became a concern. In 1983, the Social Security Act required that SSN cards be made of banknote paper and be counterfeit-resistant to the maximum extent practicable. We worked with the Bureau of Engraving and Printing, the Secret Service, and the Federal Bureau of Investigation to design a card that met these requirements.

The expertise of counterfeiters and the wide availability of state-of-the-art technology make it increasingly difficult to develop and maintain a document that cannot be counterfeited, despite our best efforts to guard against such incidents. We continue to evaluate new technology as it becomes available to determine if additional features should be included.

Pursuant to the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, we formed an interagency Task Force with DHS to establish requirements for further improving the security of Social Security cards and numbers. In

2007, we implemented numerous changes to the card based on taskforce recommendations. The new security features include:

- A guilloche background pattern, which is a unique, computer-generated, non-repeating spiral design;
- A latent image, visible only when viewed at specific angles;
- Color shifting inks, like those in the Nation's currency, that create a noticeable color shift when moved in front of a light source; and
- The card issuance date, reflecting the date we processed the card application.

The card includes other security features that we have not made public in order to protect the card's integrity.

Additional Efforts to Strengthen and Improve the Enumeration Process

We have great confidence in the integrity of our SSN records. In fact, our Office of the Inspector General (OIG) has commended the accuracy of the information in our Numident file, which is our electronic repository of all SSNs.

We continue to look for ways to improve the security and efficiency of our records. For example, we know we have to expand the pool of numbers available for assignment nationwide and plan to implement a new SSN assignment methodology, called SSN Randomization, this summer. We developed this new methodology to help protect the integrity of the SSN and to extend the longevity of the nine-digit SSN nationwide. SSN randomization will also help protect against SSN fraud and misuse. It will be more difficult to reconstruct an SSN using publicly available information, which is becoming more prevalent as public and private entities increasingly use the SSN to verify identity.

Our current SSN assignment process limits the number of SSNs available for issuance by each State, because the first three digits of the SSN are determined by the ZIP code in the mailing address on the SSN application. The new process will eliminate the geographical significance of the first three numbers, thereby extending the pool of SSNs available for assignment nationwide.

We made several other improvements to our enumeration services:

- We opened two additional Social Security Card Centers—in Sacramento, California and Minneapolis, Minnesota—bringing our nationwide total to eight card centers. These specialized centers process all applications for original SSNs and replacement cards in specific service areas. As a

result, individuals using Card Centers have shorter wait times than in the local offices help ensure accuracy because the employees only focus on SSN work, and the surrounding Social Security offices are able to focus on other critical workloads.

- We have a video service delivery (VSD) pilot that allows certain individuals to apply for replacement SSNs over video links in remote locations in North Dakota, Wyoming, Utah, and Alaska. VSD is a secure, reliable, and effective way to serve those people who might otherwise have to travel great distances to conduct business with us. VSD may help reduce the volume of applications for SSNs submitted by mail from certain remote communities, without compromising the integrity of our enumeration process.
- We expanded EAE to permit all individuals applying for an immigrant visa, regardless of age, to elect to receive a SSN at the time of their entry so that they do not have to visit a field office; and,
- We successfully implemented the Social Security Number Application Process (SSNAP). Our field office staff uses this system to process SSN card applications. SSNAP strengthens the agency's overall enumeration processes by enforcing uniform compliance with our enumeration policies and improving service to the public. We expect to release an update to this program later this year.

Congress has required changes that have also strengthened the integrity of the enumeration process. IRTPA limits an individual to three replacement SSN cards per year and ten per lifetime (with limited exceptions). IRTPA also required us to add death and fraud indicators to SSN verification routines for employers and for State agencies issuing driver's licenses and identity cards.

IRTPA also required us to establish minimum standards for verification of documents submitted in connection with an SSN. Therefore, we established rigorous new standards for evidence of United States citizenship and identity submitted in connection with an application for an SSN. We now require evidence of the highest probative value, such as a United States passport.

Expanded Use of the SSN

Contrary to the limited purpose of the SSN, more and more people and systems are using the SSN as a convenient means of identifying people in records systems. 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 an explosion in SSN usage, which came about during the advent of computer technology in the 1960s. 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. Today, both the public and private sectors use the SSN nearly universally as a personal identifier. The implications for personal privacy caused by the widespread use of a single identifier have generated concern both within the Government and in society in general. As use of the SSN has expanded, so have our workloads. SSN verifications are now a much larger piece of our workload.

We perform these verifications primarily through regular automated data exchanges. We actively participate in data matches to ensure the accuracy of Federal and State benefit payments, to verify whether applicants are eligible for benefits, to undertake debt collection activities, and to safeguard program integrity. In addition, we verify SSNs for employers to ensure the correct posting of wages and for other Federal benefit-paying programs to help reduce their program costs. Where required by law and, in certain circumstances where permitted by law, we verify that the name and SSN in the files of third parties match those on our SSN records.

SSN Verification Processes

I understand that tomorrow, this subcommittee will be hearing our testimony on the SSN verification services that we provide to the employer community. Today, I will focus on verification services we offer to government agencies and third parties.

Federal and State Agencies

Many Federal, State, and local agencies request SSN verification services for numerous purposes. Some of the agencies receive information because of legislation. These organizations include, but are not limited to:

- The Department of Education;
- The Department of Justice;
- The Office of Child Support Enforcement;
- The Internal Revenue Service;
- The Department of Veterans Affairs;
- The Selective Service System;

- Any Federal agency which uses the SSN as a numerical identifier in their record system;
- Federal, State, and local agencies for validating the SSN used in administering income or health maintenance programs;
- Federal, State, and local agencies involved in programs such as Temporary Assistance for Needy Families, Supplemental Nutrition Assistance, Medicaid, and Unemployment Insurance for which Federal statute authorizes SSN use;
- State Motor Vehicle Agencies; and
- Inspectors General for several government agencies.

Third Parties

Under the Privacy Act, we may verify or release SSNs to third parties that have obtained the written consent of the number holder, regardless of the purpose of the request. We have been providing such third party verifications for many years through existing verification processes.

Identity Theft

We want 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. We understand the fundamental role the SSN can play in helping unscrupulous individuals steal identities and obtain false identification documents. To this end, we ask that people be careful with their SSN and card; in fact, we tell people that they should not carry their card with them. A new hire should show the card to an employer to ensure employment records are correct, and then secure the card in a safe place.

To help victims of identity theft:

- We provide numbers to our Fraud Hotline and the Federal Trade Commission ID Theft Hotline;
- We provide up-to-date information about steps the person can take to work with credit bureaus and law enforcement agencies to reclaim their identity;
- We issue a replacement card when individuals have their Social Security card stolen;
- We help to correct their earnings record and issue a new SSN in certain circumstances; and

- We develop the case as a possible fraud violation and, where appropriate, refer the case to the OIG for investigation if the victim alleges that a specific individual is using the stolen SSN.

As I noted above, we have made a number of changes to the Social Security card to ensure its integrity. We have also improved our enumeration process to help ensure that we issue SSNs only to people who are entitled to them. While we cannot control the disclosure of SSNs by individuals, we are doing all that we can to ensure the integrity of our processes.

Conclusion

The architects of the Social Security program originally intended the Social Security number as a means to provide a record of the earnings of people who worked in jobs covered under the new Social Security program. The use of the SSN for other purposes has grown significantly over the years. The challenge we face is to balance our commitment to assigning numbers quickly and accurately to individuals who qualify for them and need them to work, with the equally important need to maintain the integrity of the enumeration system to prevent SSN fraud and misuse.

We will continue to provide the best service we possibly can. Our ability to deliver service to the American public depends upon sustained, timely, and adequate funding. With the full funding of the President's 2012 budget request, we can continue to fulfill our core mission and meet the needs of the public.

I want to thank the Chairman, Ranking Member, and members of the Subcommittee for inviting me here today, and I look forward to working with you to continue to improve our processes.

Chairman JOHNSON. Thank you for your testimony. And we will proceed to questions.

Let me ask you a question, first. How much does it cost to issue a Social Security card?

Ms. GRUBER. It depends on the manner in which you get the card. If you come into one of our—

Chairman JOHNSON. You mean all the offices aren't the same?

Ms. GRUBER. Well, actually, if you come into our field office, it costs about \$32. If you go through one of our automated processes, a process called "Enumeration at Birth," where we assign a Social Security number for a child who is born, that is about \$8. And—

Chairman JOHNSON. Eighty?

Ms. GRUBER. Eight dollars.

Chairman JOHNSON. Oh.

Ms. GRUBER. And if you do it through the Enumeration at Entry program that I talked about, it is about \$5.

Chairman JOHNSON. How about if we charged for that?

Ms. GRUBER. We would be happy to work with the subcommittee on exploring that option.

Chairman JOHNSON. You all think about that. Let me ask you a couple of questions.

Mr. O'Carroll, do you have all the tools you need to protect the Social Security number?

Mr. O'CARROLL. Chairman Johnson, as we have heard during the testimony here, the number is out of the box, and it is pretty widely displayed, and it is out there. So it is pretty hard to keep the SSN as private and secure as we would have preferred and liked.

But, with that, I think the tools that we could use are any ways to limit the collection of Social Security numbers, much like you were saying, when a vendor is asking for it but doesn't need it. The display of Social Security numbers is a problem. We have been trying to get SSNs off of government checks. It is being removed from some government IDs—as you are proposing now, off of the Medicare card—and that is another good tool. And the last one is just the collection of SSNs, in terms of limiting financial institutions' collection of Social Security numbers, which can end up in a PII breach, as you discussed in Texas. That is another concern of ours.

So, what we are looking for is more of any tool that will at least prevent it being displayed more than it is now, and being compromised.

Chairman JOHNSON. I understand that while we have restricted the number of Social Security number replacement cards, people can visit a local office and get a print-out with their number on it. And that they can easily be used by ID thieves. Why is it we are doing that? I mean isn't it just as easy to print them a new card?

Mr. O'CARROLL. Well, we are almost a victim of a success on that one. And under the Identity Theft Act that was passed by Congress we have limited the number of cards that are being issued. So, remember, in the past it was unlimited numbers of cards going to people. That has been restricted now, and so—

Chairman JOHNSON. Well, it is still free, isn't it?

Mr. O'CARROLL. It is still free, but we are limiting the number that can be received each year, and the number in a lifetime. And what that caused is anybody who needs a Social Security number, hasn't been safeguarding it, doesn't keep it carefully, is coming into the offices now, asking for the print-outs instead of a replacement card.

And I think a secondary problem that has come with the print-out is a lot of employers, rather than get a Xerox copy of a Social

Security card, are asking for what they think is more recently updated information, and asking for the print-outs, which is causing another group of people to come in requesting the print-outs.

And that leads to two of our concerns. One is the identification requirements for an original card are much more strict than it is to get a print-out. So what is happening now is there is this secondary market for the print-outs, and often times they are not as good a means of identification as Social Security cards.

Chairman JOHNSON. Well, why do we have to do print-outs at all? Why can't they get a replacement card, if they can?

Mr. O'CARROLL. Well, they can, but only a limited number of times. And there is also a concern due to the Freedom of Information Act—

Chairman JOHNSON. Three times ought to be enough. I mean how many times have you lost your card?

