# HEARING ON IDENTITY THEFT AND TAX FRAUD

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

AND

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MAY 8, 2012

**Serial No. 112–OS12/SS15**

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
78–817 WASHINGTON : 2013

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

DAVE CAMP, Michigan, *Chairman*

WALLY HERGER, California
SAM JOHNSON, Texas
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin
DEVIN NUNES, California
PATRICK J. TIBERI, Ohio
GEOFF DAVIS, Kentucky
DAVID G. REICHERT, Washington
CHARLES W. BOUSTANY, JR., Louisiana
PETER J. ROSKAM, Illinois
JIM GERLACH, Pennsylvania
TOM PRICE, Georgia
VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
AARON SCHOCK, Illinois
LYNN JENKINS, Kansas
ERIK PAULSEN, Minnesota
KENNY MARCHANT, Texas
RICK BERG, North Dakota
DIANE BLACK, Tennessee
TOM REED, New York

SANDER M. LEVIN, Michigan
CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
JIM MCDERMOTT, Washington
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
RON KIND, Wisconsin
BILL PASCRELL, JR., New Jersey
SHELLEY BERKLEY, Nevada
JOSEPH CROWLEY, New York

JENNIFER SAFAVIAN, *Staff Director*
JANICE MAYS, *Minority Chief Counsel*

---

## SUBCOMMITTEE ON OVERSIGHT

CHARLES W. BOUSTANY, JR., Louisiana, *Chairman*

DIANE BLACK, Tennessee
AARON SCHOCK, Illinois
LYNN JENKINS, Kansas
KENNY MARCHANT, Texas
TOM REED, New York
ERIK PAULSEN, Minnesota

JOHN LEWIS, Georgia
XAVIER BECERRA, California
RON KIND, Wisconsin
JIM MCDERMOTT, Washington

## SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

KEVIN BRADY, Texas
PATRICK J. TIBERI, Ohio
AARON SCHOCK, Illinois
RICK BERG, North Dakota
ADRIAN SMITH, Nebraska
KENNY MARCHANT, Texas

XAVIER BECERRA, California
LLOYD DOGGETT, Texas
SHELLEY BERKLEY, Nevada
FORTNEY PETE STARK, California

# CONTENTS

# HEARING ON IDENTITY THEFT AND TAX FRAUD

**TUESDAY, MAY 8, 2012**

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
*Washington, D.C.*

The subcommittees met, pursuant to call, at 10:00 a.m., in Room 1100, Longworth House Office Building, the Honorable Charles Boustany [chairman of the Subcommittee on Oversight] presiding.

[The advisory of the hearing follows:]

# *HEARING ADVISORY*

## Chairmen Boustany and Johnson Announce Hearing on Identity Theft and Tax Fraud

Tuesday, May 08, 2012

House Ways and Means Oversight Subcommittee Chairman Charles Boustany, Jr., MD (R-LA) and Social Security Subcommittee Chairman Sam Johnson (R-TX) today announced that the Subcommittees on Oversight and Social Security will hold a hearing on tax fraud involving identity theft. **The hearing will take place on Tuesday, May 8, 2012, in 1100 Longworth House Office Building, beginning at 10:00 A.M.**

In view of the limited time available to hear from 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 Committee and for inclusion in the printed record of the hearing. A list of invited witnesses will follow.

**BACKGROUND:**

The Treasury Inspector General for Tax Administration (TIGTA) recently reported that criminals are stealing identities at an alarming rate to receive fraudulent tax refunds. For Processing Year 2011, the Internal Revenue Service (IRS) reported detecting approximately 940,000 tax returns potentially filed by identity thieves and prevented issuing $6.5 billion in fraudulent tax refunds. Yet, TIGTA found that fraudulent refunds acquired through identity theft are significantly greater than the amounts detected. Recent media reports indicate criminals are engaging in previously unheard of levels of identity-theft related tax fraud, including a Tampa, Florida ring that allegedly swindled taxpayers out of $130 million by using off-the-shelf tax preparation software and prepaid debit cards to fraudulently obtain tax refunds.

One source of information for identity thieves is the Social Security Administration's (SSA) compilation of death records, which it uses to administer benefits. Since 1980, the SSA has made available for purchase by the public a file containing the Social Security numbers (SSNs), names, dates of birth and death, and zip code of those who have died. According to the Inspector General of SSA, this data file, known as the Death Master File (DMF), contains the personal information of 85 million Social Security number holders who have died since 1936, as well as the information from about 1.3 million new deaths that are added each year.

The DMF is useful to many organizations for fraud prevention and benefit administration. It has been purchased by other government agencies, financial institutions, life insurance companies, credit reporting organizations, data aggregators, medical researchers, genealogists and others; and purchasers are free to re-disclose the data they obtain. At the same time, criminals are able to exploit the availability of death information to submit fraudulent tax returns that include the decedent's SSN, including the SSNs of deceased dependent children. Only after the parents of the dead child have had their legitimate return rejected by the IRS do they and the agency discover the theft.

According to the 2011 Annual Report to Congress by the National Taxpayer Advocate, the federal government facilitates tax-related identity theft by publicly releasing significant personal information of deceased individuals. The National Taxpayer Advocate has recommended legislative action to restrict access to the DMF. The Taxpayer Advocate has also reported a 97 percent increase in taxpayer identity-theft complaints in fiscal year (FY) 2011, on top of a 23 percent increase in FY 2010.

In November 2011, SSA restricted the release of certain state records in the publicly-available file, resulting in the removal of 4.2 million death records from the DMF, and since that time has also removed zip code information from the DMF.

In addition, the Administration is developing legislation to limit the availability of death information.

In announcing the hearing, Chairman Boustany said, **"Improper payments of tax refunds have cost taxpayers over $100 billion in recent years. This hearing will explore a major source of the problem - identity thieves who steal Social Security numbers to engage in tax fraud. We need to make sure that we have a complete accounting of the size of the problem, understand why it is getting worse, and explore what can be done to combat tax fraud so we can catch and put more identity thieves in jail."**

In announcing the hearing, Chairman Johnson said, **"Worrying about a lost loved one's stolen identity is a burden no grieving family should bear. That's why I, along with a number of my colleagues, introduced H.R. 3475, the 'Keeping IDs Safe Act of 2011,' to protect the Social Security number and other personal information of those who have died. With the bipartisan support of my colleagues and the Administration we will take steps to stop these heartless identity thieves and protect American taxpayers."**

**FOCUS OF THE HEARING:**

The Subcommittees will examine how identity theft contributes to tax fraud, and whether the IRS and the SSA are doing enough to protect SSNs and prevent and detect false returns filed by identity thieves.

**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 document, in compliance with the formatting requirements listed below, **by the close of business on Tuesday, May 22, 2012.** 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 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 BOUSTANY. The subcommittees will come to order. I would like to welcome everyone to today's joint Subcommittee on Oversight and Subcommittee on Social Security hearing on identity theft and tax fraud. I am very pleased to join Chairman Johnson again as our subcommittees focus on fraud, waste and abuse and how the Federal Government might better protect taxpayer dollars.

The subject of today's hearing is not a new one, but evidence suggests it is a problem reaching unprecedented levels. Identity theft allows criminals to file false tax returns and claim thousands of dollars in refundable tax credits.

In a recent case in Florida, identity thieves alleged obtained $30 million in fraudulent refunds and nearly obtained $100 million more before being caught. They spent the money on expensive cars, homes, living lavishly under the impression that they could steal from taxpayers with impunity. Recent news stories have also told of identity thieves so brazen that they hold seminars on how to steal identities and to commit tax fraud.

In another case scam artists uploaded music video on YouTube showing cars they were able to purchase with stolen taxpayer dollars and instructing others on how they could do the same.

Confronted with emboldened identity thieves and tax cheats, the American taxpayers expect the Federal Government to better protect identities, detect fraudulent tax returns, punish those engaged in these crimes and assist taxpayers who are victimized. Today we will explore how well the Federal Government is living up to this responsibility and how we can improve these efforts.

This morning's hearing will seek to answer four questions. First, how does identity theft related tax fraud occur? Identity thieves often rely on public sources of sensitive information to engage in tax fraud, and the subcommittees look forward to hearing from the witnesses on how this information might be limited or better protected in a way that protects taxpayer identities.

Second, how big is the problem? While the IRS has estimated identity theft related tax fraud costs taxpayers more than $6 billion annually, we will hear testimony this morning that the true figure may be nearly double previous estimates.

Third, what tools are needed to better deter, detect and punish this crime? Fruitful discussions of fraud, waste and abuse should include not just details of the problem, but also talk of potential solutions, and I look forward to hearing from our witnesses on that.

And finally, this morning's hearing will focus on victimized taxpayers and what their experience is when they learn they have been victims of identity theft and how the government might better assist them in recovering from the crime and better protect their identities.

I want to thank our witnesses and I look forward to this morning's discussion. Before yielding to the ranking member, Mr. Lewis, I ask unanimous consent that all members written statements be included in the record. Without objection, so ordered.

Mr. Lewis, I now yield to you, sir.

Mr. LEWIS. I want to thank you, Mr. Chairman, you and Chairman Johnson, for holding this hearing. I am pleased to have the Internal Revenue Service and the Social Security Administration before us today. These agencies are both entrusted with personal information and they should play an important role in preventing identity theft.

Tax fraud and identity theft are growing problems for the tax administration. They harm the Federal Treasury, American citizens and their families. I commend the Internal Revenue Service for identifying and preventing over $14 billion in fraudulent tax refunds last year.

I also thank the agency for its assistance to almost 500,000 taxpayers who have been victims of identity theft. Despite this progress we need to do more, and we must do more, to help victims and stop the loss of billions of taxpayer dollars.

I continue to have serious concerns about the effects of recent budget cuts on taxpayers and the agency's ability to serve them. In this area of budget cuts, hiring freezes and staff reduction, I am also concerned that the IRS cannot fully combat identity theft and tax fraud. This year the IRS expects to spend over $330 million combating fraudulent tax refunds when its budget was cut by over $300 million.

In a most recent report to Congress, the National Taxpayer Advocate states that the most serious problem facing taxpayers is that the IRS is not adequately funded to serve taxpayers and collect taxes. We will see today that the IRS is not properly funded to handle the growing identity theft problem. We need to provide the IRS with more tools to combat identity theft today.

I look forward to learning more about the recommendation to expand the agency's to access the National Directory of New Hires. The recommendation was initially proposed by the Bush administration in 2006. It has been in the Administration's budget proposal every year since then. It appears to be a common sense solution that will be a step in the right direction.

Now the gentleman from Washington, Representative McDermott, and I have introduced a bill to expand the agency's access to this database. I ask my colleagues on both sides to join us on this bill.

Mr. Chairman, in closing I would like to thank the witnesses for appearing before us today. I look forward to your testimony, and thank you again very much for being here. With that, Mr. Chairman, I yield back.

Chairman BOUSTANY. I thank the ranking member of the Oversight Subcommittee, and now we turn to Chairman Johnson, chairman of the Social Security Subcommittee, for his opening statement.

Chairman JOHNSON. Thank you, Mr. Chairman. Chairman Boustany, I want to thank you for holding the hearing regarding identity theft and its role in the growing crime of tax fraud. Earlier

this year the Subcommittee on Social Security held a hearing on Social Security death records, including the so-called Death Master File, a publicly available listing of the personal information of those who have died, including their Social Security numbers. We learned that the Death Master File serves as a readily available source of information identity thieves need in order to file fraudulent tax returns.

We heard the heartbreaking story of the Agin family whose 4-year-old daughter Alexis had her identity stolen shortly after she passed away. Only when their tax return was rejected by the IRS did the Agins learn that an identity thief had already filed a claim, claiming their child as a dependent. No grieving family should bear this additional burden. Yet when the Agins reached out to the community of grieving cancer parents, within the first hour they heard from 14 families who had lost a child whose Social Security Number was also stolen. Alexis' father, Jonathan Agin is in the audience today. He has joined us and I thank him for his tireless efforts to stop identity thieves from accessing the Death Master File. Thank you for being with us, sir.

So why does the Federal Government make public the Social Security numbers and other personal information of those who have died? Turns out unless Congress changes the law, it is required. Social Security collects death information so it can stop benefits to those who have died and start benefits for their survivors. But a 1980 Freedom of Information Act court mandated settlement required Social Security to also make the information about deceased Social Security number holders available to the public. In response Social Security created the Death Master File. With 84 million listed individuals and 1-1/2 million new individuals added each year, many groups now purchase the Death Master File from the Commerce Department, including government agencies, credit reporting agencies, financial institutions, law enforcement organizations, and medical and genealogical researchers.

But the decades old practice of publishing personal death information that anyone can buy needs to end, and now. In the age of Internet identity thieves can all too easily get their hands on a Social Security Number and reap instant awards that no one, including the person whose number it is, knows what has happened until after the fact usually.

ID Analytics, a fraud prevention firm, recently released a study comparing death information from the Death Master File to applications for credit products and cell phone services. The study found that the identities of nearly 2.5 million deceased Americans are used by fraudsters to commit identity theft each year.

Identity theft is also a growing problem on the tax front. The Treasury Inspector General reports that IRS stopped 6.5 billion in false refunds in 2011, but much more went undetected.

Taxpayers who are victims of tax identity theft have to endure a long process of proving their real identities, submitting paper returns and waiting months to get their rightful refund. That is just wrong.

To help stop this crime I, along with a number of my colleagues, introduced H.R. 3475, Keeping IDs Safe Act of 2011. Our bill ends

the publication of the Death Master File, denying criminals easy access to the personal information of those who have died.

Make no mistake, we will stop these identity thieves and in so doing protect the American taxpayers and prevent other families from having to go through what the Agins did.

I want to thank all our witnesses for coming today and I look forward to hearing your testimony. Thank you, Mr. Chairman.

Chairman BOUSTANY. Thank you, Chairman Johnson. Now we will turn to the ranking member of the Committee on Social Security, Mr. Becerra.

Mr. BECERRA. Mr. Chairman, thank you very much. The Internal Revenue Service does a lot with a little, processing 140 million tax returns in the span of just a few months while combating fraud and enforcing our tax laws. Congress needs to do its part too by providing adequate resources and enacting legislation that strikes the right balance between efficiently processing returns and preventing fraud.

We are all concerned about tax fraud. Tax fraud increases the burden on honest taxpayers, it undermines compliance with our voluntary tax system, and it harms the U.S. Treasury. When tax fraud takes the form of identity theft, it hurts individual taxpayers more directly, as Mr. Jonathan Agin, who testified recently at our subcommittee hearing, and he is the father of a deceased child who was a victim of tax fraud, as he so eloquently testified when he appeared before us in this subcommittee.

Mr. Chairman, the IRS needs both tools and resources to combat fraud. It needs not only to work together with Congress because it is not always easy to keep a step ahead of the fraudsters, but it also, we are going to learn today, needs to do something about having the right amount of funding to get things done. We are going to learn today about some of the more creative ways that individuals actually do perpetrate tax fraud.

Unfortunately, budget cuts mean the IRS is struggling just to keep up with its core work. This year IRS's operating budget is $305 million less than it was in 2011, and it has 5,000 fewer employees who can process returns, assist taxpayers and combat fraud.

As a result, the IRS can barely answer the phone calls it receives from taxpayers. In fact this spring the large majority of callers to the special IRS phone line dedicated to assisting taxpayers with identity theft did not get through. For the most recent week measured, 75 percent of callers were unable to get through, and those that did get through waited 1 hour and 21 minutes on hold before the IRS employee could assist them.

The National Taxpayer Advocate has identified IRS's underfunding as the "number one most serious problem" in her annual report to Congress, concluding that the IRS "is not adequately funded to serve taxpayers and collect taxes."

Combating fraud requires a balancing act. The IRS must balance the time it takes to conduct antifraud checks with a statutory requirement it has to process returns and issue refunds quickly for law abiding taxpayers. Each year under current procedures it takes months for the IRS to receive and process the nearly 250 million W-2 reports and 1.5 billion other third party reports that are sub-

mitted. This is on an annual basis. At the same time, the IRS aims to issue refunds within 7 to 10 days of receiving the return. As a result the agency does not wait to issue refunds until it is able to cross-check those returns against those other reports.

I think we need to figure out a way to do a better job in the future, but there is no easy answer now on the horizon.

Similarly, the question of the Death Master File also requires striking the right balance. The Social Security Subcommittee has received testimony over the years about the value of SSA's compilation of the death records it receives into the DMF. The DMF is helpful in administering benefits and combating fraud at both government agencies and in the private sector. At the same time we know that the widespread availability of the SSA's death information means it can also be used by identity fraudsters. We are going to learn more about the challenges of combating identity fraud in the tax world today.

I commend SSA for utilizing its limited statutory authority to restrict death information. SSA recently removed zip code information from the DMF to make it harder for fraudsters to use, and promptly it received a Freedom of Information Act—a FOIA request—to reinstate it. SSA has also recently removed certain State death records which it were determined were not subject to a FOIA request from the publicly released DMF, resulting in the removal of over 4 million records from the file. However, SSA's longstanding legal opinion is that the Privacy Act and Freedom of Information Act do not allow SSA to keep its death records from the public. As a result, at our last hearing on the DMF and identity fraud SSA testified that the Administration was evaluating legislative options to restrict release of the DMF. I understand they have made significant progress and I look forward to receiving the legislative proposal.

Mr. Chairman, I look forward to working with the administration and with my colleagues on both sides of the aisle as we try to move forward with a solution to this problem, and with that I yield back the balance of my time.

Chairman BOUSTANY. I thank the ranking member for his opening statement and now I would like to welcome our panel. We have a distinguished panel with us today. This morning we will hear from the Honorable Russell George, Treasury Inspector General for Tax Administration. Welcome, Mr. George. We will also hear from the Honorable Patrick P. O'Carroll, Jr., Inspector General for the Social Security Administration. And thirdly, Mr. Steven Miller, Deputy Commissioner for Services and Enforcement for the Internal Revenue Service. Welcome, sir. Nina Olson, the National Taxpayer Advocate. Ms. Olson, welcome. And Mr. David Black, the General Counsel for the Social Security Administration.

Welcome to all of you. We thank you for being here today. You each will have 5 minutes, as is customary, to deliver your oral statements, keeping in mind that your full written statements will be included in the record.

Inspector General George, you may begin.

**STATEMENT OF THE HONORABLE J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION**

Mr. GEORGE. Thank you, Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and Members of the Subcommittees. Thank you for the opportunity to address the subject of identity theft and its impact on taxpayers and tax administration.

Since I last testified on this subject in November of 2011, TIGTA is in the process of completing an assessment of the IRS's efforts to spot and prevent identity theft. While the final report will not be released until June, I will discuss some of our most cogent findings as well as those of a recently issued report on the assistance the IRS provides to victims of tax fraud related identity theft.

TIGTA has reported previously a substantial number of individuals continue to submit tax returns reporting false income and/or withholding for the sole purpose of receiving a fraudulent tax refund. The IRS recently reported that of the more than 2 million tax returns that it identified as fraudulent approximately 900,000 tax returns with $6.5 billion in associated fraudulent tax refunds involved identity theft. However, the IRS does not know how many identity thieves are filing fraudulent tax returns or the amount of revenue being lost.

TIGTA evaluated the IRS's efforts to identify and prevent fraudulent tax returns resulting from identity theft. As part of our assessment we identified and quantified potential refund losses. Our analysis found that although the IRS detects and prevents a large number of fraudulent refunds based on false income documents, there is much more fraud that it does not detect. We identified approximately 1.5 million additional undetected tax returns with potentially fraudulent tax refunds totaling in excess of $5 billion. If this is not addressed, we estimate the IRS could issue approximately $26 billion in fraudulent tax refunds resulting from identity theft over the next 5 years.

As we previously reported, access to third party income and withholding information at the time tax returns are processed is the single most important tool the IRS could have to identify and prevent this type of tax fraud. Another important tool that could help the IRS prevent this type of fraud is the National Directory of New Hires. Again, as was pointed out earlier by Mr. Lewis, legislation would be needed to expand the IRS's authority to access the directory's wage information for use in identifying tax fraud.

In those cases involving identity theft the fraudulent tax return is often filed before the legitimate taxpayer files his or her tax return. For tax year 2010 we identified more than 48,000 Social Security numbers that were used multiple times as a primary taxpayer identification number. When the identity thief files the fraudulent tax return the IRS does not yet know that the individual's identity will be used more than once. As a result the tax return is processed and the fraudulent refund is issued. Once the legitimate taxpayer files his or her tax return the duplicate tax return is identified and the refund is held until the IRS can confirm the taxpayer's identity. These instances result in the greatest burden to the legitimate taxpayer.

We recently completed an audit that evaluated the assistance the IRS provides to victims of identity theft. We found that the IRS is not effectively providing assistance to these victims. Moreover, processes are not adequate to communicate identity theft procedures to taxpayers, resulting in increased burden for victims. Of concern is the length of time taxpayers must work with the IRS to resolve identity theft cases which, as Mr. Becerra pointed out, could take more than a year to resolve. Resources have not been sufficient to work identity theft cases dealing with refund fraud and continue to be of concern. IRS employees who work the majority of cases also respond to taxpayer calls. As a result the average wait time for a taxpayer was approximately 1 hour.

In conclusion, we at TIGTA continue to be very concerned about the scope of this problem and will provide continuing audit coverage of IRS's actions taken to stem tax fraud related identity theft and to provide prompt resolution to taxpayers who are victimized. In addition, we will continue to conduct criminal investigations of identity theft violations involving IRS employees, tax return preparers and individuals impersonating the IRS.

I hope my discussion of our work assists you with your oversight of the issue involving the IRS. Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, Members of the Subcommittee, thank you for the opportunity to address this important topic.

[The prepared statement of Mr. George follows:]

**JOINT HEARING BEFORE THE**
**COMMITTEE ON WAYS AND MEANS**
**SUBCOMMITTEES ON OVERSIGHT**
**AND SOCIAL SECURITY**
**U.S. HOUSE OF REPRESENTATIVES**

"Identity Theft and Tax Fraud"

**Testimony of**
**The Honorable J. Russell George**
**Treasury Inspector General for Tax Administration**

**May 8, 2012**

**Washington, D.C.**

TESTIMONY OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
*before the*
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEES ON OVERSIGHT
AND SOCIAL SECURITY
U.S. HOUSE OF REPRESENTATIVES

"Identity Theft and Tax Fraud"

May 8, 2012

Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and Members of the Subcommittees, thank you for the invitation to speak before you today on the subject of identity theft and its impact on taxpayers and tax administration. Since I last testified on this subject in November 2011,[1] we have completed our assessment of the IRS's efforts to identify and prevent identity theft and plan to issue our final report in June of this year. We have also recently issued a report on the assistance that the IRS provides to victims of tax fraud-related identity theft. My comments today will focus on this recently completed work.

As we have reported previously, a substantial number of individuals continue to submit tax returns reporting false income and/or withholding for the sole purpose of receiving a fraudulent tax refund. Many of these claims involve identity theft. For Processing Year 2011,[2] the IRS reported that of the 2.2 million tax returns that it identified as fraudulent, approximately 940,000 tax returns with $6.5 billion in associated fraudulent tax refunds involved identity theft.

The IRS acknowledges that it does not have complete statistics on identity theft. In Calendar Year 2011, the IRS identified over 1.1 million incidents of identity theft that affected the Nation's tax system. This figure includes incidents in which taxpayers contacted the IRS alleging that they were victims of identity

---

[1] *Identity Theft and Tax Fraud, Hearing Before the H. Comm. on Oversight and Government Reform, Subctm. on Government Organization, Efficiency and Financial Management*,112th Cong. (Nov. 15, 2011) (statement of J. Russell George).
[2] A Processing Year is the year that the tax return is processed.

theft (110,750 incidents[3]) as well as instances where the IRS identified identity theft (1,014,884 incidents[4]). Many of the taxpayers that the IRS identified were not aware they were victims of identity theft because they either did not file tax returns or did not have filing requirements.

**Detection and Prevention of Identity Theft**

At the beginning of the 2012 Filing Season, the IRS announced the results of a nationwide sweep cracking down on suspected identity theft perpetrators as part of a stepped-up effort against refund fraud and identity theft. This effort is part of the IRS's identity theft strategy to prevent, detect, and resolve identity theft cases. In addition to this crackdown by its law-enforcement division, the IRS has stepped up its internal reviews to spot false tax returns before tax refunds are issued. These efforts include designing new identity theft screening filters that the IRS believes will improve its ability to identify false tax returns before they are processed and before any fraudulent tax refunds are issued.

Tax returns identified by these new filters are held during processing until the IRS can verify the taxpayers' identity. IRS employees attempt to contact these individuals and request information to verify that the individual filing the tax return is the legitimate taxpayer. Once a taxpayer's identity has been confirmed, the tax return is released for processing and the tax refund is issued. If the IRS cannot confirm the filer's identity, it halts processing of the tax return to prevent the issuance of a fraudulent tax refund. As of April 19, 2012, the IRS reports that it has stopped the issuance of $1.3 billion in potentially fraudulent tax refunds as a result of the new identity theft filters.

The IRS also continues to expand its efforts to prevent the payment of fraudulent tax refunds claimed using deceased individuals' names and Social Security Numbers (SSNs). The IRS began a pilot program in Processing Year 2011 which locked taxpayers' accounts where the IRS Master File and Social Security Administration data showed a date of death. The IRS places a unique identity theft indicator on deceased individuals' tax accounts to lock their tax account. This will systemically void tax returns filed on a deceased taxpayer's account. As of March 1, 2012, it had locked 90,570 tax accounts and prevented approximately $1.8 million in fraudulent tax refunds claimed using deceased individuals' identities since the lock was established.

---

[3] Taxpayers can be affected by more than one incident of identity theft. These incidences affected 87,322 taxpayers.
[4] These incidences affected 553,730 taxpayers.

Recognizing that victims of identity theft can be affected in multiple tax years, the IRS also places an identity theft indicator on each tax account for which it has determined an identity theft has occurred. All tax returns filed using the identity of a confirmed victim are flagged during tax return processing and sent for additional screening before any tax refund is issued. This screening is designed to detect tax returns filed by identity thieves who attempt to re-use a victim's identity in subsequent years and to prevent the issuance of fraudulent tax refunds.

To further assist victims in the filing of their tax returns, the IRS, in Fiscal Year 2011, began issuing Identity Protection Personal Identification Numbers (IPPIN) to these individuals. The IPPIN will indicate that the taxpayer has previously provided the IRS with information that validates their identity and that the IRS is satisfied that the taxpayer is the valid holder of the SSN. Tax returns that are filed on accounts with an IPPIN correctly input at the time of filing will be processed as the valid tax return using standard processing procedures. A new IPPIN will be issued each subsequent year before the start of the new filing season for as long as the taxpayer remains at risk for identity theft. For the 2012 Filing Season, the IRS sent 252,000 individuals an IPPIN.

However, the IRS does not know how many identity thieves are filing fraudulent tax returns or the amount of revenue being lost. TIGTA evaluated the IRS's efforts to identify and prevent fraudulent tax returns resulting from identity theft.[5] As part of our assessment, we identified and quantified potential refund losses resulting from identity theft.

Using characteristics of tax returns that the IRS has identified and confirmed as fraudulent filings involving identity theft, we analyzed Tax Year 2010 tax returns to identify additional tax returns that met the characteristics of these confirmed cases. Our analysis found that, although the IRS detects and prevents a large number of fraudulent refunds based on false income documents, there is much fraud that it does not detect. We identified approximately 1.5 million additional undetected tax returns with potentially fraudulent tax refunds totaling in excess of $5.2 billion. If not addressed, we estimate the IRS could issue approximately $26 billion in fraudulent tax refunds resulting from identity theft over the next five years.

---

[5] TIGTA, Audit No. 201140044, *Efforts to Identify and Prevent Fraudulent Tax Returns Resulting From Identity Theft* (planned report issuance in June 2012).

The primary characteristic of these cases is that the identity thief reports false income and withholding to generate a fraudulent tax refund. Without the falsely reported income, many of the deductions and/or credits used to inflate the fraudulent tax refund could not be claimed on the tax return. The individuals whose identities were stolen may not even be aware that their identities were used to file a fraudulent tax return. These individuals are typically those who are not required to file a tax return. Individuals are generally not aware that they are the victims of this type of identity theft unless they file a tax return, which causes the return to be rejected as a duplicate filing.

Access to third-party income and withholding information at the time tax returns are processed is the single most important tool the IRS could have to identify and prevent this type of identity theft tax fraud. In lieu of this, another important tool that could help the IRS prevent this type of fraud is the National Directory of New Hires.[6] Legislation would be needed to expand the IRS's authority to access the National Directory of New Hires wage information for use in identifying tax fraud. Currently, the IRS's use of this data is limited by law to just those tax returns with a claim for the Earned Income Tax Credit.

The IRS included a request for expanded access to the National Directory of New Hires in its annual budget submissions for Fiscal Years 2010, 2011, and 2012. The request was made as part of the IRS's efforts to strengthen tax administration. However, expanded access has not been provided for by law. The IRS has again requested expanded access to the National Directory of New Hires in its FY 2013 budget submission.

In a report that we recently issued to the IRS, we included a recommendation to develop a process that uses information from the National Directory of New Hires (if expanded access is provided in the law) along with third-party income and withholding information that the IRS maintains for the prior year's tax filings to better identify individuals who report false income. The IRS could use this information to confirm that the individual had no reported income or withholding in the prior tax year and did not obtain new employment in the current tax year. The IRS could then freeze the tax refund and attempt to verify the reported income and withholding.

---

[6] A Department of Health and Human Services national database of wage and employment information submitted by Federal agencies and State workforce agencies.

Even with improved identification of these returns, the next step of verifying whether the returns are fraudulent will require resources. The IRS has faced budget cuts, a hiring freeze, and staffing reductions during the same time it has encountered a significant surge in identity theft refund fraud. Without the necessary resources, it is unlikely that the IRS will be able to work the entire inventory of potentially fraudulent tax refunds it identifies. The IRS will only select those tax returns that it can verify based on its resources.

Using IRS estimates, it would cost approximately $31.8 million to screen and verify approximately 1.5 million tax returns that we identified as not having third-party information to support the income and withholding reported on the tax return. The net cost of not providing the necessary resources is substantial given that the potential revenue loss to the Federal Government of these identity theft refund fraud cases is $5.2 billion annually.

The validation process that we have proposed has some limitations. It will not identify instances of identity theft in which the legitimate taxpayer is employed and has a filing requirement but has not yet filed an income tax return. The IRS needs further tools to identify those individuals who are improperly filing using the identity of a taxpayer with a tax return filing requirement.

In those cases involving identity theft, the fraudulent tax return is often filed before the legitimate taxpayer files his or her tax return. For Tax Year 2010, we identified 48,357 SSNs that were used multiple times as a primary Taxpayer Identification Number.[7] When the identity thief files the fraudulent tax return, the IRS does not yet know that the individual's identity will be used more than once. As a result, the tax return is processed and the fraudulent refund is issued. These instances result in the greatest burden to the legitimate taxpayer. Once the legitimate taxpayer files his or her tax return, the duplicate tax return is identified and the refund is held until the IRS can confirm the taxpayer's identity. In Tax Year 2010, we estimate that $70.6 million in potentially fraudulent tax refunds were paid to identity thieves who filed tax returns before the legitimate taxpayers filed theirs.[8] This is in addition to the $5.2 billion in potentially fraudulent refunds noted previously related to taxpayers who do not appear to have a filing requirement.

---

[7] This estimate includes only those tax returns filed on tax accounts that contain an Identity Theft Indicator input on or before December 31, 2011. It does not include potentially fraudulent tax returns filed on tax accounts that do not contain an Identity Theft Indicator.
[8] This estimate is based only on the duplicate use of the primary SSN.

Although the IRS is working toward finding ways to determine which tax return is legitimate, it could do more to prevent identity thieves from electronically filing (e-file) tax returns. Before a tax return can be submitted electronically, the taxpayer must verify his or her identity with either the prior year's tax return Self-Select Personal Identification Number (PIN) or Adjusted Gross Income.

However, if the taxpayer does not remember the prior year's Self-Select PIN or Adjusted Gross Income, he or she can go to IRS.gov, the IRS's public Internet website, and obtain an Electronic Filing PIN by providing his or her name, SSN, date of birth, and the address and filing status on the prior year's tax return. The IRS then matches this information with the data on the prior year's tax return filed by the taxpayer.

Authenticating taxpayers is a challenge, not only in processing tax returns, but also whenever taxpayers call or write to the IRS requesting help with their tax account. The IRS has not adopted common industry practices for authentication, such as security challenge questions (*e.g.*, mother's maiden name, name of first pet).

**Direct Deposit and the Use of Debit Cards**

Direct deposit, which now includes debit cards, is often used by identity thieves to obtain fraudulent tax refunds. Approximately $4.5 billion of the $5.2 billion in potentially fraudulent tax refunds we identified were issued by direct deposit.

In September 2008, we reported[9] that the IRS was not in compliance with direct deposit regulations that require tax refunds to be deposited into an account only in the name of the individual listed on the tax return.[10] We recommended that the IRS limit the number of tax refunds being sent to the same account. While such a limitation does not ensure that all direct deposits are in the name of the taxpayer, it does help limit the potential for fraud. The IRS was concerned about limiting the number of direct deposits to a single account because of situations in which an account is in the name of multiple individuals. In addition, the IRS places responsibility for compliance with Federal direct deposit regulations on the taxpayer. The IRS stated that it is the taxpayer's responsibility to ensure that their tax refunds are only directly deposited into their accounts. However, in our

---

[9] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (Sept. 2008).
[10] 31 C.F.R. Part 210 (2011).

opinion, the IRS is responsible for ensuring that direct deposits are made to an account in the name of the recipient. Representatives from the Financial Management Service also indicated that the IRS is responsible for enforcing the Code of Federal Regulations requirement.

To date, little has been done to ensure that tax refunds are directly deposited only into the taxpayer's account. Some bank accounts are obviously being used for the refunds of many different taxpayers. For example, we found that 4,157 of the potentially fraudulent tax refunds we identified totaling $6.7 million were deposited into one of 10 bank accounts. Each of these 10 bank accounts had direct deposits of more than 300 tax refunds.

The use of debit cards to receive tax refunds further increases the risk of tax fraud. Identity thieves are using debit cards to fraudulently obtain direct deposits of fraudulent tax refunds. For example, authorities confiscated over 5,000 debit cards during the investigation of a Tampa, Florida identity theft scheme. Individuals can obtain a debit card online or from a bank, a third-party provider, or a local retailer. This complicates the IRS's efforts to identify the holder of the debit card as well as the bank account and the tax account associated with the debit card. In addition, the debit card issuer is the only entity that can ensure the individual requesting the debit card and receiving the tax refund is the taxpayer.

The IRS has a process in place in which it works with banks to obtain information on questionable tax refunds. In December 2011, one bank associated with the confiscated debit cards from the Tampa scheme provided the IRS with a listing of 60,000 bank accounts, including debit card accounts, that it had identified nationwide with questionable tax refunds. The bank intercepted and prevented questionable tax refunds totaling $164 million from being deposited into these accounts.

IRS management has indicated that it is working to establish processes to recover potentially fraudulent tax refunds intercepted by banks. However, more action is needed to prevent tax refunds from being erroneously deposited into bank accounts. We are currently working with the IRS and the Department of the Treasury to determine ways in which the IRS could strengthen direct deposit controls. At a minimum, we believe the IRS should implement our previous recommendations to limit the number of direct deposits to a single bank or debit card account, and coordinate with financial institutions to develop a process to

ensure that tax refunds issued via direct deposit are issued only to accounts that are in the taxpayer's name.

We believe the Department of the Treasury will need improved policies and regulations to ensure that debit cards can be identified based on the direct deposit account information on tax returns and vice versa. Furthermore, because of the potential for fraud that can be perpetrated by an anonymous user of these debit cards, the Department of the Treasury should take steps to ensure that financial institutions and/or debit card administration companies authenticate the identity of individuals purchasing or obtaining debit cards before Government funds can be deposited on those cards. Direct deposits should not be made to debit cards issued by financial institutions and debit card administration companies that do not take sufficient steps to authenticate individuals' identities.

**IRS Assistance to Victims of Identity Theft**

We recently completed an audit that evaluated the assistance that the IRS provides to victims of identity theft.[11] We found that the IRS is not effectively providing assistance to these victims. Moreover, processes are not adequate to communicate identity theft procedures to taxpayers, resulting in increased burden for victims of identity theft. Of continuing concern is the length of time taxpayers must work with the IRS to resolve identity theft cases.

Identity theft cases can take more than one year to resolve. While we cannot provide specific case examples due to privacy and disclosure laws, the following timeline illustrates a typical path for an identity theft refund fraud case that is not complex:

**February** The identity thief files a fraudulent tax return and obtains a tax refund. Subsequently, the legitimate taxpayer (taxpayer) attempts to electronically file his tax return, for which he is due a tax refund. He receives an IRS rejection notice stating that his SSN cannot be used more than once on the tax return or on another tax return.

The taxpayer calls the IRS toll-free telephone line and explains the situation to the assistor. The assistor, after authenticating the taxpayer's identity, researches his tax account and determines that a tax return has already been filed using his name and SSN. The assistor advises the taxpayer to file a paper tax return, attaching an Identity Theft Affidavit (Form 14039) or a police report and a valid government-issued document such as a copy of a Social Security card, passport, or driver's license to the tax return and mailing it to the IRS.

---

[11] TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 2012).

| | |
|---|---|
| | The IRS receives the paper tax return in one of its processing sites and a technician enters the data into the IRS computer system. The paper tax return with all attachments is sent to the Files Unit. It is rejected. A technician determines it is a duplicate tax return and inputs the appropriate transaction code. The duplicate return case is received in the Duplicate function, where an assistor identifies this as a possible identity theft case. The assistor requests the paper tax return. The case is set aside in a queue to be worked after April 15, when the filing season has ended. |
| **April** | The taxpayer calls the IRS toll-free line again and asks when he will receive his tax refund. The assistor researches the taxpayer's account, determines a duplicate tax return has been filed, and advises the taxpayer that there will be processing delays and that he may receive correspondence requesting additional information. The assistor also advises the taxpayer to visit the IRS website at IRS.gov for additional information and links related to identity theft. |
| **July** | The taxpayer's tax return is worked in the Duplicate function and determined to be an identity theft case. The duplicate tax return is transferred to another unit to an assistor whose responsibilities also include answering IRS toll-free telephone calls. The case is scanned into a management information system and queued. |
| **September** | The assistor begins working the case, orders copies of original tax returns, and sends letters to the identity thief and the taxpayer to attempt to determine who the legitimate taxpayer is. The taxpayer responds, confirming that he did not file the first tax return the IRS received. |
| **October** | The taxpayer calls the Identity Protection Specialized Unit and asks when he should expect his tax refund. The customer service representative researches the case and advises him his case is being worked. This representative sends a referral to the assistor working the case. |
| **November** | The assistor determines who the legitimate taxpayer is, requests adjustments to the taxpayer's account, and sends a letter to the identity thief providing him or her with a temporary tax identity number and a letter to the taxpayer advising him he has been a victim of identity theft and his account has been flagged. |
| **December** | The taxpayer receives the letter from the IRS and calls the Identity Protection Specialized Unit to inquire when he will receive his tax refund. The assistor advises him that it has been scheduled. |
| **January** | The adjustments post to the taxpayer's account and the refund is released. The taxpayer receives another letter advising him he has been a victim of identity theft and his account has been flagged. A new tax account for the person who committed the identity theft is also established.[12] |

The above illustration provides a "best case" resolution of an identity theft case given the IRS's current processes. However, most cases are more complex and can present considerable challenges throughout the resolution process. For instance, it can be difficult to determine who the legitimate taxpayer is or if the case is actually a case of identity theft. Taxpayers sometimes transpose digits in SSNs, but do not respond to the IRS when it requests information to resolve the case. As a result, the IRS may not be able to

---

[12] Even though a tax return is fraudulent, the IRS retains a record of the tax return by creating a tax account under a tax identification number that the IRS creates, and posting the tax return.

determine who the legitimate taxpayer is. With other cases we have reviewed, taxpayers claimed to be victims of identity theft after the IRS had questioned deductions or credits or proposed examination adjustments. In certain instances, the Social Security Administration had issued two taxpayers the same SSN.

As a result of an assessment of its Identity Theft Program completed in October 2011, the IRS is currently planning improvements to its program. The IRS is reorganizing to have an Identity Theft Program Specialized Group within each of the business units and/or functions where dedicated employees work the identity theft portion of the case. It will also begin collecting IRS-wide identity theft data to assist in tracking and reporting the effect identity theft has on tax administration. Nevertheless, these improvements may not be sufficient to significantly reduce the burden identity theft has placed on tax administration and on taxpayers whose identities have been stolen.

Identity theft cases have not been prioritized during the standard tax return filing process. The IRS plans to update tax return processing procedures to include a special processing code that recognizes the presence of identity theft documentation on a paper-filed tax return. This will allow certain identity theft victims' tax returns identified during processing to be forwarded and assigned to an assistor, rather than continuing through the standard duplicate tax return procedures. This will reduce the time a taxpayer must wait to have his or her identity theft case resolved by three to five months. However, the IRS does not plan to put this change into place until June 2012.

Taxpayers could also be further burdened if the address on the tax return filed by the identity thief is used by the IRS instead of the address of the legitimate taxpayer. Many taxpayers do not notify the IRS when they move, but just use their new/current address when they file their tax returns. When the IRS processes a tax return with an address different from the one it has on file, it systemically updates the taxpayer's account with the new address. It does not notify the taxpayer that his or her account has been changed with the new address.

While the IRS is in the process of resolving the identity theft case, the identity thief's address is still the address on the taxpayer's record. Any IRS correspondence or notices unrelated to the identity theft case will be sent to the most recent address on record. The legitimate taxpayer (the identity theft victim) will be unaware the IRS is trying to contact him or her.

This situation can also create disclosure issues. For example, if the legitimate taxpayer's prior year tax return has been selected for an examination, the examination notice will be sent to the address of record—the address the identity thief used on the fraudulent tax return. The identity theft victim is now at risk at having his or her personal and tax information disclosed to an unauthorized third party (whoever resides at that address). In response to our report, the IRS stated that in January 2012, it expanded its identity theft indicator codes that annotate when there is a claim of identity theft. The IRS developed tracking indicators to mark taxpayer accounts when the identity theft incident is initially alleged or suspected. It will explore leveraging this new indicator to suspend certain correspondence.

Resources have not been sufficient to work identity theft cases dealing with refund fraud and continue to be of a concern. IRS employees who work the majority of identity theft cases also respond to taxpayers' calls to the IRS's various toll-free telephone lines. Demanding telephone schedules and a large identity-theft inventory make it difficult for assistors to prioritize identity theft cases. The IRS has dedicated 400 additional employees to the Accounts Management function to work identity theft cases. However, because of limited resources and the high taxpayer demand for telephone assistance, the IRS plans to continue to have assistors who work identity theft cases also work the telephones on Mondays (and any Tuesday following a Monday holiday).

Assistors are trained to communicate with taxpayers and know the tax laws and related IRS operational procedures. However, identity theft cases can be complex and can present considerable challenges throughout the resolution process. Assistors are not examiners and are not trained to conduct examinations, which requires skills and tools beyond those of the assistors.

Additionally, the management information system that telephone assistors use to control and work cases can add to taxpayer burden. For instance, one victim may have multiple cases opened and multiple assistors working his or her identity theft issue. Victims become further frustrated when they are asked numerous times to prove their identities, even though they have previously followed IRS instructions and sent in Identity Theft Affidavits and copies of identification with their tax returns.

Victims also receive duplicate letters at different times, wasting IRS resources and possibly confusing the victims. None of the letters advise the victims when to expect their refunds, which could still be months away.

Identity theft case histories are so limited that it is extremely difficult to determine what action has been taken on a case; for example, if research was completed to determine which individual is the legitimate taxpayer. Case histories do not note whether the assistor researched addresses, filing or employment histories, *etc.*, for the individuals associated with the cases. This increases the need to spend extra time on these cases.

When our auditors reviewed a sample of cases, they could not determine if some of the cases had been resolved or why those cases were still open. In most cases, auditors had to reconstruct the cases to determine if all actions had been appropriately taken to resolve them.

The IRS acknowledges that it does not know the exact number of identity theft incidents or the number of taxpayers affected by identity theft. It also has not been able to quantify the amount of improper payments resulting from identity theft. The IRS reports cases only for accounts with identity theft indicators. It has procedures in place to input identity theft indicators on certain taxpayer accounts, depending on how the taxpayer's identity theft case was identified and if it affects Federal tax administration. However, these procedures are inconsistent and complex. Potential identity theft cases in process do not have indicators and are not counted.

Identity theft data are captured on 22 different systems throughout the IRS. These systems are not integrated and data must be manually compiled, hindering the IRS's capability of producing accurate and reliable identity theft reports. As a result, not all identity theft cases are counted. In addition, not all cases counted are actually identity theft cases. As of June 2011, the IRS estimated the number of unmarked accounts that should have identity theft indicators in the range of 240,000 to 280,000.

Finally, in November 2011, the IRS established a Taxpayer Protection Unit to manage work arising from the identity theft indicators and filters used to identify tax returns affected by identity theft—both to stop the identity thief's tax return from being processed and to ensure the legitimate taxpayer's tax return is processed. Currently, employees have only been detailed to the unit. The IRS will determine the needs of the unit after assessing the 2012 Filing Season.

During this filing season, taxpayers found it difficult to reach employees in this unit. The unit received more than 86,000 calls during the 2012 Filing

Season, but has only been able to answer about 21,000. The average wait time for taxpayers was almost one hour. The Taxpayer Protection Unit will be a significant component in the IRS's attempt to stop fraudulent refunds and provide assistance to victims of identity theft. TIGTA is currently conducting an audit of this unit and, during the 2013 Filing Season, we will be conducting a follow-up audit to assess the IRS's actions to improve the quality of assistance provided to identity theft victims.

**Criminal Investigations of Identity Theft**

When the crime of identity theft occurs within our jurisdiction, TIGTA's Office of Investigations (OI) investigates it as it impacts the economy, efficiency, and effectiveness in the administration of the Internal Revenue Code. Identity theft directly and destructively impacts law-abiding citizens. When individuals steal identities and file fraudulent tax returns to obtain fraudulent refunds before the legitimate taxpayers file, the crime is simple tax fraud and it falls within the jurisdiction and programmatic responsibility of the IRS. However, there are other variations of IRS-related identity theft that, although not widely covered by the media, falls within TIGTA's jurisdiction and has a significant impact on taxpayers.

TIGTA focuses its limited investigative resources on the following areas as they pertain to IRS-related identity theft:

- IRS employees who are involved in committing identity theft either as the source of the identity information or through active participation in a scheme;
- Tax preparers who improperly steal and disclose client information for the purpose of committing identity theft; and
- Individuals who impersonate the IRS in furtherance of committing identity theft.

TIGTA has conducted investigations of IRS employees who use their access to taxpayer information as a means for stealing identities for the purpose of committing identity theft. Noted below is an example of identity theft by an IRS employee:

On April 14, 2011, Monica Hernandez was indicted for making a false income tax return when she was a part-time data entry clerk for the IRS. During

the course of her employment with the IRS, Hernandez stole and/or misappropriated information of other taxpayers listed on various IRS forms. Hernandez used falsified and forged IRS forms with the victim's information to obtain large tax refunds from the IRS totaling $175,144.

IRS employees are entrusted with the sensitive personal and financial information of taxpayers. Using this information to perpetrate a criminal scheme for personal gain negatively impacts our Nation's voluntary tax system and generates widespread distrust of the IRS. TIGTA's OI pursues identity theft violations and conducts criminal investigations of IRS employees involved in these crimes.

Tax preparers who improperly steal and disclose any taxpayer's Federal tax information as part of an identity theft scheme cause serious harm to taxpayers. The following case highlights an instance when a tax preparer stole and improperly disclosed the identity of her clients in order to commit identity theft:

Kathleen Lance was a public accountant and president of her company. In this capacity, Lance obtained and used the identification of six of her clients to change the direct deposit account information on clients' tax returns before she electronically submitted their returns to the IRS. Lance thereby diverted funds from the clients' bank accounts and redirected the deposits to her personal and business bank accounts. Lance also assumed and disclosed the identity of those six clients and fraudulently opened credit card accounts in her name. On May 24, 2010, she was sentenced to serve 64-months imprisonment and three-years supervised probation for wire fraud, theft of Government funds, use of unauthorized access devices, and aggravated identity theft.

Impersonation of the IRS as part of an identity theft scheme takes many forms. Often, the IRS is impersonated by individuals who seek to trick unsuspecting taxpayers into revealing their personal information. The details of each scheme tend to vary, but the common thread is the use of the IRS name to lure recipients into accessing links or providing sensitive information.

- Victims are told that they are either due a refund or that a tax payment was rejected and the taxpayer needs to click on a link which either opens an attached form or takes them to a website where they enter their Personally Identifiable Information (PII), Federal tax information, and credit card information; or

- Victims are told that they are being investigated by the IRS and need to immediately respond by clicking on a link which opens an attached form or takes them to a website, where they are prompted to provide their PII to verify the status of their tax matter.

In both of these situations, the victim is presented with a website which is designed to replicate a legitimate IRS.gov website, often by using authentic IRS images and seals. The case below is an example wherein an individual impersonated the IRS to commit identity theft:

Godspower Egbufor, together with co-conspirators, operated a scheme and stole the identities of numerous individuals and defrauded them out of more than $1 million through Internet solicitations. Egbufor obtained massive e-mail distribution lists containing thousands of e-mail addresses and sent unsolicited e-mails falsely informing targeted victims that they had won a lottery or had inherited money from a distant relative. E-mails to victims falsely indicated that a government or quasi-governmental entity, such as the IRS or the United Nations, prevented the money due to them from being awarded because advance payment of taxes and other fees were required. Follow-up e-mails instructed the victims to provide their personal and bank account information in order to receive their lottery winnings or inheritance. On December 19, 2011, Egbufor was sentenced to 108 months of imprisonment and five years of supervised release for violations of Aggravated Identity Theft and Conspiracy to Commit Wire Fraud.

In conclusion, we at TIGTA continue to be very concerned about the scope of this problem and will provide continuing audit coverage of IRS actions taken to stem tax fraud-related identity theft and to provide prompt resolution to taxpayers who are victimized. In addition, we will continue to conduct criminal investigations of identity theft violations involving IRS employees, tax return preparers, and individuals impersonating the IRS. I hope my discussion of our work assists you with your oversight of the IRS on this issue.

Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and Members of the Subcommittees, thank you for the opportunity to address this important topic and to share my views.



Chairman BOUSTANY. Thank you, Inspector General George. Inspector General O'Carroll, you may proceed.

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

Mr. O'CARROL. Good morning, Chairman Johnson, Chairman Boustany, Ranking Member Becerra, Ranking Member Lewis, and members of the both subcommittees. Thank you for the invitation to testify today.

As today's Death Master File, or DMF, makes the personal information of deceased people and sometimes the living available to the public, this creates a significant risk of SSN misuse and identity theft. I would like to share an OIG case in which available death data was used to obtain personal information and then commit fraud.

In a recent national investigation my office identified about 60 retirement benefit applications that were submitted in the names of deceased people. The claims were filed with the name, the Social Security number, and the date of birth of these individuals. The suspects found this information on a genealogy Web site that published the DMF. Our agents and other law enforcement identified the suspects, executed search warrants, and made arrests. However, the main suspect in the case took his own life before he could be arrested. His two accomplices, both relatives, were indicted and pleaded guilty. A judge sentenced them to prison and ordered them to be deported. One also was ordered to repay more than $145,000 to the SSA.

It is not only the personal information of deceased individuals that is at risk. In two recent reports our auditors identified thousands of living individuals who were mistakenly included in the DMF. These errors can have serious consequences for the affected individuals. Each month SSA erroneously includes about 1,000 living individuals in the Death Master File. That personal information could be used to obtain loans or credit, to apply for government benefits or to assume a new identity.

My office has recommended limiting the DMF to only the information required by law and ensuring the file's accuracy. Such steps would minimize these errors and reduce SSN misuse in all forms, including tax fraud.

We investigated a Colorado man who hired people to search a genealogy Web site for the names and SSNs of deceased individuals. After confirming this information against other data sources the man fabricated employment records and filed fraudulent tax returns. A judge sentenced the man to 4 years in jail for SSN misuse and making false claims. He was ordered to repay more than $282,000 to the IRS.

Limiting the content or discontinuing the availability of the DMF is a legislative and policy decision for Congress and the SSA. In November 2011, Chairman Johnson introduced the Keeping IDs Safe Act. This bill would end the sale of the DMF to the public. Whether through legislative action or policy changes, my office strongly supports any effort to limit public access to SSA's death records. Pending such changes, we advocate limiting the information made available to the extent permitted by law, and we recommend a risk based approach to the distribution of the DMF.

SSA's key uses in government and finance make it a valuable commodity for criminals. SSN misuse and identity theft remains

significant threats and failure to take action creates unnecessary public risk. My office also urges citizens to guard their personal information. We encourage people to keep their Social Security cards in a safe place, shred personal documents, and be judicious in giving out an SSN in business transactions. We will going to continue to work with your subcommittees and SSA in these and future efforts to protect personal information and reduce tax fraud.

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

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

**U.S. House of Representatives**

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

**Statement for the Record**

**Hearing on Identity Theft and Tax Fraud**

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

**May 8, 2012**

Good morning, Chairman Johnson, Chairman Boustany, Ranking Member Becerra, Ranking Member Lewis, and members of both Subcommittees. It is a pleasure to appear before you, and I thank you for the invitation to testify today. I have appeared before Congress many times to discuss issues critical to the Social Security Administration (SSA) and the services the Agency provides to American citizens; earlier this year I testified before the Subcommittee on Social Security at separate hearings on SSA's Disability Insurance program and the Death Master File (DMF).

Today, we are discussing the Social Security number (SSN) and ways to improve SSN protection and guard against misuse, identity theft, and tax fraud. Your Subcommittees have previously worked with SSA and the Office of the Inspector General (OIG) to address these issues, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft persists. My office is well aware of the central role that the SSN plays in American society, and part of our mission is to maintain its integrity along with other personally identifiable information (PII) within SSA records. To provide some context, in Fiscal Year (FY) 2011, SSA assigned about 5.4 million original SSNs, issued 10.9 million replacement cards, and processed more than 1.4 billion SSN verifications. The Agency also received about $660 billion in employment taxes related to earnings. Protecting the SSN and properly posting employees' wages is paramount to ensuring the integrity of our personal information.

Despite our efforts as well as those of SSA and the IRS to protect this critical information, we all remain targets for identity thieves. The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year. The number of identity theft-related incidents on tax returns reached about 248,000 in 2010, about five times more than in 2008, according to the Government Accountability Office. We in the OIG understand the concern your Subcommittees have for citizens and their families with regard to identity theft, and we investigate as many SSN misuse cases as our resources allow each year. As we pursue these criminal investigations, we have also conducted numerous audits and made recommendations to SSA and to the Congress to improve the SSN's security.

**SSN Misuse Investigations**

OIG's primary mission is to protect SSA programs and operations, and the majority of our investigations are related to SSA program fraud. However, our organization receives thousands of allegations of SSN misuse each year; in FY 2011, about 14 percent of all fraud referrals received involved SSN misuse. It is our experience that investigations into SSN misuse will often reveal some form of identity theft. At times, they can also involve Social Security benefit fraud and tax fraud that can lead to the recovery of significant government funds.

I would like to share with your Subcommittees some of our most recent cases involving SSN misuse for the purpose of tax fraud:

- The OIG, the IRS Criminal Investigation Division (CID), the Treasury Inspector General for Tax Administration, and other agencies conducted a joint investigation of several individuals who misused the names and SSNs of approximately 300 residents of Puerto

Rico so they could file fraudulent tax returns. This scheme caused the IRS to issue more than $2 million in fraudulent tax refunds. A judge sentenced three individuals to between 3 months and 30 months in prison, and ordered them to pay restitution of nearly $230,000 to the IRS.

- My office investigated a California woman who used fraudulent SSNs to file Federal income tax returns. The woman applied for and obtained more than 20 Social Security cards, falsely claiming she gave birth to that many children at a Los Angeles hospital in 2002. The woman then prepared and filed fraudulent tax returns, claiming multiple dependent deductions for family members and friends. She recently pleaded guilty to theft, fraudulent use of SSNs, and preparing false tax returns. A judge sentenced her to 18 months' incarceration and ordered her to pay restitution of more than $302,000 to the IRS.

- The OIG, IRS CID, and other agencies investigated two New Jersey men who misused the names and SSNs of victims who used a health-service provider in the area. The men used the victims' personal information to file false tax returns, improperly claiming about $507,000 in refunds from the IRS. The men pleaded guilty in 2011, and a judge sentenced them to 60 months and 120 months in prison and ordered them to pay restitution of more than $207,000 and about $300,000 to the IRS, respectively.

As we pursue investigations similar to these, 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.

**SSA's Death Master File**

SSA has made significant efforts to improve SSN integrity and encourage individuals to protect PII. However, the SSNs of deceased individuals are also vulnerable to misuse. As such, the public release of the DMF raises concerns related to SSN misuse and identity theft, as seen in recent news media reports and evidenced by ongoing legislative efforts. SSA has, on the Numident—the Agency's master database of SSN holders—a record of reported deaths. Because of a Consent Judgment in a 1978 *Freedom of Information Act* (FOIA) lawsuit—*Perholtz vs. Ross*—SSA was required as of 1980 to provide death records that included the SSN, the last name, and the date of death of deceased number holders; the result was the creation of the DMF, an extract of Numident data. SSA later expanded the DMF to include individuals' first and middle name, date of birth, residential state and zip code.

In November 2011, SSA made changes to the DMF. First, the Agency ceased providing the decedent's residential state and Zip code. In addition, SSA removed about 4.2 million State records from the DMF, based on a provision in the *Social Security Act* prohibiting SSA from disclosing death records the Agency receives through its contacts with the States, except in limited circumstances.

Today, each DMF record usually includes the following: SSN, full name, date of birth, and date of death. Therefore, even with SSA's recent changes, the DMF still contains more information

than required by the Consent Judgment in *Perholtz*. The file contains about 86 million records, and it adds about 1.1 million records each year.

SSA provides the DMF to the Department of Commerce's National Technical Information Service (NTIS), a clearinghouse for scientific and technical information, which, in turn, sells the DMF to public and private industries—government, financial, investigative, credit reporting, and medical customers. Those customers use the data to verify death and prevent fraud, among other uses. SSA also currently distributes all death information it maintains, including State death records, under agreements with eight government agencies, including the IRS and the Centers for Medicare & Medicaid Services. SSA provides this death information to the IRS weekly. SSA also provides IRS a weekly file that includes the names and SSNs of newborns, as well as their parents' names and SSNs.

**Criminal Use of Public Death Records**

The DMF has important and productive uses. For example, medical researchers and hospitals track former patients for their studies; investigative firms use the data to verify deaths related to investigations; and pension funds, insurance companies, and government entities need to know if they are sending payments to deceased individuals. In addition, the financial community and Federal, State, and local governments can identify and prevent identity theft by running financial and credit applications against the DMF. However, the form in which the DMF is currently distributed provides opportunity for individuals to misuse SSNs and commit identity theft.

These OIG investigations show how individuals can use available death data to obtain SSNs and commit fraud:

- In August 2010, we began investigating about 60 fraudulent retirement benefit claims that used the name, SSN, and date of birth of individuals who died decades ago. We determined that the PII used to file the fraudulent claims was available to the public through a genealogical website. The OIG and other law enforcement agencies identified suspects in the case and executed search and arrest warrants; however, the main suspect took his own life before he was taken into custody. His two accomplices, both relatives of his, were indicted and pled guilty to the charges. A judge sentenced the two individuals to 20 months' and 25 months' incarceration followed by deportation from the U.S., and one was ordered to pay restitution of more than $145,000 to SSA.
- An OIG investigation of a Colorado man revealed that he employed individuals so he could obtain names and SSNs of long-deceased individuals from a genealogical website. The man then fabricated employment records and instructed others to use the obtained names and SSNs and false employment information to create fraudulent tax returns, which were submitted to the IRS online. To determine deceased individuals' SSNs, the man said he compared data available from the public Internet site with a certain State's death data. A judge sentenced the man to 46 months in prison for SSN misuse, making false claims, and wire fraud; and ordered him to pay more than $282,000 in restitution to the IRS.

> According to news media reports, in December 2011, this genealogical website said it would no longer display the Social Security information for anyone who has died in the last 10 years; the site also said it would place its Social Security Death Index behind a pay wall and only allow access to the index to family history researchers.

The Congress has recognized the seriousness of this issue, as current bills for consideration address access to the DMF. In November 2011, Chairman Johnson and several members of the Subcommittee on Social Security introduced the *Keeping IDs Safe Act*, which would end the sale of the DMF. The bill would help protect the death data of all number holders. My office also supports an exemption to the bill that would allow government and Federal law enforcement agencies—like the OIG—to access the DMF to combat fraud.

**Reviews and Recommendations**

The OIG recognizes that limiting or discontinuing the DMF's availability is ultimately a legislative and policy decision for the Congress and SSA to make. Even so, my office has long taken the position that to the extent possible, SSA should limit public access to the DMF that required by law, and take all possible steps to ensure its accuracy. We have made several recommendations to this effect.

Our March 2011 report, *Follow-up: Personally Identifiable Information Made Available to the Public via the Death Master File*, examined whether SSA took corrective actions to address recommendations we made in a June 2008 report on the DMF. In the June 2008 report, we determined that, from January 2004 through April 2007, SSA's publication of the DMF resulted in the potential exposure of PII for more than 20,000 living individuals erroneously listed as deceased on the DMF. In some cases, these individuals' PII was still available for free viewing on the Internet—on ancestry sites like genealogy.com and familysearch.org—at the time of our report.

In the March 2011 report, we found SSA did not take actions on two of our recommendations. SSA did not implement a delay in the release of DMF updates, as the Agency indicated that public and private organizations rely on the DMF to combat fraud and identity theft. According to SSA, those organizations must have immediate and up-to-date information to be effective. The Agency also did not attempt to limit the amount of information included on the DMF, and it did not explore alternatives to the inclusion of an individual's full SSN, citing the *Perholtz* consent judgment and potential litigation under FOIA. SSA added that a deceased individual does not have a privacy interest, according to FOIA.

Our follow-up audit work indicated that between January 2008 and April 2010, SSA published at least 35,000 living numberholders' PII in the DMF. According to SSA, there are about 1,000 cases each month in which a living individual is mistakenly included in the DMF. SSA said that when the Agency becomes aware it has posted a death report in error, SSA moves quickly to correct the situation, and the Agency has not found evidence of past data misuse. However, we remain concerned about these errors, because erroneous death entries can lead to benefit termination and cause severe financial hardship and distress to affected individuals. We also have concerns that DMF update files, some with the SSNs of living individuals, are a potential

source of information that would be useful in perpetrating SSN misuse and identity theft. DMF updates can reveal to potential criminals the PII of individuals who are still alive.

**Legislative Efforts**

We support the prior bipartisan legislative efforts of these Subcommittees to limit the use, access, and display of the SSN in public and private sectors, and to increase penalties against those who misuse SSNs. Most recently, the Subcommittee on Social Security 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, or prior offenses.

The legislation would also expand the types of activities that are subject to civil monetary penalties (CMPs) 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 Supplemental 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 fraudulently obtained, 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 helps an individual assimilate into our society, and 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.

**Citizens' Accountability**

While government agencies such as SSA have controls in place to protect the SSN and other personal information, individuals must also take basic preventive steps to protect their own information from improper use. We urge everyone to keep Social Security cards in a secure place, shred personal documents, and be aware of phishing schemes, because no reputable financial institution or company will ask for personal information like an SSN via the phone or 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 some financial transactions, an SSN is not necessary for everyday transactions, like applying for a gym membership. We can monitor our financial transactions and regularly check our credit reports from the three major credit bureaus. Concerned citizens may also contact SSA at 1-800-772-1213 if they suspect someone is using their SSN work purposes; SSA will review work earnings to ensure its records are correct. Anyone who suspects identity theft should report it to the FTC at 1-877-438-4338; and may need to contact the IRS to address potential tax issues. By knowing how to protect ourselves, and actually taking these important steps, we make life much more difficult for identity thieves.

**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. Identify 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. Nevertheless, we are committed to ensuring that the information in SSA's records remains safe and secure.

While we support efforts to limit public access to this data through legislative or policy changes (such as the *Keeping IDs Safe Act)*, barring such changes, SSA should implement a risk-based approach for distributing the DMF, and the Agency should limit the amount of information included on the DMF. These actions would protect PII and reduce the potential for misuse and abuse of SSNs and identity theft.

Our investigators are committed to pursuing SSN misuse and identity theft cases, and our auditors will continue to offer recommendations to safeguard the SSN and prevent theft of government funds. Finally, we will continue to provide information to your Subcommittees and Agency decision-makers about this critically important issue. I thank you again for the opportunity to speak with you today. I am happy to answer any questions.



Chairman BOUSTANY. Thank you, Mr. O'Carroll.
Mr. Miller, you made proceed.

**STATEMENT OF STEVEN T. MILLER, DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT, INTERNAL REVENU.S.RVICE**

Mr. MILLER. Thank you, Chairman Johnson, Chairman Boustany, Ranking Member Becerra, Ranking Member Lewis, Mem-

bers of the Subcommittee. My name is Steve Miller and I am the Deputy Commissioner at the IRS.

Over the past few years the IRS has seen a significant increase in refund schemes, particularly those involving identity theft. Identity theft and the harm it inflicts on innocent taxpayers is a problem that we take very seriously. We are confronted with the same challenges that face every major financial institution in preventing and detecting identity theft. We cannot stop all identity theft. However, we are better than we were and we will get better still.

There is a delicate balance here. We cannot manually inspect 100 million refund returns to ensure all are correct. We must balance the need to make payments in a timely manner with the need to ensure that claims are proper and taxpayer rights are protected.

Let me begin by describing our efforts at upfront prevention. In 2011, the IRS identified and prevented the issuance of more than 14 billion in fraudulent refunds. A great deal of that was identity theft. We estimate that at a minimum 1.3 million returns were identity theft of the 2.2 million total returns that we stopped last year. This year we will stop even more.

We have improved upfront screening filters to spot false returns before a refund is issued. As of mid-April we have stopped more than 2.6 million returns we suspect of being fraudulent. At this time we estimate that the returns we have worked a minimum of 750,000 are identity theft, and we are just underway in working through those cases. Until we complete our review of the returns we have stopped we don't have a precise tally of how much is identity theft or the total dollars that are involved. However, we suspect that the bulk of them are inventory, which is now 2.6 million and continues to grow, will be identity theft.

More specific to this filing season we have also done the following. Despite substantial cuts in our budget we added hundreds of staff in this area and will add hundreds more. In fact we estimate that we are going to spend over $330 million on refund work this year, in the refund fraud area. Most of that is going to be specific to identity theft. We issued special identification numbers, so-called PINs, to expedite filing for those taxpayers whose identities have been stolen. There are 250,000 PINs that have been issued to date. There have been over 170,000 failed attempts to use an SSN associated with those PINs.

We have also accelerated the matching of information returns to help stop fraud. We are taking a number of actions to prevent identity thieves from stealing Social Security numbers of deceased taxpayers. For example, when we receive a final return filed on behalf of a deceased taxpayer we are putting a special marker on those accounts since those individuals have no future filing requirement. And we are working with the Administration and the Social Security Administration on modifications to the practice of making the Death Master File public.

There are new procedures to allow us to match returns on lists of taxpayer information that law enforcement officials believe may have been stolen, and we have improved collaboration with software developers and others to determine how we can better partner to prevent identity theft.

In addition, our Criminal Investigation Division continues to increase its work on identity theft. In 2012 we will spend more than 400,000 hours of investigative work in this area. In my written testimony you will see details of this work, including a description of a week long sweep in January that led to more than 900 charges across 23 States.

In addition, earlier this month we began a process for local law enforcement to obtain tax return data that is vital to their local enforcement needs. That is our work on prevention.

We are also taking a number of actions to help victims of identity theft. We have implemented new procedures and, as mentioned, we have added staff to resolve cases faster and better respond to calls, and of course the PINs I spoke of earlier will assist identity theft victims in filing future returns. We have also trained 35,000 of our employees to recognize and help when they see identity theft situations.

Let me conclude. Our work is critical. We can't be lax in stopping fraud and our treatment of those who have had their identity stolen. I can't tell you that we will beat this problem this year, but I can say that our work in 2012 represents real progress but not the end of our efforts.

I will be happy to answer any questions.

[The prepared statement of Mr. Miller follows:]

**WRITTEN TESTIMONY OF**
**STEVEN T. MILLER**
**DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT**
**INTERNAL REVENUE SERVICE**
**BEFORE THE**
**HOUSE COMMITTEE ON WAYS AND MEANS**
**SUBCOMMITEE ON SOCIAL SECURITY AND**
**SUBCOMMITTEE ON OVERSIGHT**
**ON IDENTITY THEFT**
**MAY 8, 2012**

## INTRODUCTION AND SUMMARY

Chairmen Johnson and Boustany, Ranking Members Becerra and Lewis, and Members of the Subcommittees on Social Security and Oversight, my name is Steven Miller and I am Deputy Commissioner at the Internal Revenue Service. I appreciate the opportunity to testify on the important issue of identity theft and provide you with an update on actions that the IRS is taking in this area.

Over the past few years, the IRS has seen a significant increase in refund fraud schemes in general and schemes involving identity theft in particular. Identity theft and the harm that it inflicts on innocent taxpayers is a problem that we take very seriously. The IRS has a comprehensive identity theft strategy comprised of a two-pronged effort, focusing both on fraud prevention and victim assistance.

Identity theft is the use of another person's identifying information stolen from a wide variety of places and through a wide variety of means. With respect to the IRS, identity theft manifests itself in several ways. First, it is used to defraud the government of funds through the filing of fraudulent refund claims. Second, in many instances it victimizes an innocent taxpayer by impeding his or her ability to get a refund from us. Fraudulent filings may also cause us to initiate an adverse enforcement action against the innocent taxpayer. There are also many instances where the identity stolen is not of an active filer so there is less immediate impact on the real taxpayer. In these instances, the identity may belong to a deceased individual or an individual without a filing requirement. In this category, the IRS is faced with fraud, but there is less immediacy in the need to assist the correct taxpayer because there is no return filed or other IRS activity underway with respect to that individual.

At the start let me say quite plainly that the IRS is confronted with the same challenges as every major financial institution in preventing and detecting identity theft. The IRS cannot stop all identity theft. However, we have improved and we are committed to continuing to improve our programs. We can and will continue to work to prevent the issuance of fraudulent refunds and we can and will continue to work with innocent taxpayers to clear their accounts and/or get them their money faster in a courteous and professional manner.

While I will describe for you some of the details of new programs and systems that the IRS has created to address this challenge, I would start by saying that we have put a significant amount of time into redoubling our training efforts for our IRS workforce so that they can better understand what identity theft victims are going through. Although these thieves steal the information from sources outside the tax system, the IRS is sometimes the first to inform the individual that identity theft has occurred.

The IRS has also taken actions to be better prepared in both fraud prevention and victim assistance. On the prevention side, this means implementing new processes for handling returns, new filters to detect fraud, new initiatives to partner with stakeholders and a continued commitment to investigate the criminals who perpetrate these crimes. As for victim assistance, the IRS is working to speed up case resolution, provide more training for our employees who assist victims of identity theft, and step up outreach to and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly.

The improvements that the IRS is making would not be possible without the additional resources that we have directed toward these programs. We have substantially increased our resources devoted to both prevention and assistance. Even in a declining budget environment, we are hiring and training additional staff to address the growing challenge of identity theft.

Fighting identity theft will be an ongoing battle for the IRS and one where we cannot afford to let up. The identity theft landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information and using it for their gain. We at the IRS must continually review our processes and policies to ensure that we are doing everything possible to minimize the incidence of identity theft and to help those who find themselves victimized by it.

And yet there is a delicate balance here. We cannot manually inspect 100 million refunds to ensure all are correct – nor is there any justification for doing so. That is neither practical nor in keeping with Congressional intent. The IRS has a dual mission when it comes to refunds, particularly when they are generated in whole or in part by tax credits. Refundable and other tax credits are provided to achieve important policy goals, such as relieving poverty or boosting the economy. The IRS must deliver refunds in the intended time frame, while ensuring that appropriate controls are in place to minimize errors and fraud. We must balance the need to make payments in a timely manner with the need to ensure that claims are proper and taxpayer rights are protected.

So it is indeed a difficult challenge to strike the right balance. The IRS' approach to tackling identity theft must be multi-faceted. We are improving processes to prevent fraudulent filings from being processed as well as identifying promoters and other schemes. We are also taking actions to improve handling of identity theft cases and to better serve taxpayers whose identity has been stolen for tax purposes. All of this is

being done within a very difficult budget environment. The Administration's FY 2013 budget request includes important funding for additional enforcement initiatives focused specifically on addressing refund fraud, including identity theft. Let me walk through our work to prevent the fraud up front and how we hope to improve our service to the victims of identity theft.

## PREVENTING FRAUD FROM IDENTITY THEFT

Tax filings can be affected by identity theft in various ways. For example, an identity thief steals a legitimate taxpayer's personal information in order to file a fake tax return and attempt to obtain a fraudulent refund. There are also instances where the identity stolen is of an individual who is deceased or has no filing requirement.

Overall, IRS identified and prevented the issuance of over $14 billion in fraudulent refunds in 2011. Identity theft is a subset of this overall refund fraud. From 2008 through March 2012, the IRS identified more than 490,000 taxpayers who have been affected by identity theft. These are taxpayers who have filing requirements and who are or may be impacted by the theft. With respect to these taxpayers, in calendar year 2011, the IRS protected $1.4 billion in refunds from being erroneously sent to identity thieves. This does not include identity theft of those without a filing requirement (though that value is included in the above $14 billion). The IRS is committed to improving its approaches to blocking these fraudulent refund claims. To that end, we strive to process returns in such a way that potentially false returns are screened out at the earliest possible stage.

### *Catching the Refund at the Door -- Enhanced Return Processing*

Identity theft is a key focus of an IRS program launched in 2011. Under this program, the following improvements have been made:

- Various new identity theft screening filters are in place to improve our ability to spot false returns before they are processed and before a refund is issued. For example, new filters were designed and launched that flag returns if certain changes in taxpayer circumstances are detected. It must be noted that effective filters are difficult to develop given the number of changes that many taxpayers experience in a year. For example, annually 10 million of us move and 46 million of us change jobs. Thus, changes in taxpayer circumstances do not necessarily indicate identity theft. Nonetheless, as of mid-April 2012, we have stopped over 325,000 questionable returns with $1.75 billion in claimed refunds from filters specifically targeting refund fraud.

- Moreover, this filing season, we have expanded our work on several fraud filters which catch not only identity but other fraud. In this area we have already stopped more returns this filing season than we stopped all last calendar year. Until we work these cases we will not have a solid answer as to how much of this

work is fraud, but not identity fraud, though we suspect a great deal may fall into the latter category.

- We have implemented new procedures for handling returns that we suspect were filed by identity thieves. Once a return has been flagged, we will correspond with the sender before continuing to process the return.

- We are issuing special identification numbers (Identity Protection Personal Identification Numbers or IP PINs) to taxpayers whose identities are known to have been stolen, to facilitate the filing of their returns and prevent others from utilizing their identities. The use of IP PINs is more fully described below, but we issued over 250,000 for the 2012 filing season.

- We have accelerated the availability of information returns in order to identify mismatches earlier, further enhancing our ability to spot fraudulent tax returns before they are processed.

- We are leveraging mechanisms to stop the growing trend of fraudulent tax returns being filed under deceased taxpayers' identities. First, we have coded accounts of decedent taxpayers whose SSNs were previously misused by identity thieves to prevent future abuse. Second, we are identifying returns of recently deceased taxpayers to determine if it is the taxpayer's final return, and then marking accounts of deceased taxpayers who have no future filing requirement. Of this season's filings, 91,000 returns have been stopped for this review. Third, we are working with the Social Security Administration in order to more timely utilize the information SSA makes available to us. And we are working with SSA on a potential legislative change to the practice of routine release of the Death Master File.

- We have also developed procedures for handling lists of taxpayers' personal information that law enforcement officials discover in the course of investigating identity theft schemes or other criminal activity. This is extremely valuable data that can be used to flag taxpayer accounts and help us block returns filed by identity thieves who have used the personal information of these taxpayers. Our Criminal Investigation (CI) division will utilize this data to ensure linkages are identified between criminal schemes and will also ensure that the information is shared appropriately to affect victim account adjustment and protection activity.

- We expanded the use of our list of prisoners to better utilize the list to stop problematic returns. We have stopped 190,000 questionable returns this filing season. For the fiscal year, we have prevented over $1 billion in refunds, almost double the value of refunds stopped over the same period last year. We received additional help under the United States-Korea Free Trade Agreement Implementation Act passed last year that requires federal and state prisons to provide information on the current prison population. We are engaging with prison officials to determine the best way to move forward with this new authority.

Unfortunately, the news is not all good. The authority allowing us to share return information with prisons expired at the end of 2011. The FY 2013 Budget proposal would reinstate the provision authorizing the IRS to disclose return information with respect to individuals incarcerated in Federal or State prisons whom the IRS determines may have filed or facilitated the filing of a false return.

- We are also collaborating with software developers, banks, and other industries to determine how we can better partner to prevent theft.

***Stopping It Before It Starts -- Criminal Investigation Work***

The investigative work done by our Criminal Investigation (CI) division is another major component in our effort to combat tax-related identity theft. CI investigates and detects tax fraud and other financial fraud, including fraud related to identity theft, and coordinates with other IRS divisions to ensure that false refunds involving identity theft are addressed quickly and that the IRS accounts of identity theft victims are marked to help prevent any future problems. CI recommends prosecution of refund fraud cases, including cases involving identity theft, to the Department of Justice.

CI works closely with the other IRS divisions to improve processes and procedures related to identity theft refund fraud prevention. For example, CI provides regular updates to the IRS' Wage and Investment division regarding emerging scheme trends so that processes and filters can be enhanced to prevent refund loss. These collaborative efforts have been instrumental in helping the IRS stop more refund fraud.

In response to this growing threat to tax administration, CI established the Identity Theft Clearinghouse (ITC), a specialized unit that became operational in January, to work on identity theft leads. The ITC receives all refund fraud related identity theft leads from IRS-CI field offices. The ITC's primary responsibility is to develop and refer identity theft schemes to the field offices, facilitate discussions between field offices with multi-jurisdictional issues, and to provide support of on-going criminal investigations involving identity theft.

CI investigations of tax fraud related to identity theft have increased significantly over the past two fiscal years and the trend is continuing in FY 2012. In FY 2011, 276 investigations were initiated, compared with 224 in FY 2010 and 187 in FY 2009. CI recommended 218 cases for prosecution in 2011, compared with 147 the previous year and 91 in 2009. Indictments in identity-theft related cases totaled 165 in 2011, with 80 individuals' sentenced and average time to be served at 44 months. This compares with 94 indictments, 45 individuals sentenced and a 41-month average sentence in 2010. Already in FY 2012, CI has initiated 336 cases and recommended 224 cases for prosecution. Indictments in identity theft cases total 218, with 61 individuals' sentenced and average time to be served at 45 months. The direct investigative time spent on identity theft in FY 2011 was 225,000 hours and CI is on pace to double this in FY 2012.