Mr. O'CARROLL. I haven't. I still have the one that my parents got when I was a little child.

Chairman JOHNSON. Okay.

Mr. O'CARROLL. It was with my father's stuff that I inherited from him.

But I agree with you. I think that is why there is a limit to the number of times an individual can get a replacement card. But a lot of people believe that under Freedom of Information Act they are entitled to this print-out.

So, I am more concerned with just making sure that the proper identification is used when they get the print-out so that we know it is the right person, that they are not using secondary, less reliable types of identification to get that print-out, that it has the same level of integrity as the card.

And then, as you had brought up earlier, maybe if there was a charge for getting the print-outs, it would diminish the number of times that it was asked for. As it stands now, employers are charged if they purchase a print-out from SSA; individuals are not.

Chairman JOHNSON. Okay. Well, I am not hot about that idea. Mr. Becerra, you are recognized for five minutes.

Mr. BECERRA. Thank you, Mr. Chairman. Ms. Mithal, let me ask you a question. In the private sector right now we have a patchwork of regulations to deal with the use of the Social Security number. Can you give us some examples of industries that are doing a good job of trying to protect the number, and perhaps an industry that is not doing such a good job of protecting the privacy of an individual's Social Security number?

Ms. MITHAL. I think it would be difficult to provide an industry example. We can provide examples of best practices. So, for example, if you do not need the Social Security number, do not ask for it. It is something that we have implemented as an agency, at the FTC. I remember when I started over 10 years ago, I used to have to put my Social Security number on a leave slip. And we do not have to do that any more. And I think that is a practice that we would encourage the private sector—if you do not need the Social Security number, do not collect it.

Mr. BECERRA. Okay. And I have heard that some of these information resellers have some of the worst practices around, that some of these Internet information resellers actually advertise that

with little more than your name, your city, and state, they can sell you a Social Security number for a few dollars. Is that still the case? Is there any regulation of those resellers?

Ms. MITHAL. There is. In fact, a couple of years ago we brought a number of cases against those who were posing as consumers, and getting information about them. And so we have a law that prohibits unfair or deceptive practices. And we alleged that that was an unfair practice. And so there are laws covering that practice.

Mr. BECERRA. And finally, give us a sense. If you were addressing people who are concerned about their identity and it being stolen, as each and every one of us here is, what would be the best advice you give to any American to try to safeguard his or her Social Security number?

Ms. MITHAL. There are several things I would say. I would say treat it like you would cash. Secure it. Do not carry it around. Any documents that you dispose of, get a shredder. Make sure that if you are providing your number online, that you practice safe computing, that you update your anti-spyware and anti-malware software, that you check your accounts frequently, and that you order your free credit report, which you are entitled to once a year, from the three major credit reporting agencies.

Mr. BECERRA. Good advice. Ms. Gruber, a quick question. What does SSA say to individuals as they come in contact with your offices about the integrity of their number and protecting it?

What—is there anything you tell them, other than respond to the questions they may have about the reason they are there?

They may be coming for benefits, or to apply for something. But does anyone take the time to say, “By the way, you know, you should be securing your Social Security number,” et cetera, et cetera?

Ms. GRUBER. Thank you, Ranking Member Becerra, that is a very good question. We do. Our efforts are multi-faceted. When folks come in to apply for a replacement card, we do absolutely remind them, as both my colleagues have mentioned, to not carry it with them. In fact, it says that on the card.

On our website, we have a number of publications, and frequently asked questions—in fact, I think we have 11 of them—that deal with identity theft, that deal with how to safeguard the card. And we know that they are very widely used. We get thousands of hits every month on those types of things.

And when a person does suspect that their SSN has been misused or stolen, we do talk to them about—and encourage them to take a number of steps, including working with the FTC, including working with IRS, and frequently monitoring their financial accounts, their credit reports. Even if they are not a victim of identity theft, we encourage folks to do that, which is what all of our literature, that is pretty widely available, says.

Mr. BECERRA. Well, I hope, with your good assistance, the three of you, that this perhaps will be the last time we have to hold a hearing on identity theft, because perhaps this time Congress could get together, working with our chairman, to finally pass a bill out of the House and hopefully out of the Senate, so we can deal with this, Mr. Chairman, as I think most of us believe we should

have done a long time ago, and get this taken care of. Because it is a shame that tens of billions of dollars are lost by Americans and, as well, much of their sanity in life because somebody stole their identity.

So, I thank you for your testimony, again. And, Mr. Chairman, I am pleased that you were able to bring them together to have this hearing.

Chairman JOHNSON. Thank you. We have a good panel. We are having a vote right now. I am going to recess the committee, and it will be about 30, 45 minutes before we get back. Thank you.

Mr. BRADY. Hey, Mr. Chairman?

Chairman JOHNSON. Yes?

Mr. BRADY. Can I go on the record saying I really appreciate Ms. Mithal's recommendation that we carry cash? If you could talk to my wife about giving me some, I would be very appreciative.

[Laughter.]

Mr. BRADY. I am with you on that.

[Recess.]

Chairman JOHNSON. The meeting will come back to order. Mr. Paulsen is recognized for questions.

Mr. PAULSEN. Thank you very much, Mr. Chairman. And thank you. This has been an interesting hearing. Maybe I can start with Mr. O'Carroll.

You know, in your testimony you mentioned, or you highlighted at least, the fact that temporary residents may have authorization to work in the United States for a limited time, and you questioned sort of the propriety of assigning an SSN to those folks, which is valid for life. Since an SSN number may be a key to their ability to overstay his or her visa, would you briefly overview for us your work in this area, how you reached this conclusion, and how Social Security has responded to some of those concerns you raised?

Mr. O'CARROLL. Yes, Mr. Paulsen. We have done a number of reports on this issue. We looked at both the fiancée visas, where you come into the country, you say that you are going to be here to get married, and in that time period you are allowed months in the United States prior to your marriage. At that point, the fiancée will come in, get a Social Security number, and let us say, for example, the marriage does not happen, that person leaves the country. That SSN that the person was given is now out there forever.

And then, we also looked at the visas that are issued to foreign students that come to the United States to work for summer—

Chairman JOHNSON. Wait a minute. Can I stop you—

Mr. O'CARROLL. Yes, sir.

Chairman JOHNSON. If they are going out of the country, why can't we stop them at immigration on the way out?

Mr. O'CARROLL. No, meaning what happens with the SSN, then, is that that number for that individual now exists for perpetuity.

Chairman JOHNSON. But you don't make them give the card up?

Mr. O'CARROLL. No.

Chairman JOHNSON. Can we?

Mr. O'CARROLL. That is something we will have to look at. Let me look into that and see if that is a possible solution.

Mr. PAULSEN. If you could give a follow-up to it, Ms. Gruber, just to kind of get some feedback, too. But please continue on.

Mr. O'CARROLL. And then, the other one that we were finding is with the students that are coming in for summer work. That is a very similar one to what Chairman Johnson was saying. At the end of their work, at which point they have been issued an SSN, they work for a summer, they go back to their country of residence, in many cases never to come back into the United States again, we have a concern. Why issue a Social Security number for that?

One of the solutions would be to instruct the IRS to give them a tax identification number, as opposed to having to give them an SSN would be a possible solution.

Mr. PAULSEN. Ms. Gruber, maybe you can follow up regarding the Agency's view on this, and how you and Mr. O'Carroll work together, perhaps, on some of these issues?

Ms. GRUBER. Sure. Thank you, Mr. Paulsen. A couple of things. You know, one of the reasons we actually assign an SSN to someone who might be here temporarily is that we, under law, are required to do so—if they have DHS or Department of Homeland Security authorization to work, under the law we have to assign them an SSN.

There are valid reasons why somebody who has a temporary status here—as long as they have work authorization—might actually want to work. And eventually, if they gain permanent status, they could use those credited earnings while they were here lawfully, but temporarily for their benefits in the future. In order to make a change, it would require a change to the Social Security Act, actually, to not issue an SSN to folks who are here lawfully, who do have authorization to work.

And one other final thing, Mr. Paulsen. The Social Security card itself does not really give them the ticket to work. They have to have the card plus the DHS documentation.

Mr. PAULSEN. Okay. Mr. O'Carroll, any other follow-up on that, or—

Mr. O'CARROLL. I think that pretty well covers it.

Mr. PAULSEN. Okay. Ms. Mithal, maybe I can ask you. The President's task force, you know, a few years back did a lot of work on public display of SSNs, and all the problems surrounding identity theft that I think were a part of that effort. The 2007 strategic plan referred to identity theft as a problem with no single cause and no single solution.

However, they did develop a whole list of recommendations, like 30, 31. You know, the very first recommendation was decreasing the unnecessary use of SSNs in the public sector. Why was that the number one recommendation?

Ms. MITHAL. Well, I think it is fairly obviously that one of the sources of identity theft is the ubiquity of Social Security numbers that are out there. And one of the things that we need to do to address the practice is to make sure they don't get into the hands of identity thieves in the first place. And it seems that reducing the public display of Social Security numbers, reducing the use of them, would be a natural first step. And we decided, well, let us clean our own house, start with the public sector, before we get to the private sector.

Mr. PAULSEN. Well, Mr. Chairman, I think that makes sense, in terms of a number one recommendation. So, thank you, I yield back.

Chairman JOHNSON. Mr. Becerra, do you have another question you would like to ask?

Mr. BECERRA. Mr. Chairman, I think we probably asked and had them answer these questions 17 different times. So I think we know what we have to do, and we just hope that they can continue to offer us some good advice as we try to move forward.

Chairman JOHNSON. Yes. Well, let me ask one, then. You know there is close to 50 million Medicare cards floating around with Social Security numbers on them. How can people protect themselves from medical ID theft?

Mr. O'CARROLL. Well, that was one of our recommendations from one of our audits, was the susceptibility of the public to having their number compromised, because it is on the Medicare card. And at the time, we recommended to SSA to explore ways of working with HHS, which has jurisdiction over the Medicare card, to look into having the number taken off.

And what we found at the time was a couple of things. And I will ask Terry to elaborate, but about \$30 million would be the cost to SSA of just retooling to take the number off of the card. And HHS said it would cost about \$300 million take and 8 to 12 years to do it. So with that, I will yield to SSA.

Chairman JOHNSON. Okay. Mr. Brady, do you care to question?

Mr. BRADY. Yes, sir. One, I appreciate, Chairman, you holding this hearing today in the bipartisan nature. Two, I think the bill that has been or being introduced puts a heavy emphasis on prevention of the theft in the first place. And I want to drive the point or the need for that because on the back end, my understanding is that it is rare that we catch and prosecute those who are good at identity theft.

And my question is, out of the 11 million victims in 2009, not all of them were directly victims of the theft created through the Social Security number. But the average person, senior, anyone, who is an identity theft victim through Social Security number, what are the chances that the criminal who does that gets caught and prosecuted? Any idea?

Mr. O'CARROLL. In the inspector general's office at SSA, we get about a half-a-million public contacts a year, most related to allegations of waste, fraud, and abuse at SSA. And we figure about half of those allegations relate to misuse of the Social Security number. A large portion of them are either referred to SSA, HHS, or the FTC. From that group, we generally look into anything related to misuse of Social Security benefits or related to Social Security in some other way.