The IRS conducted a coordinated identity theft enforcement sweep during the week of January 23. It was an outstanding success. Working with the Justice Department's Tax Division and local U.S. Attorneys' offices, the nationwide effort targeted 105 people in 23 states. The coast-to-coast effort that took place included indictments, arrests and the execution of search warrants involving the potential theft of thousands of identities. In all, 939 criminal charges are included in the 69 indictments and information related to identity theft.

In addition, in that same week IRS auditors and investigators conducted extensive compliance visits to money service businesses in nine locations across the country. The approximately 150 visits occurred to help ensure that these check-cashing facilities aren't facilitating refund fraud and identity theft.

These efforts send an unmistakable message to anyone considering participating in a refund fraud scheme that we are aggressively pursuing cases across the nation with the Justice Department, and people will be going to jail.

Identity theft has been designated as a priority in 2012. We also will be piloting dedicated cross-functional teams with other parts of the IRS that will allow us to create a greater footprint in one or more geographic locales.

Local law enforcement and other federal agencies play a critical role in combating identity theft. Thus, an important part of our effort to stop identity thieves involves partnering with law enforcement agencies. We collaborate on these issues and this effort will only increase going forward. It should be noted that the existing rules for protecting taxpayer privacy often make it difficult for us to provide easy access to information that may be useful for local law enforcement. Despite these difficulties, in April 2012 we implemented a new law enforcement assistance pilot program designed to aid law enforcement in obtaining tax return data vital to their local efforts in investigating and prosecuting specific cases of identity theft. The IRS will carefully assess the results and performance of the pilot program before deciding on how to proceed.

We will continue to search for other innovative ways to partner with local law enforcement. Furthermore, CI special agents throughout the country participate in at least 35 task forces and working groups with federal, state, and local law enforcement that target tax related identity theft crimes. CI personnel also coordinate with these agencies in an effort to ensure that victims are aware of the steps they need to take to resolve their affected tax accounts. We will continue to develop new partnerships with law enforcement agencies...

Some of the recent successes involving identity theft include the following cases in which sentences were handed down since December 2011:

- An Alabama woman was sentenced to 61 months in prison and ordered to pay $494,424 in restitution after she pleaded guilty to conspiracy to defraud the

United States by filing false claims, wire fraud and aggravated identity theft using stolen identities. This individual stored tens of thousands of stolen means of identification (names and social security numbers) at her house, which came from numerous sources, including private companies, health clinics, and prisons.

- A Delaware woman was sentenced to 120 months in prison and ordered to pay approximately $1.5 million in restitution after being convicted for conspiracy to commit mail and wire fraud. This individual conspired with others to obtain tax refunds by submitting fraudulent tax returns using the identifying information of prison inmates, including the inmates' social security numbers and variations of their names. The false returns were either filed electronically or mailed to the Internal Revenue Service requesting that the refunds be either electronically deposited or mailed to bank accounts or addresses controlled by the individuals and the other conspirators.

- An Alabama woman was sentenced to 75 months in prison and ordered to pay $720,067 in restitution and forfeit $593,949 after she pleaded guilty to conspiracy involving false claims, wire fraud, and aggravated identity theft. This individual conspired with workers of tax return businesses to file fraudulent tax returns and purchased identifying information for children and other dependents to use as the basis for tax deductions, the earned income credit, the child dependent care credit and other credits on tax returns for people who were not related to the dependents.

- An Arizona man was sentenced to 60 months in prison, three years of supervised release, and ordered to pay approximately $387,000 in restitution after he pleaded guilty to conspiracy involving false claims, wire fraud and aggravated identity theft. This individual used stolen identities of disabled individuals to claim more than $1 million in bogus tax refunds.

- An Alabama woman was sentenced to 184 months in prison and ordered to pay more than $1.1 million in restitution on charges of filing false claims, wire fraud and aggravated identity theft. This individual, the owner of a tax preparation business, used her business to run a scheme to steal tax refunds by filing false tax returns with stolen identities. Those tax returns claimed refunds that were directed to bank accounts and debit cards that she controlled.

- A Tennessee woman was sentenced to 108 months in prison, three years of supervised release, and ordered to pay $110,000 in restitution. This individual and an accomplice obtained names, Social Security numbers and other identifying information of various individuals, both alive and deceased, from the Social Security Death Master File and from an underground website. They prepared false W-2s, claiming false wages and withholding amounts, and used these forms to file income tax returns with the IRS to get refunds that were deposited into bank accounts they controlled.

- An Alabama woman was sentenced to 94 months in prison and ordered to pay $276,000 in restitution on charges of identity theft, wire fraud, aggravated identity theft and conspiracy to make false claims for tax refunds. This individual obtained the names and Social Security numbers of student loan borrowers from the databases at her former employer and conspired to use the stolen identifying information to file false tax returns. She also fraudulently obtained refund anticipation loans from a bank on the basis of the fraudulently filed returns.

- A Florida woman was sentenced to 108 months in prison and ordered to pay $673,000 in restitution on charges of tax fraud and mail fraud. This individual obtained identifying information from others, including Social Security numbers, and used this information to prepare and electronically file dozens of false income tax returns. In some instances, the individuals whose identities were being used were deceased.

**ASSISTING TAXPAYERS VICTIMIZED BY IDENTITY THEFT**

Along with prevention, the other key component of the IRS' efforts to combat identity theft involves providing assistance to taxpayers whose personal information has been stolen and used by a perpetrator in the tax filing process. This situation is complicated by the fact that identity theft victims' data has already been compromised outside the filing process by the time we detect and stop perpetrators from using their information.

We have taken a number of actions, including those described below to restore the account of the innocent taxpayer. We have had difficulty keeping pace with the number of cases, but we are determined to bring to bear new resources and streamline existing processes. Thus, we have committed additional resources, even in this tough budget climate, trained our people, developed an IP PIN program, and expanded our external outreach.

***Improving our work on Identity Theft Cases***

As noted above, since 2008 the IRS has identified more than 490,000 taxpayers who were victims of identity theft. We realize the importance of resolving these cases quickly and efficiently so that identity theft victims who are owed their refunds can receive them as soon as possible and so that we do not take adverse enforcement actions against such individuals.

We are implementing new procedures designed to resolve cases faster and minimize the disruption to innocent taxpayers. For example, every division within the IRS is making identity theft cases a higher priority in their work. As indicated above, new procedures and additional staff are being put in place to work cases faster where a refund has been stopped. We increased staffing last year and this year, and have plans to dedicate additional resources following the filing season. By the end of the fiscal year, staffing dedicated to identity theft will be almost 2,500 employees.

Along with taking steps toward faster resolution of identity theft cases, we are continuously improving the way we track and report on the status of all identity theft cases. We believe these improvements will reduce the time to work identity theft cases in coming filing seasons so that honest taxpayers will receive their refunds sooner. Additionally, better tracking and reporting means that we can spot – and correct – any flaws in the system more quickly.

***Identity Protection PIN Program***

In addition to helping identity theft victims clear up problems with their IRS accounts, the IRS works proactively to help ensure that these taxpayers do not encounter delays in processing their future returns. In 2011, we launched a pilot program for Identity Protection Personal Identification Numbers (IP PIN). The IP PIN is a unique identifier that establishes that a particular taxpayer is the rightful filer of the return. Under this pilot, we issued IP PINs to over 50,000 taxpayers who were identity theft victims.

The pilot program showed us that this is a very promising innovation that can dramatically reduce the number of taxpayers caught up in delays. Therefore, we have expanded the program for the new filing season, and have issued IP PINs to approximately 250,000 taxpayers who have suffered identity theft in the past.

***Employee Training***

The IRS runs one of the largest phone centers in the world, and is dedicated to providing quality service with a high degree of accuracy to every taxpayer who contacts us. Having said that, we realize that taxpayers who call the IRS with identity theft problems present unique challenges to our telephone representatives and we need to ensure taxpayers receive quality, courteous service.

As a result, last year we conducted a thorough review of the training we provide our employees to make sure that they have the tools and sensitivity they need to respond in an appropriate manner to those who have been victimized by identity theft.

Out of this review, we have done two things:

- First, we updated the training course for our telephone assistors in order to ensure that our assistors maintain the proper level of sensitivity when dealing with identity theft victims and understand the serious financial problems that identity theft poses for these taxpayers. We conducted this training at the beginning of the 2012 filing season.

- Second, we broadened the scope of our training to cover those IRS employees who are not telephone assistors but who nonetheless interact with taxpayers or work identity theft cases. We developed a new course for these employees, which includes not only sensitivity training but also ensures that employees who

process identity theft cases have the proper tools and techniques to do so. This course was provided to all employees who might come into contact with an identity theft victim. In all, 35,000 IRS employees received this training.

***Taxpayer Outreach and Education***

The IRS continues to undertake outreach initiatives to provide taxpayers, return preparers and other stakeholders with the information they need to prevent tax-related identity theft and, when identity theft does occur, to resolve issues as quickly and efficiently as possible. Recent actions in this area include the following:

- We overhauled the identity protection training provided to tax practitioners at last year's Tax Forums. These yearly events, held in several cities around the country, typically draw more than 16,000 practitioners. In addition, our Small Business/Self Employed division met with practitioners to discuss the IP PIN program, the expansion of the program, and the modified procedures, forms and notices associated with the program.

- We continue to update the identity theft information provided on the IRS.gov website. This includes emerging trends in identity theft along with fraud schemes, phishing sites and prevention strategies. We also added a direct link to our Identity Theft page, to make it easier for taxpayers who visit IRS.gov to find it.

- The IRS continues a far-reaching communications effort through traditional and social media in both English and Spanish. This effort, started last year, has intensified this filing season. In addition to consumer protection information on IRS.gov, we have done a number of news releases and tax tips to help taxpayers and highlight our continuing enforcement efforts. We have also produced new identity theft awareness videos for the IRS YouTube channel in English, Spanish and American Sign Language and relayed information out through IRS Twitter feeds and podcasts. In addition, the IRS also made identity theft the top item in this year's "Dirty Dozen" annual list of taxpayer scams. We plan to continue this sweeping communication effort through the rest of the filing season and beyond.

**CONCLUSION**

Mr. Chairman, thank you for your leadership in this area and thank you again for the opportunity to appear before the Subcommittee and update you on the steps that the IRS is taking to prevent identity theft and to assist taxpayers who have been victims of this crime. This work is a key challenge for the IRS. Our work here for filing season 2012 is a solid start but not the end of our efforts. I cannot tell you that we will beat this problem in one year. I can tell you that we have committed our talents and resources to prevent the issuance of fraudulent refunds and have developed processes to minimize the pain felt by those who have been victimized. We are committed to continuing to

look for new and innovative ways to improve our processes and techniques. I would be happy to answer any questions that you may have about our role in guarding against identity theft and assisting its victims.



Chairman BOUSTANY. Thank you, Mr. Miller.
Ms. Olson, you may proceed.

**STATEMENT OF NINA E. OLSON, NATIONAL TAXPAYER ADVOCATE, INTERNAL REVENUE SERVICE**

Ms. OLSON. Chairmen Boustany and Johnson, Ranking Members Lewis and Becerra, and Members of the Subcommittees, thank you for inviting me to testify today about tax related identity theft.

Since 2004, I have written extensively about the impact of identity theft on taxpayers and tax administration, and I have worked closely with the IRS to improve its efforts to assist taxpayers who become identity theft victims. The IRS has adopted many of my office's recommendations and made significant progress in this area in recent years. Notwithstanding these efforts, however, identity theft continues to pose significant challenges for the IRS.

I will highlight five points that I think deserve particular emphasis. First, I am concerned that the Federal Government continues to facilitate tax related identity theft by making the Death Master File, a list of recently deceased individuals that includes their full name, SSN, data of birth, date of death and the county, State, zip code, maybe, maybe not, of the last address on record. There is some uncertainty about whether the Social Security Administration has the legal authority to restrict public access to DMF records in light of the Freedom of Information Act. For that reason I strongly support legislation to restrict public access to the DMF. However, I believe the SSA has at least a reasonable basis for seeking to limit public access to the DMF under present case law under FOIA and if legislation is not enacted soon, I encourage the SSA to act on its own because everyday we delay taxpayers are harmed.

Second, I am aware that some State and local law enforcement agencies would like to access the taxpayer return information to help them combat identity theft. I have significant concerns about loosening taxpayer privacy protections and believe this is an area where we need to tread carefully. But as I describe in my written statement, the IRS is piloting a procedure that would enable taxpayers to consent to the release of their returns in appropriate circumstances. In my view, giving taxpayers a choice strikes the appropriate balance.

Third, I am pleased that this filing season the IRS has established a dedicated taxpayer protection unit to answer phone calls from legitimate taxpayers who have been caught up in our identity theft filters. However, for the week ending April 28th the level of service on this phone line was 24 percent, meaning that only 1 out of every 4 calls was answered and those callers that did get through had to wait on hold an average of 1 hour and 21 minutes. More support for this unit is clearly required.

Fourth, although my office has extensive knowledge about what victims of tax related identity theft experience as a result of handling tens of thousands of such cases, the IRS has been developing new initiatives in this area without seeking our input until late in the process. As a result the victims' perspective in several instances has not been given adequate weight in my opinion. For example, the IRS is moving away from using a single traffic cop to resolve identity theft cases, which may make the process more complicated for taxpayers to navigate and end up with cases falling into black holes.

The IRS has also been very slow to develop procedures to assist victims of preparer fraud. Congress put the Office of the Taxpayer Advocate inside the IRS precisely to ensure that the taxpayer perspective is considered and when we are not adequately consulted the result is often that the IRS does what is best for the IRS rather than what is best for the taxpayer.

Fifth, I note that even as the IRS is being urged to do much more to combat identity theft, taxpayers are clamoring for the IRS to process returns and issue refunds more quickly. While there is still room for the IRS to make improvements in both areas, these two goals are fundamentally at odds. If our overriding goal is to process tax returns and deliver refunds as quickly as possible for the vast majority of persons who file legitimate returns, it is inevitable that some identity thieves will get away with refund fraud and some honest taxpayers will be harmed.

On the other hand, if we place a greater value on protecting taxpayers against identity theft and the Treasury against fraudulent refund claims, the IRS will need more time to review returns and the roughly 110 taxpayers who receive refunds will have to wait longer to get them, perhaps considerably longer. Alternatively, the IRS will require a considerably larger staff to enable it to review questionable returns more quickly. There really is no way around these tradeoffs.

I appreciate the opportunity to testify today and would be happy to answer your questions.

[The prepared statement of Ms. Olson follows:]

Chairman BOUSTANY. Thank you, Ms. Olson.

Mr. Black, you may proceed.

WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

# IDENTITY THEFT AND TAX FRAUD

BEFORE THE

SUBCOMMITTEES ON OVERSIGHT

AND SOCIAL SECURITY

COMMITTEE ON WAYS AND MEANS

U.S. HOUSE OF REPRESENTATIVES

MAY 8, 2012

**TABLE OF CONTENTS**

Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and distinguished Members of the respective subcommittees:

Thank you for inviting me to testify today about the subject of tax-related identity theft.[1] I have written extensively about the impact of identity theft on taxpayers and tax administration and have addressed identity theft in two other congressional hearings this spring.[2] While the IRS has made significant progress in this area in recent years, I believe the IRS can do more. Identity theft is not a problem the IRS can fully solve, but I have significant concerns about certain aspects of the IRS's approach.

I first raised concerns about the IRS's processing of identity theft cases in 2004 and included identity theft as a Most Serious Problem in my 2005 Annual Report to Congress, even before the IRS acknowledged identity theft as a problem worthy of a dedicated program office.[3] The Taxpayer Advocate Service (TAS) is unique in that we work identity theft cases from beginning to end, and many TAS employees have developed expertise in this issue over the years. To its credit, the IRS has adopted many of my office's recommendations to help victims of identity theft. Indeed, a number of former TAS employees have moved to the IRS's Office of Privacy, Governmental

---

[1] The views expressed herein are solely those of the National Taxpayer Advocate. The National Taxpayer Advocate is appointed by the Secretary of the Treasury and reports to the Commissioner of Internal Revenue. However, the National Taxpayer Advocate presents an independent taxpayer perspective that does not necessarily reflect the position of the IRS, the Treasury Department, or the Office of Management and Budget. Congressional testimony requested from the National Taxpayer Advocate is not submitted to the IRS, the Treasury Department, or the Office of Management and Budget for prior approval. However, we have provided courtesy copies of this statement to both the IRS and the Treasury Department in advance of this hearing.

[2] *See* National Taxpayer Advocate 2011 Annual Report to Congress 48-73 (Most Serious Problem: *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS*); National Taxpayer Advocate 2009 Annual Report to Congress 307-317 (Status Update: *IRS's Identity Theft Procedures Require Fine-Tuning*); National Taxpayer Advocate 2008 Annual Report to Congress 79-94 (Most Serious Problem: *IRS Process Improvements to Assist Victims of Identity Theft*); National Taxpayer Advocate 2007 Annual Report to Congress 96-115 (Most Serious Problem: *Identity Theft Procedures*); National Taxpayer Advocate 2005 Annual Report to Congress 180-191 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-136 (Most Serious Problem: *Inconsistence Campus Procedures*); *Hearing on Tax Compliance and Tax-Fraud Prevention Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency, and Financial Management*, 112th Cong. (Apr. 19, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Tax Fraud by Identity Theft Part 2: Status, Progress, and Potential Solutions: Hearing Before the S. Comm. on Finance, Subcomm. on Fiscal Responsibility and Economic Growth*, 112th Cong. (Mar. 20, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, a Drain on the Public Treasury, Hearing Before the S. Comm. on Finance, Subcomm. on Fiscal Responsibility and Economic Growth*, 112th Cong. (May 25, 2011) (statement of Nina E. Olson, National Taxpayer Advocate); *Filing Season Update: Current IRS Issues, Hearing Before the S. Comm. on Finance*, 111th Cong. (Apr. 15, 2010) (statement of Nina E. Olson, National Taxpayer Advocate); *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance*, 110th Cong. (Apr. 10, 2008) (statement of Nina E. Olson, National Taxpayer Advocate).

[3] National Taxpayer Advocate 2005 Annual Report to Congress 180-191 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-136 (Most Serious Problem: *Inconsistence Campus Procedures*).

Liaison, and Disclosure (PGLD), the organization in charge of coordinating identity theft efforts servicewide.

Today, I am concerned that the IRS is proceeding with certain efforts to assist identity theft victims without seeking my office's involvement. TAS has an important perspective to offer in that we are the "voice of the taxpayer" within the IRS, yet we are not being given the opportunity to weigh in at the early stages when the IRS develops new procedures in this area.

For example, the IRS recently decided to adopt a specialized approach to assisting identity theft victims. As I understand it, each affected IRS function will create its own specialized unit whose employees will work solely on identity theft cases and will be trained to resolve related account problems. These specialized, embedded employees will adjust the taxpayers' accounts themselves, rather than sending them to the servicewide Accounts Management (AM) unit. Because TAS will continue to receive and resolve identity theft cases that meet our case criteria, TAS employees will work closely with these units.

In general, I support the concept of a specialized unit approach, but "the devil is in the details." Thus, I would like my staff to have an opportunity to review the procedures being developed by the various functions. Our review would serve two purposes: (1) to ensure that the rights of identity theft victims are adequately protected and (2) to allow the Taxpayer Advocate Service to update its internal procedures so that our requests for help in resolving identity theft cases reach the appropriate contacts throughout the IRS. When we asked to be a part of the review process, we were initially told that it was not our role to comment on procedures being created by other functions. Only when we recently raised this issue with the Director of PGLD were we permitted to participate in the review process. Just in the past week or so, my staff was given access to the procedures developed by the specialized units. Including TAS at such a late stage severely limits the opportunity for the IRS to adequately consider our suggestions. In the meantime, my office continues to receive identity theft cases at a record pace, and our case advocates are uncertain about where to send their identity theft-related Operations Assistance Requests (OARs).[4] In fact, I hear reports from my offices that the IRS functions are improperly rejecting our OARs. With all this confusion, taxpayers are being harmed. This is simply unacceptable.

*The IRS's track record in assisting victims of return preparer fraud does not bode well for victims of identity theft.*

I am concerned at the moment about the IRS's ability to develop procedures to promptly assist taxpayers who are victimized by identity theft, in part because of how the IRS has handled a related issue involving fraud by tax return preparers. The IRS has struggled

[4] An OAR (Form 12412) is used by TAS case advocates to request assistance from the IRS when TAS does not have the statutory or delegated authority to take the required action(s) on a taxpayer's case. *See* Internal Revenue Manual (IRM) 13.1.19.1, *TAS OAR Process* (Feb. 1, 2011).

to unwind the harm done to victims – even when it had plenty of time to develop procedures.

More specifically, TAS has received a significant number of cases involving preparer refund fraud. These preparers alter taxpayers' returns by inflating income, deductions, credits, or withholding without their clients' knowledge or consent, and pocket the difference between the revised refund amount and the amount expected by the taxpayer. The IRS ultimately discovers that the taxpayer's return is incorrect and attempts to recover the excess refund from the taxpayer through levies, liens, and other enforcement actions. In one egregious instance involving several returns prepared by the same tax return preparer – and despite the IRS's concurrence that the returns it processed were not the returns signed by the taxpayers – our Local Taxpayer Advocate could not persuade the IRS Accounts Management function (AM) to adjust the taxpayers' accounts to remove the fabricated income or credits.

In these cases, the Local Taxpayer Advocate issued Taxpayer Assistance Orders (TAOs)[5] to AM in December 2010. After AM refused to comply, I elevated these TAOs to the Commissioner of the Wage and Investment (W&I) division in July 2011. After receiving no response, I further elevated the TAOs in August 2011 to the Deputy Commissioner for Services and Enforcement, who agreed that the IRS needed to correct the victims' accounts. It was not until the end of March 2012 that the IRS finally made the adjustments.

Because this was a systemic issue that required guidance to W&I employees, I issued a Proposed Taxpayer Advocate Directive (TAD) to the Commissioner of W&I on June 13, 2011.[6] This Proposed TAD directed W&I to establish procedures for adjusting the taxpayer accounts in instances where a tax return preparer alters the return without the taxpayer's knowledge or consent in order to obtain a fraudulent refund. The Proposed TAD pointed out that the IRS has been aware of the issue of unscrupulous tax return preparers altering returns in this manner for at least eight years. In particular, in March of 2003, the Refund Crimes section of the IRS's Criminal Investigation (CI) division had identified a scheme in which a particular tax return preparer had altered several hundred of his clients' returns without their knowledge in order to increase the total amount of each refund, and he then diverted the excess refund into his bank account. CI sought advice from the IRS Office of Chief Counsel, which issued an opinion

[5] Internal Revenue Code (IRC) § 7811 authorizes the National Taxpayer Advocate to issue a Taxpayer Assistance Order upon a determination that a taxpayer is suffering or about to suffer a significant hardship as a result of the manner in which the internal revenue laws are being administered by the Secretary. *See* IRC § 7811.

[6] Pursuant to Delegation Order No. 13-3, the National Taxpayer Advocate has the authority to issue a TAD to mandate administrative or procedural changes to improve the operation of a functional process or to grant relief to groups of taxpayers (or all taxpayers) when implementation will protect the rights of taxpayers, prevent undue burden, ensure equitable treatment, or provide an essential service to taxpayers. IRM 1.2.50.4, Delegation Order 13-3 (formerly DO-250, Rev. 1), *Authority to Issue Taxpayer Advocate Directives* (Jan. 17, 2001). *See also* IRM 13.2.1.6, *Taxpayer Advocate Directives* (July 16, 2009).

concluding that a return altered by a tax return preparer *after* the taxpayer has verified the accuracy of the return is a nullity (*i.e.*, not a valid return).[7] Counsel also advised that the taxpayer's account should be corrected by having the taxpayer file an accurate return and then adjusting the account to reflect the correct information reported on that return.[8] The Office of Chief Counsel issued an additional opinion in 2008, concluding that the IRS *can and should* adjust each taxpayer's account to remove any entries attributable to the invalid return filed by the preparer.[9] And in 2011, shortly after I issued the Proposed TAD, Counsel reaffirmed the conclusion that such altered returns were not valid.[10]

After receiving an unsatisfactory response to concerns raised about this matter in the Proposed TAD and my 2011 Annual Report to Congress,[11] I issued a TAD to the W&I Commissioner and the Small Business/Self-Employed (SB/SE) division Commissioner on January 12, 2012.[12] While both have acknowledged their intent to comply with the substance of the TAD, they appealed the TAD solely in an effort to extend the time allowed to comply with the actions, notwithstanding that they already had over eight years to develop procedures to assist these victims of fraud.

It has been almost a year and a half since TAS first raised this issue with Accounts Management. In this time, I have issued a Proposed TAD and a TAD directing the IRS to develop procedures, and have discussed this concern in my 2011 Annual Report to Congress. I and my employees have issued Taxpayer Assistance Orders in specific cases. I find it entirely unacceptable that the IRS needs more time to develop guidance for its employees about a type of return preparer fraud that it has known about for more than eight years, is growing, is closely related to identity theft, and is potentially very harmful to the impacted taxpayers. The taxpayers are the victims here, and the IRS should act with all due haste to correct their accounts and eliminate the risk of unlawful collection.

Because of experiences like this, I believe it is critical that TAS be included in pre-decisional meetings at which changes in IRS identity theft procedures are discussed in order to ensure that the victims' perspective is adequately considered.

In my testimony today, I will make the following points with respect to identity theft:

---

[7] *See* IRS Office of Chief Counsel Memorandum, *Horse's Tax Service*, PMTA 2011-13 (May 12, 2003).

[8] *Id.*

[9] IRS Office of Chief Counsel Memorandum, *Refunds Improperly Directed to a Preparer*, POSTN-145098-08 (Dec. 17, 2008).

[10] IRS Office of Chief Counsel Memorandum, *Tax Return Preparer's Alteration of a Return*, PMTA 2011-20 (June 27, 2011).

[11] *See* National Taxpayer Advocate 2011 Annual Report to Congress 59-60.

[12] *See* Taxpayer Advocate Directive 2012-1 (*Establish procedures for adjusting the taxpayer's account in instances where a tax return preparer altered the return without the taxpayer's knowledge or consent, and the preparer obtained a fraudulent refund*) (Jan. 12, 2012).

1. The IRS and TAS continue to see unprecedented levels of identity theft casework.

2. The Social Security Administration should restrict access to the Death Master File.

3. Creating new exceptions to taxpayer privacy protections poses risks and should be approached carefully, if at all.

4. There is a continuing need for the IRS's identity protection specialized unit to play a centralized role in managing identity theft cases.

5. The Taxpayer Protection Unit needs significantly more staffing to increase its level of service.

6. The IRS should clarify the purpose and impact of identity theft indicators.

7. When analyzing the impact of identity theft, a broad perspective is necessary.

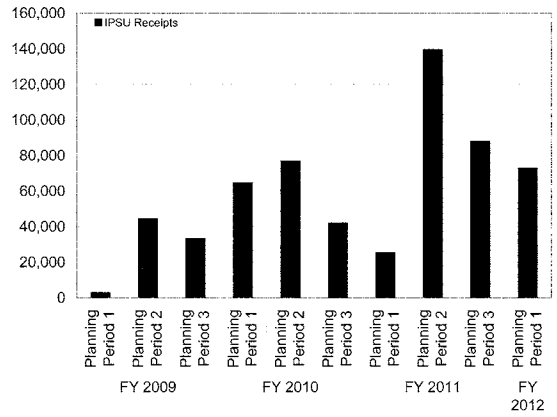
## I. The IRS and TAS Continue to See Unprecedented Levels of Identity Theft Casework.

Tax-related identity theft is a serious problem – for its victims, for the IRS and, when Treasury funds are improperly paid to the perpetrators, for all taxpayers. In general, tax-related identity theft occurs when an individual intentionally uses the Social Security number (SSN) of another person to file a false tax return with the intention of obtaining an unauthorized refund.[13] Identity theft wreaks havoc on our tax system in many ways. Victims not only must deal with the aftermath of an emotionally draining crime, but may also have to deal with the IRS for years to untangle the resulting tax account problems. Identity theft also impacts the public fisc, as Treasury funds are diverted to pay out improper tax refunds claimed by opportunistic perpetrators. In addition, identity theft takes a significant toll on the IRS, tying up limited resources that the IRS could otherwise shift to taxpayer service or compliance initiatives.

[13] This type of tax-related identity theft is referred to as "refund-related" identity theft. In "employment-related" identity theft, an individual files a tax return using his or her own taxpayer identifying number, but uses another individual's SSN in order to obtain employment, and consequently, the wages are reported to the IRS under the SSN. The IRS has procedures in place to minimize the tax administration impact to the victim in these employment-related identity theft situations. Accordingly, I will focus on refund-related identity theft in this testimony.

Today, identity theft can be an organized, large-scale operation. Indeed, the most recent IRS data show more than 450,000 identity theft cases servicewide.[14] The Identity Protection Specialized Unit (IPSU), the centralized IRS organization established in 2008 that assists identity theft victims, is experiencing unprecedented levels of case receipts.[15] As this chart shows, IPSU receipts increased substantially over the two previous years.

**Chart 1: IPSU Paper Inventory Receipts, FY 2009 to FY 2012 by Planning Period[16]**




The Taxpayer Advocate Service has experienced a similar surge in cases, as TAS identity theft receipts rose 97 percent in fiscal year (FY) 2011 over FY 2010. The upward trend has continued in the current fiscal year. In the first two quarters of FY 2012, TAS received 9,988 identity theft cases, a 43 percent increase over the same period in FY 2011.[17] The growth in casework reflects the both the increase in identity theft incidents and the IRS's inability to address the victims' tax issues promptly.

[14] Data provided by the IRS Office of Privacy, Governmental Liaison, and Disclosure (e-mail dated Apr. 17, 2012).

[15] With the IRS moving to a specialized approach to identity theft victim assistance, it is unclear what role the IPSU will play in the future. The National Taxpayer Advocate believes it is important for the IPSU to continue to serve as the "traffic cop" and serving as the single point of contact with the identity theft victim, as discussed later in this testimony.

[16] Data obtained from IRS Identity Protection Specialized Unit (Mar. 13, 2012). The IPSU tracks cases by "planning period." Planning Period 1 covers Oct. 1 to Dec. 31, Planning Period 2 covers Jan. 1 to June 30, and Planning Period 3 covers July 1 to Sept. 30.

[17] There were 6,999 stolen identity (Primary Issue Code 425) cases in TAS during the same period in FY 2011. Data provided by TAS Technical Analysis and Guidance (Apr. 16, 2012).

## II. The Social Security Administration (SSA) Should Restrict Access to the Death Master File.

I am concerned that the federal government continues to facilitate tax-related identity theft by making public the Death Master File (DMF), a list of recently deceased individuals that includes their full name, Social Security number (SSN), date of birth, date of death, and the county, state, and ZIP code of the last address on record.[18] The SSA characterizes release of this information as "legally mandated,"[19] but the extent to which courts currently would require dissemination of death data under the Freedom of Information Act (FOIA)[20] has not been tested. To eliminate uncertainty, I have recommended that Congress pass legislation to clarify that public access to the DMF can and should be limited.[21]

The public availability of the DMF facilitates tax-related identity theft in a variety of ways. For example, a parent generally is entitled to claim a deceased minor child as a dependent on the tax return that covers the child's year of death. If an identity thief obtains information about the child from the DMF and uses it to claim the dependent on a fraudulent return before the legitimate taxpayer files, the IRS will stop the second (legitimate taxpayer's) return and freeze the refund. The legitimate taxpayer then may face an extended delay in obtaining the refund, potentially causing an economic hardship, and will bear the emotionally laden burden of persuading the IRS that the deceased child was really his or hers. As a practical matter, legislation could relieve survivors of this burden by simply delaying release of the information for several years.

In light of the practical difficulties of passing legislation, however, I also urge the Social Security Administration to reevaluate whether it has the legal authority to place limits on the disclosure of DMF information administratively. In 1980, the SSA created the DMF, now issued weekly, after an individual filed suit in the U.S. District Court for the District of Columbia seeking certain data fields pursuant to FOIA and the court entered a consent judgment in the case pursuant to an agreement reached by the parties.[22] While the 1980 consent judgment may have seemed reasonable at the time, the factual and legal landscape has changed considerably over the past three decades.

---

[18] *See* Office of the Inspector General, SSA, *Personally Identifiable Information Made Available to the General Public via the Death Master File*, A-06-08-18042 (June 2008).

[19] *Social Security and Death Information* 1, Hearing Before H. Comm. on Ways & Means, Subcomm. on Soc. Security (statement of Michael J. Astrue, Commissioner of Social Security) (Feb. 2, 2012).

[20] FOIA generally provides that any person has a right to obtain access to certain federal agency records. *See* 5 U.S.C. § 552.

[21] *See* National Taxpayer Advocate 2011 Annual Report to Congress 519-23 (Legislative Recommendation: *Restrict Access to the Death Master File*).

[22] *See Perholtz v. Ross*, Civil Action Nos. 78-2385, 78-2386 (D.D.C. Apr. 11, 1980).

From a factual standpoint, DMF information was sought in 1980 as a way to prevent fraud by enabling pension funds to identify when a beneficiary died so they could stop the payment of benefits. Today, DMF information is used to commit tax fraud, so there is a factual reason for keeping the information out of the public domain.

From a legal standpoint, judicial interpretations of FOIA and its privacy exceptions have evolved in several important respects, including the recognition of privacy rights for decedents and their surviving relatives.

In general, agencies receiving FOIA requests for personal information must balance (1) the public interest served by release of the requested information against (2) the privacy interests of individuals to whom the information pertains.[23]

In 1989, the Supreme Court reiterated that the public's FOIA interest lies in learning "what their government is up to."[24] The Court continued:

> Official information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct.[25]

Following the Supreme Court's reasoning, the Court of Appeals for the D.C. Circuit rejected a request for a list of names and addresses of retired or disabled federal employees, concluding that the release of the information could "subject the listed annuitants 'to an unwanted barrage of mailings and personal solicitations,'" and that such a "fusillade" was more than a *de minimis* assault on privacy.[26]

The courts have increasingly found that privacy rights do not belong only to living persons. In 2001, the D.C. Circuit stated that:

> the death of the subject of personal information does diminish to some extent the

---

[23] *See, e.g., Department of Defense v. Federal Labor Relations Authority*, 510 U.S. 487, 497 (1994); *Department of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. 749, 773 (1989). This balancing applies to information described in FOIA Exemption 6, 5 U.S.C. § 552(b)(6) ("personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"), which would encompass files like the DMF. *See Department of State v. Washington Post Co.*, 456 U.S. 595, 599-603 (1982); *see also Judicial Watch, Inc. v. Food & Drug Administration*, 449 F.3d 141, 152 (D.C. Cir. 2006).

[24] *Department of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. at 773 (quotation omitted).

[25] *Id. See also National Archives & Records Administration v. Favish*, 541 U.S. 157, 171 (2004) (quotation omitted) ("FOIA is often explained as a means for citizens to know 'what the Government is up to'").

[26] *National Association of Retired Federal Employees v. Horner*, 879 F.2d 873, 876 (D.C. Cir. 1989) (quotation omitted), *cert. denied*, 494 U.S. 1078 (1990).

> privacy interest in that information, though it by no means extinguishes that interest; one's own and one's relations' interests in privacy ordinarily extend beyond one's death.[27]

The courts have reiterated that decedents and their surviving relatives possess privacy rights in numerous cases.[28] In the decided cases, the privacy interest at issue generally has consisted exclusively of emotional trauma. Where there is tax-related identity theft, the privacy interest is much stronger because there is a financial as well as an emotional impact. For example, a parent who has lost a child to Sudden Infant Death Syndrome and then discovers an identity thief has used the DMF to claim his child as a dependent must not only devote time trying to prove to the IRS that he was the legitimate parent, but he must also deal with the financial burden of having his tax return (and refund) frozen.

Consider two legitimate uses of DMF information. One is by pension funds that use the information to terminate benefits as of the date of a beneficiary's death. The other is by genealogists who use DMF information to help them build a family tree. While both uses are reasonable, neither fits within the core purpose of FOIA of alerting the citizenry about "what their government is up to." The D.C. Circuit has held that where disclosure does not serve the core purpose of FOIA, no public interest exists, and any personal privacy interest, however modest, is sufficient to tip the balance in favor of nondisclosure.[29] Even if a court were to decide that the DMF does serve a core FOIA purpose, it would balance the public and privacy interests and could easily conclude that the privacy interests predominate.

Thus, if legislation is not forthcoming, I hope the SSA will reconsider its legal analysis and decide to take steps to restrict access to the DMF.[30]

---

[27] *Schrecker v. Department of Justice*, 254 F.3d 162, 166 (D.C. Cir. 2001) (citations omitted), *reiterated on appeal following remand*, 349 F.3d 657, 661 (D.C. Cir. 2003).

[28] *See, e.g., National Archives & Records Administration v. Favish*, 541 U.S. at 170 ("FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images."); *Accuracy in Media, Inc. v. National Park Service*, 194 F.3d 120, 123 (D.C. Cir. 1999) (noting that the D.C. Circuit "has squarely rejected the proposition that FOIA's protection of personal privacy ends upon the death of the individual depicted"); *Campbell v. Department of Justice*, 164 F.3d 20, 33 (D.C. Cir. 1998) ("The court must also account for the fact that certain reputational interests and family-related privacy expectations survive death."); *New York Times v. National Aeronautics & Space Administration*, 920 F.2d 1002, 1005 (D.C. Cir. 1990) (*en banc*) (concluding that NASA was not required to release audio tapes of the final minutes aboard the Challenger space shuttle).

[29] *National Association of Retired Federal Employees v. Horner*, 879 F.2d 873, 879 (D.C. Cir. 1989).

[30] The SSA may be able to restrict access to the DMF without even asking the court to modify its consent judgment in *Perholtz v. Ross*, Civil Action Nos. 78-2385, 78-2386 (D.D.C. Apr. 11, 1980). By its terms, the consent judgment applies only to requests for updated information submitted by Mr. Perholtz himself, is limited to one request per year, and covers only a decedent's "social security number, surname and (as available) date of death." Our understanding is that Mr. Perholtz has not submitted requests for updated information in recent years, that the SSA is now making DMF information available weekly, and that the SSA is making public considerably more information than the three data fields described.

## III. Creating New Exceptions to Taxpayer Privacy Protections Poses Risks and Should Be Approached Carefully, If at All.

In my most recent Annual Report to Congress, I recommended that Congress enact a comprehensive Taxpayer Bill of Rights, and I suggested that the right to confidentiality is one of those core taxpayer rights. Taxpayers have the right to expect that any information they provide to the IRS will not be used or disclosed by the IRS unless authorized by the taxpayer or other provision of law.[31]

The Internal Revenue Code (IRC) contains significant protections for the confidentiality of returns and return information. IRC § 6103 generally provides that returns and return information shall be confidential and then delineates a number of exceptions to this general rule. "Return information" is defined broadly and includes a taxpayer's identity; the nature, source, or amount of income; payments; receipts; deductions; exemptions; credits; and similar items.[32] For example, information furnished on a Form W-2 constitutes return information.

Section 6103(i)(2) authorizes the disclosure of return information (other than "taxpayer return information"[33]) in response to requests from federal law enforcement agencies for use in criminal investigations. The head of the federal agency (or the inspector general of that agency)[34] must request the information in writing and can only disclose it to officers and employees of that agency who are personally/directly engaged in: (1) the preparation of a judicial or administrative proceeding regarding enforcement of a nontax federal criminal statute, (2) an investigation which may result in such a proceeding, or (3) a grand jury proceeding relating to enforcement of a nontax federal criminal statute to which the United States or such agency is or may be a party.[35] Section 6103(i)(3)(A) authorizes the IRS to disclose return information (other than "taxpayer return information"[36]), if the information may constitute evidence of a violation of a *nontax* federal criminal law, to apprise the head of the appropriate federal agency charged with responsibility for enforcing that law.

---

[31] National Taxpayer Advocate 2011 Annual Report to Congress 505.

[32] IRC § 6103(b)(2).

[33] "Taxpayer return information" is defined as return information "which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates." IRC § 6103(b)(3).

[34] If the request is being made by the Department of Justice, multiple specifically named high level officials can make the written request for the information. *See* IRC § 6103(i)(2)(A).

[35] *See* IRC § 6103(i)(2)(A)(i)-(iii).

[36] *See* IRC § 6103(b)(3). The information disclosed can include the taxpayer's identity only if there is information other than taxpayer return information that may constitute evidence of a taxpayer's violation of a nontax federal criminal law. IRC § 6103(i)(3)(A)(ii). "Return information" that is not "taxpayer return information" may include a taxpayer's identity, amount of income, deductions, etc., that is not filed with (or furnished to) the IRS by the taxpayer to whom the return information relates. IRC § 6103(b)(2) & (3). In the typical "bad return" case, the thief's identity, if discovered, will almost always come from other than taxpayer return information.

There is no corresponding exception in IRC § 6103 that allows for the release of identity theft information to *state or local* agencies.[37] However, IRC § 6103(c) provides that a taxpayer may consent to disclosure of returns and return information to any person designated by the taxpayer. Under this exception, the IRS has developed a pilot that would facilitate a consent-based sharing of identity theft information with state and local law enforcement agencies.

It is my understanding that some have called for the expansion of exceptions to IRC § 6103, ostensibly to help state and local law enforcement combat identity theft. I have significant concerns about loosening taxpayer privacy protections and I do not believe that such an expansion of this statute is appropriate at this time. I believe the current framework of IRC § 6103 includes sufficient exceptions to allow the IRS to share information about identity thieves.

The IRS Office of Chief Counsel has advised that under IRC § 6103(i)(3)(A), the IRS may share the "bad return" and other return information of an identity thief with other federal law enforcement agencies investigating the identity theft. In addition, the Office of Chief Counsel has advised that because a "bad return" filed by an identity thief may be considered return information of the victim, an identity theft victim can consent to the disclosure of the "bad return" filed by the alleged identity thief to state and local law enforcement agencies in connection with state and local law enforcement investigations related to the identity theft.

In light of this advice, the IRS has developed a pilot in which tax data related to the "bad return" may be shared with state and local law enforcement agencies based on the victim's written consent. I believe this approach strikes an appropriate balance – protecting taxpayer return information while simultaneously giving state and local law enforcement authorities more information to help them investigate and combat identity theft. However, I am concerned that once the information is in the hands of state and local law enforcement, there is no prohibition in the tax code against redisclosure. Therefore, I suggest that Congress consider modifying IRC § 6103(c) to explicitly limit the use of tax return information to the purpose agreed upon by the taxpayer (*i.e.*, to allow state or local law enforcement to use the information solely to enforce state or local laws) and to prohibit the redisclosure of such information.[38]

---

[37] Note, however, that certain disclosures to state law enforcement are permissible. *See* IRC § 6103(i)(3)(B)(i) (disclosure of return information, including taxpayer return information, can be made to the extent necessary to advise appropriate officers or employees of any state law enforcement agency of the imminent danger of death or physical injury to any individual; disclosure cannot be made to local law enforcement agencies). While identity theft may cause emotional and economic injury, the typical identity theft situation does not pose an imminent danger of death or physical injury.

[38] *See* National Taxpayer Advocate 2011 Annual Report to Congress 505.

## IV. There Is a Continuing Need for the IRS's Identity Protection Specialized Unit to Play a Centralized Role in Managing Identity Theft Cases.

Commissioner Shulman, in his written response to Senator Baucus's follow-up questions stemming from an April 2008 hearing, described the specialized unit (IPSU) as providing "a central point of contact for the resolution of tax issues caused by identity theft." His response further stated, "This unit will provide end-to-end case resolution. Victims will be able to communicate with one customer service representative to have their questions answered and issues resolved quickly and efficiently."[39] While this description fits the model for which my office advocated, it does not accurately reflect how the IPSU works in practice.

The IPSU does not "work" an identity theft case from beginning to end. Instead, it coordinates with up to 27 other functions within the IRS to obtain relief for the victim.[40] That is, the IPSU is designed to act as the "traffic cop" for identity theft cases, ensuring that cases move along smoothly and timely, and are not stuck in one function or another. In some cases (such as when the victim faces no immediate tax impact), the IPSU simply routes the case to other IRS organizations and "monitors" the account every 60 days.[41] In other cases, the unit uses Identity Theft Assistance Requests (ITARs) to ask other IRS functions to take specific actions.[42]

While the procedures call for the receiving functions to give ITARs priority treatment, there are no "teeth" to ensure that this happens.[43] Unlike TAS, which can issue a Taxpayer Assistance Order if an operating division (OD) does not comply with its request for assistance in a timely manner, the IPSU procedures do not specify any consequences for functions that are unresponsive to a case referral or an ITAR. Moreover, TAS has negotiated agreements with the ODs that clearly define when and how the ODs will respond to a TAS request for action. I have urged the IPSU to enter into similar agreements with other IRS ODs and functions that set forth the timeframes for taking the requested actions and to develop tracking procedures to report to heads of office when functions regularly fail to meet these timeframes.

---

[39] *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance*, 110th Cong. (Apr. 10, 2008) (response of IRS Commissioner Douglas H. Shulman to questions from Chairman Max Baucus), *available at* http://finance.senate.gov/hearings/hearing/download/?id=f989b16e-5da3-452d-9675-b75d796fe2b4.

[40] IRS, Identity Theft Executive Steering Committee, *Identity Theft Program Enhancements, Challenges and Next Steps* 14 (Oct. 19, 2011).

[41] IRM 21.9.2.4.3(7) (Oct. 1, 2011).

[42] IRM 21.9.2.10.1 (Oct. 1, 2011).

[43] IRM 21.9.2.1(4) (Oct. 1, 2011) provides:

> All cases involving identity theft will receive priority treatment. This includes…Form 14027-A *Identity Theft Case Monitoring*, and Form 14027-B, *Identity Theft Case Referral*….Identity Theft Assistance Request (ITAR) referrals are also included.

IRM 21.9.2.10.1(1) (Oct. 1, 2011) provides that "Cases assigned as ITAR will be treated similar to Taxpayer Advocate Service (TAS) process including time frames."

Although the IRS has now shifted gears and plans to take a specialized approach to assisting identity theft victims, I firmly believe there remains a need for a centralized body such as the IPSU to serve as the "traffic cop." Identity theft cases are often complex, requiring adjustments by multiple IRS functions, and without a coordinator, there is a high risk that these cases will get "stuck" or fall through the cracks. The IPSU should continue to play a central role in this process by conducting a global account review and then tracking each identity theft case from start to finish, from one specialized function to another.

## V. The Taxpayer Protection Unit Needs Significantly More Staffing to Increase Its Level of Service.

For the 2012 filing season, the IRS designed and implemented several identity theft filters intended to weed out suspicious returns. Through data mining, programmers can detect trends based on a variety of factors and develop customized filters to isolate suspicious claims for refunds.

When the IRS proposed these filters, I was consulted and I said I could support them on the condition that the IRS also expeditiously address legitimate returns that happen to have the characteristics of a fabricated return. Significantly, the IRS must be able to answer phone calls from legitimate taxpayers who are caught up in the filters. I was assured there would be a mechanism for filtered tax returns to be retrieved and quickly processed, and a dedicated unit would be sufficiently staffed to take taxpayers' calls.

The IRS now notifies affected taxpayers by letter that it had a problem processing the return and instructs them to call the new Taxpayer Protection Unit (TPU) to provide more information.[44] Unfortunately, this unit is woefully understaffed to handle the volume of calls from taxpayers trying to figure out why their returns are not being processed. For the week ending March 10, the level of service on this unit's phone line was 11.7 percent, meaning that only about one out of every nine calls was answered.[45] And callers who did get through had to wait on hold an average of an hour and six minutes![46]

---

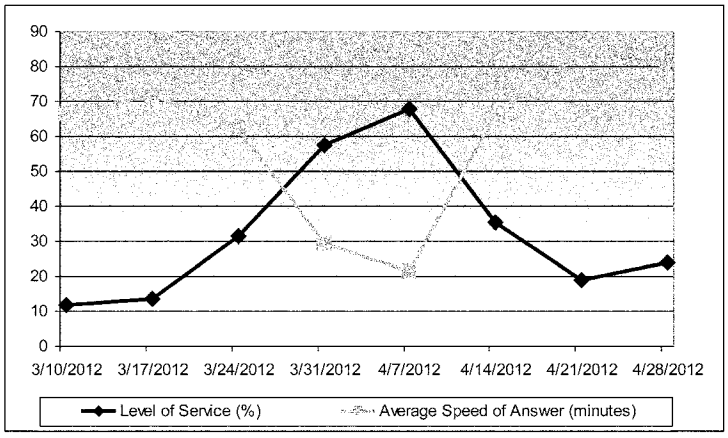
[44] The Taxpayer Protection Unit should not be confused with the Identity Protection Specialized Unit, which assists victims of identity theft. The number to the TPU phone line is provided to taxpayers who receive a letter as a result of the identity theft filters implemented in the 2012 filing season. Victims of identity theft are still instructed to call the toll-free line operated by IPSU.

[45] IRS, Joint Operations Center Executive Level Summary Report (Mar. 13, 2012). Level of service (LOS) measures the relative success rate of taxpayers that call for toll-free services seeking assistance from customer service representatives (CSRs). LOS is calculated by dividing the number of calls answered by the total number of callers attempting to reach the CSR queue. *See* IRS Performance Measures 2009 Data Dictionary (Aug. 4, 2009).

[46] The average speed of answer was 3,991 seconds. IRS, Joint Operations Center Executive Level Summary Report (Mar. 10, 2012).

In the following weeks, the IRS provided additional staffing for the TPU, yet the level of service for this line has not risen to an acceptable level. For the week ending April 28, the TPU achieved a 24.0 percent level of service, with the average wait time increasing to one hour and 21 minutes.[47] This performance is simply unacceptable. The TPU clearly requires more support. I note, however, that in a zero-sum budget environment, providing more resources for this unit means another IRS unit will have less. The table below shows the level of service and average wait time for this "Taxpayer Protection" toll-free line for the past two months.

**Chart 2: Taxpayer Protection Unit Toll-Free Line Data**




It seems not only that the IRS misjudged the number of customer service representatives needed to staff this line, but also that the identity theft filters have picked up more returns than anticipated. *With such a low level of service, it is impossible to assign legitimacy to any estimate the IRS has of the filters' accuracy.* If less than a quarter of the taxpayers calling the number listed in the notice get through to the TPU, how can the IRS ascertain the success of the identity theft filters?

The IRS leadership has assured me this problem has been identified and resolved, and additional resources have been allocated to TPU staffing. Yet the actual LOS data cast doubt on these assurances. Accordingly, my staff and I will monitor the situation and continue to have conversations with the IRS concerning how we can better serve the honest taxpayers caught up in the identity theft filters. From this point on, I will be less

[47] The average speed of answer was 4,868 seconds for this period. IRS, Joint Operations Center Executive Level Summary Report (Apr. 28, 2012).

willing to lend my support to additional filters until I see actual staffing plans and commitments, beyond mere verbal assurances, that the IRS will address the needs of legitimate taxpayers ensnared by the filters.

The IRS often receives lists of compromised identities from its Criminal Investigation function, law enforcement agencies, and other third parties. Information that can identity a taxpayer comes in various forms, such as a series of debit cards, Treasury checks, or personally identifiable information retrieved from an alleged identity thief's laptop. The TPU will be responsible for the review, verification, and resolution of potential identity theft cases referred to the IRS. This process includes checking and verifying returns, determining refund status, and taking appropriate action based on verification results. By identifying and preventing these schemes, the TPU should help protect taxpayers against identity theft-related fraud and enhance IRS revenue protection capabilities.

I am pleased that there is now a process in place to work these referrals, but I am concerned they will be worked by the same TPU employees who are now inundated with identity theft filter calls. With the current level of service on the phones at 24 percent, can we realistically expect that this unit will be able to devote much attention to referral lists?

**VI. The IRS Should Clarify the Purpose and Impact of Identity Theft Indicators.**

The IRS is making efforts to improve its tracking and reporting of identity theft cases.[48] Each function that works a case is required to input an identity theft marker on the purported victim's account. This initial indicator simply marks the account as belonging to a potential identity theft victim. For any filing or refund protections to be activated, a second identity theft marker must be placed on the account after the theft has been verified.

With the backlog of identity theft cases, it often takes months to determine which filer is the rightful owner of the SSN where there have been duplicate filings. By this time, the next filing season may already be underway. When the identity theft victim files the following year's tax return, he or she may assume, mistakenly, that the IRS has taken steps to protect the account from would-be identity thieves when, in reality, the IRS has simply flagged the account as a potential identity theft account.

I have asked that additional training be provided to remind IRS employees (including TAS employees) that the initial identity theft marker provides no protection to the victim's account and is used solely for tracking purposes. It is imperative that we quickly resolve the account problem and apply the subsequent identity theft marker, both to protect revenue and to protect the legitimate taxpayer.

[48] The National Taxpayer Advocate first recommended that the IRS develop an electronic indicator to mark the accounts of identity theft victims in 2005, an idea the IRS ignored in its response. *See* National Taxpayer Advocate 2005 Annual Report to Congress 185, 191. It was not until 2008 that the IRS developed such an indicator. *See* National Taxpayer Advocate 2007 Annual Report to Congress 110 ("In collaboration with the TAS and representatives from IRS business and operating divisions, the IRS has developed a process for using a universal identity theft indicator that will be placed on a taxpayer's account, beginning in 2008, when the taxpayer self-identifies as an identity theft victim.").

In addition to applying an identity theft marker to a victim's account, the IRS should also notify victims in writing that their personal information has been misused. I made this recommendation in my 2007 Annual Report to Congress.[49] While such a letter would not directly stop identity theft, it would alert innocent taxpayers that their personal information has been compromised and allow them an opportunity to take measures to protect themselves from further harm. Only recently has the IRS developed such a letter, and my understanding is that over 16,000 letters have gone out thus far in the 2012 filing season.[50] However, not every function appears to be issuing these notification letters.[51] The fact that it took over four years to develop such a simple and helpful letter suggests the IRS has not placed adequate emphasis on victim assistance. The fact that not all appropriate functions currently issue these letters reveals the need for a stronger identity theft program office that does not rely on individual functions to develop their own procedures without sufficient oversight.

## VII. When Analyzing the Impact of Identity Theft, a Broad Perspective Is Necessary.

I want to take a moment to provide much-needed perspective on the IRS's overall mission and the challenges and trade-offs that addressing tax-related identity theft presents. As the nation's tax collection agency, the IRS is responsible for processing over 145 million individual income tax returns annually, including more than 109 million requests for refunds.[52] In 2011, the average refund amount was approximately $2,913, representing a significant lump-sum payment for those taxpayers with incomes below the median adjusted gross income of $31,494 for individual taxpayers.[53]

During the filing season and throughout the year, the IRS must protect the public fisc from illegitimate refund claims while expeditiously processing legitimate returns and paying out legitimate refunds. The dual tasks of fraud prevention and timely return processing present challenges even in simple tax systems, and ours is far from simple. The recent trend of running explicit economic stimulus or disbursement programs through the tax code that require the IRS to make large payments to taxpayers, combined with a reduction in IRS funding, has made the IRS's job much harder.

---

[49] National Taxpayer Advocate 2007 Annual Report to Congress 112.

[50] Data obtained from the Notice Gatekeeper intranet site (May 3, 2012).

[51] For example, there is no guidance in the IRM for the Automated Underreporter function to issue Letter 4310c to taxpayers whose SSNs have been misused.

[52] In calendar year 2011, the IRS processed 145,320,000 individual tax returns, with 109,337,000 requests for refunds. IRS, *Filing Season Statistics – Dec. 31, 2011*, *at* http://www.irs.gov/newsroom/article/0,,id=252176,00.html (last visited Mar. 12, 2012).

[53] IRS, *Filing Season Statistics – Dec. 31, 2011*, *at* http://www.irs.gov/newsroom/article/0,,id=252176,00.html (last visited Mar. 12, 2012); Compliance Data Warehouse, Individual Returns Transaction File for CY 2011.

To better protect the public fisc from a surge of new refund schemes, the IRS has expanded its use of sophisticated fraud detection models based on data mining. In FY 2011, the IRS's Electronic Fraud Detection System (EFDS) selected over one million questionable returns for screening, a 72 percent increase from the previous year.[54] While it is important for the IRS to address the one million questionable returns, we should not lose sight of the fact that the IRS also has a duty to the other 144 million individual taxpayers in this country. Taxpayers have become accustomed to filing their returns shortly after they receive their Forms W-2 or Forms 1099 (reporting wages and interest, respectively, and available to taxpayers by January 31). Approximately 77 percent of U.S. taxpayers file electronically, meaning the IRS can process most refund requests within a week or two of filing.[55] With the introduction of e-filing, combined with the increasing number of refundable credits run through the tax code, our tax system has shifted, for better or worse, to one of instant gratification.

The benefit of enjoying such a tax system is somewhat offset by the increased ability of perpetrators to defraud the government. While the IRS seeks to implement automated filters to screen out as many suspicious refund claims as possible, it is unrealistic to expect the IRS to detect and deny all such claims. Because the fraud detection algorithms are constantly evolving in response to new patterns, there will always be a lag in the filters.

If we wanted to be absolutely certain that no improper refunds are paid out to identity thieves or other individuals filing bogus returns, we could keep the April 15 filing deadline, but push the date on which the IRS will issue refunds a few months into the summer, after the return filing due date, as some other tax systems do. Such a shift would allow the IRS sufficient time to review every suspicious return. More importantly, the IRS would have at its disposal nearly the full arsenal of information reporting databases – including complete data on wages and withholding, interest income, dividends, and capital gains – and could better detect and resolve discrepancies and questionable returns before refunds are issued.

However, this would be an extreme shift and it would take considerable effort to change a culture in which taxpayers have become accustomed to receiving their refunds within a week or two of electronically filing their returns. Delaying the delivery of a $3,000 refund to a family that is relying on these funds to meet basic living expenses may inflict severe financial hardships. Many taxpayers have grown accustomed to the existing cycle and make financial decisions based on the assumption they will receive their refunds in February or March.

There would be other costs associated with such a drastic shift as well. Third-party lenders may welcome the opportunity to provide bridge loans to taxpayers who feel they

---

[54] The volume of returns selected to be screened rose from 611,845 in CY 2010 to 1,054,704 in CY 2011 (through Oct. 15, 2011), a 72 percent increase. *See* National Taxpayer Advocate 2011 Annual Report to Congress 28.

[55] IRS, *IRS e-file Launches Today; Most Taxpayers Can File Immediately*, IR-2012-7 (Jan. 17, 2012).

cannot wait six months for a refund. Because experience has shown that such lenders will be tempted to charge predatory interest rates, we would need to be prepared to further regulate this industry.

Alternatively, if we prefer not to delay the processing of refunds for six months but still insist on greater fraud detection than the IRS can now manage, then Congress should authorize significantly more funding for the IRS so it can expeditiously work cases where returns and associated refunds have been flagged but may be legitimate. In my 2011 Annual Report, I noted that while questionable returns selected by EFDS increased by 72 percent, the staffing of the IRS unit conducting the manual wage and withholding verification grew by less than nine percent.[56] It is unrealistic to expect the IRS to keep up with its increasing workload without either allocating a corresponding increase in resources or extending the timeframe for the necessary wage and withholding verification. Absent one of these steps, honest taxpayers will continue to be harmed and overall taxpayer service and compliance will suffer as the IRS directs resources from other IRS activities to combat fraud and identity theft.

Recently, the IRS started exploring the feasibility of using an e-authentication system. The White House is promoting the development of an "Identity Ecosystem" – essentially a marketplace of trusted credential providers that individuals could choose to use in order to better authenticate and protect themselves online.[57] The IRS is in discussions with the National Strategy for Trusted Identities in Cyberspace (NSTIC) to see how this e-authentication system can both make it more difficult for individuals to commit identity theft and offer increased convenience to taxpayers.[58] The IRS will conduct a cost-benefit analysis of participation in this NSTIC program.

## VIII. Conclusion

Identity theft poses significant challenges for the IRS. Opportunistic thieves will always try to game the system. From their perspective, the potential rewards of committing tax-related identity theft may be worth the risk. We can do more both to reduce the rewards (by continuing to implement targeted filters) and to increase the risk (by actively pursuing criminal penalties against those who are caught). In making the tax system less attractive to such criminal activity, we cannot impose significant burden on

---

[56] The Accounts Management Taxpayer Assurance Program (AMTAP) staff increased from 336 in FY 2010 to 366 in FY 2011, a gain of nearly nine percent. *See* National Taxpayer Advocate 2011 Annual Report to Congress 29.

[57] *See* The White House, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy* (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf; The White House Blog, *The National Strategy for Trusted Identities in Cyberspace*, http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace (last visited May 3, 2012).

[58] For more information about the NSTIC program, see http://www.nist.gov/nstic.

taxpayers, including those who are identity theft victims. Moreover, identity theft is not a problem the IRS can solve on its own.

At a fundamental level, we need to make some choices about what we want most from our tax system. If our goal is to process tax returns and deliver tax refunds as quickly as possible, the IRS can continue to operate as it currently does – but that means some identity thieves will get away with refund fraud and some honest taxpayers will suffer harm. If we place a greater value on protecting taxpayers against identity theft and the Treasury against fraudulent refund claims, we may need to make a substantial shift in the way the IRS does business. Specifically, we may need to ask all taxpayers to wait longer to receive their tax refunds, or we may need to increase IRS staffing significantly. Under current circumstances, it is simply not possible for the IRS both to process legitimate returns rapidly and to combat identity theft effectively.

**STATEMENT OF DAVID F. BLACK, GENERAL COUNSEL, SOCIAL SECURITY ADMINISTRATION**

Mr. BLACK. Chairman Johnson, Chairman Boustany, Ranking Members Becerra and Lewis, and Members of the Subcommittees on Social Security and Oversight, thank you for this opportunity to testify about identity theft.

With the exception of an 8-month deployment to Afghanistan between 2010 and 2011, I have served as the General Counsel of the Social Security Administration since November 2007. I also serve as the senior agency official for privacy.

The agency maintains sensitive and personal information on almost every American and takes seriously its responsibility to protect it. I can attest to the agency's tireless efforts to protect the personal information the public has entrusted to it.

Let me begin by reiterating Commissioner Astrue's recent testimony before the Social Security Subcommittee that the Administration is committed to strike any balance between transparency that helps prevent fraud and protecting individuals from identity theft, which is consistent with the framework for Chairman Johnson's bill, H.R. 3475.

Since Commissioner Astrue's testimony we have submitted to the subcommittee specifications for a bill that expresses the Administration's current thinking on how best to strike that difficult balance. We continue to stand ready to work with you, other agencies and interested organizations to advance a bill that promotes our common goals.

We at Social Security do not generate death data. Rather, we collect it from a variety of sources so we can run our programs. We use death data to stop benefits and to determine eligibility for survivors benefits.

Individuals and entities became aware that we were gathering this high value information. In 1978, Ronald Perholtz filed a lawsuit against us under the Freedom of Information Act, or FOIA, to gain access to the death information in our file. In 1980, the parties entered into a court-approved consent decree that required the

agency to release to Mr. Perholtz the data requested in his lawsuit. The Department of Justice advised us that Congress had not provided an exemption to the FOIA or the Privacy Act that would justify withholding the data covered by the court-approved consent decree.

In 1983, Congress added subsection (r) to Section 205 of the Social Security Act. This subsection requires us to collect death information from States to update our program records, provides the circumstances under which certain agencies may receive such information from us, and, notably, exempts the death information we receive from States from FOIA and the Privacy Act.

However, Congress did not act to exempt from FOIA our release of death information we receive from other sources. In order for us to manage the demand for FOIA requests and for death information and because we had no legal basis to withhold the information, we created a file that we could make available to the public. That file is commonly known as the Death Master File.

Since 1992 we have provided that file to the Department of Commerce's National Technical Information Service, or NTIS, to distribute because NTIS functions as a national clearinghouse for a wide array of government data. NTIS reimburses us for the file under a contractual arrangement. NTIS recovers its dissemination costs by making the Death Master File available to 630 entities, including banks, hospitals, universities, insurance companies, and genealogical services.

In addition, NTIS makes the file available for online searching by many organizations with similar requirements, but who do not wish to load the raw data on their internal systems. The financial services community in particular expressed a desire for this ability when the Ways and Means Subcommittee on Social Security and the Financial Services Subcommittee on Investigations and Oversight held a joint hearing on the Death Master File in November of 2001.

Our practice involving the Death Master File remains legally sound based on FOIA case law, the Department of Justice FOIA guidance, and OMB's Privacy Act guidance. Any attempt to limit disclosure of death information under current law would undoubtedly spawn additional litigation. More importantly, we see no new judicial interpretation of FOIA or the Privacy Act that would allow to us withhold data on deceased individuals. Accordingly, the administration is seeking congressional action to exempt this information from the FOIA to protect countless Americans from the threat of identity theft through abuse of the Death Master File.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Black follows:]


HEARING BEFORE

THE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
SUBCOMMITTEE ON SOCIAL SECURITY

UNITED STATES HOUSE OF REPRESENTATIVES

MAY 8, 2012

STATEMENT
OF
DAVID F. BLACK
GENERAL COUNSEL
SOCIAL SECURITY ADMINISTRATION

Chairman Johnson, Chairman Boustany, Ranking Members Becerra and Lewis, and Members of the Subcommittees on Social Security and Oversight, thank you for this opportunity to testify about the Death Master file.

With the exception of an 8-month deployment to Afghanistan between 2010 and 2011, I have served as the General Counsel of the Social Security Administration since November 2007. I also serve as the Senior Agency Official for Privacy. The agency maintains sensitive and personal information on almost every American and takes seriously its responsibility to protect it. I can attest to the agency's tireless efforts to protect the personal information the public has entrusted to it.

Let me begin by reiterating Commissioner Astrue's recent testimony before the Social Security Subcommittee that the Administration is committed to striking a balance between transparency that helps prevent fraud and protecting individuals from identity theft, which is consistent with the framework for Chairman Johnson's bill, H.R. 3475. Since Commissioner Astrue's testimony, we have submitted to the Subcommittee specifications for a bill that expresses the Administration's current thinking on how best to strike that difficult balance. We continue to stand ready to work with you, other agencies, and interested organizations to advance a bill that promotes our common goals.

We at Social Security do not generate death data; rather, we collect it from a variety of sources so that we can run our programs. We use death data to stop benefits and to determine eligibility for survivors' benefits.

Individuals and entities became aware that we were gathering this high-value information. In 1978, Ronald Perholtz filed a lawsuit against us under the Freedom of Information Act (FOIA) to gain access to the death information in our files. In 1980, the parties entered into a court-approved consent decree that required the agency to release to Mr. Perholtz the data requested in his lawsuit. The Department of Justice advised us that Congress had not provided an exemption to the FOIA or the Privacy Act that would justify withholding the data covered by the court-approved consent decree.

In 1983, Congress added subsection (r) to section 205 of the Social Security Act. This subsection requires us to collect death information from States to update our program records, provides the circumstances under which certain agencies may receive such information from us, and, notably, exempts the death information we receive from States from FOIA and the Privacy Act. However, Congress did not act to exempt from FOIA our release of death information that we receive from other sources.

In order for us to manage the demand for FOIA requests for death information and because we had no legal basis to withhold the information, we created a file that we could make available to the public. That file is commonly known as the Death Master File. Since 1992, we have provided the file to the Department of Commerce's National Technical Information Service (NTIS) to distribute because NTIS functions as a national clearinghouse for a wide array of Government data. NTIS reimburses us for the file under a contractual arrangement. NTIS recovers its dissemination costs by making the Death Master File available to 630 entities including banks, hospitals, universities, insurance companies, and genealogical services. In addition, NTIS makes the file available for online searching by many organizations with similar requirements but who do not wish to load the raw data on their internal systems. The financial services community in particular expressed a desire for this ability when the Ways and Means Subcommittee on Social Security and the Financial Services Subcommittee on Investigations and Oversight held a joint hearing on the DMF in November 2001.

Our practice involving the Death Master File remains legally sound, based on FOIA, case law, the Department of Justice FOIA guidance, and OMB's Privacy Act guidance. Any attempt to limit disclosure of death information under current law would undoubtedly spawn additional litigation. More importantly, we see no new judicial interpretation of FOIA or the Privacy Act that would allow us to withhold data on deceased individuals from the general public. Accordingly, the Administration is seeking congressional action to exempt this information from the FOIA to protect countless Americans from the threat of identity theft through abuse of the Death Master File.

Thank you for the opportunity to testify.



Chairman BOUSTANY. Thank you, Mr. Black.

Inspector General George, your testimony referenced identity theft related tax fraud that might go undetected, and we heard some figures, IRS reports $6.5 billion in identity theft tax fraud for fiscal year 2011. You had a different figure that you laid out in your testimony. Can you just describe again the total amount of fraud in 2011?

Mr. GEORGE. Yes. The figure that the IRS identified we do not contest. We have had the benefit of being able to look at the issue subsequent to the IRS's release of their figure. A perennial prob-

lem, Mr. Chairman, that the IRS confronts in their worthwhile effort to expedite refunds to the taxpayers they do not have either the benefit of or, whatever term I would defer to Mr. Miller to describe, the time to wait until all third party reporting information has been received by them, meaning W-2, 1099 and the like. And so when we looked at this number we were able to benefit from the fact that we saw the W-2s and the 1099s and that an additional $5.2 billion was on top of the number that the IRS reported. So it is almost double the problem that they initially reported, sir.

Chairman BOUSTANY. Mr. Miller, do you want to comment on that?

Mr. MILLER. Yes, I would actually. We don't disagree with the number that General George and the Inspector General are utilizing. I would point out that we probably do disagree with the large number over a 5-year period because what—and we received the report last week—what we see is actually a good story, not a bad story. It is true that money got out in 2010, which is the year they were looking at. The Inspector General utilized four scenarios to try to look through the data. The Schedule C work that they suggested we are now doing. The work on Social Security income we now have fixes in place for that. Interest income, which was a third of their rules that they were utilizing, we have what they are suggesting being done there as well. So I will say yes, it is true in 2010. The fourth piece was the W-2s are missing, and I think that is correct. What we have done is moved up by as much as a couple of months when we can look at those W-2s, but it continues to be less than optimal not to have all the data that we need to look at as a return is in front of us in determining whether it is fraudulent or not. But I think what we would see is a much lower number today because of the efforts that we have done than with 2010.

Chairman BOUSTANY. So are you suggesting that the Inspector General's number was based on a snapshot before you implemented certain things that will have an impact on that 5-year figure?

Mr. MILLER. Absolutely.

Chairman BOUSTANY. Okay.

Inspector General George.

Mr. GEORGE. I have no information to contradict what he states.

Chairman BOUSTANY. Okay. The subcommittee is not only interested in the size of the fraud but also in how we might prevent it from occurring and continuing to occur. And I would like each of you to comment on what Congress needs to do legislatively. We are all aware of Chairman Johnson's bill. I think there seems to be broad agreement that it is a good bill that needs to move forward. But what more do we need to consider to assist your agencies to combat this growing problem?

Mr. GEORGE. Mr. Chairman, the new hire directory would be an immensely helpful tool for the IRS for a variety of reasons, but some of it is the fact that it would give the IRS a tool to determine whether or not someone who is claiming deductions or income for which they would seek a refund if they didn't have a job in the previous year or the year prior to that, you know, it raises alarm bells that the IRS can use internally to determine whether or not the information that they are supplying seeking the refund is valid, sus-

pect, what have you. And this again, as was pointed out by Mr. Lewis, is something that has been sought for by both the various administrations and various Secretaries of the Treasury.

Chairman BOUSTANY. Thank you. Mr. Miller.

Mr. MILLER. So if I could add to that, I think the new hire database would be a great add, a new tool in our tool box in this area, not a panacea, none of these are panaceas to be honest with you. But we could use all the help we can get and that would be a good one. Another one actually is the Death Master File which is the subject of discussion today. We need, the IRS needs maybe 2 years without having a decedent's Social Security number in the public domain because a decedent has a filing requirement, the executor must file on behalf of the decedent for the year of his or her death. So we need a little bit of time, we can't just lock the account when we understand someone has passed. We have to allow that person to file with us.

I will go back to obviously the big one for us is the budget. We could use any help that you can give us in terms of bridging some of the gaps we are seeing right now on the budget.

Lastly, I will mention there is a little known provision in Section 6103, the tax privacy rules, that has expired, and that allows us to share information with prisons. And that allows the prisons to utilize that information in disciplinary hearings on people who are prisoners who are cheating, and we have 1990,000 returns from prisoners that we believe are fraudulent. That would help as well.

Chairman BOUSTANY. Despite IRS's creation of a centralized identity protection unit, the Taxpayer Advocate reports at least 28 different units within IRS are charged with helping ID theft victims and sit on a somewhat bureaucratic maze. Taxpayers sometimes work more than a year to resolve their identity issues, according to TIGTA. I would like you each to comment on how this affects taxpayers and what changes could be made to streamline that process and better serve the victims of these crimes.

Mr. GEORGE. As you can imagine, if you call American Express or any credit card company and you are relating a problem to them and every time you are requested to give the same information you gave the first time you called and to explain the problem over and over again, how frustrating that can be. While Mr. Miller pointed out that the IRS is providing additional resources towards this, we noted in our research, Mr. Chairman, that during the height of the tax filing season, people who are normally assigned to address identity theft problems were actually taken away from that responsibility and reassigned to answer tax questions that any citizen who rightfully has a question and calls the 1–800 number expects to receive. And so the identity theft issue is actually set aside for a while and then assigned to someone who may not have any information at all regarding that particular case. And so again the taxpayer has to start anew. And we think they could readily institute policies where you have a single individual assigned to a case and almost as many police departments do with detectives and the like.

Chairman BOUSTANY. Mr. Miller, has that been considered?

Mr. MILLER. It is in some fashion, but let me rephrase sort of the question. We have, the vast majority of the identity theft work we are doing with victims is when the person files and they are

blocked from going through because somebody has stolen their identity and it has gone through first. That work resides—and it is anywhere between 150,000 or more of those cases—resides with a unit specifically working on those cases. I don't think we have pulled people off, we may have, but I am unaware of that. What I can say is with the number of cases that we had, we were understaffed. And so there is no question about that in terms of working through these cases. They are difficult cases. They can take anywhere between 40 days and what the Inspector General has mentioned on average right now they are taking 280 days, and that is about 250 days too long in probably all of our view. That is a question of staffing. We started the year working those cases with 200 people. Now the filing season is over, we will have 1,200 people working those cases.

What I am trying to do is make sure that by the end of this calendar year nobody who has been a previous victim has the chance of being a victim again. We want to work that inventory during the summer.

Chairman BOUSTANY. Thank you. And one final question, are there any practices in the private sector that we at the Federal level might adopt that would both limit tax fraud or better assist victims? Briefly if you could comment on that.

Mr. GEORGE. Mr. Chairman, yes. The short answer is there is something called shared secrets. If you call again a credit card company in addition to asking for your name and your card number, they will ask many times your mother's maiden name or date of birth. The IRS simply doesn't do that and that is something that they can easily do. But just to go back to your earlier point, sir, something that is somewhat perverse in that the victim of identity theft reaches the point where the refund was sent to someone else's account, the thief's account, bad guy's account, information that is later sent by the IRS to try to resolve the information is sent to the same address as that which the thief provided. And so there is still even more of a chance of the unwilling or I don't think intentional divulgence of privacy information, personally identifiable information. So the IRS, there are certain commonsensical actions that I think are needed that I don't think would cost a lot of money but the IRS simply hasn't done.

Chairman BOUSTANY. Thank you. Mr. Miller.

Mr. MILLER. Just a couple points. One, I believe statutorily we have to at least start with the address the record that we have, and if it is the wrong address unfortunately that is the address we probably will have to send it to. We do follow up and we work these cases. It is one the barriers we have.

In terms of shared secrets I think it is a wonderful idea and we are working on it. I don't think it is cheap, quite frankly. We don't have a database sitting there waiting to be utilized for this. Part of our authentication process I hope to roll out before the next filing season, but it is not a small list to be honest with you.

Chairman BOUSTANY. Thank you. I now yield to Mr. Lewis the ranking member of the Oversight Subcommittee.

Mr. LEWIS. Thank you, Mr. Chairman. Let me thank each witness for being willing to testify and being here today. Thank you so much.

Inspector General George, your written testimony states that the IRS has faced budget cuts, a hiring freeze, and staff reductions during the same time it has encountered a large surge in identity theft refund fraud. Is identity theft something that the IRS is fully able to combat given its resources and budget constraints?

Mr. GEORGE. Notwithstanding and again obviously, sir, you understand the role that I play.

Mr. LEWIS. I understand your role very well.

Mr. GEORGE. Where they can make improvements. Notwithstanding all of my statements, I would have to give the IRS credit in this area. They are doing a better job in terms of assisting people who are victims of identity theft and in terms of improving processes, but they obviously could do a better job and there is no question that if they had additional resources they could do more and do it better.

Mr. LEWIS. But do you have any suggestions or recommendations of what amount of additional resources would be helpful to the IRS?

Mr. GEORGE. That I don't have at this time, sir.

Mr. LEWIS. Mr. Miller, in your original testimony you stated that in some cases identity theft, the identity that is stolen may belong to a deceased individual. Why doesn't the IRS immediately turn off Social Security numbers of deceased individuals?

Mr. MILLER. Mr. Chairman, Mr. Lewis, we can't do that. As I mentioned, a person who died in 2011 will have to have their executor file a tax return in their name, and so if I passed on the 1st of January, for example, all the way through the extension date of October 15th of the next year, there is a possibility that that decedent will have to use their Social Security number to file their return. We have filters in place to try to make sure that those returns coming in are not fraudulent, but it is impossible for us really to lock that account down until that final return has been filed.

We are marking them as best we can at this point, but we can't just block that social until they no longer have a filing requirement with us.

Ms. OLSON. If I might add, sir, if you are a surviving spouse, under the law you are able to file married filing jointly with your deceased spouse for the year of death, and I believe 2 years after the year of death, if you do not remarry. So that is really three, you know, the year of death, plus two more years that in certain instances, you would need the Social Security number to be live.

Mr. LEWIS. Thank you, Ms. Olson. Mr. Miller, you further stated in your written testimony that the IRS has a significant increase in refund fraud involving identity theft. Given your budget cut, how do you address identity theft and keep up with your current workload? I understand that the telephone service is suffering with identity theft victims waiting over 1 hour to speak with someone. What else is suffering?

Mr. MILLER. So it is a zero-sum game. We have a dollar to spend on various things, and we have gone from, our estimate would be maybe $190 million in 2011 to $330 million this year on these issues. So obviously, service is stretched; enforcement is stretched. We are making sure we fund what we need to fund to

have a fair and equitable, balanced program of service and enforcement. But there is no doubt that we are stretched.

And I would speak a moment on the line that everyone refers to. Nothing to be proud of for us, obviously. It is not a defensible position to have that low ability to answer the phone. We have taken steps to address it. We are right now in the 70s, because we have put another 100 folks on that line, but it took a while to do that. We had to wait for the filing season, to be honest with you, before we pulled people off and put them on that line. And that is the line, by the way, we should be clear, that is not the line that if I am the subject of identity theft, I pick up and the phone and call the service. That line, seven out of ten people are getting through and we are doing much better on. This is the line where we sent something to the person saying, your return is being held up, we have some questions. That is the line that we frankly were swamped on, and have now taken appropriate steps, late but appropriate steps to try to get past that backlog.

Mr. LEWIS. Thank you. Now, Miss Olson in your testimony you stated that a broad perspective is needed on the IRS's overall mission, and the challenges and tradeoffs that a tax-related identity theft present. Please explain. Can you explain to us further? Can you inform and educate Members of the Committee?