So we investigate about 500 SSN misuse cases a year. That is about five percent of our investigations. Almost every one of them will end up with a conviction because by the time we open a case, we know that it is sufficient enough of a violation that we will have a positive result.

But again, that is a very small percentage, as you are seeing. From 500,000 contacts down to about 500 investigations is what we

are looking at from our agency. And I will yield to the FTC on the more global—

Ms. MITHAL. Yes, but we are not a criminal enforcement agency, so I would have to defer to DoJ on that. But I can say that the crime really ranges from a pick-pocket, taking your credit card for a joy ride, to a terrorist that is stealing people's identity to commit bad acts against the country.

And so, I think the—there is really no hope of catching all the identity thieves. And I think you are absolutely right, that we need to focus on prevention, victim assistance, and making sure that Social Security numbers do not fall into the wrong hands.

Mr. BRADY. And actually, just to clarify, I am frustrated by the lack of prosecution. I am not looking to your agencies, but overall, I think it is just very rare. My pet peeve is I see a lot of resources being used, when I turn on the TV and see time and money being used to pursue Marion Jones or Bobby [sic] Bonds or Roger Clemens, or issues like that. I look at those teams and think, "How many victims of Social Security identity theft could be helped, you know, if we applied the same type of rigor and ambition toward catching those?" One, we should be preventing in the first place, and two, really prosecuting them harshly if they are caught. I think it is right to put an emphasis on prevention. I do think we need to have a much higher prosecution rate on the back end, as well.

So, Chairman, thank you very much. And, Ms. Gruber, I did not mean to ignore you. Any comments?

Ms. GRUBER. I think that both of my colleagues summed it up pretty well, and we certainly know how tough it is when we have an interview with somebody who is a victim of identity theft. Their life is turned upside down. And so we understand.

Mr. BRADY. Thank you, Chairman.

Chairman JOHNSON. Thank you. Mr. O'Carroll, you got any ideas how we can, you know, stem the tide of identity theft or stolen cards or something like happened in Texas, for instance? Can you talk to that issue? And how can we fix it?

Mr. O'CARROLL. We have several concerns. One, of course, is identity theft for financial purposes. The other one that we are running into is identity theft where people are illegally using other people's numbers to live and work in the United States. And we all know the problems that follow. Either you are going to be much like the doctor I talked about, where you are going to have someone else's wages posted against your record that the IRS is expecting to pay taxes on, and it takes years to get that straightened out.

So as we said before, any way that we can prevent the use of the Social Security number out there is going to shrink the problem down in size from where it is right now, where everybody has that concern of losing your identity.

If we are not getting very good results from the prosecution side, let us focus on the prevention side. And prevention is a lot of the different tools that we have talked about. And everybody has got to be very careful with their information. For instance, sometimes phone calls are made, where there is the phishing scam to get your information out there, so don't volunteer it yourself.

Also, I think we are all concerned that the material that is in your mailbox can be stolen that has all of your personal information. Often times there is an application for a credit card in the same stack of mail with your personal information on it.

So, I think if this committee could consider ways of preventing the publication of Social Security numbers, it would be a step in the right direction.

Chairman JOHNSON. Well, we can look at that. You know, I do not know exactly how we would do that, though. You know, you can make laws until you are blue in the face, and people do not follow them.

Mr. O'CARROLL. I encourage the enforcement side, too, as a deterrent, I must say.

Chairman JOHNSON. Yes. Well, thank you all. I appreciate you waiting for us.

Do you have any further questions, Mr. Becerra?

I appreciate you all being here today. I look forward to working with all of you to stem the tide of theft by better protecting our Social Security numbers. And I thank you for being here. The hearing is adjourned.

[Whereupon, at 3:34 p.m., the subcommittee was adjourned]

[Submissions for the Record follow:]

**Victim Impact Statement of Juan J. Martinez, Ph.D.
Submitted for the Record
Committee on Ways and Means, Subcommittee on Social Security
Hearing on the Role of Social Security Numbers in Identity Theft and Options to
Guard Their Privacy**

April 13, 2011

The following is a statement that I would like to be read into the hearing record before the Ways and Means Subcommittee on Social Security:

Chairman Sam Johnson, Ranking Member Xavier Becerra and members of Congress,

One often associates theft as a violent crime where something is physically taken from an individual usually by force. This may be in the form of armed robbery, a forced break-in, a car jacking or a "hold-up." I, fortunately, was not subjected to any of these ordeals, but I am a victim. Something significantly more valuable than material goods was taken from me and for 5 years (and possibly more years to come) I have been working to regain that which was stolen from me. I am speaking of my identity that in 2005, Mr. Roberto Ramos-Carvente willfully, knowingly and unlawfully took from me.

It is possible that the defendant came to this country to gain a better life for himself and his family. It is also possible that in taking my name, my social security number, my birth date and other information, Mr. Ramos-Carvente thought that he wasn't hurting anyone. The problem is that in taking this information, the defendant initiated a cascade of events that has made certain aspects of my life rather unpleasant.

Mr. Ramos-Carvente, starting in 2005 and continuing into 2010, utilized my identity (including, but not limited to the use of my name, social security number, and date of birth) to unlawfully gain employment and establish savings and checking accounts in various states of the USA including Colorado and Missouri. During this time, the defendant did not pay the required federal or state income taxes on the wages he earned. Since he had utilized my personal information to gain employment, his reported income on W2 forms were linked to federal and Illinois state tax returns that my wife and I filed as required by law. Suffice it to say, I have spent more time than I would like to admit trying to regain something that is rightfully mine: my identity, what I feel makes me, me. I have spent numerous work days, weekends and any available free time gathering information for audits, contacting credit bureaus, contacting the IRS, contacting the Social Security Administration, contacting banks, contacting telephone companies, contacting various local and federal law enforcement authorities to report the defendant's actions as identity theft. Meanwhile, the defendant led his life not caring about the wake of a mess that he left behind as he made his way from town to town, employer to employer.

One of the major headaches that resulted from the defendant's criminal activity was that my family's tax returns to the IRS were consistently "flagged" and subjected to re-examination by auditors. This was due to our filing tax returns that contained un-reported wages that were unknown to me (those unlawfully earned by the defendant posing as me) year after year. I have

had to prove to the IRS that the wages reported by the defendant in each fiscal year were in fact unlawfully earned by him and not by me. For example, the burden of proof was placed on me to prove that wages earned in the state of Colorado were not earned by me as I have never resided in Colorado nor worked in that state. As one can imagine, trying to prove one's own identity when another has documentation in the same name, with the same social security number and same date of birth can be a rather trying and difficult task. Trying to do this to federal agencies such as the IRS and the Social Security Administration has not been in any way easy as the wheels of bureaucracy do not always turn at a reasonable rate.

I am proof that ID theft is not a victim-less crime. Mr. Ramos-Carvente stole from me and whether or not he did this knowingly is not my concern. I want him to know that he hurt my family and at this time, I have very little sympathy for him. He deserves the punishment that he has received and I am grateful to the various local and federal law enforcement agencies across the country whose collective efforts resulted in his arrest. I take solace knowing that has been incarcerated and that the nightmare that he put us through is now hopefully over.

Respectfully,

/s/

Juan J. Martinez, Ph.D.
Assistant Professor
The University of Chicago
Department of Microbiology

I believe that a big problem arises from the theft and/or loss of Medicare cards and the information on the cards. The cards show the Social Security number of the beneficiary as the Medicare Claim Number.

As examples, in addition to identifying myself when I obtain medical care I hand over my card to porters on trains and to movie ticket window tellers who could take advantage and steal my identity.

An alternate system to the Social Security number should be devised for the Medicare card and the beneficiary's identification in order to safeguard against identity theft and to protect privacy.

Very respectfully,

Helene Perry
Lafayette Hill, PA





May 4, 2011

The Honorable Sam Johnson
 Chairman, Subcommittee on Social Security
 U.S. House Committee on Ways and Means
 1102 Longworth House Office Building
 Washington, DC 20515

The Honorable Xavier Becerra
 Ranking Member, Subcommittee on Social Security
 U.S. House Committee on Ways and Means
 1106 Longworth House Office Building
 Washington, DC 20515

RE: April 13, 2011 Social Security Subcommittee Hearing on the Role of Social Security Numbers in Identity Theft and Options to Guard Their Privacy – Comments of LifeLock, Inc.

Dear Chairman Johnson and Ranking Member Becerra:

LifeLock, Inc. ("LifeLock") appreciates the opportunity to respond to the U.S. House Committee on Ways and Means Subcommittee on Social Security's hearing on "The Role of Social Security Numbers in Identity Theft and Options to Guard Their Privacy," held April 13, 2011. LifeLock applauds the Subcommittee for its continued efforts with regard to identity theft and personal data protection and deep concern for this important issue. As Ranking Member Becerra noted in his opening statement, this is the 18th hearing the Subcommittee has held on identity theft and the protection of Social Security Numbers since January 2000. The most recent hearing once again reaffirmed the need for comprehensive privacy legislation.

In the current economic climate, federal and state policymakers must remain focused on crimes that prevent a strong recovery. As the fastest growing type of fraud in the United States, identity theft is one of those crimes. Last year, the Congressional Research Service estimated that in 2009 identity theft cost 11.1 million Americans a total of \$50 billion.¹ And according to the Privacy Rights Clearinghouse, since early 2005 more than 500 million records have been compromised due to security breaches.² Breaches involving Social Security Numbers continue to be a regular occurrence. With an increasingly globalized world powered by the information economy, Congress must work to reduce opportunities for identity theft, help to mitigate its effects on consumers, and provide tools to investigate and prosecute this crime.

¹ *Hearing on the Role of Social Security Numbers in Identity Theft and Options to Guard Their Privacy Before the H. Subcomm. on Social Security of the H. Comm. on Ways and Means*, 112th Cong. (statement of Rep. Sam Johnson, Chairman, H. Subcomm. on Social Security).

² *Id.*

As you know, in mid-April the Texas Comptroller's Office announced the largest data security breach in state history. In addition, there have been several other massive data security breaches that have exposed the Social Security Numbers of millions of individuals. For example, in 2006, the Department of Veterans Affairs announced a breach of personal information of more than 26 million veterans.³ Today, the New York Times reported that: "It's become almost a weekly occurrence: another online company letting customers personal and private information leak because of an Internet breach."^{3a}

Products, such as those offered by LifeLock, offer consumers significant protection against identity theft. But proactive public policy initiatives that take into account currently available technologies – such as those that proactively help prevent identity theft – are essential. We believe public and private sector organizations must do a better job attacking identity theft, protecting personal data, and having a plan to help consumers in case of a data breach, and we believe that this should be accomplished through public and private sector partnerships. Therefore, we strongly support Chairman Johnson's call for Congress to "get to work on identity theft," and echo Ranking Member Becerra's statement that while Democrats and Republicans may have differing views on the importance of Social Security benefits, the parties "are united in our concern about identity theft."