Ms. OLSON. We were trying to raise a really broad policy issue, which is the conflict between the fact that we have 80 percent of our individual taxpayers getting refunds and they want them quickly, and then the need of the IRS to basically screen returns, and rout out identity theft or other refund fraud and make sure we are protecting the government fisc, and those two issues are inherently in conflict. And part of my raising this was to say we should perhaps consider, and this a very big issue, doing what many other countries do in their filing season, which is that they actually delay the date of issuance of refunds until after the return filing season is over. So you know that, you know if the return filing season is going to end on April 15th, and refunds are going to be issued on June 1st, or June 15th, then the IRS would have the time to do the matching with the information return documents, and things like that, and that you would be much more likely to have the legitimate refunds going out.

That is a very big issue, but I think that is about the only way that you are really going to resolve these competing tensions, the need for refunds, and then the need to protect revenue.

Mr. LEWIS. Thank you. Thank you, Mr. Chairman. I yield back.

Chairman BOUSTANY. I thank the ranking member.

Chairman JOHNSON.

Chairman JOHNSON. Thank you, Mr. Chairman. Before I get to any of my questions I would like to briefly speak about a tax fraud issue I have been working on for over 2 years.

Mr. Miller, the other week NBC Indianapolis, Station WTHR ran a report entitled: "Tax Loopholes Cost Billions." According to the report, the IRS is handing out refundable child tax credits to illegal immigrants who are claiming children who don't even live in the United States.

Without objection, I would like to submit that report for the record.

Chairman BOUSTANY. Without objection.
[The report follows, The Honorable Sam Johnson #1:]

**NBC WTHR 13**
**Tax loophole costs billions**
*Posted: Apr 26, 2012 9:55 PM EDT Updated: Jul 05, 2012 10:03 AM EDT*
By Bob Segall

***Millions of illegal immigrants are getting a bigger tax refund than you. Eyewitness News shows a massive tax loophole that provides billions of dollars in tax credits to undocumented workers and, in many cases, people who have never stepped foot in the United States. And you are paying for it!***

INDIANAPOLIS - Inside his central Indiana office, a longtime tax consultant sits at his desk, shaking his head in disbelief.

"There is not a doubt in my mind there's huge fraud taking place here," he said, slowly flipping through the pages of a tax return.

The tax preparer does not want you to know his name for fear of reprisal, but he does want you to know about a nationwide problem with a huge price tag.

He came to 13 Investigates to blow the whistle.

"We're talking about a multi-billion dollar fraud scheme here that's taking place and no one is talking about it," he said.

The scheme involves illegal immigrants -- illegal immigrants who are filing tax returns.

**How it works**

The Internal Revenue Service says everyone who is employed in the United States – even those who are working here illegally – must report income and pay taxes. Of course, undocumented workers are not supposed to have a social security number. So for them to pay taxes, the IRS created what's called an ITIN, an individual taxpayer identification number. A 9-digit ITIN number issued by the IRS provides both resident and nonresident aliens with a unique identification number that allows them to file tax returns.

While that may have seemed like a good idea, it's now backfiring in a big way.

Each spring, at tax preparation offices all across the nation, many illegal immigrants are now eagerly filing tax returns to take advantage of a tax loophole, using their ITIN numbers to get huge refunds from the IRS.

The loophole is called the Additional Child Tax Credit. It's a fully-refundable credit of up to $1000 per child, and it's meant to help working families who have children living at home.

But 13 Investigates has found many undocumented workers are claiming the tax credit for kids who live in Mexico – lots of kids in Mexico.

"We've seen sometimes 10 or 12 dependents, most times nieces and nephews, on these tax forms," the whistleblower told Eyewitness News. "The more you put on there, the more you get back."

The whistleblower has thousands of examples, and he brought some of them to 13 Investigates. While identifying information such as names and addresses on the tax returns was redacted, it was still clear that the tax filers had received large tax refunds after claiming additional child tax credits for many dependents.

"Here's a return right here: we've got a $10,3000 refund for nine nieces and nephews," he said, pointing to the words "niece" and "nephew" listed on the tax forms nine separate times.

"We're getting an $11,000 refund on this tax return. There's seven nieces and nephews," he said, pointing to another set of documents. "I can bring out stacks and stacks. It's just so easy it's ridiculous."

**20 kids = $30,000**

WTHR spoke to several undocumented workers who confirmed it *is* easy.

They all agreed to talk with WTHR investigative reporter Bob Segall and a translator as long as WTHR agreed not to reveal their identity.

One of the workers, who was interviewed at his home in southern Indiana, admitted his address was used this year to file tax returns by four other undocumented workers who don't even live there. Those four workers claimed 20 children live inside the one residence and, as a result, the IRS sent the illegal immigrants tax refunds totaling $29,608.

13 Investigates saw only one little girl who lives at that address (a small mobile home). We wondered about the 20 kids claimed as tax deductions?

"They don't live here," said the undocumented worker. "The other kids are in their country of origin, which is Mexico."

He later explained none of the 20 children have ever visited the United States – let alone lived here.

So why should undocumented workers receive tax credits for children living in a foreign country, which is a violation of IRS tax rules?

"If the opportunity is there and they can give it to me, why not take advantage of it?" the worker said.

Other undocumented workers in Indiana told 13 Investigates the same thing. Their families are collecting tax refunds for children who do not live in this country. Several of the workers told WTHR they were told it was legal for them to claim the tax credit for a child who does not live in the United States.

**IRS was repeatedly warned**

"The magnitude of the problem has grown exponentially," said Russell George, the United States Department of Treasury's Inspector General for Tax Administration (TIGTA).

And he says the IRS has known about the problem for years.

George has repeatedly warned the IRS that additional child tax credits are being abused by undocumented workers. In 2009, his office released an audit report that showed ITIN tax filers received about $1 billion in additional child tax credits. Last year, the inspector general released a new report showing the problem now costs American tax payers more than $4.2 billion.

"Keep in mind, we're talking $4 billion per year," he said. "It's very troubling."

What George finds even more troubling is the IRS has not taken action despite multiple warnings from the inspector general.

"Millions of people are seeking this tax credit who, we believe, are not entitled to it," said the inspector general. "We have made recommendations to [IRS] as to how they could address this, and they have not taken sufficient action in our view to solve the problem."

Other information obtained from the TIGTA audits include:

· Claims for additional child tax credits by ITIN filers have skyrocketed during the past decade, from $161 million in 2001 to $4.2 billion in tax year 2010.

· Undocumented workers filed 3.02 million tax returns in 2010. 72% of those returns (2.18 million) claimed the additional child tax credit.

· In 2010, the IRS owed undocumented workers more in claimed additional child tax credits than it collected from those workers in taxes.

**Agency responds – sort of**

What does the IRS have to say about all this?

The agency sent WTHR a statement, defending its policy of paying tax credits to illegal immigrants.

"The law has been clear for over a decade that eligibility for these credits does not depend on work authorization status or the type of taxpayer identification number used. Any suggestion that the IRS shouldn't be paying out these credits under current law to ITIN holders is simply incorrect. The IRS administers the law impartially and applies it as it is written," the statement said.

George disagrees with that position and believes the IRS should be doing more to prevent undocumented workers from getting billions in US tax dollars.

"The IRS is not doing something as simple as requesting sufficient documentation from people seeking this credit," he said. "Once the money goes out the door, it's nearly impossible for the IRS to get it back."

Over the past month, WTHR has tried to ask the IRS more questions about its efforts to prevent abuse involving additional child tax credits.

Despite repeated phone calls, e-mails and a visit to IRS headquarters in Washington, the agency said none of its 100,000 employees had time to meet with 13 Investigates for an interview. An IRS spokeswoman said all staff were too busy because of the tax filing deadline in mid-April.

Apparently, the IRS doesn't have time to respond to some tax preparers, either.

Last year, our whistleblower noticed dozens of undocumented workers had used phony documents and false income to claim tax credits. He reported all of it to the IRS.

"These were fraudulent, 100% fraudulent tax returns, but I got no response; absolutely none. We never heard a thing," he said. "To me, it's clear the IRS is letting this happen."

The IRS tells WTHR it can do nothing to change the current system unless it gets permission from Congress. In other words, according to the IRS, closing the loophole would require lawmakers to pass a new law specifically excluding illegal immigrants from claiming additional child tax credits.

The big questions now: Is Congress willing to do that?

**Full statement to WTHR from the Internal Revenue Service**

The law has been clear for over a decade that eligibility for these credits does not depend on work authorization status or the type of taxpayer identification number used. Any suggestion that the IRS shouldn't be paying out these credits under current law to ITIN holders is simply incorrect. The IRS administers the law impartially and applies it as it is written. If the law were changed, the IRS would change its programs accordingly.

The IRS disagrees with TIGTA's recommendation on requiring additional documentation to verify child credit claims. As TIGTA acknowledges in this report, the IRS does not currently have the legal authority to verify and disallow the Child Tax Credit and the Additional Child Tax Credit during return processing simply because of the lack of documentation. The IRS has procedures in place specifically for the evaluation of questionable credit claims early in the processing stream and prior to issuance of a refund. The IRS continues to work to refine and improve our processes.

http://www.wthr.com/story/17798210/tax-loophole-costs-billions

Chairman JOHNSON. It is outrageous that by all accounts the IRS is simply turning a blind eye to this type of fraud which is costing the American taxpayer billions. Now the IRS has said it doesn't have the authority to require Social Security numbers for this refundable tax credit. However, as you well know, one of the requirements for the child tax credit is for the child to actually live in America. Unfortunately, it does not appear that the IRS is enforcing this simple requirement, and I feel that is unacceptable.

As you well know, I have got a common-sense measure to stop the IRS from giving out refundable child tax credits to illegal immigrants by requiring tax filers to provide their Social Security number. It is my hope that we will finally pass this into law. Until we do so, I fully expect and call on the IRS to do all it can to stop this, multi-million dollar fraud. I think the taxpayer deserves no less, and I think you agree with me.

Mr. O'Carroll, criminals seem to always be one step ahead of us, particularly when the government makes it easy for them. Can you tell us more about the case in Puerto Rico and why obtaining Social Security numbers of those from Puerto Rico are so valuable?

Mr. O'CARROL. Yes, Mr. Chairman. As you are saying, it is a commodity out there, the misuse of the SSNs, and SSN information, and what happened in Puerto Rico is that there was a theft of a lot of birth certificates and other identifying documents that went on to the black market and were sold and then were used for people to basically adopt identity and adopt identities of children from also school records that were taken from there, and both were being then used for identity theft and fraud. And we have been, again, very keeping, I guess the law enforcement community is informed of this and trying to keep as much information out there to keep it from becoming too widespread. And we think that probably through the sharing of information it has been contained.

Chairman JOHNSON. Given your experience, are there other ways, in addition to ending the public availability of the Death Master File, that you could recommend for fighting tax-related fraud resulting from identity theft?

Mr. O'CARROL. Yes, I can. As I had said in my oral testimony, most of it is common sense on the part of individuals, not to be, you know, be phished into giving information out to people that you don't know, to safeguard your Social Security number. Don't carry it with you. Shred any personal information that has your identifiers on it so that it is not going to be, you know, picked up by something doing the dumpster diving and trying to get your personal information. So we try at every opportunity that we can when we talk to people at our hotline is to give that information out, is that it is a valuable commodity and to safeguard your Social Security number whenever you can.

Chairman JOHNSON. Thank you. Ms. Olson, I know in your annual report to Congress you supported legislation to limit public access to the Death Master File, and you also suggested Social Security might have legal authority to limit access to the Death Master File, but when Social Security tried to simply remove the zip code from the file, the agency was besieged by inquiries and lawyers. Protecting personal information by limiting access is Congress' responsibility.

Isn't eliminating the publication of the Death Master File as we propose the best way to make sure none of the information about the deceased is made public?

Ms. OLSON. Sir, I support having a legislative solution to this. I think that that is the cleanest and least controversial approach, but my concern is, as I said in my oral testimony, every single day that we do not have that legislation taxpayers are being harmed. And my reading of the case law since the 1980s, although there may be litigation over the Social Security withholding this information, my reading of the United States Supreme Court case law is that there are exemptions that would cover Social Security withholding that information, and Social Security would prevail. So that is my point, is that we could take administrative steps as we are trying to get the more perfect solution, which is legislation.

Chairman JOHNSON. Thank you, ma'am. Thank you, Mr. Chairman.

Chairman BOUSTANY. Mr. Becerra, you are recognized.

Mr. BECERRA. Thank you, Mr. Chairman, and thank you all for your testimony. Let me first submit for the record a couple of matters, Mr. Chairman. I would like to submit a letter from April the 17th, 2012, by the United States Conference of Catholic Bishops opposing, as they say, our strong opposition to unfair proposals that would alter the child tax credit to exclude children of hard-working immigrant families, and a January 30th, 2012, New York Times editorial which also opposed the unfair proposal to target hard-working immigrant families on the child tax credit and it is titled: "A Harder Squeeze on the Poor," for the record.

Chairman BOUSTANY. Without objection.

[The letters follow, The Honorable Xavier Becerra #1, The Honorable Xavier Becerra #2:]

**New York Times**
**A Harder Squeeze on the Poor**
Editorial
Published: January 30, 2012

House Republicans have hit upon a noxious scheme to help pay for an extension of the payroll tax cut: a tax increase on millions of poor working families. A bill passed by the House and now in conference seeks to deny cash refunds under the child tax credit to those who file tax returns using "individual taxpayer identification numbers" issued by the Internal Revenue Service. Only those using Social Security numbers would be eligible.

The refundable portion of the child tax credit is a life-saver for the working poor. Families that would be cut off by this policy change make an average of $21,000 per year, according to the Treasury Department. They would lose an average of $1,800. About 80 percent of those families are Hispanic. The taxpayer identification numbers are used frequently, though not exclusively, by unauthorized immigrants to pay the taxes because they are not eligible for Social Security numbers. The I.R.S. accepts their tax payments and allows families to claim the child tax credit regardless of immigration status. This policy is an effective antipoverty tool that protects children, most of whom are American-born citizens.

The Republicans who have flatly rejected tax increases on the rich have settled instead on limiting this refund, which kept about 1.3 million children from falling into poverty in 2009.

Leaving aside the cruelty of squeezing the poorest workers for a greater portion of their wages to make a point about illegal immigration, the bill punishes not just the undocumented, but the communities they live in, because a poor family's hard-earned wages get spent: on things like groceries, child care, utilities, gas and rent. This would be the bottom line of the House bill: a Congress that has failed for years to fix the immigration system, using its failure to harm children and hurting those at the bottom of the ladder to avoid the slightest pressure on millionaires. The Senate would be mad to go along with it.

http://www.nytimes.com/2012/01/31/opinion/a-harder-squeeze-on-the-poor.html?_r=1

Committee on Domestic Justice and Human Development
3211 FOURTH STREET NE • WASHINGTON DC 20017-1194 • 202-541-3160
WEBSITE: WWW.USCCB.ORG/JPHD • FAX 202-541-3339

April 17, 2012

The Honorable Dave Camp
Chairman
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Sander M. Levin
Ranking Member
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C.20515

Dear Chairman Camp and Ranking Member Levin:

As you prepare your response to the reconciliation instructions contained in the Fiscal Year 2013 budget resolution, I wish to renew our strong opposition to unfair proposals that would alter the Child Tax Credit to exclude children of hard-working, immigrant families.

The bishops' conference has long supported the Child Tax Credit because it is pro-work, pro-family, and one of the most effective antipoverty programs in our nation. In 2009, 2.3 million people, including 1.3 million children, were kept out of poverty by the Child Tax Credit. Proposals to deny the credit to children of working poor immigrant families--the large majority of whom are American citizens--would hurt vulnerable kids, increase poverty, and would not advance the common good. To exclude these children who are American citizens from the Child Tax Credit is unjust and wrong. We urge you to actively and publically oppose such measures.

The *Compendium of the Social Doctrine of the Church* clearly states the importance of ensuring that workers make a family wage, "a wage sufficient to maintain a family and allow it to live decently. . . . There can be several different ways to make a family wage a concrete reality. Various forms of important social provisions help to bring it about, for example, family subsidies and other contributions for dependent family members. . ." (no. 250).

The Child Tax Credit is a clear example of this. We must protect those programs that help low-income workers escape poverty and raise their children in dignity.

If you must find savings, I urge you to consider cuts that will not harm poor and vulnerable families and to refrain from cutting essential programs such as the Child Tax Credit.

Sincerely,

Stephen E. Blaire

Most Reverend Stephen E. Blaire
Chairman
Committee on Domestic Justice and Human Development

---

Mr. BECERRA. Miss Olson, you are the Taxpayer Advocate. Let's make sure we are clear. That doesn't mean you are the IRS's advocate before Congress. It means you are the advocate for the millions of Americans who file voluntarily their tax returns to pay their taxes.

Ms. OLSON. Yes, sir.

Mr. BECERRA. So you are the eyes and ears for Americans who can't afford to be in D.C. to talk to Congress every day.

Ms. OLSON. Right.

Mr. BECERRA. Okay. You have said that the number one most serious problem facing the IRS is underfunding, or as you put it, the IRS quote does not adequately—"is not adequately funded to serve taxpayers and collect taxes." You have said that today. You have said it before.

$300 million less in funding this year for the IRS than in last year's budget. IRS is dealing with workloads that are increasing

with 5,000 fewer employees than it had before, so to combat fraud, take care of taxpayers' filings, fewer employees. Does anyone disagree with what Miss Olson has said that the IRS is not adequately funded to serve taxpayers and collect taxes? And I would actually ask the two IGs, Inspectors General, do you, either of you disagree with Miss Olson's statement that the IRS is not adequately funded? And I am not going to get into the whole thing, but I am just wondering, do you think they have got enough money or they don't?

Mr. GEORGE. As was stated by Mr. Miller——

Mr. BECERRA. Mr. George, I am going to run out of time real quickly. I can get into it more, but I am just wondering, do you concur or not with Miss Olson?

Mr. GEORGE. No. I have not conducted an assessment as to the adequacy of IRS funding.

Mr. BECERRA. So you can't pass judgment, that is fair. Okay, Mr. O'Carroll.

Mr. O'CARROL. I am focusing more on Social Security's funding than IRS, so I am not going to weigh in there.

Mr. BECERRA. Maybe we should ask the IGs to examine whether or not the IRS is adequately funded. Mr. Miller, you said that no doubt we are stretched. You just said that a few minutes ago, and so I think you would concur with Miss Olson that your budget is strained and you are trying to do as much as you can with what you have when you are answering only one out of every four phone calls from folks who are calling about identity theft, and those who do get their phone call answered are waiting more than an hour on hold. I suspect you are distressed having to deal with that type of outcome.

Mr. MILLER. We are. That is a disappointment to us as well as to the taxpayer.

Mr. BECERRA. Okay now, so let me ask this. I think Mr. George, it was in your testimony that you said that with $32 million in additional funding to do some of this work on identity theft, we probably could collect some of the, or avoid paying out the $5.5 billion in refunds that were sent out based on fraudulent returns that involved identity theft. Is that correct?

Mr. GEORGE. That is, yes, that is my testimony, sir.

Mr. BECERRA. So for a tenth of the money that the IRS didn't get of the $300 million, they could actually get us back $5.5 billion?

Mr. GEORGE. Yeah, the return on investment, you know, is something that in many of the activities that the IRS engages in would benefit them in terms of getting more of taxpayer dollars back to the Treasury. There is no question about that, sir.

Mr. BECERRA. Is there a more clear definition of being penny wise and pound foolish than to cut the IRS millions of dollars and cost the taxpayers at the end of the day billions of dollars?

Mr. GEORGE. There is no question that if the IRS received additional resources, it could do more.

Mr. BECERRA. I appreciate that. Let me ask Miss Olson and Mr. Black to engage in a bit of a colloquy with me in the time I have remaining. Okay, Miss Olson, you said you think IRS has the ability to restrict some of the Death Master File information from getting out there without having to resort to Congress for a change

in statute. Mr. Black, you say you don't believe that authority exists and you have to abide by the existing laws. And you also mentioned—I don't think you mentioned, but it seems like you would need to be defended if you were sued because you tried to restrict, as Miss Olson said, some of that information. The Department of Justice ultimately would have to take on your case and defend you in court if you were to restrict access to that information because someone, a consumer, a business, decided to sue you because all of a sudden you were restricting access to that Death Master File.

Can I ask a question? Why not talk to each other? Why not ask Justice to sit in a room with you all instead of asking us to perhaps write a new law; can we find out if Justice first would defend you in court and say, yeah, I think there is a case here. If they say no, we wouldn't defend you, then I think it is clear, Miss Olson, that we need to have a new statute. But at the end of the day, every day that we don't restrict access, someone is using information to commit fraud, and it seems to me that it is almost—I hate to say this—but it almost would be worth testing how far we can take the existing laws on privacy to see if you can start restricting—give legitimate stakeholders, there are a lot of insurance companies, a lot of others—and I will conclude with this, Mr. Chairman—a lot of others who need to have access to the Death Master File so fraud isn't committed against them. I know an insurance company would say, wait a minute, if we can't have access to this information, fraud will be committed against consumers by people using it, without us having the correct information. So I think we have to be careful, but giving legitimate stakeholders access to the information. Let's test the limit so that we can avoid this and if ultimately we find that the statutes aren't sufficient to restrict access to private information, then Congress will be better guided. But would you be willing to reach out to Justice and perhaps report back to Congress on what conversations between IRS, Taxpayer Advocate, SSA, and the Department of Justice would turn up?

Chairman BOUSTANY. Briefly.

Mr. BECERRA. Yes. I apologize, Mr. Chairman.

Mr. BLACK. It is difficult for attorneys to be brief, but yes, we would be happy to discuss this with Justice, but as both the chairman and yourself have pointed out, there is both positive and negative uses of the Death Master File.

Mr. BECERRA. Okay.

Mr. BLACK. We would prefer the legislative approach that strikes that balance between the two, and we would prefer to leave a decision like that made up to Congress as opposed to the courts determining what that proper balance is. I think the better approach is that Congress working with the Administration determines what that balance is about the appropriate access to the Death Master File versus the improper access to the Death Master File.

Mr. BECERRA. And I probably should have added Mr. Miller since he is with the IRS as well, and I hope that Mr. Miller would be willing to work with Ms. Olson on that as well.

Chairman BOUSTANY. The gentleman's time is expired. Ms. Jenkins.

Ms. JENKINS. Thank you, Mr. Chairman. Thank you for holding this hearing and thank the panel for being here. And Mr. Miller, or in Mr. George's testimony, he states that their office has recommended that the IRS limit the number of tax refunds being sent to the same account, however, that IRS has not yet acted. And according to Mr. George, his office found 10 bank accounts that had direct deposits of more than 300 tax refunds, which begs the question, you know, why hasn't it been fixed. So is it not possible for the computer system to flag an account after a threshold number of returns has been sent?

Mr. MILLER. So I believe it is possible. It does make sense to look at that. There—I will start by saying it is not exactly the IRS that would be doing this, but FMS, but it is part of Treasury, so it can be done. The issue is a little more complex than just doing that, however, because there are numerous accounts that will receive multiple refunds, including tribes, for example, return preparers, so we would have to find a way to figure out who is whom in that area as we move forward. We did go down this road once before to a bit of a muddle, but we are going to look at it again, absolutely.

Ms. JENKINS. Okay, thank you, and could maybe one or more of you just comment or explain the interaction between the Department of Justice, local law enforcement, and your agencies when identity theft-related tax fraud occurs and kind of walk us through a typical investigation and prosecution of how law enforcement interacts with one another when this occurs?

Mr. O'CARROL. Ms. Jenkins, I will take this at least to start. We work very closely, or our office and our investigators work very closely with the Department of Justice and we are on 45 national task forces that are out there trying to, you know, on identity theft, bankruptcy, and through that we try to assist, you know, local law enforcement with the information on it. We are able to share a lot of our information with them. They share their information back. One of the things we have a little bit of a limitation on is anything in relation to IRS data we don't share and we can't share with law enforcement, but we share all of the information that we have from Social Security on it. We are very proactive with it. We try to work with U.S. Attorneys' offices, and get the word out there that there is punishment for identity theft.

Mr. MILLER. So if I could add on to that, we also work really very hard in this area. I mentioned that 400,000 hours of our criminal investigators' time is spent on identity theft. We have, as the Inspector General mentioned, we have numerous task forces that we are on. We have some issues. We have some issues with local law enforcement because 6103 works in a fashion that allows us to share taxpayer data with State enforcement officials if the State enforcement official is working on State tax. If it is a tax charge that they are working on, and so in States like Florida, for example, where there is no State income tax, there is a gap in what we can do. What we have tried to do, and local law enforcement has been very vocal and annoyed with us, 6103 makes it difficult. We have just started a path forward that I think will help, and that is where you have been a victim and want to help local law enforcement we will go to you. We will say, do you mind if we

share? Do you waive your right to 6103 privacy on behalf of the local law enforcement official? So far, very early to be able to tell whether that is going to work or not, but our attempt there is to help local law enforcement, but it is a difficult path.

Ms. OLSON. I was going to say, if I might add, another thing that local law enforcement and the IRS are doing now including the—and also the Department of Justice, is where someone has identified a scheme and the IRS is not yet involved in it, and they get lists of people's numbers that have been compromised, the IRS now has a place for those lists to go to and, you know, the taxpayer accounts get an identity theft marker because we know that they are possibly compromised even if they haven't been actually yet with us. Again, that takes more resources, more people to enter those markers, and that is sort of on the bottom of the pile. But at least there is that protective device that is going on now.

Ms. JENKINS. Okay, thank you, Mr. Chairman. I yield back.

Chairman BOUSTANY. Mr. Stark, you may inquire.

Mr. STARK. Thank you, Mr. Chairman, both chairmen for holding this hearing, and thank the witnesses for being with us today.

Just my very first question would be directed towards Mr. Miller, and you could just send us a note. I would like to know during that hour and 20 minutes that I might have to wait what music you play, and do you pay your ASCAP fees on that? That would be helpful to know what days to call.

On a more serious note, directed towards Mr. Black and Mr. O'Carroll. Something that we have talked about before, but 19 States are stealing basically about $6,000 bucks a year per foster care child. What happens, those of us who have children who receive Social Security payments, my own case, my young three children, because of my age and that I am on Social Security. Many States unhappily, including our own State of California, take that money from foster care children and dump it into the State general fund, and they don't fill out the annual form that you require me to fill out saying what did I do with that money? Did I save it for the child? Where is it now? How much is saved? Did I spend it? What did I spend it on?

You are not requiring the States to do that. And consequently, we have, as I say, I think it is about 19 States now that are taking the money that should be set aside. These kids when they turn 18 might very well have 15- or 20,000 bucks which they could buy a car, go to college, do a lot of things, and the State is just using it to pave potholes and pay the Governor's salary. That is unfair. And I would like to ask Mr. Black, what are you going to do to see that the States obey the law and fill out the form and return it to you so that you can see that those foster children, whose money that is, receive it when they mature out of foster care?

Mr. BLACK. Congressman Stark, unfortunately I spent all of my preparation time getting into the ins and outs of the Death Master File, but when I return I will sit down with our policy folks, the Office of General Counsel will look at that issue and submit a response for the record.

[The information follows, David F. Black]

Insert for the Record – page 58:

All representative payees (except for certain State mental institutions), including State Foster Care agencies, are required to submit an annual report accounting for the use of beneficiary funds. In addition to these annual reports, we conduct several other reviews to monitor the performance of agencies that serve as payees for our beneficiaries. These include periodic site reviews of agencies that serve 50 or more beneficiaries, reviews of payees not scheduled or selected for a periodic site review, and targeted reviews conducted in response to a "trigger" event such as a beneficiary or third party complaint of benefit mishandling.

We provide ongoing education and support to individuals and organizations that serve as payees. We provide our field personnel with updated program instructions that help them conduct thorough reviews and address cases of misuse correctly. We recently updated the "Guide for Organizational Representative Payees" to provide more information about how to manage benefits and we keep our representative payee website up to date with useful information for payees.

In general, our experience with State foster care agencies that serve as payee has been good. Our review of their reports shows that they use the benefits they receive properly – to meet the needs of the child. We promptly and thoroughly investigate any problems, and take necessary action based on what we find in those investigations.

Mr. STARK. Because it is the law, and it takes enforcement. And Mr. O'Carroll, you are also familiar with this.

Mr. O'CARROL. Yes, I am because I met with you one time. We talked about it. And to be truthful on it, we haven't done our audit work on it. As a result of your bringing it up to me, it is on our list for our work plan for next year.

Mr. STARK. It started with Mr. DeLay and myself. I mean, this is an issue, as I say, for the poorest of the poor, the kids who need it most. And as I say, I am sorry the States are doing this, but I want to see that they get what they deserve and receive the funds they should. So I can fill in any of my colleagues on the details of their own State, but this is something which I guess we have oversight on, and I would like to see that these children somehow get that money saved or the State does. Now, they may need mental health care, which would be a logical thing for this money to be spent on that, special hospitalizations, special treatments. Any of those things are valid ways to spend it, but I am afraid the States who assume the locus parenti for these kids don't do it. And I hope that I can encourage both of you to look into this more and see that these children get the savings and the funds they deserve.

I am sorry to digress, Mr. Chairman, but it is an important issue for young kids. Thank you very much. I thank the witnesses.

Chairman BOUSTANY. I thank the gentleman. Miss Black.

Mrs. BLACK of Tennessee. Thank you, Mr. Chairman. Mr. Miller, I have a question for you. In Mr. George's testimony, he says that the office has recommended that the IRS limit the number of tax refunds that are sent to the same account. However, the IRS has not acted on that, and according to Mr. George and his office, they found that 10 bank accounts had direct deposits of more than 300 tax refunds.

Do you have any idea about how you can fix this, or do you have plans for fixing this so that you might be able to make that determination and helping to make sure that that one account doesn't get that kind of refund?

Mr. MILLER. Well, Congresswoman, I have previously touched on this, but it is something we are working on, and it is something we will look at. We have tried to do that once in the past with mixed results. What I have mentioned is that there are absolutely valid reasons why a single account can be the recipient of many refunds. At the short end of it, it can be a family account for several people, all the way up through the fact that certain Indian tribes maintain an account for the unbanked within their tribal membership, and also return preparers. So we would have to find a way to know that that account was an account that was going to be able to receive many refunds, and we are going to work on that.

Mrs. BLACK of Tennessee. I think with the exception of, as you say, maybe an Indian account, I think 300 tax returns for even a family would seem to be quite excessive. I mean, that would have to be a mighty large family to get 300 tax refunds.

Mr. MILLER. Agreed, but the return preparers are another issue.

Mrs. BLACK of Tennessee. Okay. Thank you.

Mr. GEORGE. Miss Black, if I may just, in addition, because I didn't address this during my oral testimony. In addition to the issue that you just raised, we are finding a growing problem with the use of prepaid debit cards, and having Federal refunds, not only in the realm of the IRS, but Social Security, and other governmental benefits going to these prepaid cards which people can literally buy at stores and bodegas and the like, and finding growing examples of fraud associated with that, with very little oversight being conducted by anyone on this area. And so again, I have to continue my response by saying tax policy is an issue that the Secretary of the Treasury has given solely to the Office of Tax Policy, so I am not in a position to give you any policy advice on this but I did want to make this committee aware of a growing problem in an area that is, you know, something that is beneficial, not everyone has a bank account, but at the same time it is being used inappropriately.

Ms. OLSON. If I might comment on that, please.

Mrs. BLACK of Tennessee. Sure.

Ms. OLSON. My office has recommended in the past that just as you have a Social Security debit card to load benefits for the unbanked onto that, that the government should have a Federally funded, you know, card for people to get their refunds on, those unbanked individuals. And that card would only be available if they went into a financial institution and produced evidence of identity and things like that; rather than clicking a button on a software package, you know, software package that sent you a card without any identification information, and it just came to you in the mail. And I think that might be one way to reach the balance between trying to get the unbanked into the banking system, but also protecting us against identity theft in some way. We can learn from Social Security on that.

Mrs. BLACK of Tennessee. Mr. George?

Mr. GEORGE. Yes, Mrs. Black. There is no question that the IRS and Treasury should be working with financial institutions to develop policies. This is an issue that is of importance, as Ms. Olson just noted, and it is something that is resolvable. It is something that we think can be addressed, but just simply isn't being done so.

Mr. MILLER. And if I could just add on a little bit. We are working with financial institutions. I do not want to give the subcommittee the view that the debit card companies and that the financial institutions are not working with us. They absolutely are and they have been very helpful. We are not as far as we need to be yet, but they are working with us.

Mrs. BLACK of Tennessee. And Mr. Miller, is there any idea about when, I mean, I hear you say you are working on this, but obviously time is of the essence, because there is so much of this going on. Do you have any idea about when you might be able to come up with some resolution that would help us, because we are obviously at tax season and I can just imagine how much is happening right now.

Mr. MILLER. Well, it has happened already, Congresswoman, so we have a little bit of time but not that much time to prepare for the next filing season.

Mrs. BLACK of Tennessee. Yeah.

Mr. MILLER. But as I have mentioned I think to the subcommittees, there is no panacea here, and really should not—absent some ability of the community to act in a fashion that doesn't allow a Social Security number to be stolen, the service will always be working in small places to do things to stop this. There is no one single thing that we can do to stop identity theft.

Mr. GEORGE. But if I may just close on this. The exact problem that you noted regarding 300 refunds going to a single account, you are having— while I don't have an exact number, but we do know that many additional tax refunds are going to a single debit card, so it is really, it is a mirror image of the problem.

Mrs. BLACK of Tennessee. Sure. Thank you, Mr. Chairman. I yield back.

Chairman BOUSTANY. Mr. George, let me put on the record that over a year ago, a letter to, I think it was Secretary Geithner, expressing major concerns about the debit card issue and the potential for fraud, and the responses have been very, very slow on that and we are still pushing to get further information on the potential problems with the use of these debit cards.

Mr. GEORGE. I was unaware of that. Thank you, Mr. Chairman.

Chairman BOUSTANY. We will get a copy of the letter to you.

Mr. GEORGE. Thank you, sir.

Chairman BOUSTANY. Thank you. Mr. Paulsen, you are recognized.

Mr. PAULSEN. Thank you, Mr. Chairmen. I want to thank you and the ranking members for holding our hearing today. And the topic of identity theft is certainly very important and we need to be doing all that we can to combat the problem. I remember last week in Minnesota, actually I held an identity theft seminar with the Minnesota Financial Crimes Task Force for seniors, and I will tell you the object was to give them insight on how to better protect

themselves, and it was a packed house. The line was overflowing out the hallway. In fact, they were so interested in getting information that they hung around for an extra hour, so we ran over time. And I think one way we can help protect, certainly seniors, is to remove that Social Security number from that Medicare ID card. And I am cosponsor of Chairman Johnson's legislation. I thank him for bringing that forward and working on that issue.

But I do want to turn for a moment, if I could, to fraud and ID theft in the area of tax returns, in particular, and Miss Olson, in your 2011 report to Congress, you gave that outline on an issue regarding tax fraud where the tax preparer fraudulently alters a completed tax return and then retains the illicit benefit without the knowledge of the taxpayer even. And you recommended an increase in the penalty to give greater incentive to go after these fraudulent preparers, and so today actually, along with Mr. McDermott and both the chairmen and the ranking member of the Oversight Subcommittee, we are introducing legislation, the Fighting Tax Fraud Act, which essentially doubles the current penalties, giving greater incentive for prosecutions against this type of theft.

So Commissioner, I want to thank you and your office for your diligence and being a great resource to not only myself but my staff throughout the drafting process, and I am just wondering if you could talk a little bit more about what you saw that encouraged you to add this as one of your top 10 recommendations, essentially.

Ms. OLSON. Well, the IRS is seeing many more of these schemes coming in involving return preparers that are filing tax returns, after the taxpayer has approved the return and they actually have a copy of what they think is going to be filed, the preparer alters the return in some way and then uses the split refund procedure to get the difference in the additional refund deposited into their account. The taxpayer doesn't find out about this until much later. They get the refund that they are expecting and it is only until the IRS comes out trying to collect this erroneous refund from the taxpayer that they find out that the return has been altered. And what we learned was really to go after the preparer you have some very-low dollar civil penalties that are really about negligence, and then you have a very expensive route, which is to try to build a case to get to the Department of Justice to bring a prosecution and get restitution for the dollars that are lost to the public fisc, and what we tried to propose was some sort of civil penalty that would really serve as restitution, where you could build the case that the preparer had, in fact, committed this act. It was fraudulent. It was willful and fraudulent and then the preparer would be 100 percent liable for the amount that was erroneously taken out. So it fills a gap in our ability to recover what the public fisc is out, and it also heightens the risk to the preparer in engaging in this activity.

Mr. PAULSEN. And so in these cases, as you mentioned, the taxpayer doesn't really know that he or she has been defrauded at all until they get the notice from the IRS letting them know that their returns were faulty, and this means that they are unaware that anything took place, actually for quite some time. So part of the problem in cases like this is that the return is going to two separate bank accounts, essentially?

Ms. OLSON. It can go to two bank accounts, or as, you know, Commissioner Miller was saying, it can go to the preparer, the preparer could set up a bank account, and then distribute, have the return go to that bank account and then send to the taxpayer the amount that they are expecting. But either way, the taxpayer won't know that this is happening.

Mr. PAULSEN. And other than doubling penalties to enhance the crackdown, or for enforcement of this, do you have any other ideas or suggestions on helping raising the flags earlier in the process to identify where the problems are? Do you have any idea what the prevalence of this type of a fraud activity might be out there?

Ms. OLSON. It is very hard to know about this, but just recently the State of Illinois brought some actions against a large return preparation firm that also operates in many other States where they had identified some alleged fraud, and in fact, they contacted my office, and we all worked together with the IRS, myself, and the Illinois AG to develop a message for taxpayers who might be impacted by this.

And I think to your point about a town hall, we would be more than happy to provide some information to all of the Members of Congress so they could go out in their town halls and alert taxpayers to this risk.

Mr. PAULSEN. Good. Thank you, Mr. Chairman. I yield back.

Chairman BOUSTANY. I thank the gentleman. Mr. Smith, you are recognized.

Mr. SMITH. Thank you, Chairmen Johnson and Boustany, for holding this hearing and thank you to our witnesses. I do have a news article from my district that I would like to ask for unanimous consent to submit for the record.

Chairman BOUSTANY. Without objection.

[The news article follows, The Honorable Adrian Smith]

**"I'm not dead!" Student fights to prove he's alive**
by Josh Egbert
Story Created: Apr 30, 2012 at 5:57 PM CDT
Story Updated: May 1, 2012 at 9:42 AM CDT

A local high school senior is set to graduate and is preparing for college. But at a time when most teenagers are having fun and looking forward to the future, his plans are on hold.

A simple trip to the bank revealed a couple alerts on Corbin Russell's credit score and those alerts have his future in jeopardy.

Life was good for Corbin Russell. The Harvard High School senior will graduate in just a few days and this fall go to college. But those college plans may be derailed.

"I had been dead for the past couple of years," said Corbin.

A simple trip to the bank to get a car loan had turned Corbin's world upside down.

"I was shocked. I really couldn't believe it because I had been getting a bunch of tax returns back from when I was working," Corbin said.

His social security number came back flagged.

"After they ran a credit check score, it came back with a couple alerts," said Corbin.

Corbin's social security number had been used in a death benefit claim for a man in South Carolina who died in January of 2010.

"Without my social security number credit being correct, right now they have it red flagged. Without it being correct I can't get a loan because I'm deceased," said Corbin.

"How could anybody have death benefits on a senior in high school?" said Corbin's mother Monica Russell.

Now the problem has gone beyond just that car loan.

College scholarship applications have been rejected because of the flagged credit report. And he can't get student loans without a valid Social Security number.

"My social security number - if someone just took a couple minutes of their time and said, hey, look, this social security number doesn't match with this person, we need to fix this, everything could be fixed," said Corbin.