We urge Congress to require better collection of data about identity theft, rather than relying upon surveys and victim reporting. A variety of organizations have important data about this problem, and this data should be an additional source included in national reporting about the scope of this important problem. This will result in comprehensive information that can be most efficiently used to combat identity theft.

We also commend the Federal Trade Commission ("FTC") on its efforts to update the current privacy framework to meet the privacy challenges of the 21st century, while continuing to support beneficial uses of information and technological innovation. In particular, we strongly applaud the FTC's support of national data breach notification standards requiring organizations to notify affected consumers when their data has been breached and the adoption by Congress of national data security standards.

In addition, LifeLock is supportive of the FTC's suggestions regarding reducing dependence upon Social Security Numbers, including establishing alternative customer authentication standards and implementing national standards regarding the public display of Social Security Numbers, as the continued, prevalent use of Social Security Numbers as identifiers is a significant structural vulnerability exploited by identity thieves today.

I. About LifeLock

³ Sidath Viranga Panangala, *Department of Veterans Affairs: Information Security and Information Technology Management Reorganization*, Congressional Research Service Report for Congress, Aug. 14, 2006, available at <http://congressionalresearch.com/RL33612/document.php?study=Department+of+Veterans+Affairs+Information+Security+and+Information+Technology+Management+Reorganization>.

^{3a} Nick Bilton, *Holding Companies Accountable for Privacy Breaches*, New York Times, May 4, 2011.

LifeLock is an industry leader in identity theft protection. Since 2005, LifeLock has provided a wide range of services to consumers with respect to privacy protection, including identity theft protection and data breach response services. For example, LifeLock offers products that offer consumers the opportunity to proactively sign up for identity theft protection services that will work in advance to help stop an identity theft before it happens.

The company has a strong focus on educating consumers and working with law enforcement and elected officials to better understand the increasing threats of identity theft. Headquartered in Arizona, LifeLock, in 2010, was ranked 8th on Inc. magazine's 29th Annual Inc. 500 List,⁴ a ranking of the nation's fastest-growing private companies. LifeLock also has been recognized by the American Business Awards as having the Best New Product or Service of the Year for the LifeLock Identity Alert® system.⁵

LifeLock works actively with elected officials to help serve as a vocal and effective voice for consumers everywhere to create legislation that helps protect consumers. LifeLock will continue to work relentlessly to educate consumers, support law enforcement, and work closely with government officials to help decrease identity fraud.

II. Support for More Comprehensive Data Collection Methods and for the FTC's Proposals to Prevent Misuse of Social Security Numbers

We believe it is very important that Congress require better collection of data about identity theft, rather than relying upon surveys and victim reporting. Congress should look to the numerous entities that accumulate important data about identity theft as an important additional source of data in accurately reporting about the scope of this important problem. This will result in complete and comprehensive information that can be used to prevent identity theft.

LifeLock also supports the FTC's proposed recommendations to prevent the misuse of Social Security Numbers: (1) establishing national consumer authentication standards to verify customers; (2) creating national standards to reduce the public display of Social Security Numbers; (3) implementing national data security standards that cover use of Social Security Numbers; and (4) implementing national data breach notification standards that require private companies to announce breaches of person information.

First, establishing national, alternative consumer authentication standards would greatly reduce the value associated with Social Security Numbers, given that one of the primary reasons identity thieves steal Social Security Numbers is to authenticate themselves as someone else. If an alternative method of authentication was implemented, identity thieves would have significantly less incentive to steal Social Security Numbers, and a significant structural vulnerability exploited by identity thieves today to steal identities would be fixed.

Second, and related to the point above, reducing the public display of Social Security Numbers would make it significantly more difficult for identity thieves to gain access to Social Security Numbers. This reduction could be accomplished by establishing national standards

⁴ See <http://www.inc.com/inc5000/list>.

⁵ See http://www.stevieawards.com/pubs/awards/403_2630_20419.cfm.

regarding the public display of Social Security Numbers and, as discussed above, by establishing alternative authentication methods, thereby reducing consumers' disclosure of Social Security Numbers.

Finally, LifeLock supports both national data security and data breach notification standards. Such national standards will provide consistency across industries regarding how data breaches are treated (rather than varying state-by-state) and the security requirements that must be implemented to protect Social Security Numbers (rather than varying business-to-business). In addition, LifeLock supports focusing on currently available technology to prevent, rather than merely protect against, identity theft in implementing national security requirements. Private industry can work with the FTC and others to best implement these evolving technologies to prevent identity theft.

III. Summary

Chairman Johnson observes that “the problem of identity theft is not going to be addressed with one piece of legislation.” While this is certainly true, with privacy legislation that includes thoughtful identity theft management provisions, Congress can make significant progress a bipartisan issue.

It is time for action. As stated before, identity theft is the fastest growing type of fraud in the United States—affecting more than 11.1 million victims in 2009—and costs Americans close to \$50 billion annually.⁶ The FTC receives 15,000 to 20,000 calls *per week* regarding identity theft.⁷

Chairman Johnson believes “Americans are rightly worried about the security of their personal information.” Assistant Deputy Commissioner Gruber believes “the implications for personal privacy caused by the widespread use of a single identifier [SSN] have generated concern both within the Government and in society in general.” Across the country, people are alarmed. So are we. Therefore, we call on Congress to pass comprehensive privacy legislation in a quick and timely manner, because, as FTC Associate Director Mithal testified, “[i]dentity theft remains a serious problem in this country, causing enormous harm to consumers, businesses, and ultimately our economy.”

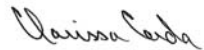
⁶ *Supra* note 1.

⁷ *Prepared Statement of the Federal Trade Commission Before the Subcommittee on Social Security of the House Committee on Ways and Means on Protecting Social Security Numbers from Identity Theft*, April 13, 2011, available at <http://www.ftc.gov/os/testimony/110411ssn-idtheft.pdf>.

IV. Conclusion

We thank you for considering our views and are eager to work with you in a constructive fashion to help the Subcommittee achieve its goal of better protecting consumers from the serious problem of identity theft.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "Clarissa Cerda".

Clarissa Cerda
Senior Vice President, General Counsel & Secretary
LifeLock, Inc.

[Questions for the Record follow:]



June 22, 2011

The Honorable Sam Johnson
Chairman, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

Attention: Kim Hildred

Dear Mr. Chairman:

This is in response to your June 9, 2011 correspondence asking questions for the record, further to my testimony on April 13, 2011 before the Subcommittee on Social Security at a hearing on the role of Social Security numbers in identify theft and ways to guard their privacy. I appreciate the opportunity to provide additional information regarding this critical issue. Below are responses to your specific questions.

1. K-12 schools continue to use students' Social Security numbers (SSN) as authenticators. Would you provide an update of this practice? How can we encourage school systems to stop this practice?

In July 2010, the Social Security Administration (SSA) Office of the Inspector General (OIG) issued an audit report, *Kindergarten Through 12th Grade Schools' Collection and Use of Social Security Numbers* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-10-11057.pdf>). At the time of our audit, we identified laws in seven States¹ that required K-12 schools to obtain students' SSNs. Additionally, we identified schools in at least 26 other States² that collected students' SSNs at registration, even though no State law required it.³ We also noted that a recent university study identified a trend among State departments of education to establish longitudinal databases of all K-12 children to track students' progress over time.⁴

¹ The States were Alabama, Arkansas, Florida, Georgia, Kentucky, Virginia, and West Virginia. Although these States require an SSN for enrollment, they also may provide alternative numbers for individuals who refuse to provide their SSN or who are not eligible for an SSN.

² The States were Connecticut, Delaware, Hawaii, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Hampshire, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Wisconsin, and Wyoming.

³ We do not suggest that these are the only States in which K-12 schools collect SSNs at registration.

⁴ Joel R. Reidenberg et al., Fordham Law School Center on Law and Information Policy, *Children's Educational Records and Privacy*, October 2009.

The study found that privacy protections for these databases were generally lacking in most States.

In our report, we acknowledged that four States had enacted laws to prohibit K-12 schools or State educational agencies from using SSNs as primary student identifiers.⁵ However, we believe Federal legislation is needed to limit the collection, use, and disclosure of SSNs by K-12 schools—and by others who do not have a legitimate need for this information. SSA, the Congress, and the U.S. Department of Education can educate States about the dangers of this practice, and encourage them to use an alternate student identifier. Without Federal law and regulation, States may not have a strong incentive to change this practice.

2. Do you believe we are winning or losing the growing battle of ID theft? Why or why not?

We believe the Federal Trade Commission (FTC) would be better suited to provide this information, as it maintains comprehensive information on identity theft statistics and trends. With regard to our experience, SSN misuse cases made up approximately five percent of our investigative casework during fiscal years (FY) 2009 and 2010, totaling 350 and 318 cases, respectively. Although these statistics reflect a short period, we believe our focus on this issue has remained generally consistent over time.

Identity theft is a complex issue, and therefore, winning this battle involves many factors. We appreciate the work of this Subcommittee and believe there has been progress through legal changes championed by your current and past members. Additionally, my office is passionate in its responsibility to protect the SSN, and SSA has been proactive in making significant changes to improve controls within its enumeration process. However, tackling this problem necessitates widespread changes in areas such as immigration law, employment eligibility requirements, regulations over the collection and use of personal information, resources dedicated to enforcement on the Federal, State, and local levels, and even larger societal behaviors and beliefs. Therefore, we would be hard-pressed to opine that we are “winning” this battle.

3. How has ID theft changed over the last several years? Is it more widespread, sophisticated and harder to stop? Are there trends towards organized crime or state sponsored ID theft?

We believe FTC would be better able to identify trends in identity theft. Based on our limited investigative data, we have not seen an increase in organized crime or state-sponsored identity theft.

4. What is the most common form of ID theft? Is it lost or stolen Social Security cards, death records that are sold with SSNs, or via some public listing or even the internet? Are there other trends that you can discuss?

⁵ The States were New Hampshire, Ohio, Rhode Island, and Wisconsin. However, such laws may not prevent K-12 schools from collecting and using SSNs for other purposes.

Currently, we do not track the form of identity theft on cases we investigate. However, we are concerned about the availability of personally identifiable information on the internet, including death records that include the individual's SSN—sold as the SSA Death Master File. FTC may have more data regarding common forms of identity theft.

5. Can you tell us what burdens may occur by removing 'unnecessary' display of SSNs? Is there a way to encourage proper use of SSNs while minimizing those burdens?

Although we have not conducted specific audit work to identify burdens associated with removing SSNs from display, anecdotally we know that such challenges involve significant systems changes, as well as the process of physically redacting SSNs from documents or websites. However, we identify below examples from past audit work in which governments and private entities took steps to protect sensitive information.