But that could take some time.

"In some cases it's taken two years and he can't go to college until it's fixed," said Monica.

Which has Corbin's mom Monica worried about his future.

"The only thing that scares me is if he waits two years will he still want to go," Monica said.

The family has been trying to get the issue fixed, talking with the Federal Trade Commission and the Social Security Administration in Seattle Washington, but so far, nothing.

"That's all I do is cry on the phone because I can't get nowhere," said Monica.

Corbin will start college in September and with a price tag of nearly $40,000 and no way to get a loan.

"I really want to try and make it through it, but it may come down to the fact I have to wait a year or two before I can even go before they get it fixed," said Corbin.

News 5 spoke with the Social Security administration Monday. In their records, Corbin in alive and well. The issue lies with the credit bureau.

The three major credit companies say it can be fixed, but they need documentation, to eradicate the situation.

The only problem is that it could take time and time is not on Corbin's side when it comes to school.

News 5 also spoke with Senator Johanns office, they were able to get Corbin's Free Application for Student Aid form approved, which pays for about 1/3 of his school.

http://www.khastv.com/news/local/f-149577885.html

Mr. SMITH. Thank you. Mr. O'Carroll, on the piece I submitted, and I assumed that you——

Mr. BECERRA. Mr. Chairman, I hate to interrupt the gentleman, but could the gentleman identify the article, so we——

Mr. SMITH. I am getting there. Thank you. It has to do with a student whose Social Security number was utilized by someone fraudulently.

Mr. BECERRA. I thank the gentleman.

Mr. SMITH. The Article I submitted has to do with a young man from my district, Corbin Russell, actually. He found when he went to apply for some student loans that he was denied because someone else had used his Social Security number to file a death claim in South Carolina over 2 years ago. And so now Social Security says that everything is fine with them, but with other agencies it is not yet. And so there is a lot of time that may need to pass before it is clarified or rectified. And so I was wondering why isn't

there the automatic red flag on a tax return when the name and Social Security number do not match?

Mr. O'CARROLL. I will take the first crack at it. In terms of, I am well aware of that, with the identity theft that was taken by your constituent, and again, we are concerned on SSA's information on it, when they get the—in this case we realized that it was falsely reported as death on it. SSA changed the record on it and from our standpoint, with SSA, I think we rectified his problem, which again now leads over to the tax issues, which I will——

Mr. SMITH. Well, would SSA further take any action with other agencies, credit bureaus, and so forth, to correct that?

Mr. O'CARROLL. I guess no, is the short answer on it, is that what SSA will do is, we will—and I will from, I guess advice to the individuals, they will give it to them. They will tell them how they can go about it. They will give them the record from SSA that can be used to be taken to other locations, but SSA isn't proactive in terms of going out to the credit bureaus and the financial institutions and even other government agencies on sharing any of the identity theft. It is probably a good concept in the future of sharing that type of identity theft, but we are not involved in it now.

Mr. SMITH. Okay, anyone else wishing to comment?

Mr. MILLER. Only to say that we do a name check with the Social as it comes into us on the return.

Mr. SMITH. Okay. Mr. Miller, you have mentioned that the multiple refunds are mailed to tax preparers. Could you outline a scenario where that would be commonplace?

Mr. MILLER. I think we are talking direct deposits, which would not be a mailing at all actually.

Mr. SMITH. Okay, but transmitting multiple deposits to one entity?

Mr. MILLER. So there are split refund accounts. My understanding is, and I can get back to the subcommittees on this, but, yeah, there are return preparers who have an account that receives sometimes the refunds of the clientele.

Ms. OLSON. Sir, if I might. There is—preparers are barred from negotiating a check or a deposit for the taxpayer. There are serious penalties about that, but where taxpayers are unbanked, there may be an account set up where the refund can be direct deposited into it on behalf of the taxpayer, and then—and my understanding is, it is actually an account, or a subaccount for that taxpayer in particular, but it may be a larger account number and that might be where the problem is. But again, there are preparers, as I described earlier, who are actually violating the law, using the account, their account to receive the taxpayer's funds and then distribute it out.

Mr. GEORGE. Mr. Smith, if I may, my office investigates many allegations such as what Miss Olson just outlined, where tax preparers have directed refunds from legitimate clients for their own benefit, in effect stealing money from their clients.

Mr. SMITH. Thank you. Also, Ms. Olson, in your earlier testimony, you talked about perhaps holding refunds until the end of the filing season. Is the filing season basically January through the middle of April, or how would you define filing season?

Ms. OLSON. Yes, January through April 15th, and I realize this is a radical suggestion, but I am trying to point the contrast, you know, the tension out between our dual responsibilities here. So, and it is basically the model that is followed by most large tax administrations that give out refunds in the world. They allow themselves time to do these reviews, you know, even waiting to see what kind of duplicate returns we get in. So the first to file isn't always the one that gets the refund. And then we freeze all the later ones.

Mr. SMITH. Okay. Thank you, Mr. Chairman.

Chairman JOHNSON. Mr. Chairman, I would like to submit for the record my letter to the editor to the New York Times editorial earlier submitted for the record, in response.

Chairman BOUSTANY. Without objection.

[The letter to the editor follows, The Honorable Sam Johnson #2]

**New York Times**
**Restricting Tax Credits**
**Letter**
**Published: February 7, 2012**

**To the Editor:**

Re "A Harder Squeeze on the Poor" (editorial, Jan. 31):

A recent government report reveals that in 2010, the Internal Revenue Service awarded $4.2 billion in taxpayer dollars to illegal immigrants through the refundable additional child tax credit. That's just wrong. American taxpayers should not have to pay for benefits for illegal immigrants.

The earned income tax credit, a refundable tax credit for low-income workers, requires a Social Security number for eligibility. Defying logic, the child tax credit does not.

This is a bipartisan issue, as evidenced by Senator Claire McCaskill's call to the Internal Revenue Service last fall to immediately end the fraudulent child tax credit payments.

We need to stop illegal immigrants from taking money out of hard-working American taxpayers' pockets every year by claiming this credit. My bill requiring a Social Security number does that.

SAM JOHNSON
Washington, Feb. 2, 2012

*The writer, a Republican, represents the Third Congressional District of Texas.*

http://www.nytimes.com/2012/02/08/opinion/restricting-tax-credits.html?_r=2

Chairman JOHNSON. Thank you, Mr. Chairman.

Chairman BOUSTANY. Mr. Reed, you are recognized.

Mr. REED. Thank you very much, Mr. Chairman, and thank you to the witnesses. Essentially, to everyone or anyone who would like to respond, in preparing for the hearing today, I was reading about the ability for the IRS to lock accounts on deceased tax filers. And I can appreciate that ability, because of the reports of millions of dollars worth of checks going to deceased folks and the issues that

it represents in regards to waste, fraud, and abuse. And I was just wondering, is it working from any of your points of view, and would a more ambitious approach using tools such as that one help? Can anyone offer any——

Mr. MILLER. So if I could start on that, Congressman. We do lock accounts of the deceased. As I have mentioned, there is a whole group of folks who have died within the last couple of years or even 3 years that still a filing requirement, so we can't really lock their account. We can run them through our filters.

Mr. REED. But isn't that a filing number off the estate? Doesn't the estate have to get the taxpayer identification number rather than the Social Security number?

Mr. MILLER. Right now they will be filing as an estate entity, and they will be filing as the last year of the decedent.

Mr. REED. Okay, please continue. I am sorry.

Mr. MILLER. And so locking accounts, marking accounts is what we are doing, running them through, running them through the filters, and we have caught like 90,000 questionable returns in the traps, is something we are pursuing now, and we will get better at it, but that is really where we are at this point. I think locking of accounts and getting smarter about filters is our best approach going forward.

Mr. REED. So just so I am clear, when you lock that account, that is reported to the Treasury, so that if there is a refund due or anything like that, I know it is a little outside of the purview of the committee today, but does the Treasury still issue refunds when that account is locked?

Mr. MILLER. No. The locking of the account means that basically that return is going to come in and it is not going to be able to be filed with us.

Mr. REED. Okay. So now if there is an erroneous reporting on that filing, on that locked out account, what are the steps that you take specifically to make sure that that gets corrected, and what is the time frame upon which that correction occurs?

Mr. MILLER. Sir, I don't know about the time frame. The approach would be, a person would call in and say you are not letting me file. I need to file. Generally what would happen at that point is we would ask them to file on paper and we would take a look at that return. And that will take a while, but that is the approach that we are taking at this point.

Mr. REED. Because I believe Mr. George had mentioned that it can take IRS more than 1 year to resolve an identity theft case, right? So that is not what we are talking about here.

Mr. MILLER. Could be, but, and if it is, it will take a while for us to work through that case. These coming in through paper are worked, I think, a lot faster especially if there is no first return that has come in.

Mr. REED. Okay, so just looking forward, what could you offer to us, or what would be your best recommendation as to how to better enhance your ability to solve this issue or what would be the kind of the prioritization of additional tools that you could use in order to address the concerns?

Mr. MILLER. So is this for decedents or for identity theft in general?

Mr. REED. Let's do both if we could, decedents. I have got plenty of time.

Mr. MILLER. I will roll through the list.

Mr. REED. See, oh, there is the buzzer now. See look it, now we wasted some more time.

Mr. MILLER. So obviously, we have talked about our budget, which is stretched pretty tight right now.

Mr. REED. And I hear that one, I should—whenever I ask that question of any panel from the—I always hear resources, and need for money and people. Beyond that, because we have no money, and obviously, if you have no money you can't hire any people, so . . .

Mr. MILLER. Well, if we have no money and we can't hire people then we aren't going to be able to do the IT things that I need either, Congressman, and that is going to be a very difficult place for the Internal Revenue Service to be.

Mr. REED. Okay, so with the staff that you have, what authority, what tools could you be given to make your job more efficient so you could do it within the resources that you do have?

Mr. MILLER. We have obviously talked about the Death Master File here, and we have talked a little bit about the new hires database. Both of those would be incremental improvements to what we do. There is also some expired statutory language around sharing with prisons taxpayer information so that we can do a better job of letting those prisons do disciplinary action with respect to prisoners. Those are sort of the things that we would be looking for, and to be honest, simplification would be a good thing for us and for taxpayers as well here.

Mr. REED. Simplification of the actual——

Mr. MILLER. Of the Code.

Mr. REED. Excellent. Any other suggestions anyone had on either on death or identity theft cases? Mr. George, how about you?

Mr. GEORGE. I would just note, and because this hasn't been discussed today, a lot of victims of identity theft don't know they are victims because they don't have filing requirements. And so that is something where I don't know whether it is the IRS or whether it is Congress needs to take a closer look at in terms of informing people who do not have a requirement to file a tax return, that they may need to check their credit records, or whether the IRS has a way of alerting them to something that they should be aware of, but that is an issue that needs to be looked at.

Mr. REED. That is a great point. I appreciate you bringing that up, because eventually, hopefully, they will have to file because—in that position, and times will get better for them and then they can head off a lot of problems that they otherwise would have to deal with at that point in time.

I see my time has expired, Mr. Chairman. I do appreciate it and I yield back.

Chairman BOUSTANY. I thank the gentleman. Mr. Marchant, you are recognized.

Mr. MARCHANT. Thank you, Mr. Chairman. Recently I had a phone call from a constituent that asked me to come over to his office. I went over there and sat down with him and he showed me next door where there was a storefront that, literally, there were

people streaming into this storefront on a constant basis for the entire hour that I was there, in the middle of the day.

And I asked him what his concern was, and he said, you know, this goes on for day after day, after day, after day, and in this case it was primarily Hispanic families. And he said, we share a common block of mailboxes. And he said, I, from time to time I will go to the mailbox to open my box up, and inadvertently the postal worker will have put some of the mail from this place next door into my mailbox. And then I look through it to see which is my mail and which is not my mail. And he says that there are dozens and dozens of IRS checks that are made out to various different people. And I have listened to the testimony today, and I don't know that I was able to decipher what this particular problem was but they were all using this same address of this tax preparer in this case. He asked me to look into it. Frankly, I did not know where to start in looking into it. I did not know where, what governmental agency to start with. The first was the IRS, but then after listening today to the panel, can you suggest to me what a Congressman should do when a constituent cares this much about how the system is being played and what action I might take, and then describe to me what possible fraud is going on in this case?

Mr. Miller.

Mr. MILLER. So if I could start, Congressman. So I would recommend that you do contact us. The postal inspector as well has lines that do this, and we work very well with the postal inspector. You know, in any given case I have no idea whether it is fraudulent or not because it may be that that is their mailing stop. That is where they are receiving their refund and they come back and grab it. It also is possible, obviously, that it is a drop for fraudulent returns that are being procured. So we wouldn't know in any given case. It certainly would raise our antenna, as it did yours, and we would look at it. So I would recommend coming to us. The postal inspector works with us very closely looking for exactly this sort of pattern and stopping a whole lot of these things.

I will mention one other thing since we are talking about mail, and we have talked about debit cards and the problems on debit cards, but there is one thing I do want to make sure everyone is aware of. That debit card, when it goes out, when you order it online or however you are ordering it, it doesn't go out with money on it. So if we stop that refund, it never has money on it. That money goes into an account with sub-accounts, as the Taxpayer Advocate mentioned, but it may be when you see these rows of cards that they are devoid of money on them. So that is another thing I will mention.

Mr. MARCHANT. You mentioned earlier that a person can use pretty much any mailing address for his address for his return?

Mr. MILLER. Generally not. I will have to come back. That is a specificity I don't have at my fingertips, so I will have to come back on that.

[The information follows, Steven T. Miller]

Steve Miller (IRS Witness)
Transcript Insert: Page 80
Hearing on Identity Theft and Tax Fraud on May 8, 2012
The Subcommittees on Social Security and Oversight

A tax refund is mailed to the address on the tax return. One indicator of possible identity theft fraud is a number of refunds directed toward the same address. This action may suggest that the person committing fraud is filing multiple tax returns; possibly using multiple social security numbers; but is using one mailing address to get refunds. Or, as Mr. Marchant described, a tax practitioner might be using the practitioner's address on the tax returns and direct the refund checks to the practitioner's business address. While it is legal for practitioners to have tax refund checks directly deposited into their business account as a service to their clients; it may cause confusion with the taxpayer's future returns as the address that the IRS uses to correspond with the taxpayer is the last address on record. In this example, the last address on record would be the tax practitioner's address.

---

Mr. MARCHANT. But a preparer could designate that the person's mailing address be the preparer's mailing address?

Mr. MILLER. Yes.

Mr. MARCHANT. Okay, thank you.

Mr. GEORGE. Mr. Marchant, I would just point out that because there is some overlapping responsibilities here, the Treasury Inspector General for Tax Administration, which was once the inspection service within the IRS, we have primary oversight of an IRS employee who is accused of committing some type of tax or other criminal wrongdoing, a preparer who steals their client's information or someone who is using the IRS's symbol. It could be anyone, but if they mimic the IRS eagle and attempt to defraud a person or an entity, that is primarily our jurisdiction.

Whereas, the Criminal Investigations Division, which is within the IRS itself, truly has the primary responsibility to investigate in a matter such as the example you gave along with the Postal Service, which would also have the postal inspector who would also have some responsibility. And then there are instances where the overlap to would be an IRS employee who sells the information about a taxpayer to a bad person and that bad person then engages in the tax fraud. So that is where there would be some overlapping jurisdiction among other examples.

Mr. MARCHANT. Thank you very much. Yield back.

Chairman BOUSTANY. I thank the gentleman. Mr. Berg, you are recognized.

Mr. BERG. Thank you, Mr. Chairman. And I thank the panel for being here. I want to also recognize Mr. Black, who also is from North Dakota. There are so few of us, we have got to stick together when we get together. He is actually from Rugby, which is the geo-

graphical center of North America. So sometimes people are not sure where North Dakota is. It is the geographical center of North America.

You know, as we look at this issue, as I think about it, obviously, there is not unlimited money, not unlimited people, and so it is kind of a tradeoff, it's a tradeoff between how do we get these things processed and get them out quickly versus how much time do we take verifying Social Security numbers, verifying addresses, and verifying those types of issues.

So I kind of have a question for the whole panel individually, but really as you look at that balance, that tradeoff between getting the returns out quickly versus being more thorough and more investigative, my question is, are we at that right balance or do you think it should be shifted one way or the other?

Mr. GEORGE. Let me start by quickly saying, as you are aware, sir, the IRS recently released its most recent figure on what is called the tax gap, the amount of money owed, not paid on time by the taxpayer in full, without the IRS having to take some compliance action. That is estimated at $400 billion per year, and I submit to you that that is a low ball estimate because it doesn't include other aspects, meaning international dollars involved, tax dollars involved and the like. So while we are talking billions here, and in my mind that is still a heck of a lot of money, much more needs to be done, much more can be done. As we discussed during the course of this hearing, some require legislative fixes, others are just, we believe, procedural/policy decisions, changes that the IRS can make. Some need to be done in conjunction with other agencies, as was pointed out by one of the members earlier. It is so disconcerting, so frustrating for someone to have their identity stolen and not be able to get a student loan, and yet the IRS is not in a position to help resolve that aspect of the problem.

So there needs to be more, you know, mutual interaction between Federal agencies, and again, using common sense as we have discussed during the course of this hearing.

Mr. BERG. Thank you.

Mr. O'CARROLL. Mr. Berg, just—probably the one thing I always like to always remind when we are talking here about the benefits as opposed to the returns, on the benefits side, we are always saying that stewardship and using risk-based approaches to make sure that the right person is getting the benefit for it; that their information isn't being taken and their benefits are being diverted to the wrong, you know, through fraud or whatever. So we always say that the biggest issue with the Social Security is that balance between service and stewardship. And our biggest one is that you always have to focus on the stewardship, no matter what the budgets are or anything else, is just to make sure that due diligence is out there so that the right people are getting the right benefits.

Mr. MILLER. Congressman, in terms of the balance, I don't know whether it is the right balance at this point. That is exactly, we are on the cusp of having that discussion, and we should have that discussion. I will say a couple of things a we think about that discussion.

If you think that we have 2.6 million fraudulent returns to date, that is against a very large number of returns, you know, the 90 plus million refund returns, so far. And so we have to think about that. And we also have to think about the fact that some people really do, I mean, when their refunds are late, these people are relying on them for some, at the lower end of our income spectrum, these people are—it is the largest payment they receive in a year. And to change their expectations around that is not—is no small thing. And those are things we are going to have to think about and talk about, and I would welcome you all to be a part of that discussion, obviously.

Ms. OLSON. I agree with what Mr. Miller said. I think that it is a very delicate decision, and that is really why I was raising it. I think that the IRS in the filing season can do better talking to taxpayers and explaining to them the risk of identity theft, and explaining to them through releases and conversations the steps that we are taking and why there might be delays. And I think if we educate taxpayers better, we can tamp down a little bit that hysteria, that clutching in the throat, you know, about if their refund gets caught up in there.

I think the IRS is taking a lot of steps that are very positive in this, and I think some of the work that they are doing trying to get the W-2 information earlier in the process in a form where they can process returns going, you know, that as they come in, against this information, also helps us protect things without creating too much more of a delay. So I think there is some things that they are doing in the right direction before we have gotten the balance that we need.

Mr. BERG. Thank you.

Mr. BLACK. I will take the balance of your time and thank you for recognizing me as a native from the great State of North Dakota. As the IG from SSA recognizes, the Social Security Administration also struggles with this balance of getting the right benefit to the right person at the right time, and we have tried to balance that approach with better use of technology to do that work, as well as a better use of technology to match data with other agencies so that we can prevent things like fraud from happening up front.

Mr. BERG. Thank you. Mr. Chairman, I yield back.

Chairman BOUSTANY. I want to thank all the witnesses for coming here today and providing your testimony. This has been a very helpful hearing for us. I want to remind each of you that members may have additional questions that they will submit or may submit and that those questions and your answers will be made part of the official record. And with that, this hearing is now adjourned.

[Whereupon, at 12:01 p.m., the subcommittees were adjourned.]

## Member Submissions For The Record

**The Honorable Sam Johnson #1**

**NBC WTHR 13**
**Tax loophole costs billions**
*Posted: Apr 26, 2012 9:55 PM EDT Updated: Jul 05, 2012 10:03 AM EDT*
By Bob Segall

***Millions of illegal immigrants are getting a bigger tax refund than you. Eyewitness News shows a massive tax loophole that provides billions of dollars in tax credits to undocumented workers and, in many cases, people who have never stepped foot in the United States. And you are paying for it!***

INDIANAPOLIS - Inside his central Indiana office, a longtime tax consultant sits at his desk, shaking his head in disbelief.

"There is not a doubt in my mind there's huge fraud taking place here," he said, slowly flipping through the pages of a tax return.

The tax preparer does not want you to know his name for fear of reprisal, but he does want you to know about a nationwide problem with a huge price tag.

He came to 13 Investigates to blow the whistle.

"We're talking about a multi-billion dollar fraud scheme here that's taking place and no one is talking about it," he said.

The scheme involves illegal immigrants -- illegal immigrants who are filing tax returns.

**How it works**

The Internal Revenue Service says everyone who is employed in the United States – even those who are working here illegally – must report income and pay taxes. Of course, undocumented workers are not supposed to have a social security number. So for them to pay taxes, the IRS created what's called an ITIN, an individual taxpayer identification number. A 9-digit ITIN number issued by the IRS provides both resident and nonresident aliens with a unique identification number that allows them to file tax returns.

While that may have seemed like a good idea, it's now backfiring in a big way.

Each spring, at tax preparation offices all across the nation, many illegal immigrants are now eagerly filing tax returns to take advantage of a tax loophole, using their ITIN numbers to get huge refunds from the IRS.

The loophole is called the Additional Child Tax Credit. It's a fully-refundable credit of up to $1000 per child, and it's meant to help working families who have children living at home.

But 13 Investigates has found many undocumented workers are claiming the tax credit for kids who live in Mexico – lots of kids in Mexico.

"We've seen sometimes 10 or 12 dependents, most times nieces and nephews, on these tax forms," the whistleblower told Eyewitness News. "The more you put on there, the more you get back."

The whistleblower has thousands of examples, and he brought some of them to 13 Investigates. While identifying information such as names and addresses on the tax returns was redacted, it was still clear that the tax filers had received large tax refunds after claiming additional child tax credits for many dependents.

"Here's a return right here: we've got a $10,3000 refund for nine nieces and nephews," he said, pointing to the words "niece" and "nephew" listed on the tax forms nine separate times.

"We're getting an $11,000 refund on this tax return. There's seven nieces and nephews," he said, pointing to another set of documents. "I can bring out stacks and stacks. It's just so easy it's ridiculous."

**20 kids = $30,000**

WTHR spoke to several undocumented workers who confirmed it *is* easy.

They all agreed to talk with WTHR investigative reporter Bob Segall and a translator as long as WTHR agreed not to reveal their identity.

One of the workers, who was interviewed at his home in southern Indiana, admitted his address was used this year to file tax returns by four other undocumented workers who don't even live there. Those four workers claimed 20 children live inside the one residence and, as a result, the IRS sent the illegal immigrants tax refunds totaling $29,608.

13 Investigates saw only one little girl who lives at that address (a small mobile home). We wondered about the 20 kids claimed as tax deductions?

"They don't live here," said the undocumented worker. "The other kids are in their country of origin, which is Mexico."

He later explained none of the 20 children have ever visited the United States – let alone lived here.

So why should undocumented workers receive tax credits for children living in a foreign country, which is a violation of IRS tax rules?

"If the opportunity is there and they can give it to me, why not take advantage of it?" the worker said.

Other undocumented workers in Indiana told 13 Investigates the same thing. Their families are collecting tax refunds for children who do not live in this country. Several of the workers told WTHR they were told it was legal for them to claim the tax credit for a child who does not live in the United States.

**IRS was repeatedly warned**

"The magnitude of the problem has grown exponentially," said Russell George, the United States Department of Treasury's Inspector General for Tax Administration (TIGTA).

And he says the IRS has known about the problem for years.

George has repeatedly warned the IRS that additional child tax credits are being abused by undocumented workers. In 2009, his office released an audit report that showed ITIN tax filers received about $1 billion in additional child tax credits. Last year, the inspector general released a new report showing the problem now costs American tax payers more than $4.2 billion.

"Keep in mind, we're talking $4 billion per year," he said. "It's very troubling."

What George finds even more troubling is the IRS has not taken action despite multiple warnings from the inspector general.

"Millions of people are seeking this tax credit who, we believe, are not entitled to it," said the inspector general. "We have made recommendations to [IRS] as to how they could address this, and they have not taken sufficient action in our view to solve the problem."

Other information obtained from the TIGTA audits include:

· Claims for additional child tax credits by ITIN filers have skyrocketed during the past decade, from $161 million in 2001 to $4.2 billion in tax year 2010.

· Undocumented workers filed 3.02 million tax returns in 2010. 72% of those returns (2.18 million) claimed the additional child tax credit.

· In 2010, the IRS owed undocumented workers more in claimed additional child tax credits than it collected from those workers in taxes.

**Agency responds – sort of**

What does the IRS have to say about all this?

The agency sent WTHR a statement, defending its policy of paying tax credits to illegal immigrants.

"The law has been clear for over a decade that eligibility for these credits does not depend on work authorization status or the type of taxpayer identification number used. Any suggestion that the IRS shouldn't be paying out these credits under current law to ITIN holders is simply incorrect. The IRS administers the law impartially and applies it as it is written," the statement said.

George disagrees with that position and believes the IRS should be doing more to prevent undocumented workers from getting billions in US tax dollars.

"The IRS is not doing something as simple as requesting sufficient documentation from people seeking this credit," he said. "Once the money goes out the door, it's nearly impossible for the IRS to get it back."

Over the past month, WTHR has tried to ask the IRS more questions about its efforts to prevent abuse involving additional child tax credits.

Despite repeated phone calls, e-mails and a visit to IRS headquarters in Washington, the agency said none of its 100,000 employees had time to meet with 13 Investigates for an interview. An IRS spokeswoman said all staff were too busy because of the tax filing deadline in mid-April.

Apparently, the IRS doesn't have time to respond to some tax preparers, either.

Last year, our whistleblower noticed dozens of undocumented workers had used phony documents and false income to claim tax credits. He reported all of it to the IRS.

"These were fraudulent, 100% fraudulent tax returns, but I got no response; absolutely none. We never heard a thing," he said. "To me, it's clear the IRS is letting this happen."

The IRS tells WTHR it can do nothing to change the current system unless it gets permission from Congress. In other words, according to the IRS, closing the loophole would require lawmakers to pass a new law specifically excluding illegal immigrants from claiming additional child tax credits.

The big questions now: Is Congress willing to do that?

**Full statement to WTHR from the Internal Revenue Service**

The law has been clear for over a decade that eligibility for these credits does not depend on work authorization status or the type of taxpayer identification number used. Any suggestion that the IRS shouldn't be paying out these credits under current law to ITIN holders is simply incorrect. The IRS administers the law impartially and applies it as it is written. If the law were changed, the IRS would change its programs accordingly.

The IRS disagrees with TIGTA's recommendation on requiring additional documentation to verify child credit claims. As TIGTA acknowledges in this report, the IRS does not currently have the legal authority to verify and disallow the Child Tax Credit and the Additional Child Tax Credit during return processing simply because of the lack of documentation. The IRS has procedures in place specifically for the evaluation of questionable credit claims early in the processing stream and prior to issuance of a refund. The IRS continues to work to refine and improve our processes.

http://www.wthr.com/story/17798210/tax-loophole-costs-billions

---

**The Honorable Sam Johnson #2**

**New York Times**
**Restricting Tax Credits**
**Letter**
**Published: February 7, 2012**

**To the Editor:**

Re "A Harder Squeeze on the Poor" (editorial, Jan. 31):

A recent government report reveals that in 2010, the Internal Revenue Service awarded $4.2 billion in taxpayer dollars to illegal immigrants through the refundable additional child tax credit. That's just wrong. American taxpayers should not have to pay for benefits for illegal immigrants.

The earned income tax credit, a refundable tax credit for low-income workers, requires a Social Security number for eligibility. Defying logic, the child tax credit does not.

This is a bipartisan issue, as evidenced by Senator Claire McCaskill's call to the Internal Revenue Service last fall to immediately end the fraudulent child tax credit payments.

We need to stop illegal immigrants from taking money out of hard-working American taxpayers' pockets every year by claiming this credit. My bill requiring a Social Security number does that.

SAM JOHNSON
Washington, Feb. 2, 2012

*The writer, a Republican, represents the Third Congressional District of Texas.*

http://www.nytimes.com/2012/02/08/opinion/restricting-tax-credits.html?_r=2

---

**The Honorable Adrian Smith**

**"I'm not dead!" Student fights to prove he's alive**
by Josh Egbert
Story Created: Apr 30, 2012 at 5:57 PM CDT
Story Updated: May 1, 2012 at 9:42 AM CDT

A local high school senior is set to graduate and is preparing for college. But at a time when most teenagers are having fun and looking forward to the future, his plans are on hold.

A simple trip to the bank revealed a couple alerts on Corbin Russell's credit score and those alerts have his future in jeopardy.

Life was good for Corbin Russell. The Harvard High School senior will graduate in just a few days and this fall go to college. But those college plans may be derailed.

"I had been dead for the past couple of years," said Corbin.

A simple trip to the bank to get a car loan had turned Corbin's world upside down.

"I was shocked. I really couldn't believe it because I had been getting a bunch of tax returns back from when I was working," Corbin said.

His social security number came back flagged.

"After they ran a credit check score, it came back with a couple alerts," said Corbin.

Corbin's social security number had been used in a death benefit claim for a man in South Carolina who died in January of 2010.

"Without my social security number credit being correct, right now they have it red flagged. Without it being correct I can't get a loan because I'm deceased," said Corbin.

"How could anybody have death benefits on a senior in high school?" said Corbin's mother Monica Russell.

Now the problem has gone beyond just that car loan.

College scholarship applications have been rejected because of the flagged credit report. And he can't get student loans without a valid Social Security number.

"My social security number - if someone just took a couple minutes of their time and said, hey, look, this social security number doesn't match with this person, we need to fix this, everything could be fixed," said Corbin.

But that could take some time.

"In some cases it's taken two years and he can't go to college until it's fixed," said Monica.

Which has Corbin's mom Monica worried about his future.

"The only thing that scares me is if he waits two years will he still want to go," Monica said.

The family has been trying to get the issue fixed, talking with the Federal Trade Commission and the Social Security Administration in Seattle Washington, but so far, nothing.

"That's all I do is cry on the phone because I can't get nowhere," said Monica.

Corbin will start college in September and with a price tag of nearly $40,000 and no way to get a loan.

"I really want to try and make it through it, but it may come down to the fact I have to wait a year or two before I can even go before they get it fixed," said Corbin.

News 5 spoke with the Social Security administration Monday. In their records, Corbin in alive and well. The issue lies with the credit bureau.

The three major credit companies say it can be fixed, but they need documentation, to eradicate the situation.

The only problem is that it could take time and time is not on Corbin's side when it comes to school.

News 5 also spoke with Senator Johanns office, they were able to get Corbin's Free Application for Student Aid form approved, which pays for about 1/3 of his school.

http://www.khastv.com/news/local/f-149577885.html

**The Honorable Xavier Becerra #1**

**New York Times**
**A Harder Squeeze on the Poor**
Editorial
Published: January 30, 2012

House Republicans have hit upon a noxious scheme to help pay for an extension of the payroll tax cut: a tax increase on millions of poor working families. A bill passed by the House and now in conference seeks to deny cash refunds under the child tax credit to those who file tax returns using "individual taxpayer identification numbers" issued by the Internal Revenue Service. Only those using Social Security numbers would be eligible.

The refundable portion of the child tax credit is a life-saver for the working poor. Families that would be cut off by this policy change make an average of $21,000 per year, according to the Treasury Department. They would lose an average of $1,800. About 80 percent of those families are Hispanic. The taxpayer identification numbers are used frequently, though not exclusively, by unauthorized immigrants to pay the taxes because they are not eligible for Social Security numbers. The I.R.S. accepts their tax payments and allows families to claim the child tax credit regardless of immigration status. This policy is an effective antipoverty tool that protects children, most of whom are American-born citizens.

The Republicans who have flatly rejected tax increases on the rich have settled instead on limiting this refund, which kept about 1.3 million children from falling into poverty in 2009.

Leaving aside the cruelty of squeezing the poorest workers for a greater portion of their wages to make a point about illegal immigration, the bill punishes not just the undocumented, but the communities they live in, because a poor family's hard-earned wages get spent: on things like groceries, child care, utilities, gas and rent. This would be the bottom line of the House bill: a Congress that has failed for years to fix the immigration system, using its failure to harm children and hurting those at the bottom of the ladder to avoid the slightest pressure on millionaires. The Senate would be mad to go along with it.

http://www.nytimes.com/2012/01/31/opinion/a-harder-squeeze-on-the-poor.html?_r=1

**The Honorable Xavier Becerra #2**

*Committee on Domestic Justice and Human Development*
3211 FOURTH STREET NE • WASHINGTON DC 20017-1194 • 202-541-3160
WEBSITE: WWW.USCCB.ORG/JPHD • FAX 202-541-3339

April 17, 2012

The Honorable Dave Camp
Chairman
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Sander M. Levin
Ranking Member
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C.20515

Dear Chairman Camp and Ranking Member Levin:

As you prepare your response to the reconciliation instructions contained in the Fiscal Year 2013 budget resolution, I wish to renew our strong opposition to unfair proposals that would alter the Child Tax Credit to exclude children of hard-working, immigrant families.

The bishops' conference has long supported the Child Tax Credit because it is pro-work, pro-family, and one of the most effective antipoverty programs in our nation. In 2009, 2.3 million people, including 1.3 million children, were kept out of poverty by the Child Tax Credit. Proposals to deny the credit to children of working poor immigrant families--the large majority of whom are American citizens--would hurt vulnerable kids, increase poverty, and would not advance the common good. To exclude these children who are American citizens from the Child Tax Credit is unjust and wrong. We urge you to actively and publically oppose such measures.

The *Compendium of the Social Doctrine of the Church* clearly states the importance of ensuring that workers make a family wage, "a wage sufficient to maintain a family and allow it to live decently. . . . There can be several different ways to make a family wage a concrete reality. Various forms of important social provisions help to bring it about, for example, family subsidies and other contributions for dependent family members. . ." (no. 250).

The Child Tax Credit is a clear example of this. We must protect those programs that help low-income workers escape poverty and raise their children in dignity.

If you must find savings, I urge you to consider cuts that will not harm poor and vulnerable families and to refrain from cutting essential programs such as the Child Tax Credit.

Sincerely,

Most Reverend Stephen E. Blaire
Chairman
Committee on Domestic Justice and Human Development

**Witness Inserts For The Record**

**Steven T. Miller**

Steve Miller (IRS Witness)
Transcript Insert: Page 80
Hearing on Identity Theft and Tax Fraud on May 8, 2012
The Subcommittees on Social Security and Oversight

A tax refund is mailed to the address on the tax return. One indicator of possible identity theft fraud is a number of refunds directed toward the same address. This action may suggest that the person committing fraud is filing multiple tax returns; possibly using multiple social security numbers; but is using one mailing address to get refunds. Or, as Mr. Marchant described, a tax practitioner might be using the practitioner's address on the tax returns and direct the refund checks to the practitioner's business address. While it is legal for practitioners to have tax refund checks directly deposited into their business account as a service to their clients; it may cause confusion with the taxpayer's future returns as the address that the IRS uses to correspond with the taxpayer is the last address on record. In this example, the last address on record would be the tax practitioner's address.

**David F. Black**

Insert for the Record – page 58:

All representative payees (except for certain State mental institutions), including State Foster Care agencies, are required to submit an annual report accounting for the use of beneficiary funds. In addition to these annual reports, we conduct several other reviews to monitor the performance of agencies that serve as payees for our beneficiaries. These include periodic site reviews of agencies that serve 50 or more beneficiaries, reviews of payees not scheduled or selected for a periodic site review, and targeted reviews conducted in response to a "trigger" event such as a beneficiary or third party complaint of benefit mishandling.

We provide ongoing education and support to individuals and organizations that serve as payees. We provide our field personnel with updated program instructions that help them conduct thorough reviews and address cases of misuse correctly. We recently updated the "Guide for Organizational Representative Payees" to provide more information about how to manage benefits and we keep our representative payee website up to date with useful information for payees.

In general, our experience with State foster care agencies that serve as payee has been good. Our review of their reports shows that they use the benefits they receive properly – to meet the needs of the child. We promptly and thoroughly investigate any problems, and take necessary action based on what we find in those investigations.

**Questions For The Record**

**The Honorable J. Russell George**

**Committee on Ways and Means**
**Subcommittees on Oversight and Social Security**
**QFRs from May 8, 2012 hearing on Identity Theft and Tax Fraud**

1. **How can the Internal Revenue Service (IRS), the U.S. Treasury Inspector General for Tax Administration (TIGTA), and other law enforcement work to catch criminals sooner? Are there additional tools that you need which would require legislative action?**

   Reducing identity theft-related tax fraud and detecting it sooner is a growing challenge. In many cases, the IRS and TIGTA are not aware that an identity theft-related fraudulent refund has been issued until the victim taxpayer notifies authorities or the criminals are caught trying to negotiate the fraudulent refunds. This can often be months or even years after the initial crime has occurred, making it even more difficult to address.

   No single law enforcement agency possesses the necessary resources to curtail, through classic criminal investigation and prosecution methods, the current increase in identity theft. TIGTA has a limited number of criminal investigators to cover our broad law enforcement jurisdiction and mission. We have directed our management team to coordinate with their counterparts in IRS Criminal Investigation to address identity theft-related tax fraud that falls within TIGTA's jurisdiction. TIGTA investigates identity theft when an IRS employee is involved in the scheme or uses their access to taxpayer identity information to commit the crime. TIGTA also has jurisdiction if a tax preparer steals client information in furtherance of an identity theft scheme or if an individual or group impersonates the IRS to carry out identity theft schemes.

   The best way to prevent the identity theft epidemic would be to ensure the IRS has the necessary information and time to better identify and stop the fraudulent refund before it is issued. Once a fraudulent refund is issued by the IRS, the prospects of recovering the erroneous refund are significantly diminished.

   In addition, the IRS can expand the use of information gathered from known identity theft cases to improve identity theft fraud screening tools. These tools are used to identify questionable tax returns for further review before tax refunds are issued.

   The IRS is currently working with the Department of Justice to pilot an approach in Florida of providing to local law enforcement, with the victim's consent, information from the return that was filed by the suspected identity thief. This would help local law enforcement identify those who may be part of a criminal enterprise involving identity theft-related tax fraud.

   Regarding possible legislative changes, the IRS can significantly improve the detection of false tax returns and the issuance of fraudulent tax refunds if it had

access to third-party income and withholding documents at the time tax returns were filed. Employers and other businesses are not required to file income and withholding documents until the end of February (end of March, if filed electronically), which is well after individuals start filing their tax returns.

As an alternative to the income and withholding documents, the IRS could benefit from expanded access to the Department of Health and Human Services' National Directory of New Hires (NDNH). Such access would enable the IRS to verify income for many individuals at the time tax returns are filed and before tax refunds are paid. The IRS has included a request for expanded access to the NDNH in its past annual budget submissions, including those for Fiscal Years 2010, 2011, and 2012. The request was made as part of the IRS's efforts to strengthen tax administration. However, expanded access has not been provided for in the law. The IRS has again included a request for expanded access to the NDNH as part of its Fiscal Year 2013 budget submission.

2. **Your testimony indicates that identity theft is growing and will be with us for the foreseeable future. Has this year been the largest year ever for attempts at tax fraud through identity theft? Do you see this trend continuing in the years ahead?**

   Yes, based on IRS statistics, it appears to be the largest year for attempts at tax fraud through identity theft. Since Calendar Year 2009, when the IRS began tracking identity theft incidents, the number of incidents of identity theft that the IRS identified has grown from about 366,000 in Calendar Year 2009 to over 1 million in Calendar Year 2011. Unfortunately, it does appear that the trend will continue for the foreseeable future.