- In a December 2004 audit report, *Universities' Use of Social Security Numbers as Student Identifiers in Region IV* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-05-15034.pdf>), we noted that several schools had reduced or eliminated their reliance on SSNs; and some States enacted laws to regulate colleges' use of SSNs. For example, in 2003, the Georgia Institute of Technology (Georgia Tech) stopped using SSNs of students, faculty, and staff on identification cards and as the primary means of identification in campus databases, because of increased identity theft concerns. The university created the Georgia Tech Identification Number, which identifies students in most campus databases. The Associate Registrar told us the conversion took two years of planning, but was not difficult. In fact, she stated the actual conversion took place over a weekend. We heard similar stories from universities across the country.
- In a September 2007 audit report, *State and Local Governments' Collection and Use of Social Security Numbers* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-07-17086.pdf>), we identified 11 States that had taken steps to remove SSNs from public documents, and 24 States that passed laws to prohibit SSNs from being on public documents. We also identified 15 States that passed laws to prohibit publicly displaying SSNs, printing them on cards, transmitting them over the Internet, and mailing them without safety measures. For example, Maricopa County, Arizona, had begun redacting SSNs from 83 million public documents posted on the Internet. County officials told us they undertook this \$4.5-million project in response to identity theft concerns, constituent complaints about the online SSN postings, and the desire to take a proactive approach to this issue. The county hired a contractor to redact the SSNs, and required that the contractor manually review each document to ensure all SSNs were removed. In fact, the county specified that two individuals review each document to ensure a 99.95-percent accuracy rate. The county also planned to purchase redaction software for its own future use.
- Finally, in a May 2008 audit report, *Removing Social Security Numbers from Medicare Cards* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-08-18026.pdf>), we identified Federal agencies, including the Departments of Veterans Affairs and Defense, that had removed the SSN from health insurance cards. Additionally, the Office of Personnel Management (OPM) directed all health insurance carriers affiliated with the Federal Employees Health Benefit Program to eliminate SSNs from insurance cards as soon as

practical. In making this change, OPM acknowledged that SSNs can serve as a critical link in identity theft cases and other crimes. In recent years, almost all health insurance carriers have removed SSNs from their health insurance cards. For example, a Blue Cross and Blue Shield of Texas official told us the company removed SSNs from about 10 million insurance cards (for both Federal and non-Federal subscribers). Although Blue Cross and Blue Shield still uses SSNs internally, it developed a unique identifier for use on insurance cards and correspondence.

6. Would you agree that thieves would have a harder time stealing a person's identity if we had better methods of authenticating consumers, or, in other words, better ways to prove a person is who they say they are?

Theoretically, we agree that thieves would have a harder time committing identity theft if there were better ways to prove a person is who they say they are. While SSA and the Department of Homeland Security (DHS) offer several authentication programs, they are neither fail-safe nor mandatory. These programs allow users to verify that a person's name and SSN combination is valid; and they identify deceased individuals. However, the programs will not detect all instances of identity theft, such as the misuse of a valid name and SSN combination. Therefore, other types of authentication, such as biometric verification, could be useful tools to verify a person's true identity. However, we have not performed audit work on biometric technologies to provide an opinion on their value. We describe SSA's and DHS' existing programs below.

- **Consent Based Social Security Number Verification (CBSV):** CBSV is a fee- and consent-based SSN service available to private businesses (including banks) and Federal, State, and local government agencies that need client SSN verification. Participating companies are required to obtain written consent from the individual before verifying the individual's SSN through CBSV, as required by the *Privacy Act of 1974*. CBSV verifies whether a name and SSN combination match the data in SSA's records. As of Calendar Year (CY) 2010, 124 companies had submitted about 1.3 million verification requests.
- **Social Security Number Verification Service (SSNVS):** SSNVS is a free online system, with a batch option, that allows employers and third-party submitters to verify employees' names and SSNs; and identifies deceased individuals. SSNVS helps ensure employees' names and SSNs match SSA records before their wage reports are submitted to SSA. In CY 2010, SSNVS processed about 106 million verification requests.
- **Employment Verification Program (E-Verify):** SSA supports DHS in administering the E-Verify program, which allows employers to verify electronically employee information taken from the *Employment Eligibility Verification* form (Form I-9) against Federal databases to verify the employment eligibility of newly hired citizens and noncitizens. E-Verify is voluntary for most employers and is provided at no charge. As of September 4, 2010, about 222,000 employers were enrolled to use E-Verify—and those employers had submitted approximately 15 million queries.

7. With respect to the Dr. Martinez case are there good examples of private or public sector entities doing more to recognize what has happened to a victim and in some way

“certify” his or her experience so he or she can move on with his or her life and not be repeatedly questioned about who they are?

Although we have not examined the practices of other private and public sector entities, we are aware of two initiatives that are intended to assist ID theft victims. First, when SSA assigns a new SSN because a person has been disadvantaged by the misuse of his/her number, SSA places a special indicator on the old SSN record to block issuance of replacement SSN cards and SSN printouts. In addition, FTC has an identity theft affidavit that the individual can fill out and keep as a permanent record to present to public and private entities if questioned about crimes committed using their identities.

If the Subcommittee would like my office to examine this issue further, we would be pleased to do so at your request.

8. What are your recommendations for legislation that Congress needs to pass regarding SSN protection?

We have worked closely with the Subcommittee in providing recommendations for legislation we believe Congress should enact to enhance SSN protection. Many of these recommendations have been included in prior legislation introduced by previous Chairmen of this Subcommittee, the most recent being H.R. 3306, introduced in the last session of Congress. Our recommendations focus on several areas.

- *The display, sale, and purchase of the SSN in the public and private sectors.* Among our recommendations for the protection of the confidentiality of the SSN:
 - uniform truncation of the SSN when displayed; i.e., using only the last four digits;
 - limiting access to those in government and the private sector with a need for access to the SSN for the effective administration of their duties;
 - prohibiting the display of the SSN on cards or tags required for access to goods services, or benefits, as well as on employee identification cards or tags; and
 - allowing for consent of the affected individual pursuant to regulations.
- *Enhanced enforcement.* Several of our recommendations regarding criminal penalties are in H.R. 3306, including amending section 208 of the *Social Security Act* to include:
 - possession of an SSN without lawful authority;
 - possession of an SSN card knowing it to have been stolen, counterfeited, or forged, or obtained from SSA by the use of false information;
 - disclosure, sale, or transfer by an individual of their own (or their child’s or relative’s) SSN with intent to deceive;
 - to offer on the internet for a fee, to acquire for any individual, or to assist in acquiring for any individual an SSN or a number that purports to be an SSN but is not acquired by the individual through SSA; and
 - penalties for SSA employees who knowingly and fraudulently issue SSNs or SSN cards (this would be a progressive penalty—up to 5 years for 50 or fewer, up to 10 years for 51 up to 100, and up to 20 years for over 100).

Additionally, several Assistant United States Attorneys (AUSA) have inquired as to whether section 208 of the *Social Security Act* contains a misdemeanor provision. It does not. Providing for a misdemeanor would provide AUSAs with greater leeway in plea negotiations with individuals charged under section 208.

Further, in the *Social Security Protection Act of 2004*, titles II, VII, and XVI were amended to provide that the court *may* order restitution pursuant to sections 3612, 3663, and 3664 of title 18 of the United States Code. If the court does not order full restitution, it has to explain on the record why it did not. Since the enactment of this legislation, several AUSAs have told my office that this provision should be mandatory. In addition to substituting “shall” for “may” in the statute, we would suggest that 18 U.S.C. § 3663A be substituted in place of 18 U.S.C. § 3663. 18 U.S.C. § 3663A(c)(1)(A)(ii) & (B) provides, in part, for mandatory restitution for an offense that is an offense against property under [title 18], ... including any offense committed by fraud or deceit; and, in which an identifiable victim or victims has suffered a physical injury or pecuniary loss.”

We also recommend amending the criminal provisions of title II, VIII, and XVI to provide for enhanced penalties relating to SSN misuse for more than one conviction, terrorism, drug trafficking, and crimes of violence. The recommendation is for up to 10 years if the individual has a prior offense under the applicable statute; up to 20 years if the crime facilitates drug trafficking or a crime of violence; and up to 25 years if it facilitates domestic or international terrorism.

Finally, we recommend amending section 1129 of the *Social Security Act*, to allow SSA to impose civil monetary penalties (CMP) for those who violate the current criminal provisions of section 208 relating to the SSN, and for the recommended criminal provisions above. The CMP program supplements the criminal enforcement tools available against SSN misuse. We have seen instances in the past in which an AUSA indicates they will decline criminal and civil prosecution in favor of our proceeding against the individual pursuant to the CMP program. Moreover, cases are often declined criminally because the fraud loss does not reach a minimum threshold required by the United States Attorney’s Office, which can range from \$25,000 up to \$100,000. In these cases, the ability to pursue a CMP has helped ensure that a person who has committed fraud against SSA’s programs will face consequences for that action.

- *Exempting the SSA OIG from the Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a.* This would allow us to compare any Federal records with other Federal or non-Federal records, while conducting an audit, investigation, inspection, evaluation, or other review authorized to identify weaknesses that may lead to fraud, waste, or abuse, and to detect improper payments and fraud.

My office is available at the Subcommittee’s convenience to provide technical assistance in pursuing any of the aforementioned recommendations.

9. **The Subcommittee is interested in removing the SSN from the Medicare card and inserting another identifying number for Medicare use, much like the military is doing with its ID cards. The SSA systems would not have to make any changes except**

interfacing with CMS to identify the new number with the correct SSN already in their system. Is this the simplest way to alter the system, and if so what are the costs and the time frames for achieving the change?

We issued an audit report regarding this issue in May 2008, *Removing Social Security Numbers from Medicare Cards* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-08-18026.pdf>). Nevertheless, we believe SSA and the Centers for Medicare and Medicaid Services would be better able to answer specific questions about costs, required system changes, and the time needed to make this change.

- 10. As you all testified, ID theft is one of the fastest growing crimes in America, and one of the reasons for this is the ease of finding SSNs on unprotected documents. In many states, each foster child receives an identity card with his or her SSN on the card, and the SSN is the primary identifier of the child. The federal government allows for an SSN change when a foster child is going through the adoption process. A new SSN largely cleans the financial slate for these children. Is issuing a new SSN a solution for minors, such as foster youth, who have been victims of ID theft? What is the impact of issuing a new SSN?**

First, we are also concerned with the issue of identity theft among foster children. Therefore, we plan to initiate an audit of this issue in the next few months. We will share the results with the Subcommittee, and may be better able to respond to your questions at that time.

In general, however, SSA permits foster children (and other number holders) to obtain a new SSN if they continue to be disadvantaged by identity theft. According to SSA policy, if an individual (or, for a minor, their guardian) decides to apply for a new number, he or she must prove age, U.S. citizenship or lawful immigration status, and identity. He or she must also provide evidence that he or she is still being disadvantaged by the misuse. SSA cautions those who request a new SSN that a new number may not always stop the problems caused by identity theft. As SSA states (see <http://www.socialsecurity.gov/pubs/10064.html#new>):

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit-reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

- 11. When a person uses an SSN to apply for credit or open an account, what mechanisms are there for the creditor to check the legitimacy of the SSN and whether or not it belongs to a minor? Would it raise a red flag if a creditor discovered the SSN belonged to a minor? Do creditors routinely check to determine if an SSN belongs to a minor?**

We have not conducted audit or investigative work to respond adequately to these questions. However, we would be happy to review this issue at the Subcommittee's request. Alternatively, the Subcommittee may wish to pose these questions to FTC or to the major credit bureaus.

12. What are your recommendations for issuing SSNs to temporary workers? For foreign workers with SSNs, should it be possible for those numbers to be rescinded or suspended when the foreign worker leaves the country?

We have issued several audit reports highlighting vulnerabilities associated with assigning SSNs to certain noncitizen temporary workers. While we did not recommend that these SSNs be rescinded or suspended when these workers leave the country—and have performed no audit work to determine the feasibility of such actions—we have made several other recommendations, including changes in Federal law. While we could examine the possibility of SSN suspension or rescission at the request of the Subcommittee, in general, we believe these options would be logistically challenging for SSA to administer. To our knowledge, DHS still does not have *complete* information regarding departure dates of noncitizens. Without such information, SSA would have to rely on visa expiration dates, which often change. Thus, significant systems improvements and data-sharing arrangements would need to be in place before SSA could implement an accurate SSN suspension or rescission process.

Nevertheless, we do encourage legislation to address the requirement that SSA assign SSNs to noncitizens who are permitted to work temporarily in the country. In July 2007, we issued an audit report, *Assignment of Social Security Numbers to J-1 Exchange Visitors* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-07-17076.pdf>). J-1 exchange visitors who enter the United States as camp counselors or as a part of the “summer work/travel” program may work in the United States for 4 months, and must then return to their home countries. Under current law and regulation, because J-1s are eligible to work, they are eligible to obtain an SSN—even though they are exempt from paying Social Security taxes. Based on our estimates, SSA assigned approximately 100,000 SSNs to these categories of J-1 exchange visitors during FY 2005.

We believe this practice creates opportunities for potential SSN misuse. For example, an SSN makes it easier for exchange visitors to remain in the country and to continue working after their visa expires, which weakens SSN integrity and could affect homeland security. In addition, some exchange visitors leave their employer or return to their home country before receiving their SSN card, increasing the potential for dishonest individuals to obtain and misuse these cards. Further, some of the employers and SSA field office personnel with whom we spoke stated that exchange visitors who receive their SSN cards do not always adequately safeguard them—often misplacing the cards and requesting replacements. For these reasons, employers, international cultural exchange organizations, and field office personnel we interviewed questioned the assignment of SSNs to exchange visitors, and shared our concerns about the potential for SSN misuse.

We believe SSA and the Congress can reduce the risk of SSN misuse by considering alternatives to assigning SSNs to noncitizens who work in the United States for only a few months. One alternative could be to require the IRS to issue exchange visitors Individual Taxpayer Identification Numbers. We recommended that SSA seek such legislation in our audit report. However, the Agency disagreed with this proposal because our audit report did not identify specific instances of SSN misuse, and because such a policy would complicate SSA’s enumeration procedures.

We have similar concerns with K-1 fiancé visa holders, another category of noncitizens who may work temporarily in the United States. In May 2008, we issued an audit report, *Assignment of Social Security Numbers to Noncitizens with Fiancé Visas* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-07-17044.pdf>). U.S. citizens who consider marrying a citizen of another country may petition the U.S. Department of State to allow the noncitizen to enter the United States with a K-1 visa. The Department of State issues such visas for a 6-month period, during which the individual may enter the United States only once. Upon admission, however, the individual has 90 days to marry the U.S. citizen and apply for a change of status, or depart the country. Because they are eligible to work in the United States for this 90-day period, SSA must assign an SSN to K-1 applicants with proper DHS documentation.

K-1 visa holders are required to pay Social Security taxes. Further complicating this matter, section 466(a)(13) of the *Social Security Act*, 42 U.S.C. 666(a)(13), requires that anyone seeking a marriage license provide his or her SSN to the recording State. We believe assigning an SSN to a K-1 visa holder creates significant opportunities for SSN misuse, and could provide an avenue for those who choose not to marry to remain in the United States illegally. We believe laws should be revised so that K-1 visa holders are not assigned an SSN—until they marry a U.S. citizen and apply for permanent residency.

- 13. The number of replacement Social Security cards is now restricted. However, the number of printouts or “Numi Lites” is growing as individuals, or individuals prompted by law firms or other businesses, comes into the field offices for new printouts. The level of identity required for these is less than a new replacement card making them more open to ID theft. Should we be charging fees to remove the incentive to obtain repeat printouts and if so at what level should the fee be to cover costs and provide the proper disincentive? Should we also be charging a fee for replacement cards and what is the proper level to cover cost and still provide a disincentive to get multiple replacement cards?**

We share the Subcommittee’s concern over the growth in demand for SSN printouts (Numi Lites), as well as the less probative identity documents required for number holders to obtain these documents. In December 2007, we issued an audit report, *Controls for Issuing Social Security Number Verification Printouts* (see <http://www.ssa.gov/oig/ADOBEPDF/A-04-07-27112.pdf>), making a number of recommendations to strengthen SSA’s process for issuing these sensitive documents. We are currently completing a second review to examine whether vulnerabilities still exist, and will issue that review by the end of FY 2011. We will provide a copy of this report to the Subcommittee.

Additionally, at Chairman Johnson’s request, we are examining the feasibility of charging user fees for certain SSA services, including issuing replacement Social Security cards and SSN printouts. We plan to issue the results of this study to the Subcommittee by the end of July 2011. In our report, we will discuss SSA’s estimated cost for processing these two workloads (an average of \$32 for issuing Social Security cards, and roughly \$20 for issuing

SSN printouts).⁶ We will also provide information regarding SSA's estimated cost for processing remittances (\$26). Given our short timeframe, we will not be able to provide definitive costs that we feel would dissuade customers seeking these documents. However, we will provide options for your consideration. We would be happy to discuss the results of our review—and to explore further areas in which you may still have concerns.

14. In your testimony, you mentioned the Freedom of Information Act as a factor in obtaining printouts and replacement cards. Can you explain further the nexus between the two?

In compliance with both the *Privacy Act of 1974* and the *Social Security Act*, SSA's information disclosure policy dictates that it will protect the privacy of individuals to the fullest extent possible, while permitting the exchange of information needed to fulfill its administrative and program responsibilities. Notwithstanding some exceptions, Federal law gives individuals the right to access information about themselves that is in SSA's records.

Generally, individuals have access to SSA records that the Agency can retrieve by name, SSN, or other personal identifier. This includes SSN-related records, such as the original *Application for a Social Security Card*, the Numident,⁷ and the SSN printout. SSA's policies for issuing SSN printouts are less stringent than those for issuing replacement SSN cards, because the Agency has attempted to comply with the spirit of the *Privacy Act*. That is, in compliance with the *Privacy Act* and OMB guidelines, Agency policies allow individuals to obtain these documents without undue burden. Nevertheless, SSA continues to issue a large number of SSN printouts—and this number has grown each year since the Agency began issuing them. As such, we believe SSA should improve its procedures to control and account for the issuance of SSN printouts, while also making efforts to reduce the unnecessary demand for the document as a form of SSN verification.

Thank you for the opportunity to clarify these issues for the Subcommittee on Social Security. I trust that I have been responsive to your request. If you have further questions, please feel free to contact me, or your staff may contact Misha Kelly, Congressional and Intra-Governmental Liaison, at (202) 358-6319.

Sincerely,

S

Patrick P. O'Carroll, Jr.
Inspector General

⁶ SSA charges third parties \$46 to provide an SSN printout with consent of the number holder (for example, an employer who requests an SSN printout with the consent of the employee). Of this fee, SSA estimates \$26 recovers the remittance cost for collecting the fee and \$20 recovers the cost of work performed in providing the SSN printout.

⁷ The Numident is an electronic record of the information contained on an individual's original application for an SSN and subsequent applications for replacement cards. Numident printouts are not issued by SSA field offices. To obtain a Numident, an individual must send a written request to SSA's Central Office, and pay a \$16 fee.

Maneesha Mithal

(1) The Federal Trade Commission (FTC) has been at the forefront of educating the public about protecting their identities. You have also put agencies on notice about eliminating the unnecessary use and display of SSNs. What trends are you seeing with respect to ID theft and the use of SSNs in those thefts? Are things getting better or worse?

In 2010, as in prior years, identity theft was the leading complaint category that the Commission received from consumers. Government documents/benefits fraud (19%) was the most common form of reported identity theft in 2010, followed by credit card fraud (15%), phone or utilities fraud (14%), and employment fraud (11%). Government documents/benefits fraud increased 4% since 2008, while identity theft-related credit card fraud declined 5% during the same period. Our complaint data does not specifically track the use of SSNs in those identity thefts. Moreover, in many instances identity theft victims cannot determine with precision the specific personal information that led to the crime. As a result, we are not able to assess trends regarding the use of SSNs specifically in identity theft.

(2) The President's Identity Theft Task Force referred to identity theft as "a problem with no single cause and no single solution" in its 2007 Strategic Plan. Please give us an update on what has improved since 2007 and what you see as the remaining challenges in preventing ID theft. Which public agencies, either Federal, State or local, expose the greatest number of Americans to ID theft and fraud by continuing to publicly use SSNs? Have you or your agency spoken with any of these agencies? Is there legislation that was recommended by the task force that has not been enacted but should be? Please provide a status report on the recommendations relating to authentication.

Since 2007, coordination among federal agencies on the issue of identity theft has vastly improved. An interagency Task Force, consisting of staff from DOJ, FTC, FBI, IRS, HHS and others meets bi-monthly to discuss emerging trends and issues. FTC staff regularly speaks with staff from these other government agencies regarding a variety of identity theft-related topics, including continued use of SSNs by government agencies. In addition, the Commission and other Task Force agencies have conducted extensive consumer and business education on identity theft prevention and recovery, and data protection. Many of the published educational materials discuss SSNs specifically. The Commission has not, however, surveyed which agencies at which levels of government have exposed the most consumer SSNs.

In its written testimony, the Commission cited two legislative recommendations to address the risks posed by the use of SSNs in the private sector – improved consumer authentication and standards to reduce the public display and transmission of SSNs. To date, neither of these recommendations has been enacted.

As to the authentication recommendations, the Commission believes that improved authentication can be achieved by encouraging or requiring all private sector business that have consumer accounts to adopt appropriate risk-based consumer authentication

systems that do not rely on an individual's SSN alone. Accordingly, the Commission recommends that Congress consider establishing national consumer authentication standards to verify that consumers are who they purport to be.

(3) K-12 schools continue to collect students' SSNs and use them as authenticators. Would you provide an update on this practice? How can we encourage school systems to stop this practice?

The Commission staff is currently examining the practice of schools using SSNs as authenticators. On July 12, 2011, the FTC and the Department of Justice's Office for Victims of Crime will host "Stolen Futures: A Forum on Child Identity Theft." (See www.ftc.gov/bcp/workshops/stolenfutures). One of the panels at the forum will focus on securing children's data in the educational system, especially in the K-12 arena. At the forum, leaders in the field will provide an update on current practices and explore ways to encourage school systems to better safeguard student information, including SSNs as authenticators and alternatives.

(4) I appreciate the work that the Federal Trade Commission has done to address the problems of ID theft, especially ID theft among children and foster children. I hope that you will continue to address these issues. In terms of ID theft among foster children, how widespread is the problem and why are foster youth particularly vulnerable to identity theft?