   Additionally, using characteristics from tax returns the IRS identified and confirmed as filed by identity thieves, we identified approximately 1.5 million additional undetected Tax Year 2010 tax returns with potentially fraudulent tax refunds totaling in excess of $5.2 billion. Combined with the identity theft the IRS was able to detect, this indicates individuals used stolen identities to file approximately 2.4 million false tax returns and claimed $11.7 billion in potentially fraudulent tax refunds in Tax Year 2010.

3. **Your report indicates the only way to deal with this crime is to act offensively to thwart the criminal from the start. Once it gets to the IRS, chances are the criminal is going to be rewarded with a refund. Do you have any other suggestions for stopping ID theft related tax fraud, particularly like those thefts that occurred in Florida and Puerto Rico?**

   To effectively combat identity theft, several aspects need to be addressed: real-time access to income and withholding documents at the time tax returns are

filed, improving the IRS's ability to detect the fraudulent claims for refund prior to issuing tax refunds, continued collaborative law enforcement intervention that targets those cases that send the strongest deterrent message, and ensuring that the victim taxpayer's IRS tax accounts are timely resolved and corrected.

The IRS should also work with financial institutions to improve authentication controls for the direct deposits of tax refunds, including deposits to debit cards. In addition, the IRS needs to limit the number of tax refunds that can be deposited to one bank account or debit card and implement Treasury regulations requiring Federal tax deposits to be made only to accounts in the taxpayer's name.

The IRS implemented a number of initiatives during the 2012 Filing Season to improve the detection and prevention of fraudulent tax refunds from identity theft. These include new identity theft screening filters. The IRS also expanded the use of deceased taxpayer account locks and Identity Protection Personal Identification Numbers (IP PINs) to deter identity theft and prevent victims of identity theft from being victimized again. The IRS stated that it worked with the Social Security Administration to obtain records of Social Security benefits paid and the associated withholding earlier than in the past and is now using this information to verify tax returns as they are filed. The IRS has also initiated efforts to improve its ability to recover questionable tax refunds held by financial institutions. We have not yet audited these new initiatives, but plan to do so in the next fiscal year.

**4. Your report sates it can take the IRS more than one year to resolve an identity theft case. Is that a best-case scenario or is there a range?**

The time it takes to resolve identity theft cases is calculated using a range and is dependent on various factors, including the actual time an IRS assistor has to work a case to the time it takes the taxpayer to respond to IRS requests for information. The IRS does not have standards for how long it should take to work identity theft cases. Each function and office that works identity theft cases sets its own standards.

The IRS calculated that it took an average of 234 days to resolve identity theft cases involving duplicate tax returns in Calendar Year 2011. However, the system the IRS used to track and manage the majority of identity theft cases was implemented as an inventory control system, not to track and work the complex identity theft taxpayer correspondence cases. The IRS calculated the time from when it received the correspondences to the time when the case is closed. However, one taxpayer's case may be opened and closed multiple times as it changes case category codes (category codes denote the source of the case). This will skew the results.

Our review of a judgmental sample of 17 unique taxpayer cases classified as identity theft and originating in five functions showed:

- Case resolution averaged 414 days; cases were open from three to 917 days. Time was calculated from the date a taxpayer's case(s) was first opened until the last day when the case(s) closed.[1] This does not include the additional time after a case is closed for the taxpayers to receive any applicable tax refunds.
- Inactivity on cases averaged 86 days; inactivity ranged from 0 to 431 days.
- Concerning these 17 taxpayers, the IRS opened 58 different cases and assigned multiple assistors to work each case. The case histories did not state why the cases were reassigned. However, it appears that the cases were reassigned to manage inventory, i.e., reassigned to an assistor who had fewer cases in his or her inventory. Additionally, when the IRS received new documentation from the taxpayer or another IRS office, a new case was opened rather than the documentation correctly linked to the existing case. We made numerous recommendations, which should help the processes.

**5. What can the IRS do to better assist victims and reduce the time to resolve their cases? What has the IRS done to address the problems identified by TIGTA and the Taxpayer Advocate?**

In our May 2012 audit report,[2] we reported that communications between identity theft victims and the IRS were limited and confusing, and victims were asked multiple times to substantiate their identity. We recommended that the IRS conduct an analysis of the letters sent to taxpayers regarding identity theft and ensure that taxpayers are notified when the IRS has received their identifying documents.

Most identity theft cases involving individual duplicate tax returns are worked by the IRS's Accounts Management function. IRS employees who work in the Accounts Management function are assistors, who also spend hours working the telephones responding to taxpayer requests as well as working paper cases. However, Accounts Management function assistors are not examiners and are not trained to conduct examinations. We recommended that the IRS create a specialized unit in the Accounts Management function to exclusively work identity theft cases.

In August 2011, the IRS issued the *Identity Theft Program Future State Report*,[3] which provides its vision for the future state of the Identity Theft Program. It plans to reorganize to have an Identity Theft Program Specialized Group within each of the business units and/or functions, strengthen roles and responsibilities of the office responsible for the Identity Theft Program, and begin collecting IRS-wide

[1] Some taxpayers had multiple cases open involving more than one tax year.
[2] TIGTA, Ref. No 2011-40-050, *Most Taxpayers Whose Identities Have Been Stolen Do Not Receive Quality Customer Service* (May 2012).
[3] IRS, *IRS Identity Theft Program Future State Report* (Aug. 2011).

identity theft data to assist in tracking and reporting the effect of identity theft on tax administration. The IRS has begun revising guidelines and providing training for employees who interact with identity theft victims and work identity theft cases. In Fiscal Year 2012, the IRS plans to begin collecting IRS-wide identity theft data to be used to oversee the Identity Theft Program and issue a report to stakeholders.

The IRS also took a number of steps in the 2012 Filing Season to detect identity theft tax refund fraud before it occurs. These efforts included designing new identity theft screening filters that the IRS indicates will improve its ability to identify false tax returns before those tax returns are processed and prior to issuance of a fraudulent tax refund. As of April 19, 2012, the IRS had stopped the issuance of approximately $1.3 billion in potentially fraudulent tax refunds as a result of the new identity theft filters.

In addition, the IRS expanded efforts to place identity theft indicators on taxpayer accounts to track and manage identity theft incidents. For example, at the initiation of the 2012 Filing Season, the IRS and the U.S. Department of Justice announced the results of a massive nationwide crack down on suspected identity theft perpetrators as part of stepped-up efforts to combat tax refund fraud. This national effort is part of a comprehensive identity theft strategy by the IRS that is focused on preventing, detecting, and resolving identity theft cases as quickly as possible.

The IRS expanded its efforts to prevent the payment of fraudulent tax refunds claimed using deceased individuals' names and Social Security Numbers. Similar to last filing season, the IRS placed a unique identity theft indicator on deceased individuals' tax accounts. The indicator alerts the IRS when a tax return is filed using the deceased individual's Social Security Number. According to the IRS, as of March 31, 2012, the IRS placed a deceased lock on more than 164,000 tax accounts and has prevented approximately $1.8 million in fraudulent tax refunds claimed using deceased individuals' identities since the lock was established.

Once identity thieves successfully use an identity to obtain a fraudulent tax refund, they often attempt to reuse the identity in subsequent years to continue to file fraudulent tax returns. To prevent recurring identity theft, the IRS places an identity theft indicator on each tax account for which it has determined an identity theft has occurred. All tax returns filed using the identity of a confirmed victim of identity theft are flagged during tax return processing and sent for additional screening before any tax refund is issued. This screening is designed to detect tax returns filed by identity thieves who attempt to reuse a victim's identity in subsequent years and to prevent the issuance of fraudulent tax refunds.

Finally, the IRS is issuing the IP PIN to selected victims of identity theft. The IP PIN tells the IRS that the tax return was filed by the legitimate taxpayer and bypasses additional screening for identity theft, thus reducing delays in issuing the tax refund. The IRS issued an IP PIN to 251,568 individuals for the 2012 Filing Season and plans to issue an IP PIN to all taxpayers with identity theft indicators on their accounts for the 2013 Filing Season.

**6. Are the victims notified?**

The IRS notifies some victims of identity theft. The IRS has processes in place to detect multiple filings of tax returns using the same Social Security Number. When the IRS detects a tax return that uses a Social Security Number that has already been used to file a tax return, it notifies the taxpayer that the Social Security Number has already been used. The IRS then begins research to determine which tax return is the valid filing. However, the IRS does not tell the taxpayer that he or she may be the victim of identity theft.

Instead, when the taxpayer's tax return is rejected, the taxpayer is asked to complete Form 14039, *Identity Theft Affidavit*, and mail it with a paper tax return to the IRS. Once the IRS receives the paper tax return, a technician enters the data into the IRS's computer system, and forwards the tax return and affidavit to assistors who determine if it is an identity theft case and attempt to resolve it.

However, many identities that are used for tax refund fraud involve those individuals who do not have a tax return filing requirement. Since these individuals do not file a tax return, the IRS may only receive the false tax return filed by the identity thief and may not realize that the legitimate taxpayer's identity has been stolen. In these situations, the legitimate taxpayers may never know that they have been victims of tax-refund-fraud identity theft.

**7. Should State and local law enforcement have access to taxpayer information, such as refund data, in pursuing identity theft cases? Why or why not?**

An identity theft victim may consent to the disclosure of the false return filed by the alleged identity thief to State and local law enforcement agencies. As mentioned above, the IRS is currently piloting an approach in Florida of providing to local law enforcement, with the victim's consent, information from the return that was filed by the suspected identity thief.

Whether State and local law enforcement should have expanded access to information without the consent of the identity theft victim, or access to other investigative information currently protected by the confidentiality provisions of the Internal Revenue Code, is a question of tax policy and, pursuant to Treasury Order 111-01, should be posed to the Department of the Treasury's Office of Tax Policy.

**8. Can you comment on the content of the returns that are resulting in fraudulent refunds through identity theft? Are these individuals claiming that they paid more taxes than were due, or are they generally claiming refundable tax credits, such as the Earned Income Tax Credit and Additional Child Tax Credit?**

The common characteristic of the approximately 1.5 million confirmed identity theft cases and the additional tax returns TIGTA identified is that false income and sufficient withholding were reported on the tax return to generate a refund. Without the false income, many of the deductions and/or credits used to inflate the fraudulent tax refund could not be claimed on the tax return.

The top credit claimed was the Making Work Pay Credit (73 percent of the identity theft cases). Most of the returns involving tax fraud refund identity theft identified for Tax Year 2010 received this credit. After the Making Work Pay Credit, 36 percent claimed the Earned Income Tax Credit, and 20 percent claimed the Additional Child Tax Credit. A small percentage (less than 1 percent) claimed the First-Time Homebuyer's Credit.

Direct deposit, which now includes debit cards,[4] is often used by identity thieves to obtain fraudulent tax refunds. Of the 1.5 million confirmed identity theft tax returns, 1.2 million (82 percent) used direct deposit to obtain potentially fraudulent tax refunds totaling approximately $4.5 billion, according to an upcoming TIGTA audit report.

**9. Law enforcement and Federal prosecutors make decisions on what cases to pursue based on competing priorities and varying levels of fraud. People hear of the $130 million cases being pursued, but how much of this problem exists at lower levels - $5,000 in fraud or $20,000 in fraud – and are these cases vigorously pursued? Do prosecutors only get interested when fraud reaches the incredible levels we read about in newspapers?**

The Department of Justice has established general criteria for Federal prosecutions. The criteria are largely based upon the Department of Justice annual prosecution priorities along with each United States Attorney's Office's available resources.

The substantial growth in this form of crime has quickly outstripped available resources. Based on such limitations, the role of Federal law enforcement is to select those cases that will have a broad impact on the criminal activity and that will send a strong deterrent message. The Department of Justice is also challenged with ensuring that they bring significant prosecutions throughout their spectrum of prosecution priorities and consistent with their available resources.

[4] These include prepaid debit cards as well as reloadable cards.

In addition, there do not appear to be any significant proposed increases in future budget years for additional investigative or attorney resources to address the challenges of the increasing identity theft criminal activity.

**Questions from Congressman Tom Reed:**

**10. I have submitted an article from a Florida newspaper for the record that reports that most fraudulent IRS refunds are made on prepaid debit cards. I am concerned that the government is moving to the debit card payments system, not only for tax refunds, but all government payments before adequate measures to prevent fraud are in place. Are you aware of any analysis or studies that were available to Treasury or completed by Treasury outlining the hazards versus the benefits of debit card and electronic payments rather than paper checks?**

We contacted the Department of the Treasury for its response to this question. Its response is as follows:

*There are documented instances of fraudulent enrollments resulting from various identify theft scams where the perpetrator obtains sufficient information about the legitimate beneficiary. Similar fraud has occurred with other prepaid card providers and affiliated financial institutions.*

*As widely reported in the media, fraudsters use various techniques including lottery scams to obtain banking and other personal information needed to make unauthorized changes to direct deposit enrollments. Identify theft can also occur when a paper check is stolen from a recipient's mailbox.*

*Statistics show that electronic payments remain substantially safer than paper checks and are part of the reason why the Treasury Department has been promoting Direct Deposit for over 30 years and is currently moving to an all-electronic environment. In FY 2011, Treasury issued approximately 106 million Social Security and Supplemental Security Income checks. Of those checks, 440,000 or .0042% were reported lost or stolen and had to be replaced. As a comparison, that same year, Treasury issued over 661 million Social Security and Supplemental Security Income direct deposit payments, including many to prepaid cards. For example, the 4,007 fraud cases reported for Treasury's Direct Express program represent a tiny fraction of all direct deposit payments and the over 18 million Direct Express deposits made last year. Additionally, this past year, $70 million worth of Treasury-issued checks were fraudulently endorsed vs. the approximate $1.8 million reported with the Direct Express fraud cases (of which $900,000 has already been recovered). The reported fraud cases associated with the electronic payments*

*represent a tiny fraction when compared to those associated with the significantly lower volume of checks.*[5]

**11. What plans did Treasury have ready to address the crime of identity theft when they promulgated their regulation?**

We contacted the Department of the Treasury for its response to this question. Its response is as follows:

*Treasury is working closely with Comerica Bank (Treasury's financial agent for Direct Express) and SSA on efforts related to fraud detection, the monitoring of phishing scams, and other mitigating actions to reduce the occurrence of fraudulent enrollments. This includes suspending website enrollment functionality, flagging suspicious accounts, implementing more stringent processes for authenticating individuals enrolling and changing addresses and shifting enrollments to alternate channels with more stringent authentication.*[6]

**12. In your testimony, you recommend Treasury establish policies ensuring that only those institutions that can authenticate the identities of the card users be permitted in the debit card program for purposes of tax refunds. Can you expand on your suggestion? Should that same policy be used for payment of government benefits? Do you have other suggestions for protecting payment of benefits from identity theft?**

We believe a policy which addresses both authenticating the identity of the card user and ensuring that the tax refund is deposited to an account only in the name of the individual is needed. Such a policy would help ensure that the Federal Government can identify and verify that the correct taxpayer will receive the tax refund. A broader policy for all government benefits would have the same effect; however, it is beyond the scope of our authority to make such a recommendation for all government benefits.

In a September 2008 report, we found that the IRS was not in compliance with direct deposit regulations that require tax refunds to be deposited to an account only in the name of the individual listed on the tax return.[7] The IRS still has not developed sufficient processes to ensure tax refunds are deposited to an account in the name of the filer. We recommended that the Department of the Treasury coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that tax refunds issued via direct deposit to either a bank

[5] U.S. Department of the Treasury, Office of Financial Access, Financial Education, and Consumer Protection.
[6] Ibid.
[7] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (Sept. 2008).

account or a debit card account are made only to an account in the taxpayer's name.

There continues to be a problem with a substantial number of refunds going to a single account, which increases the likelihood that the deposits are fraudulent. From the cases we identified with characteristics of identity theft, we identified 10 bank accounts that each had over 300 questionable Tax Year 2010 tax refunds deposited by the IRS. We have previously recommended, and continue to recommend, that the IRS limit the number of tax refunds issued via direct deposit to the same bank account or debit card account in an attempt to reduce the potential for fraud.

**13. Last year, the Treasury Department conducted a pilot program where low-income Americans could choose to receive their tax refund on a debit card instead of a check. I understand the report on this pilot program was sent to Treasury in late 2011, but has not yet been released publically. When can we expect a copy of the report?**

Department of the Treasury officials advised us that they are preparing the report to be released and shared with Congress in July 2012.

**The Honorable Patrick P. O'Carroll, Jr.**

SOCIAL SECURITY
Office of the Inspector General

June 26, 2012

The Honorable Charles Boustany
Chairman, Subcommittee on Oversight
Committee on Ways and Means
U.S. House of Representatives
B-317 Rayburn House Office Building
Washington, D.C. 20515

Attention: Kim Hildred

Dear Mr. Chairman:

This is in response to your June 15, 2012 correspondence asking questions for the record, further to my testimony on May 8, 2012 before the Subcommittees on Oversight and Social Security at a hearing on identity theft and tax fraud. I appreciate the opportunity to provide additional information regarding these critical issues. Below are responses to your specific questions.

1. **The Social Security Administration has made the annual Social Security Statement available online, whereby a user must answer a series of questions to prove their identities. Are there any lessons the Internal Revenue Service could take from this, as it and other government agencies move to update their authentication techniques?**

In May 2012, the Social Security Administration (SSA) implemented Electronic Access (EA) for its online statement, but has yet to expand EA to other Internet applications. Authentication through EA occurs completely online, eliminating the mailing of Password Request Codes for its PIN/Password applications. Although we have not audited SSA's EA protocols, we believe IRS can learn from SSA's experience—especially with respect to the lessons learned from the delays SSA experienced in attempting to make EA operational. We do know that the EA protocol uses multiple factors to authenticate users, which we believe is more effective than a single-factor authentication mechanism, such as a username and password.

In the 4th quarter of Fiscal Year 2012, we plan to initiate two audits related to SSA's EA and associated authentication. In the first review, *Security of the Social Security Administration's Public Facing Web Applications*, we will assess SSA's process to establish eAuthentication requirements for its public-facing web applications. Specifically, we will determine whether SSA's public-facing web application eAuthentication reasonably protects the confidentiality, availability, and integrity of the sensitive information used in the applications. Our contractor, Grant Thornton, LLP, will assess SSA's risk that an intruder could gain entry to the Agency's

Internet-accessible web application(s). To meet our objectives, the contractor will perform Web Application Penetration tests of SSA's sensitive and critical web applications, that will

- identify vulnerabilities within the information systems,
- determine opportunities that could be used to compromise the system or data,
- identify risks that could be reduced, and
- propose recommendations that could reduce opportunities to compromise the system based on weaknesses identified.

These tests will also assess the controls and security configurations in place to prevent a non-authorized individual from undermining the confidentiality, availability, or integrity of the sensitive information maintained at SSA.

Our second planned review, *The Social Security Administration's Public-facing Web Application Testing Process*, will assess whether (1) SSA's testing process for its public-facing web applications complies with Federal standards and best practices; and (2) implementation of or changes to public-facing web applications followed SSA's system-development life-cycle testing process. We will use any findings from our first review to identify where in the testing process the security weaknesses could have been prevented. Once these reviews are completed, we will have more definitive information on the effectiveness of the EA protocols.

**2. Should State and local law enforcement have access to taxpayer information, such as refund date, in pursuing identity theft cases? Why or why not?**

In cases involving Social Security number (SSN) misuse and identity theft, taxpayer information can be invaluable to law enforcement. Specifically, information regarding current and former employers, as well as past earnings reported under an SSN, might provide crucial investigative leads and evidence to support criminal charges of identity theft; to substantiate legitimate earnings versus illegal proceeds or concealment of work activity; or to assist law enforcement in locating a subject, fugitive, witness, or even a missing person.

The law enforcement community relies on assistance at all levels of government to conduct joint investigations of mutual interest and overlapping jurisdiction. Although currently we are able to share certain information contained within our case files with other law enforcement agencies during the course of joint investigations, we are prohibited from sharing "tax return" information, as the Internal Revenue Code strictly limits such disclosure. Pursuant to 26 U.S.C. § 6103, the OIG may disclose tax return information from its files only to the Department of Justice and if the disclosure is for the purpose of administering the *Social Security Act*. As such, the sharing of even basic tax return information, such as an individual's name, SSN, and employer, with our State/local law enforcement partners and prosecutors is restricted. We would support any exemption from these restrictions for law enforcement purposes.

**3. Have you investigated any cases in which the Death Master File or a genealogical website was used to commit identity theft? In the last fiscal year, how many cases of Social Security number misuse cases did your office open?**

Yes. In 2007, we participated in a joint investigation with IRS-Criminal Investigation regarding a fraudulent tax filing scheme. The investigation revealed that a Colorado man employed individuals so he could obtain names and SSNs of long-deceased individuals from a genealogical

website. The man then fabricated employment records and instructed others to use the obtained names, SSNs, and false employment information to create fraudulent tax returns, which were submitted to the IRS online. To determine deceased individuals' SSNs, the man said he compared data available from the public Internet site with a certain State's death data. The man was eventually convicted and sentenced to 46 months in prison for SSN misuse, making false claims, and wire fraud. He must also make restitution of over $282,000 to the IRS.

Also, in August 2010, we began investigating about 60 fraudulent retirement benefit claims that used the name, SSN, and date of birth of individuals who died decades ago. We determined that the personally identifiable information (PII) used to file the fraudulent claims was available to the public through a genealogical website. The OIG and other law enforcement agencies identified suspects in the case and executed search and arrest warrants; however, the main suspect took his own life before he was taken into custody. His two accomplices, both relatives of his, were indicted and pled guilty to the charges. The two individuals received 20 months' and 25 months' in prison, respectively, and one was ordered to pay restitution of more than $145,000 to SSA. In addition, they will be deported from the United States at the end of their sentences.

In Fiscal Year 2011, the OIG opened 286 cases involving SSN misuse, which accounted for approximately 3.9 percent of all cases opened during that period. We prioritize SSN misuse allegations that involve

- links to terrorist activities or other threats to national security,
- benefit fraud or other links to Social Security programs,
- Social Security employee misconduct, or
- counterfeiting or selling of Social Security cards.

**4. I have submitted an article from a Florida newspaper for the record that reports that most fraudulent IRS refunds are made on prepaid debit cards. I am concerned that the government is moving to the debit card payment system, not only for tax refunds, but all government payments before adequate measures to prevent fraud are in place. Have you uncovered cases regarding debit card and other electronic payment systems where Social Security benefit payments are diverted to criminals? If so, are these also crimes of identity theft and how does that theft occur? How pervasive is this fraud?**

We are currently investigating fraud involving the unauthorized diversion of Social Security benefits through the direct deposit process. Many of these scams involve the use of the Direct Express Debit MasterCard Program or some other type of reloadable pre-paid debit card account(s), as a means to redirect an individual's benefits without his or her knowledge and facilitate the movement of money.

There appear to be variations in how the fraud is being perpetrated against Social Security beneficiaries. These victims' PII may be compromised through some method of social engineering, or information may be acquired from those businesses or entities with access to PII, such as financial services, health care-providers, etc.

Our investigations confirm that this appears to be a "cottage industry" scam. The majority of our victims are elderly beneficiaries, and they are geographically dispersed throughout the country. We estimate there are thousands of victims, consisting of individuals who have either had their

benefits fraudulently redirected, or an attempt was made to redirect their benefits. Regardless, all these individuals appear to be victims of identity theft.

**5. What action should be taken to prevent debit card fraud?**

Our investigations disclose that fraud involving pre-paid debit cards can be perpetrated anonymously and remotely, potentially minimizing a subject's risk of being caught. Reloadable pre-paid debit cards raise concerns because there are limited controls to authenticate the cardholder. Individuals can simply purchase these cards online or through a local retailer; and after providing the necessary information, can receive direct deposit payments onto the card.

We would encourage examining the strength of existing authentication procedures for the auto-enrollment process established between the Department of Treasury, financial institutions, and those government agencies charged with the responsibility of administering Federal benefit programs. We would also encourage agencies to review their authentication and verification methods for altering payment information.

Thank you for the opportunity to clarify these issues for the Subcommittees on Oversight and Social Security. I trust that I have been responsive to your request. I have sent a similar letter to Chairman Johnson.

If you have further questions, please feel free to contact me, or your staff may contact Misha Kelly, Special Agent-in-Charge of Congressional Affairs, at (202) 358-6319.

Sincerely,

Patrick P. O'Carroll, Jr.
Inspector General

**Steven T. Miller**

**Ways and Means Subcommittees on Oversight and Social Security**
**QFRs**
**Hearing on Identity Theft and Tax Fraud**
**May 8, 2012**

1. How can the Internal Revenue Service (IRS), the U.S. Treasury Inspector General for Tax Administration, and other law enforcement work to catch criminals sooner? Are there additional tools that you need which would require legislative action?

The IRS has taken aggressive measures to improve its filters and processes in an effort to prevent identity theft tax fraud on the front end of the tax filing process. In January 2012, the IRS's Criminal Investigation (CI) established a specialized unit to work almost exclusively on identity theft leads. This unit, known as the Identity Theft Clearinghouse (ITC), is comprised of two working groups within the North Atlantic Scheme Development Center (SDC). The ITC receives all refund fraud related identity theft leads from IRS-CI field offices. The ITC's primary responsibility is to develop and refer identity theft schemes to the field offices, facilitate discussions between field offices with multi-jurisdictional issues, and to work with the other SDCs to provide support for on-going IRS criminal investigations involving identity theft.

One way in which CI has proactively reached out to other law enforcement agencies is via a law enforcement alert bulletin that was developed and distributed to all CI field offices to share with their law enforcement partners. This bulletin helps law enforcement officers identify signs of identity theft related refund fraud and provides a local CI field office point of contact to assist. CI field offices have frequent contact with other federal law enforcement as well as state and local law enforcement in an effort to identify and address new trends in tax crimes. Additionally, Criminal Investigation continues to work closely in many states around the nation with multi-agency task forces designed to identify and disrupt identity theft related crime. These task forces pool resources to more quickly address identity theft allegations and allow for a more concentrated focus on combating identity theft related crimes.

The IRS also initiated a pilot program in the state of Florida to assist state and local law enforcement in identity theft investigative efforts. Through this pilot, identity theft victims can authorize the release of tax information on their accounts to Florida law enforcement authorities. Such information has allowed the participating agencies to obtain tax return information submitted by fraudsters to assist in their investigations of identity theft crimes.

Increasingly, the proceeds of identity theft and tax fraud, including tax refunds obtained by identity theft or fraud, are delivered onto prepaid devices, such as a prepaid card. The prepaid card industry, through the Prepaid Association Fraud Forum, is currently working with the IRS and Treasury/FMS to create a special "DD" rejection code for the prepaid card industry that suggests possible tax fraud that the IRS and Treasury/FMS can then tag as a high risk return.

Additionally, on July 29, 2011, the Financial Crimes Enforcement Network (FinCEN) issued final regulations for the prepaid access industry under the Bank Secrecy Act (BSA) that will assist in the early detection of this type of fraud. These regulations require the prepaid access industry to implement a comprehensive anti-money laundering framework which includes the filing of suspicious activity reports, collection and retention of customer and transactional information, and customer identification. Through the application of the BSA regulations, the prepaid providers and sellers will be in a better position to identify and report on cases of identity theft and tax fraud. This will provide the IRS and law enforcement with additional leads. Furthermore, the increased communication between IRS, other law enforcement agencies and the prepaid access industry should help in developing typologies and patterns so that industry and law enforcement can proactively recognize, prevent, and report on identity theft and tax fraud.

Two additional tools requiring legislative action would further assist us in combating identity theft. First, expanded access to information in the National Directory of New Hires which contains wage and unemployment insurance data, would improve the IRS's ability to identify fraudulent returns claiming fraudulent refunds, including, but not limited to, fraudulent refunds claimed by identity thieves. Second, reinstatement of the provisions under section 6103(k)(10) of the Internal Revenue Code authorizing the IRS to disclose return information with respect to individuals incarcerated in Federal or State prisons whom the IRS determined may have filed or facilitated the filing of a false return would allow the IRS to combat tax fraud from identity theft committed by prisoners. This authorization expired on December 31, 2011. Both of these tools are included in the tax proposals of the Administrations' FY 2013 Budget. Additionally, the President's FY2013 Budget proposes an amendment to the BCA to permit program integrity cap adjustments in support of additional IRS investments. The Budget request includes a total program integrity cap adjustment of $691,028,000 in additional appropriation for tax enforcement and compliance activities. These new initiatives are projected to generate more than $1.48 billion in additional enforcement revenue annually once the resources are fully mature.

2. Should state and local law enforcement have access to taxpayer information, such as refund data, in pursuing identity theft cases? Why or why not?

   As noted in the response to the previous question, the IRS has commenced a pilot program in the state of Florida that provides a means for state and local law enforcement to access just such data. This pilot program is still underway. The results will be analyzed in the coming months. As part of this analysis, the IRS will review whether the tax return information is beneficial to state and local law enforcement. The IRS will also analyze what additional resources would be required to sustain and/or expand the program.

3. Law enforcement and federal prosecutors make decisions on what cases to pursue based on competing priorities and varying levels of fraud. People hear of the $130 million cases being pursued, but how much of this problem exists at lower levels- $5,000 in fraud or $20,000 in fraud- and are these cases vigorously pursued? Do prosecutors only get interested when fraud reaches the incredible levels we read about in newspapers?

   While each case needs to be evaluated on its own merits, it is clear that not every instance of identity theft involving tax fraud can be addressed by a criminal prosecution. Resource constraints within IRS Criminal Investigation, competing prosecutorial priorities of the United States Attorney's Offices, as well as overall capacity issues in the Federal court system make it impossible to address every instance of identity theft related refund fraud criminally.

   Generally speaking, it is the more egregious cases that receive priority. While egregiousness can be measured in part on dollar amount, the number and type of victims, and the actual tax loss sustained by the fraud scheme are also considered among other factors. In all instances, sufficient evidence must still be developed before a case can be successfully prosecuted.

   The IRS believes that continued improvement to tax fraud filters and processes, combined with criminal investigation and prosecution at the state, local, and Federal levels, is the best way to reduce tax fraud from identity theft going forward.

4. You reported to the Senate Finance Committee's Subcommittee on Fiscal Responsibility and Economic Growth hearing that as of March 9, 2012, IRS had stopped 215,000 questionable returns with $1.15 billion in claimed refunds from filters specifically targeting refund fraud. Can you tell us how much money has gone out the door due to fraud this year, or last year?

Historically, we have not tracked revenue loss in this manner due to systems limitations, but we are pursuing whether there is a means to aggregate the losses based on post-refund tax returns that we subsequently confirmed as fraudulent. Also, moving forward we are looking into developing a process to assess and calculate revenue lost due to tax fraud through identity theft. This will give us a better estimate of the revenue loss though not a complete picture.

5. Please tell us what the IRS is doing to further protect taxpayers from identity theft and tax fraud for next filing season. Will the IRS continue its collaboration with software developers, financial institutions and others to explore industry best practices and new innovations to better prevent theft for 2013?

   We are implementing new processes for handling returns, new filters to detect fraud, and a continued commitment to investigate the criminals who perpetrate crimes. We will continue partnering with our stakeholders including software developers, financial institutions, the prepaid card industry, tax professionals, and other law enforcement agencies, etc. For victim assistance, the IRS is working to speed up case resolution, provide more training for our employees who assist victims of identity theft, and step up outreach to and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly. For example, we will implement a systemic locking mechanism that will prevent the filing of a tax return by an identity thief for certain taxpayer accounts, improve systemic capabilities, and expand the use of the Identity Protection PIN (IP PIN) and improve its functionality to validate returns using the IP PIN earlier in the e-file process. We have also streamlined the IP PIN replacement process for those taxpayers who have lost or misplaced their IPPIN. In addition, our ongoing Return Preparer Program, will aid in curbing identity theft by unscrupulous return preparers.

   As stated in response to Question 1 above, there are additional tools requiring legislative action which would allow the IRS to better prevent fraudulent refunds from identity theft.

**Nina E. Olson**

TAXPAYER ADVOCATE SERVICE

YOUR VOICE AT THE IRS

THE OFFICE OF THE TAXPAYER ADVOCATE OPERATES INDEPENDENTLY OF ANY OTHER IRS OFFICE AND REPORTS DIRECTLY TO CONGRESS THROUGH THE NATIONAL TAXPAYER ADVOCATE.

July 16, 2012

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

Dear Chairman Boustany and Chairman Johnson:

I am writing in response to your letter dated June 15, 2012, which requested that I answer two questions for the record submitted in connection with the subcommittees' May 8, 2012, hearing on identity theft and tax fraud. The questions, and my responses, follow.

Question 1

How can the Internal Revenue Service, the U.S. Treasury Inspector General for Tax Administration, and other law enforcement work to catch criminals sooner? Are there additional tools that you recommend which would require legislative action?

Response 1

For identity thieves, tax return fraud may be viewed as a low-risk, high-reward venture. Identity theft has become a large-scale operation, with "boiler room" operations involving the theft of massive lists of Social Security numbers. Apparently, there are networks of criminals who not only share stolen personal information but even present seminars about how to use this information to file bogus returns.[1] Such brazen behavior suggests that identity thieves are not sufficiently concerned with the possibility of criminal prosecution.

[1] *See, e.g.*, Tampa Bay Times, "49 Accused of Tax Fraud and Identity Theft," (Sept. 2, 2011), *available at* http://www.tampabay.com/news/publicsafety/crime/49-accused-of-tax-fraud-and-identity-theft/1189406; Tampa Bay Online, "Police: Tampa Street Criminals Steal Millions Filing Fraudulent Tax Returns," *at* http://www2.tbo.com/news/politics/2011/sep/01/11/police-tampa-street-criminals-steal-millions-filin-ar-254724/.

The IRS's Criminal Investigation division (CI) initiated 276 fraud cases related to identity theft in FY 2011, with 81 convictions – up from 224 investigations and 40 convictions in FY 2010.[2] With hundreds of thousands of tax-related identity theft incidents reported each year, the figure of 81 convictions is a drop in the bucket. To respond more nimbly to identity theft situations, CI now has a designated liaison for identity theft in each of its major offices, but more action is required.

In addition to possible criminal prosecution, I believe identity thieves should be subject to significant civil penalties. Currently, the IRS does not have the authority to assess civil penalties against perpetrators for the amounts by which they have defrauded the government. I believe that civil monetary penalties would (1) be easier for the IRS to pursue than criminal prosecution, (2) have an increased deterrent effect on potential identity thieves, and (3) hit perpetrators where it matters – in their pocketbooks. I therefore recommend that Congress consider legislation to authorize the IRS to impose such civil penalties.

In April of this year, Representative Wasserman Shultz introduced a bill that would encourage the Attorney General to use all existing resources to bring perpetrators of identity theft to justice.[3] While I agree that existing resources should be devoted to prosecuting identity thieves, I believe a significant increase in such resources (*i.e.*, funding) will be necessary to have a meaningful impact on identity theft prosecutions. I have not heard the IRS Criminal Investigation function claim that it needs greater authority to prosecute identity thieves, so I have no reason to believe that additional statutory tools are necessary at this time (except for additional funding). However, my office will remain actively engaged on this issue and may make additional recommendations in the future.

Question 2

Should State and local law enforcement have access to taxpayer information, such as refund data, in pursuing identity theft cases? Why or why not?

Response 2

Taxpayers have the right to expect that any information they provide to the IRS will not be used or disclosed by the IRS unless authorized by the taxpayer or by other provisions of law. The Internal Revenue Code (IRC) contains significant protections for the confidentiality of returns and return information. IRC § 6103 generally provides that returns and return information shall be confidential and then delineates a number of exceptions to this general rule. There is no exception for the release of identity theft information to state or local agencies.[4]

---

[2] Data obtained from the IRS Criminal Investigation division's research function (Mar. 13, 2012).

[3] *See* H.R. 4362, *Stopping Tax Offenders and Prosecuting Identity Theft Act of 2012.*

[4] Note, however, that certain disclosures to state law enforcement are permissible. *See* IRC § 6103(i)(3)(B)(i) (disclosure of return information, including taxpayer return information, can be made to the extent necessary to advise appropriate officers or employees of any state law enforcement agency of the imminent danger of death or physical injury to any individual;

However, IRC § 6103(c) provides that a taxpayer may consent to disclosure of returns and return information to any person designated by the taxpayer.

It is my understanding that some have called for the expansion of exceptions to IRC § 6103, ostensibly to help state and local law enforcement combat identity theft. I have significant concerns about loosening taxpayer privacy protections, and I do not believe that such an expansion of the statute is appropriate at this time. I believe the current framework of IRC § 6103 includes sufficient exceptions to allow the IRS to share information about identity thieves. The IRS Office of Chief Counsel has advised that the IRS may share the "bad return" and other return information of an identity thief with other federal law enforcement agencies investigating identity theft.[5] In light of this advice, the IRS has implemented a pilot program in the State of Florida to facilitate a consent-based sharing of identity theft information with state and local law enforcement agencies.[6]

I believe this approach strikes an appropriate balance – protecting taxpayer return information while simultaneously giving state and local law enforcement authorities more information to help them investigate and combat identity theft. However, I am concerned that once the information is in the hands of state and local law enforcement, there is no prohibition in the tax code against redisclosure. Therefore, I suggest that Congress consider modifying IRC § 6103(c) to explicitly limit the use of tax return information to the purpose agreed upon by the taxpayer (i.e., to allow state or local law enforcement to use the information solely to enforce state or local laws) and to prohibit the redisclosure of such information.[7]

* * * * *

I hope you find these responses useful. If you have further questions, please feel free to contact my office at (202) 622-6100.

Sincerely,

Nina E. Olson
National Taxpayer Advocate

---

disclosure cannot be made to local law enforcement agencies). While identity theft may cause emotional and economic injury, the typical identity theft situation does not pose an imminent danger of death or physical injury.

[5] IRS Office of Chief Counsel Memorandum, *Disclosure Issues Related to Identity Theft, PMTA 2012-05* (Jan. 18, 2012).

[6] *See* http://www.irs.gov/privacy/article/0,,id=256965,00.html (last visited June 8, 2012).

[7] *See* National Taxpayer Advocate 2011 Annual Report to Congress 505.

**Public Submissions For The Record**

**IAJGS**


# International Association of Jewish Genealogical Societies (IAJGS)

**6052 Hackers Lane Agoura Hills, CA 91301**
**818-889-6616 tel 818-889-0189 fax**
www.iajgs.org


**STATEMENT FOR THE RECORD, U.S. HOUSE OF REPRESENTATIVES COMMITTEE WAYS & MEANS, SUBCOMMITTEES ON OVERSIGHT AND SOCIAL SECURITY, MAY 8, 2012 JOINT HEARING ON IDENTITY THEFT AND TAX FRAUD**

## I. INTRODUCTION:

The U.S. House of Representatives Ways and Means Subcommittees on Oversight and Social Security held a joint hearing on 8 May 2012, on Identity Theft and Tax Fraud including the accuracy and uses of the Social Security Administration's Death Master File. The genealogical community was not extended an invitation to testify at the hearing, however, public comments were solicited. This statement is accordingly submitted.

## II. IAJGS BACKGROUND & CONTACT INFORMATION:

The International Association of Jewish Genealogical Societies is the umbrella organization of 70 genealogical societies and Jewish historical societies worldwide whose approximately 10,000 members are actively researching their Jewish roots. We want to ensure that our members will be allowed continued and maximum access to these records. The IAJGS and its predecessor organization were formed in 1988 to provide a common voice for issues of significance to its members and to advance our genealogical avocation. One of our primary objectives is to promote public access to genealogically relevant records. In 2012, we are holding our 32nd consecutive annual International Conference on Jewish Genealogy (www.iajgs.org).