Foster children are particularly vulnerable to identity theft because their personal information is easily accessible by many people, including relatives, foster parents, and state employees. Moreover, since foster children often lack a strong familial or social safety net, they tend to have fewer resources to help them once they become victims. Finally, the consequences of identity theft may be more severe for foster children because once they are emancipated from foster care, establishing good credit is essential in their process to establishing a strong start to adulthood. At the upcoming forum on child identity theft, a panel will focus on these challenging issues, as well as discuss enacted and proposed state and federal legislation related to foster children and identity theft.

(5) What types of actions is the Commission taking to assist child welfare agencies in preventing ID theft and helping victimized youth recovery their identities?

The July 12th forum on child identity theft will include a panel on the issue of identity theft in the foster care context. One of the panelists, Howard Davidson of the ABA's Commission on Children and the Law, will explore what child welfare agencies can do to help prevent identity theft. We plan to work with Mr. Davidson and other panelists after the forum to continue to collaborate on foster child identity theft issues.

(6) Are there any policy recommendations that you would make to Congress to reduce the number of foster children who are victims of ID theft?

FTC staff is currently examining the issue of identity theft in the context of foster care. Although the July 12 forum is focused on developing and disseminating outreach

messages to prevent identity theft and assist victims, the Commission staff will be sure to offer any policy recommendations as appropriate.

(7) In your written testimony, you say that the Commission recommends eliminating the unnecessary display of SSNs, including on identification cards. Does the Commission recommend ending the use of the SSN as an identifier for foster children?

As explained above, this is an issue that staff will be exploring at the July 12 forum. Based upon what staff learns, policy recommendations may be provided at a later date.

(8) Do you believe that we are winning or losing the battle against ID theft?

Identity theft continues to be a significant problem, which the Commission is trying hard to address in several ways, as described in its written testimony. Commission staff believes that its robust data security enforcement program has encouraged companies to invest in better data security to avoid having consumers' information fall into the hands of identity thieves. The Commission has also worked hard to educate consumers in how to better protect themselves from identity theft. It has disseminated millions of copies of its consumer education materials. Of course, much work remains to be done, and the Commission continues to devote resources to this important issue.

(9) How has ID theft changed over the last several years? Is it more widespread, sophisticated and harder to stop? What are the trends with respect to organized crime or state sponsored ID theft?

(10) What is the most common cause of ID theft? Is it lost or stolen Social Security cards, death records that are sold with SSNs, or via some public listing or even the internet? Are there some trends you can discuss?

[Answer to questions 9 and 10] In response to question 1, we have provided information about some trends relating to consumer complaints that the FTC has received over the past several years. However, we do not want to suggest that the unverified complaints we receive are indicative of broader trends in identity theft. The number and types of complaints we receive vary with press stories about identity theft and other unrelated factors. Because the Commission has never attempted to conduct year-to-year surveys or analyses of general trends in identity theft, we cannot speak to issues such as the level of sophistication of identity thieves or what percentage of identity theft is state-sponsored.

That said, we do know that there are many causes of identity theft including high-tech (e.g., hacking, phishing, malware, spyware and keystroke logging) and low-tech causes (e.g. dumpster diving, stealing workplace records, stealing mail or wallets, and accessing public records containing SSNs). Some thieves fabricate SSNs that correspond to active SSNs that have been issued previously to individuals, especially children. Identity theft

can also occur when an individual uses someone else's personal information, including their SSN, to obtain employment, file tax returns, or obtain other government benefits.

(11) Can you tell us what burdens may occur by removing 'unnecessary' display of SSNs? Is there a way to encourage proper use of SSNs while minimizing those burdens?

The challenge in combating the misuse of SSNs is to find the proper balance between the need to keep SSNs out of the hands of identity thieves and the need to give businesses and government entities sufficient means to attribute information to the correct person. Business and governments use SSNs to ensure accurate matching of consumers with their information. SSN databases are also used to fight identity theft – for example, to confirm that a SSN provided by a loan applicant does not, in fact, belong to someone who is deceased. To encourage proper use of SSNs while minimizing burdens of removing SSNs, the Commission has identified two key legislative recommendations – improved consumer authentication and standards to reduce the public display and transmission of SSN. In terms of the second recommendation, the Commission recommends eliminating the unnecessary display of SSNs on publicly-available documents and identification cards and limiting how SSNs can be transmitted. Such steps would reduce the availability of SSNs to thieves, without hindering the use of SSNs for legitimate identification and matching purposes.

(12) One of the interesting parts of Mr. O'Carroll's testimony is the story of Dr. Martinez, which thankfully has been successfully resolved through the arrest of his ID thief. However, Dr. Martinez had yearly audits from the IRS, even though they knew after the first contact that his wages were falsely reported due to ID fraud. Are there good examples of private or public sector entities doing more to recognize what has happened to a victim and in some way "certify" his or her experience so he or she can move on with his or her life and not be repeatedly questioned about who they are?

Some states offer identity theft victims a "passport" that the victim can carry to prove who they are. The passport – which typically may be obtained through a state's Office of Attorney General – may be useful in the event that an identity theft victim is confused with an actual or suspected criminal. In addition, the Commission staff recommends that identity theft victims obtain a detailed police report that will help to prove their innocence and enable them to clear their name, especially if new accounts are opened.¹ The Commission also recommends that Congress consider creating national standards for the public display and transmission of SSNs.

¹ A police report, coupled with an identity theft affidavit, creates an ID Theft Report, which enables victims to exercise certain federal rights to clear their name. Among other things, an ID Theft Report enables victims to place an extended fraud alert on their credit files for seven years, to block erroneous information on their credit files, and obtain documents underlying the crime that can be used to prove their innocence.

(13) What can individuals do to protect themselves through any public or private institutions before SSN fraud starts?

To protect themselves from SSN fraud, consumers should avoid carrying their SSN in their wallets or purses. They should be wary about giving out their SSN to any public or private institution unless it is clear why that institution needs the SSN. Consumers should also regularly check their credit reports and financial statements. Consumers may get free annual credit reports from the three credit reporting agencies through www.annualcreditreport.com.

(14) What are three things that everyone can do to prevent becoming a victim of ID theft?

Although there are no iron-clad methods for preventing identity theft, everyone should: (1) check their bank statements and credit card statements monthly, and credit report at least annually; (2) secure their personal information – if it is paper, lock it and/or shred it; if it is online, use secure Internet connections and regularly update anti-virus software; and (3) not give out their personal information in person, on the phone, through the mail, or over the Internet unless they know who they are dealing with.

(15) Federal, state and local governments still display, or sometimes truncate, SSNs on public documents. To what extent does the public display of SSNs contribute to ID theft? What findings do you have on the display of SSNs by government at all levels and what are your recommendations?

As a result of the President's Task Force on Identity Theft, many federal agencies have eliminated or reduced their collection and display of SSNs. Further, OPM has issued guidelines to federal agencies on the appropriate and inappropriate use of SSNs in federal employee records. Most recently, the Department of Defense recently announced its elimination of SSNs as an identifier. As noted above, the Commission has supported legislation to minimize public display and transmission of SSNs.

(16) The latest trend in credit cards is to use smart phones to make credit card purchases. Given the recent agency and congressional concerns about data security and tracking through the phones, do you have any concerns about SSNs and credit card use by smart phones?

The Commission staff is analyzing the developments in the mobile marketplace, including how new services and technologies offered through smart phones treat personal information – such as SSNs and credit cards data. The use of mobile phones as payment mechanisms is still evolving. To address emerging issues in the mobile arena, the Commission has established a Bureau-wide team working extensively on issues related to the mobile marketplace, examining both privacy and data security issues. We have several active mobile investigations focusing on the collection of consumer data in

general and we will continue to closely watch the security of data collected by -- and through -- mobile devices.

(17) Can you give us any recommendations on how to prevent the growing ID theft problems with children and even unborn children? What should parents do to protect their children's financial record? Are there any policy changes we can make to help parents resolve ID theft issues on behalf of their children?

At the July 12th Forum, panelists from the government, the private sector, and advocacy and non-profit organizations will explore existing and potential solutions to child ID theft. The panelists specifically will explore solutions, as well as the best advice for parents to prevent and remedy child ID theft. Armed with this information, the Commission staff will be better able to advise parents on how to safeguard their children's personal information and resolve identity theft issues.

Theresa L. Gruber

Enclosure – Page 1

**Committee on Ways and Means, Subcommittee on Social Security
Hearing on Identity Theft – April 13, 2011
Questions for the Record**

1) The President's Identity Theft Task Force recommended that the Social Security Administration (SSA) become a clearinghouse for federal agencies that minimize the use of SSNs by the fourth quarter of 2007. What progress can you report on this recommendation?

The Task Force's recommendation read:

“Establish a Clearinghouse for Agency Practices That Minimize Use of SSNs”
To encourage agencies to share best practices on minimizing the use of SSNs, the Task Force recommended that we develop a clearinghouse to promote successful government initiatives in this area and to facilitate information sharing. The Task Force made the recommendation to build upon OMB's recent review of how agencies use SSNs, as well as to leverage successful efforts across the Federal government.

We implemented this recommendation in two steps. First, we formed the Social Security Number (SSN) Best Practices Collaborative, which included representatives from 36 Federal departments and agencies and met regularly in 2007 to explore, develop, and share best practices for reducing reliance on SSNs. The Collaborative formed a subcommittee chaired by the Internal Revenue Service (IRS) and comprised of agencies that handle high volumes of SSNs and personally identifiable information (PII), such as the Department of Defense, Department of Veterans Affairs, the Department of Homeland Security (DHS), the Centers for Medicare and Medicaid Services (CMS), and us.

Second, we established a clearinghouse on a bulletin board website in July 2007; over 25 agencies have registered as users to date. The clearinghouse, which remains operational and is located at www.idtheft.gov/takeaction.html, provides a forum to share materials regarding SSN use and display by Federal agencies. It highlights best practices as well as contacts for specific programs and initiatives.

2) What is SSA doing to end the practice of K-12 schools collecting students' SSNs and using them as authenticators?

We actively encourage schools and universities, as well as other entities, to reduce the unnecessary collection of SSNs by:

- Establishing a website with links to our publications, policy, frequently asked questions (FAQs), and best practices for protecting SSNs and promoting our website to State and local governments as part of our on-going educational outreach efforts;
- Coordinating with State Departments of Education and K-12 school systems to inform the education community about the potential risks of using the SSN as a student identifier;

Enclosure – Page 2

- Encouraging State Departments of Education and K-12 school systems to implement safeguards to protect SSNs when collected; and
- Promoting the best practices States and K-12 school systems have taken to limit the use of the SSN.

We also publish pamphlets, such as *Your Social Security Number and Card*, that tell individuals not to carry their SSN card. The pamphlet also advises individuals to avoid giving out their SSN unnecessarily.

- These publications are available in our field offices and on our website.
- They also are available free of charge through the [Federal Citizen Information Center](#) in Pueblo, Colorado.

In addition, we post FAQs on our website that address identity theft and how we protect SSNs. About 50,000 people view these FAQs each month.

3) How does the SSA alert or educate cardholders on the proper protection of their SSNs? Do you inform the public on how to protect their SSNs? Does SSA conduct public outreach to institutions and businesses with respect to the display of SSNs? Does the agency provide best practices information for the handling of personal data?

We take the protection of SSNs very seriously. We keep our records confidential and disclose information only when the law permits.

We routinely inform and remind the public about ways they can protect their SSNs:

- We advise individuals to be careful about sharing their SSNs with others, even when requested;
- We encourage individuals to keep their SSN card in a safe place and not carry the card, or any document displaying their SSN, with them;
- We offer pamphlets that tell individuals not to carry the SSN card unless an employer or service provider insists on seeing it, and to avoid giving out their SSN unnecessarily (see response to question 2 for links to specific publications and the Federal Citizen Information Center);
- We post FAQs on our website that address identity theft and how we protect SSNs. About 50,000 people view these FAQs each month;
- We write stories for local newspapers across the country urging people to protect their SSN and card;
- We broadcast “Tips to Prevent Identity Theft” on our field offices’ TV monitors, which explains how individuals can protect themselves from becoming identity theft victims; and,
- We partner with the Federal Trade Commission to educate the public through local seminars and public information materials.

We created a publicity campaign for the employer community entitled, “*Do You Really Need to See the Card?*” We emphasize that employers do *not* need to see the SSN card. Instead, they can quickly verify if the employee’s name and SSN match our records using our free SSN

Enclosure – Page 3

verification services. We regularly speak to the employer community, work with payroll and tax stakeholders, produce publications, and provide SSN-related information on our website.

We stress to employers and payroll professionals the importance of keeping the Social Security card and number safe and secure.

We work with the American Association of Motor Vehicle Administrators, National Association of Motor Vehicle Boards and Commissions, American Association of University Administrators, and the American Association of Collegiate Registrars and Admissions Officers to decrease and limit the use and display of the SSN on drivers' licenses or as student identifiers.

In 2010, we joined the National Cybersecurity Alliance led by DHS. This group works to increase public awareness of cybersecurity and decrease identity theft by sharing knowledge and resources among Federal agencies.

4) If someone knows their SSN has been stolen or compromised, but no actual fraud has occurred to date, can the individual apply for a new number? What guidelines does the SSA follow for when a replacement card is issued? Can the SSA help an individual protect a stolen number?

When a member of the public contacts us regarding identity theft, we take immediate action to assist them:

- We verify the accuracy of our record of the individual's reported earnings.
- We issue a replacement card with the same number if the individual's SSN card has been stolen.
- We consider assigning a new SSN if the victim requests a new SSN, and we determine the person has been harmed by misuse of the SSN.
- We provide publications such as, *Identity Theft and Your Social Security Number* and the above mentioned, *Your Social Security Number and Card*.
- We refer the individual to the FTC, which will assist the individual in placing a fraud alert with the major credit reporting bureaus (Equifax, Experian, and TransUnion), closing financial accounts, and filing necessary reports with the police.
- We refer cases of identity theft to our Office of the Inspector General (OIG). OIG will work with the United States Attorney to determine whether to prosecute the person misusing the SSN.
- We advise tax fraud victims to contact the Internal Revenue Service.

We will assign a new SSN if we determine:

- that misuse has taken place;
- there is documentation, such as a police report, of the misuse;
- the misuse was committed with criminal or harmful intent;
- the misuse has caused the individual to be personally or economically disadvantaged;
- and,
- the individual has been disadvantaged by the misuse within the past year.

Enclosure – Page 4

An individual requesting a new SSN must prove age, U.S. citizenship or lawful immigration status, and identity.

An individual should consider changing his or her SSN only as a last resort. Because of the widespread use of the SSN, getting a new SSN may adversely affect a person's ability to interact with Federal agencies, State agencies, employers, schools, medical institutions, and others, as many of the individual's records may be identified under the former SSN. An individual who obtains a new SSN will have to notify banks, schools, medical institutions, etc., so that records can be properly tracked and cross-referenced. Since a new SSN can also be stolen, assigning a new SSN is not a guaranteed solution to identity theft.

We will not assign a new SSN:

- to avoid the consequences of filing for bankruptcy;
- to avoid the law or legal responsibility; or
- if no evidence exists that another person is using that number.

5) The Subcommittee is interested in removing the SSN from the Medicare card and inserting another identifying number for Medicare use, much like the military is doing with its ID cards. The SSA systems would not have to make any changes except interfacing with the Centers for Medicare and Medicare Services to identify the new number with the correct SSN already in their system. Is this the simplest way to alter the system, and if so, what are the costs and the time frames for achieving the change?

We defer to CMS with respect to the analysis of the Subcommittee's idea, costs, and timeframes. The specific effects on our systems, including costs and timeframes, would be dependent on CMS specifications to remove the SSN from the Medicare card.

We appreciate the importance of addressing potential identity theft and fraud issues. Nevertheless, we must balance the benefits of removing the SSN from the Medicare card against the additional resources required to do so. We expect that any proposal would require changes to our systems and would increase visits to our field offices and calls to our toll-free number. Congress cut \$1 billion from our fiscal year 2011 budget request, and we are concerned about our resource ability to implement changes.

6) As you may know, the Department of Education recently proposed a rule known as the "gainful employment" ruling that would limit the use of Title IV funding at proprietary, or for-profit, colleges. This rule would employ a formula based on a student's debt and income to determine whether students at these schools meet the Department's definition of holding gainful employment after graduation. Many Members of Congress have concerns with this rule, as evidenced by the 289 votes in the U.S. House of Representatives in favor of an amendment to block Fiscal Year 2011 funding for the implementation of this rule. One of my concerns is the use of SSNs to collect confidential taxpayer data to determine whether or not graduates are earning what the government has defined as gainful income in order for their degree program to maintain eligibility for Title IV funding.

Enclosure – Page 5

What is the SSA doing to protect students and schools from data loss and theft? What assurances can be provided that this new system of records will not be exposed to cyber security risks, privacy risks or be subject to law enforcement or national security investigatory demands for information? In other words, has a privacy and data security impact assessment been done and, if so, what were the findings?

The IRS owns tax return data. Our authority to use and share tax return data for disclosure purposes is subject to section 6103 of the *Internal Revenue Code* (IRC).

We will provide strictly statistical aggregate data, including mean and median calculations, to the Department of Education (DOE). These data will not contain any information on individual taxpayers, and we will not identify any taxpayer, either directly or indirectly. As such, the data we will provide is not tax return information protected by section 6103 and our use will fully comply with the requirements of the IRC. The *E-Government Act of 2002* requires agencies to conduct privacy impact assessments (PIA) for new electronic information systems and collections containing PII and make them publicly available. Since we are not collecting or sharing new PII in this instance, we do not need to conduct a PIA.

We discussed our proposal for providing aggregate data to DOE with IRS Counsel before preparing the reimbursable agreement. We plan to use the taxpayer identifying information we receive from DOE to match our records and perform an electronic data exchange in accordance with all applicable privacy and security laws and regulations. Once we draft the data exchange agreement, we will share the agreement with IRS Counsel to ensure that we comply with all provisions of the IRC.

7) As you know identity theft is one of the fastest growing crimes in America, and one of the reasons for this is the ease of finding SSNs on unprotected documents. In many states, each foster child is issued an identity card with his or her SSN on the card and the SSN is used as the primary identifier of the child. The federal government allows for a SSN change when a foster child is going through the adoption process. A new SSN largely cleans the financial slate for these children. Is issuing a new SSN a solution for minors, such as foster youth, who have been victims of identity theft? What is the impact of issuing a new SSN?

With respect to identity theft, our treatment of minors is identical to our treatment of adults. Please see our answer to question 4 above.

8) When a person uses an SSN to apply for credit or open an account, what mechanisms are there for the creditor to check the legitimacy of the SSN and whether or not it belongs to a minor? Would it raise a red flag if a creditor discovered the SSN belonged to a minor? Do creditors routinely check to determine if an SSN belongs to a minor?

We offer a fee and consent-based verification service, Consent Based SSN Verification (CBSV), which provides instant, automated verification to enrolled private companies. Using CBSV,

Enclosure – Page 6

participating companies can confirm that a name, SSN, and date of birth match information in our records.

Because this is a consent-based service, a company must have written permission from the number-holder to conduct the match. We charge a fee to cover the costs of this service because it does not relate to the administration of our programs. Of the 153 companies currently enrolled, 72 companies have used CBSV since 2008. Based on the information contained in each company's profile, 66 companies identified themselves as "Mortgage/Banking Services" as the reason for using CBSV.

Regarding the issuance of credit to minors, we do not have any oversight of the financial industry. The Federal Reserve Board, the Consumer Financial Protection Bureau, and other agencies responsible for the banking industry have oversight in this matter.

9) As a result of setting a limit with respect to the number of Social Security cards an individual can have, there has been an increase in the number of individuals coming into field offices asking for printouts of SSNs, also known as "Numi-Lites." What are your thoughts on charging individuals for these printouts both as a way to cover costs and discourage individuals and businesses from requesting them? Is it also true that the SSA requires less proof of identity for the print outs than for a new Social Security card?

The Freedom of Information Act requires us to provide copies of our records to number-holders upon request. The main reason individuals request printouts is because an employer has requested such a document. We may consider charging a fee for the printout in the future, but current statutory language does not allow us to charge a fee for this service.

We require an individual to submit certain documents as proof of identity for an SSN card. An acceptable document must be current (not expired) and show the person's name, identifying information, and preferably a recent photograph. We will not issue an original SSN card without proper evidence of identity, age, and citizenship. In the case of noncitizens, we also require proof of work authorization.

When an individual requests a "NUMI-Lite" or any other information, the requester must provide the SSN and establish his or her identity by supplying certain identifying information. We compare the information provided to us with information in our records. These evidence requirements provide sufficient proof to release information to the individual.

10) When it comes to enumerating foreign workers, why does the SSA not issue SSNs to temporary workers? Why are SSNs that are issued for work authorization not rescinded or suspended when the non-citizen leaves the country?

The *Social Security Act*¹ requires us to issue SSNs to aliens with work authorization, regardless of the duration of the work authority. The SSN cards we issue to foreign workers with

¹ Section 205(c)(2)(B)(i)(I).

Enclosure – Page 7

temporary work authority bear the restrictive legend “valid for work with DHS authorization” on the face of the card.

We issue SSNs in order to keep track of workers’ earnings and to correctly calculate and pay benefits. Under totalization agreements, temporary workers may become eligible for benefits based, in part, on earnings in the U.S. long after they have left the U.S., just as U.S. citizens may receive benefits based, in part, on work they performed outside the U.S.

The SSN does not provide work authorization, only documents issued by DHS can provide such authority to a non-citizen. DHS can extend work authority for a non-citizen and DHS determines when a non-citizen must leave the country.

11) More children, and in fact, unborn children are having their identities stolen because thieves have figured out the algorithm SSA uses to generate the numbers. SSA is changing this now. Why can't SSA issue a new number to a child?

Please see our answer to question 4 above with respect to issuing a new SSN to a child. Our treatment of children is identical to our treatment of adults.

As you note, we are randomizing the SSN assignment process. Through randomization, we can include previously excluded area numbers and thus increase the pool of SSNs available for assignment from 288 million to 422 million. We also believe randomization will impede reconstructing an individual's SSN.