IAJGS is a voting member of the Records Preservation and Access Committee (RPAC) that is a joint committee whose other voting members include The National Genealogical Society (NGS) and the Federation of Genealogical Societies (FGS). The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), and the American Society of Genealogists (ASG) also serve as participating members. RPAC also includes participation from several of the commercial providers of genealogical information.

**Contact Information:**
IAJGS official mailing address is:
IAJGS
PO Box 3624
Cherry Hill, NJ 08034-0556

However, for purposes of this statement please use the following contact information:


Jan Meisels Allen,
Vice President, IAJGS
6052 Hackers Lane Agoura Hills, CA 91301 (818) 889-6616 tel (818) 991-8400 fax (call before submitting a fax)
e-mail: vicepresident@iajgs.org

**Previous Hearings**

The Social Security Subcommittee held a hearing on the issue on 2 February 2012, and the Senate Finance Committee Fiscal Responsibility & Economic Growth Subcommittee also held a hearing on 20 March 2012. IAJGS submitted Statements for the Record for the 2 February 2012 and 20 March 2012 hearings. These previous Statements are incorporated by reference into this statement.

## Introduction

Thank you for the opportunity to present the IAJGS concerns regarding the Subcommittees' proposed reduction or elimination of public access to the commercial version of the Death Master File (DMF), the Social Security Death Index (SSDI). For the purposes of this statement, we will be addressing access to the SSDI rather than the DMF, as the SSDI is the version that genealogists are permitted to access.

It is ironic that a system that is used to prevent identity theft (by permitting employers, financial organizations, insurance companies, pension funds, and others the ability to check names against those deceased as reported on the Death Master File), [http://www.ntis.gov/products/ssa-dmf.aspx], is now being determined – inappropriately—as an instrument of identity theft.

We support the Subcommittees' intent to protect the residents of the United States from improper usage of their personal information, and to protect them from identity theft. We support, the provisions in S1534, H 3215 and HR 3482 which propose strong criminal penalties for those who willfully misuse or disclose another's personal tax identity number (Social Security Number) resulting in a personal gain. Only strong criminal penalties will hopefully, deter those who are misusing another's Social Security Number (SSN) for their own gain.

Violations occur due to computer breaches from government and private enterprises and government and private enterprise personnel misusing or stealing Social Security numbers. A recent study (2012) by ID Analytics estimates of 100 million applications examined to the entire annual volume of applications submitted for credit products and services in the U.S., that nearly 6.8 million applications have at least a partial match to the DMF. Many of these—roughly 2.4 million—are simply SSN typos. Approximately 1.6 million applications are instances of a fraudster using a fabricated SSN that **unintentionally** matches the SSN of a deceased person [1]. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen" [i]. Many computer breaches have been well documented in the press.[2]. In addition, there have been newspaper accounts of Social Security numbers found in dumpsters and other places [3] where they can be easily found and used by "fraudsters".

**Genealogists Are Not the Cause of Identity Theft**

Genealogists rely on the Death Master File/Social Security Death Index for legitimate reasons. Their access to the SSDI is not the cause of identity theft. Thieves are the cause of identity theft. Preventing genealogists access to the SSDI will not prevent the aforementioned type of illegal use of SSNs. Financial institutions and government agencies have been hacked into numerous times and that has been documented [1, 2], but was not mentioned during the hearing. Nor was there mention of returning to using non-computerized data to avoid the inevitable hacking that occurs daily in the 21st century. If we accept the continued use of computerized data, and the continued likelihood of hacking occurring to any given database at any time, then we must also accept that, occasionally, misuse of data will occur. This is why it is imperative that the IRS take more aggressive action to prevent fraudsters from using fraudulently obtained SSNs on fraudulently filed tax returns. It is not reasonable, constitutional, or in the nation's interests, to remove public documents from public access. For a real solution to this problem, see below "IRS Needs to be More Proactive."

In Mr. J. Russell George, Treasury Inspector General for Tax Administration statement before the joint subcommittees' hearing, he commented: " The IRS began a pilot program in Processing Year 2011 which locked taxpayers' accounts where the IRS Master File and Social Security Administration data showed a date of death. The IRS places a unique identity theft indicator on deceased individuals' tax accounts to lock their tax account." While it is gratifying that, the IRS is **finally** using Social Security Administration information to prevent tax identity fraud—it is unfortunate that the IRS was not using the DMF information all along to prevent fraudulent filings of deceased individuals.

What was even more striking in Mr. George's statement was that the tax identity fraud of living individuals was the overwhelming cause of identity theft and tax fraud, including the billions of dollars of falsely used debit cards and not depositing refunds directly into the taxpayers' bank accounts. These fraudulent practices by the living are not part of the DMF--and therefore, the focus of closing the commercial version, the Social Security Death Index, appears as if it will have no impact at all on the overwhelming problem of identity theft and tax fraud. Therefore, we ask, why are the Subcommittees focused on the SSDI when closing that off will have virtually no bearing on the overwhelming problem.

Detective Sol Augeri noted, in his oral statement during the March 20th hearing before the Senate Finance Committee Subcommittee on Fiscal Responsibility and Economic Growth, that once the genealogical websites withdrew the SSDI from public access, identity theft did not abate. Rather, Detective Augeri said the access to Social Security Numbers to be used in identity theft moved to institutions: hospitals, nursing homes, physician offices and other institutions. In his written statement, Detective Augeri said "...they turned to individuals who [sic] worked in Assisted Living Facilities who would obtain necessary information on patients. Lists of names are now being sold by those having access to personal information in businesses, medical offices, and schools." This documents that removal of the SSDI from public access does not necessarily reduce the problem of fraudulent use of a Social Security number. Indeed, we heard at the March 20th hearing that identity theft continues to grow, in spite of genealogy and family history sites' removal of the SSDI from public access. For example, medical identity theft, whereby medical employees have been found to steal patient's identification has become a growing business.[4] If Congress limits public access to SSDI, it will no longer be available as a reference check to many who use it as an identity theft deterrent, there well may be an increase in identity theft.

**Loss of Critical Data in Death Master File If States Prevent Inclusion in the Commercial Version**

Many organizations---state and local government, financial, insurance and other businesses---rely on the SSDI for fraud prevention. Recently, the New York City Employee Retirement System started a new system comparing the SSDI with their pension data bank. This was initiated due to a number of recent fraudulent pension filings [5]. As states assert their rights to retain control over the sale of their data in the SSDI, the recent notification from over 30 states that state data can no longer be included in the SSDI is of compelling concern. The elimination of data from the SSDI raises the concern about the resulting loss of a meaningful fraud deterrent used by various organizations including state and local government as well as financial, insurance, medical and other businesses. How do the Subcommittees plan to "replace" this effective fraud deterrent?.

**Interest in Family History/Genealogy**

Millions of Americans are interested in their family history. The Harris Interactive Poll taken in August 2011 found that four in five Americans have an interest in learning about their family history. The Poll also reported 73% of Americans believe it is important to pass along their family's lineage to the next generation.[6] Genealogists doing U.S. research located both in and outside the United States rely on the Social Security Death Index.

**Certification for Certain Genealogists With Need For Immediate Access to the Death Master File/Social Security Death Index**

While IAJGS advocates all genealogists should have immediate access to the SSDI, we would support the two year delay in access as proposed in S 1534, HR 3215 and HR 3482-and if necessary the third year that National Taxpayer Advocate Nina Olson advocated during her oral testimony during the May 8th and March 20th hearings. This support is based on amending the bill to include that certain genealogists are to be eligible for certification for immediate access under the bills' provisions. These genealogists include:

- Forensic genealogists. These are genealogists who work, for example by contract on specific cases with the Department of Defense in identifying next of kin of deceased military personnel from prior conflicts and working with local, county, and state coroners to help find the next of kin of deceased in order for the deceased to have a proper burial;

- Heir researchers who are working under contract with law firms to prove or disprove that someone is eligible as part of a deceased's estate or Native American tribal funds;

- Those researching **individual** genetically inherited diseases to help current and future generations obtain necessary medical testing to determine if they currently need prophylactic treatments. We are aware that medical researchers may already be eligible for certification, but many work with aggregate data and the individual needs to know about their own medical genetically inherited history.

While some organizations currently are certified for immediate access, individual genealogists working within the above three categories are not covered and certification for immediate access needs to be specifically addressed in the legislation. The Records Access and Preservation Committee, which is described on page one of this statement, is willing to work with the Subcommittees in determining who would qualify.

See below for more detail.

**Family Medical History**

Genealogists use Social Security Numbers (SSNs) to appropriately identify records of people when tracing **family medical history**, especially if the person has a common name: Sara Cohen, Tom Jones, Jose Martinez, Mary Smith, etc. During the March 20th hearing before the Senate Finance Subcommittee on Fiscal Responsibility, it was mentioned that perhaps genealogists could make do with the last four digits of the Social Security Number. Unfortunately, this was proven not to be true in the February 2nd House Subcommittee on Social Security hearing. Mr. Pratt, representing the Consumer Data Industry Association (CDIA), mentioned CDIA had conducted a study and found some people with common names, i.e. Smith, also had the same last four digits on their Social Security number, validating why the complete Social Security number is necessary.

Genealogy assists researchers in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The SSN is essential to make certain that one is researching the correct person. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family [7]. Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative [8].

There are many genetically inherited diseases, but for the purposes of this statement, we will mention the *BRCA1* and *BRCA2* genes' mutations and breast and ovarian cancer. The following information is from the National Cancer Institute [9].

> "A woman's risk of developing breast and/or ovarian cancer is greatly increased if she inherits a deleterious (harmful) *BRCA1* or *BRCA2* mutation. Men with these mutations also have an increased risk of breast cancer. Both men and women who have harmful *BRCA1* or *BRCA2* mutations may be at increased risk of other cancers.
>
> The likelihood that a breast and/or ovarian cancer is associated with a harmful mutation in *BRCA1* or *BRCA2* is highest in families with a history of multiple cases of breast cancer, cases of both breast and ovarian cancer, one or more family members with two primary cancers (original tumors that develop at different sites in the body), or an Ashkenazi (Central and Eastern European) Jewish background.
>
> Regardless, women who have a relative with a harmful *BRCA1* or *BRCA2* mutation and women who appear to be at increased risk of breast and/or ovarian cancer because of their ***family history*** [emphasis added] should consider genetic counseling to learn more about their potential risks and about *BRCA1* and *BRCA2* genetic tests.
>
> **The likelihood of a harmful mutation in *BRCA1* or *BRCA2* is increased with certain familial patterns of cancer** [emphasis added]. These patterns include the following for women of Ashkenazi Jewish descent:
>
> - Any first-degree relative diagnosed with breast or ovarian cancer; and
> - Two second-degree relatives on the same side of the family diagnosed with breast or ovarian cancer."

This form of breast cancer is something not unique to Ashkenazi Jews. Studies have demonstrated that this has also been found in the Hispanic communities of New Mexico and Colorado--who did not know they

were descended from Sephardic Jews who had hidden their Jewish identity to survive the Inquisition in the 15th century. This is described in Jon Entine's *Abraham's Children: Race, Identity and the DNA of the Chosen People*, by the Smithsonian in their article, *The Secret Jews of San Luis Valley,* and *The Wandering Gene and the Indian Princess: Race, Religion, and DNA* [10]

People who have had members of their families diagnosed with breast cancer need to know whether past family members may have also died from this disease, in order to determine if it is inherited. Both current and future generations need to have this information in order to make decisions about whether to prophylactically remove both breasts and ovaries (which can mean the difference between early detection and treatment versus possible early death). This is something both men and women need to be able to research--as either can be carrying the gene mutation. The SSDI is a critical tool in assuring researchers that the records they have located on possible ancestors are indeed the correct persons, especially when they have a common name.

We use this as only one example of inherited diseases that require the ability to research ancestry using a SSN—regardless of ethnicity.

**Working with Coroners to Identify Deceased's Next of Kin**

People are going to their graves with no family to claim them. Medical examiners and coroners' offices—frequently overstretched with burgeoning caseloads—need help in finding next of kin of the deceased. The deceaseds' identities are known; it is their next of kin that are unknown in these cases. Over 400 genealogists are now offering their volunteer services to help locate the next of kin for unclaimed persons. The identities of these people are known, but the government agencies are not always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See unclaimedpersons.org

**Working with the Military**

There are literally tens of thousands of United States Veterans' remains left unclaimed throughout the Nation. Sometimes decades pass while these remains are waiting to be identified as Veterans and given a proper military burial. Genealogists work with the military to locate relatives of soldiers who are still unaccounted for from past conflicts. By finding relatives, the military can identify soldiers using DNA, and notify the next of kin so the family can make burial decisions. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family [11].

**Genealogy as a Profession**

While there are millions of people who actively study and research their family history as an avocation, there are many others who earn their livelihoods as professional genealogists. Professional genealogists use the SSDI to (1) help track heirs to estates, (2) find title to real property, (3) find witnesses to wills that need to be proved, (4) work on the repatriation projects [see Working with the Military], (5) track-works of art—including stolen art—and repatriation of looted art work during the Nazi era of World War II, and (6) assist in determining the status of Native American tribes and tribal members to prove–or disprove—that they are entitled to share in Tribal casino revenues.

**IRS Needs to Be More Proactive**

While we are heartened that the IRS has begun a fraud identification program in 2011 with various new identity theft screening filters -- this is not enough. They need to do more to work with the identity theft victims and even more to prevent identity theft-which includes more flagging of returns of not only the deceased, but of others covered under the same tax return: spouses and dependents. This "simple" notation in the file can further prevent tax refunds being generated by the fraudulent filer. It is a positive outcome that the IRS has undertaken various preventive activities. However, much more is required to address the growing blight of identity theft and actions need to be undertaken now.

If the IRS were to routinely run Social Security numbers included in tax returns against the Death Master File, they might avoid giving refunds to deceased individuals. This is a data match between two government computer programs—something that should be routinely undertaken. The difference between data security and data stewardship is excellently described in Kenneth Ryesky's statement to the Subcommittee relative to the

March 20th and May 8th hearings. Ryesky testified that, along with failure of the IRS for data stewardship, "The social security numbers (SSNs) were not verified, even though the means to verify the numbers should have been readily available to the IRS… data security practices alone do not constitute sound stewardship of taxpayer personal data.". [12]

"Operation Rainmaker" (also known as Operation TurboTax), was a tax fraud operation in the Tampa Bay area as discussed by Tampa Police Department Lieutenant Augeri during the Senate Finance Subcommittee hearing. Law enforcement interviews specified that the IRS, while cooperating with other law enforcement officers, is not authorized to share information with local law enforcement departments, hampering efforts to protect their citizens. If the federal government is serious about addressing identity theft that uses a person's Social Security number, then the IRS needs to be given legislative authority to share information with local, county, and state law enforcement organizations. Perhaps as a minimum, the subcommittees through legislation can adopt the suggestion by National Taxpayer Advocate Olson in her written and oral statements for both the May 8th and March 20th hearings, that the identity theft victim be able to receive the "bad return". Currently, this is a pilot project where information filed by the alleged identity thief, enabling the victim to then provide the information to local law enforcement or provide a release for the IRS to share the information directly with local law enforcement. It was also stated that filing tax refunds for under $10,000 will not get any attention. As "Operation Rainmaker" found the average tax, fraud was about $9,500, below the $10,000 threshold [13]. This is another practice that the Congress needs to review, as the criminals who are perpetrating this fraud know they will be undetected!

It became apparent through Mr. McClung in his testimony at the Senate Finance Subcommittee's 25 May 2011 Hearing,[14] together with the testimony of Mr. Agin at the House Ways & Means Subcommittee's 2 February 2012 Hearing, [15] that the IRS assumes the first person filing is the "legitimate" filer and by inference, the second filer is the fraudulent party. The IRS needs to amend their practice to require some verification to determine which is a valid filing, when the filing involves a deceased child.

Unfortunately, since the IRS advocated electronic filing of tax returns, one unexpected consequence is the remarkable increase in tax identity theft.

**Support For Efforts to Cease Identity Theft**

- If income tax returns were electronically compared to the Master Death File, matching cases could be flagged for special processing, and the person attempting to create a tax fraud could be stopped before the fraud occurs.
- A parent's social security number should be required when filing a tax return for any minor. It is an extremely rare occurrence that a minor child would not be listed as a dependent on the parent or guardian's tax filing. If the minor dies, the IRS could have a procedure to flag any filings without the parent's social security number, again preventing the fraud. Draft legislative language developed by the Records Preservation and Access Committee [16] (see Attachment A) would facilitate just this prevention of identity theft perpetrated on children. The *National Taxpayer Advocate's Report to Congress for 2011* specifically highlights the benefits of the IRS Issued Identity Protection PINs [17] and suggests that taxpayers should be allowed to turn off their ability to file tax returns electronically. Any family that suffers a death could elect to turn off the electronic filing ability.
- Criminal penalty statutes for those who fraudulently use Social Security Numbers, including, but not restricted to, those who misuse their positions (*e.g.*, hospital, medical institution and office personnel, financial and credit card organizations personnel, prison corrections officer, college or university registrar etc.)

For the reasons stated above:

- Genealogists are **NOT** the cause of identity theft;
- Genealogists have legitimate, professional and life saving reasons to have immediate access to the SSDI; and

- Proactive measures are needed to prevent identity theft and vigorously pursue and punish the **TRUE** identity thieves, and
- "Fraudsters" are focusing on stealing the Social Security Numbers of live people not the dead-- when fraudulent tax filings are being rendered to the IRS; and
- SSDI is a deterrent to fraud and removing access to this database will cause more harm than good.

IAJGS respectfully and vehemently encourages the Subcommittees to continue public access to the commercial version of the Death Master File, known as the Social Security Death Index, to be available to the public. If any time period for withholding this from the public is required, then it should not be greater than two or three years including the year of death with certain genealogists being eligible for certification for immediate access to the Death Master File.

On behalf of the International Association of Jewish Genealogical Societies, we appreciate the opportunity to submit our comments, and for the occasion to bring to the Subcommittees' attention the many services the genealogy community performs for local, state, and federal government offices. We look forward to working with the Subcommittees and staff to find an accommodation that provides genealogists with immediate and reasonable access to the SSDI.

Respectfully submitted,

Jan Meisels Allen

Jan Meisels Allen
IAJGS Vice President
Chairperson, IAJGS Public Records Access Monitoring Committee

Endnotes

[1] http://www.idanalytics.com/news-and-events/news-releases/2012/4-23-2012.php
http://www.identitytheft.info/breaches09.aspx

[2] http://www.boston.com/business/articles/2008/03/18/grocer_hannaford_hit_by_computer breach/
http://www.nctimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html
http://www.qctimes.com/news/local/article_06d38e24-146a-11df-91c6- 001cc4c03286.html
http://www.washingtonpost.com/politics/tricare-military-beneficiaries-being-informed-of-stolen-personal-data/2011/11/23/gIQAcRNHtN_story.html
http://sundayherald.com/news/heraldnews/display.var.2432225.0.0.php
Understanding Identity Theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, Copes, H., and Vicraitis, L.M. (2009) *34*(3), 329-349.

[3] http://www.ksat.com/news/Personal-documents-found-in-trash-can/-/478452/8282132/-/59y7ox/-/index.html;

http://www.phiprivacy.net/?p=5405
http://www.abc15.com/dpp/news/region_northern_az/payson/state-agency-leaves-arizonans-sensitive-documents-in-dumpster
http://www.databreaches.net/?p=16205
http://www.vcstar.com/news/2012/mar/30/lost-data-may-have-exposed-800000-people-in/

[4] http://consumerist.com/2010/03/id-theft-ring-used-hospital-records-for-300k-shopping-spree.html;
http://articles.sun-sentinel.com/2010-11-11/health/fl-hk-holy-cross-id-20101110_1_identity-theft-ring-patient-files-emergency-room
http://www.miamiherald.com/2011/12/07/2536190/miami-va-hospital-employee-charged.html;

[5] http://www.dnainfo.com/new-york/20120509/new-york-city/family-of-dead-city-workers-stole-nearly-400k-pension-cash-report-says

[6] http://corporate.ancestry.com/press/press-releases/2012/01/ancestry.com-partners-with-historical-society-of-pennsylvania-to-bring-the-states-rich-history-online/
*This survey was conducted online within the United States by Harris Interactive via its QuickQuery omnibus product on behalf of Ancestry.com from August 5-9, 2011 among 2,950 adults ages 18 and older*

[7] Mayo Clinic staff: "Medical History: Compiling your medical family tree," http://www.mayoclinic.com/health/medical-history/HQ01707;

[8] https://familyhistory.hhs.gov/fhh-web/home.action

[9] http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA

[10] Abraham's Children: Race, Identity, and the DNA of the Chosen People. Jon Entine, Grand Central Publishing, New York, N.Y. 2007.
http://www.smithsonianmag.com/science-nature/san-luis-valley.html
The Wandering Gene and the Indian Princess: Race, Religion, and DNA. Jeff Wheelwright. WW Norton & Co. New York, NY, 2012.

[11] http://www.aarp.org/relationships/genealogy/info-06-2011/genealogy-tips.html
http://www.familiesforforgottenheroes.org/Genealogist.htm

[12] Kenneth H. Ryesky, Esq., Statement for the Record, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility & Economic Growth, Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions March 20, 2012.
Kenneth H.Ryesky, Esq. Statement for the Record, United States House of Representatives, Committee on Ways and Means, Subcommittees on Oversight and Social Security, Joint Hearing on Identity Theft and Tax Fraud May 8, 2012

[13] http://www.youtube.com/watch?v=gpgTFO7nMBk

[14] Statement of Terry D. McClung, Jr., Hearing on the Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth (25 May 2011). http://finance.senate.gov/imo/media/doc/Testimony%20of%20Terry%20McClung.pdf.

[15] Statement of Jonathan Eric Agin, Esq., Hearing on the Accuracy and Uses of the Social Security Administration's Death Master File, House Committee on Ways and Means Subcommittee on Social Security (2 February 2012), http://waysandmeans.house.gov/UploadedFiles/Agin_Testimony202ss.pdf.

[16] The Records Preservation and Access Committee is a joint committee, which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS) and the International Association of Jewish Genealogical Societies (IAJGS) as voting members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), the American Society of Genealogists (ASG), ProQuest and Ancestry.com also serve as participating members.

[17] http://www.irs.gov/pub/irs-pdf/p2104.pdf

Attachment A

To address the tax issues surrounding the misuse of Social Security Numbers, the following language captures the concept that if a child under the age of 18 has their social security number associated with that of their parents or legal guardian, and if that information is afforded to the Internal Revenue Service, then administrative procedures may be put in place that would flag claims where the social security number of the deceased child did not match the social security numbers of its parents and appropriate action may be taken by the IRS, as follows:

Existing law requires the Social Security Administration to release the data contained in the Death Master File and arrange it for publication according to Perholtz v. Ross, C.A. Nos. 78-2385, 78-2386 D.D.C. Since that time, the data contained in the Death Master File has been widely used to prevent identity theft for fraudulent purposes through the wide dissemination of the information that the person identified with a uniquely identifying Social Security number is deceased.

This bill would require the Social Security Administration to add additional information to the Death Master File to be shared with the Internal Revenue Service for the purpose of prohibiting the criminal act of claiming unrelated deceased dependents.

SECTION 1. (1) The Commissioner of the Social Security Administration shall arrange and permanently preserve the social security numbers of dependent children with the associated social security numbers of their legal parents or guardians for all applications registered.

(2) The Commissioner of Social Security may release the indices and data files described in paragraph (1) to the Internal Revenue Service. The Internal Revenue Service having obtained the index pursuant to this paragraph may not release any portion of its contents to any other party or government agencies.

(3) The Internal Revenue Service or other government agency may not sell or release Social Security indices prepared and maintained by the Social Security Administration except as authorized by law.

(4) In addition to the indices prepared pursuant to paragraph (1), the Commissioner of Social Security shall prepare separate non-comprehensive electronic indices of all deceased individuals with Social Security numbers that shall be made available for public inspection.

(5) For purposes of this bill, the following definitions apply:

(a) "Data files" means computerized data compiled from Social Security Applications registered with the Social Security Administration.

(b) "Person" means any individual, firm, corporation, partnership, limited liability company, joint venture, or association.

(c) "Personal identifying information" means first name, middle name, last name, mother's maiden name, and father's surname, and a social security number that is contained in the file.

(d) "Financial institution" means any commercial bank, trust company, savings and loan company, insurance company, or person engaged in the business of lending money.

(e) "Commercial or non-profit company" means any company or not-for-profit organization engaged in sharing information about deceased individuals for the pursuit of heir searches, genetic research, blood quantum research, genealogy or family history research, or other legal uses of the information as authorized by law.

(6) The Social Security Death Master File as presently constituted will be made available for a reasonable fee to financial institutions, commercial companies, non-profit organizations and educational institutions as authorized by law.

(7) Any person who, in violation of this section, uses, sells, shares, or discloses any information provided pursuant to this section, or who uses information provided pursuant to this section in a manner other than as authorized pursuant to this section, may be subject to the assessment of a civil penalty by the Internal Revenue Service in the amount of $_____. The

penalty provided in this section shall not be construed as restricting any remedy, criminal, provisional, or otherwise, provided by law for the benefit of the agency or any person.

(8) The Social Security Administration and the Internal Revenue Service shall adopt any regulations necessary to implement this section.

**Kenneth Ryesky**



**KENNETH H. RYESKY, ESQ., STATEMENT FOR THE RECORD, UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE WAYS & MEANS, SUBCOMMITTEES ON SOCIAL SECURITY AND ON OVERSIGHT, JOINT HEARING ON IDENTITY THEFT AND TAX FRAUD:**

## I. INTRODUCTION:

The House Ways & Means Committee, Subcommittees on Social Security and on Oversight, held a Hearing on 8 May 2012, regarding the use of identity theft by tax fraudsters. Public comments were solicited. This Commentary is accordingly submitted.

## II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:

Background: The Commentator, Kenneth H. Ryesky, Esq., is a member of the Bars of New York, New Jersey and Pennsylvania, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York, where he teaches Business Law courses and Taxation courses. Prior to entering into the private practice of law, Mr. Ryesky served as an Attorney with the Internal Revenue Service ("IRS"), Manhattan District. In addition to his law degree, Mr. Ryesky holds BBA and MBA degrees in Management, and a MLS degree. He has authored several scholarly articles and commentaries on taxation, including one made part of the printed record of a previous hearing before the full Senate Finance Committee [1] and also cited in a report by Her Majesty's Treasury's Office of Tax Simplification. [2]

As explained in greater detail in commentaries to previous related Hearings, the Commentator has a personal and sometime professional interest in genealogy.

Contact Information: Kenneth H. Ryesky, Esq., Department of Accounting & Information Systems, 215 Powdermaker Hall, Queens College CUNY, 65-30 Kissena Boulevard, Flushing, NY 11367. Telephone 718/997-5070; E-mail: khresq@sprintmail.com.

Disclaimer: Notwithstanding various consultations between the Commentator and other interested individuals and organizations, this Commentary reflects the Commentator's personal views, is not written or submitted on behalf of any other person or entity, and does not necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

---

[1] *Tax: Fundamentals in Advance of Reform*, Hearing before the Committee on Finance, U.S. Senate, 110th Congress, 2nd Session, April 15, 2008, S. Hrg. 110–1037, pp. 113 - 150 <http://finance.senate.gov/library/hearings/download/?id=fead52be-a791-4105-96da-0010264cd7ed>.

[2] Her Majesty's Treasury, Office of Tax Simplification, *Review of Tax Reliefs, Interim Report*, pp 9 - 10 (December 2010) <http://www.hm-treasury.gov.uk/d/ots_review_tax_reliefs_interim_report.pdf>.

**III. COMMENTARY ON THE ISSUES:**

A. Previous Hearings:

The instant proceeding of 8 May 2012 is not written on a blank slate. The Social Security Subcommittee already held a hearing on the issue on 2 February 2012, and the Fiscal Responsibility & Economic Growth Subcommittee of the Senate Finance Committee also held hearings on 25 May 2011 and on 20 March 2012.

The Commentator submitted Statements for the Record for the 2 February 2012 [3] and 20 March 2012 [4] Hearings. These previous Statements are incorporated by reference into this instant Statement.

B. Of Mice and SSNs:

The Subcommittees would do well to take to heart the Talmudic dictum to not blame the mouse, but to blame the hole. [5] If indeed the Social Security Death Master File (DMF) [6] is the "mouse," then cutting off all public access to it will not close the "mousehole." Enterprising fraudsters have a plethora of other available sources for Social Security Numbers (SSNs) with which to commit tax fraud through identity theft.

SSNs have been inadvertently posted on websites.[7] SSNs are to be found in trash cans and dumpsters,[8] including those of such entities as hospitals, [9] law firms, [10] schools, [11] banking

---

[3] Posted on the internet at <http://www.fgs.org/rpac/wp-content/uploads/2012/02/wm-ssdmf-comments-2012.pdf>, *also available at* 2012 TNT 25-32.

[4] Posted on the internet at <http://www.fgs.org/rpac/wp-content/uploads/2012/04/senfincomm-taxfraud-20120320-corrected2.pdf>, *also available at* 2012 TNT 56-30.

[5] TALMUD, GITTIN 45a.

In using the mouse and mousehole metaphor, the Commentator does not in any way intend to insult or denigrate rodents by equating them to the depraved reprobates who, inter alia, expropriate the identities of deceased children in order to defraud the public treasury.

[6] The DMF is available and utilized in another incarnation known as the Social Security Death Index (SSDI), and is often referred to as such.

[7] *See, e.g.* Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102 (N.D. Cal. 2010).

[8] *E.g.* Mike Salinero and Peter Bernard, *Personal Data Found in Trash Bins*, TAMPA TRIBUNE, 18 October 2009, p. 9; Lukas I. Alpert and Matthew Nestel, *WTC Identity Crisis - Ground Zero Workers' Personal Info Exposed*, N.Y. POST, 22 April 2008, p. 8; Cathy Zollo, *An Identity Trove Intact in the Trash*, SARASOTA HERALD-TRIBUNE, 23 October 2007, p. A1.

and finance institutions, [12] and casinos. [13] SSNs can be found amongst the images stored on the archival hard drives of copy machines, [14] and can, inadvertently or otherwise, be posted on bulletin boards in union halls. [15]

Paper records in transit can, in the event of a crash or other misadventure, be spilled, strewn and dispersed along the highway; [16] indeed, even the IRS's own couriers are susceptible to such traffic mishaps. [17]

Nor have the local law enforcement authorities always fully appreciated the significance of personal data in the wrong hands. [18]

---

[9] *E.g. Patients' Records Tossed into Dump*, RECORD [Stockton, CA], 16 June 2011.

[10] *E.g.* Mary Mitchell, *Lax Document Disposal Leaves Privacy in Shreds*, Chicago Sun-Times, 29 July 2010, p. 12.

[11] *See, e.g.* Elizabeth Lazarowitz, *PS Workers' Info Dumped for All to See*, N.Y. DAILY NEWS, 25 September 2009, p. 62..

[12] *E.g.* ILLINOIS ATTORNEY GENERAL, PRESS RELEASE, ATTORNEY GENERAL MADIGAN SUES PAYDAY LOAN STORE AFTER CUSTOMERS' PERSONAL INFORMATION ENDS UP IN THE TRASH (15 October 2010), *available on the Internet at* <http://www.illinoisattorneygeneral.gov/pressroom/2010_10/20101015.html>.

[13] *See, e.g.* United States v. Greer, 640 F.3d 1011 (9th Cir. 2011, *cert. denied* ___ U.S. ___, 132 S. Ct. 834, 181 L. Ed. 2d 540 (2011).

[14] *E.g.* Jennifer Saranow Schultz, *Identity Theft and Copiers*, N.Y. TIMES, 22 May 2010, p. 5.

[15] *See, e.g.* Fisher v. Communication Workers of America, 716 S.E.2d 396 (N.C. Ct. App. 2011), *appeal dism'd* 721 S.E.2d 231 (N.C. 2012).

[16] *E.g.* Will Jayson Marin, *Privacy Concerns Raised about Paperwork Spilled in Marin Highway 101 Mishap*, CONTRA COSTA TIMES, 5 May 2011.

[17] IRS, PROBLEM ALERT: IRS REPORTS SOME TAX PAYMENTS FROM 13 STATES LOST (September 23, 2005), available at 2005 TNT 185-56 (26 September 2005), formerly posted on Internet at <http://www.irs.gov/newsroom/article/0,,id=98129,00.html> (accessed December 12, 2005), (reporting that, in aftermath of traffic accident, approximately 30,000 tax payments sent to the IRS "were ejected into the San Francisco Bay and are not recoverable").

The apparent disappearance of the document from the IRS's website is not inconsistent with the IRS's cultural norm which places low priority on the proper preservation of its own historical records and documents. *See* SHELLEY L. DAVIS, UNBRIDLED POWER 38 - 47 (HarperBusiness, N.Y., 1997).

[18] *See, e.g.* Paul Walsh, *Stolen Data On 3.3 Million Loans is Found; Despite Publicity About the Theft, the Stolen Data Sat in a Minneapolis Police Evidence Room for Three Weeks*, MINNEAPOLIS STAR TRIBUNE, 17 April 2010, p. 1B.

And if the inadvertent release of SSNs poses a threat to individuals' identity security, then the intentional misappropriation of SSNs by fraud-minded individuals who abuse their trusts is all the more nefarious. This has already occurred in numerous incidents and settings, including but not limited to misdeeds by employees of hospitals and health care facilities, [19] real estate brokers, [20] Banks and mortgage lenders, [21] debt collection agencies and skip tracers, [22] tax return preparers, [23] military installations, [24] and government agencies [25] (including the IRS and state taxation authorities [26]). Enterprising identity thieves have been known to recruit individuals

---

[19] *See, e.g.* United States v. Brown, 399 Fed. Appx. 949 (5th Cir. 2010); United States v. Cage, 458 F.3d 537 (6th Cir. 2006); Managed Care Solutions, Inc. v. Community Health Systems, Inc., 2011 U.S. Dist. LEXIS 138968 (S.D. Fla. 2011), *reconsideration denied* 2012 U.S. Dist. LEXIS 54901 (S.D. Fla. 2012); *see also* FBI, New Orleans Division, Press Release, *Pair Pleads Guilty to Stealing Patient Information to be Used for Personal Gain* (5 January 2012), *available on the Internet at* <http://www.fbi.gov/neworleans/press-releases/2012/pair-pleads-guilty-to-stealing-patient-information-to-be-used-for-personal-gain>.

[20] *See, e.g.* United United States v. Akinkoye, 185 F.3d 192 (4th Cir. 1999), *cert. denied* 528 U.S. 1177 (2000).

[21] *See, e.g.* FBI, Los Angeles Division, Press Release, *Former Employee of Countrywide Home Loans Ordered to Pay $1.2 Million in Restitution for Data Breach Involving Information for Millions of Individuals* (28 September 2011), available on the Internet at <http://www.fbi.gov/losangeles/press-releases/2011/former-employee-of-countrywide-home-loans-ordered-to-pay-1.2-million-in-restitution-for-data-breach-involving-information-for-millions-of-individuals>.

[22] *See, e.g.* United States v. Cummings, 395 F.3d 392 (7th Cir. 2005).

[23] *See, e.g.* United States v. Peck, 62 Fed. Appx. 561 (6th Cir. 2003).

[24] *See, e.g.* United States v. Perkins, 287 Fed. Appx. 342 (5th Cir. La. 2008).

[25] *See, e.g.* United States v. Concepcion, 795 F. Supp. 1262 (E.D.N.Y. 1992); N.Y. City Dept. of Investigation, Release #26-2007, *A Former City Employee Arrested by DOI in Tax Scam is Sentenced to Three Years of Probation in Federal Court* (23 April 2007), *available on the Internet at* <http://www.nyc.gov/html/doi/downloads/pdf/pr26vaught_04232007.pdf>.

[26] *See, e.g.* Testimony of J. Russell George, instant Hearing, pp. 13 - 14 (8 May 2012), *available at* 2012 TNT 90-56; *see also* New York State Office of the Attorney General, Press Release, *Former State Tax Department Employee Sentenced for Using Position to Steal Taxpayer Identities* (25 January 2010), *available on the Internet at* <http://www.ag.ny.gov/press-release/new-york-state-attorney-general-andrew-m-cuomo-former-state-tax-department-employee>.

employed in one or more of the aforementioned industries (and/or other lines of work which give them access to SSNs of employees, customers or clients) to commit fraud on a wholesale basis. [27]

In his Statement submitted for the Record of the 20 March 2012 Hearing of the Senate Finance Subcommittee on Fiscal Responsibility & Economic Growth, [28] the Commentator discusses the distinction between data security and the more inclusive concept of data stewardship.

Deficient data stewardship practices by the New York City Human Resources Administration (HRA) left that agency wide open for fraud. As noted by the court in sentencing some of the perpetuators of that fraud:

> At the most basic level, HRA did not run simple computer checks with the federal Social Security Administration to determine if the social security numbers being used by the defendants had been issued. HRA also failed to forward prompt warnings to the local centers where a problem was brought to its attention. Many HRA workers were so poorly supervised that they did not understand the nature of the warnings they did receive. Information on computers indicating that many families shared the same apartment prompted no action. HRA also neglected to use the Department of Health's database of birth certificates to vet applicants.
>
> While not criminally liable, those responsible for such lackadaisical administration must be considered key participants in this series of frauds. [29]

New York City's HRA interacts with approximately 3 million individuals (out of New York City's population of 8.2 million).[30] The deleterious effects caused by HRA's poor data stewardship practices can only be dwarfed exponentially by analogous data stewardship deficiencies on the part of the IRS, an agency which interacts with almost every business and household in America. The IRS itself must be considered a key participant in the identity thefts it has allowed to be perpetuated upon the public by, inter alia, its failure to correctly match and verify the SSNs of the purported dependents claimed by identity thieves.

The "mousehole" must be plugged by improving the IRS's data stewardship procedures and processes. The IRS's unvigilant practices in failing to verify the SSNs and other personal

---

[27] *See, e.g.* United States Attorney's Office, Southern District of Florida, Press Release, Last Three of Twelve Defendants Sentenced in Massive Bank Fraud and Identity Theft Ring (30 September 2011), *available on the Internet at* <http://www.justice.gov/usao/fls/PressReleases/110930-04.html>.

[28] Posted on the internet at <http://www.fgs.org/rpac/wp-content/uploads/2012/04/senfincomm-taxfraud-20120320-corrected2.pdf>, also available at 2012 TNT 56-30.

[29] United States v. Concepcion, 795 F. Supp. 1262, 1270 (E.D.N.Y. 1992).

[30] *See* N.Y.C. Human Resources Administration / Dept. of Social Services, *About HRA/DSS*, *available on the Internet at* <http://www.nyc.gov/html/hra/html/about/about_hra_dss.shtml>.

data need to be targeted; deep-freezing the DMF will not stop identity theft tax fraud practices such as those recounted by the witnesses at the various Hearings.

Of particular concern is IRS Deputy Commissioner Miller's testimony at this instant Hearing, wherein he states that the IRS is:

> [L]everaging mechanisms to stop the growing trend of fraudulent tax returns being filed under deceased taxpayers' identities. First, we have coded accounts of decedent taxpayers whose SSNs were previously misused by identity thieves to prevent future abuse. Second, we are identifying returns of recently deceased taxpayers to determine if it is the taxpayer's final return, and then marking accounts of deceased taxpayers who have no future filing requirement. Of this season's filings, 91,000 returns have been stopped for this review. Third, we are working with the Social Security Administration in order to more timely utilize the information SSA makes available to us. And we are working with SSA on a potential legislative change to the practice of routine release of the Death Master File. [31]

Conspicuous by its absence is any reference to flagging the SSNs of deceased ***dependents of taxpayers***. [32] Flagging the SSNs of ***taxpayers*** without also flagging the SSNs of decedents who might be the taxpayers' spouses or dependents would certainly not have prevented identity theft fraud such as that described by Mr. Agin at the 2 February 2012 Hearing [33] and by Mr. McClung at the 25 May 2011 Hearing [34] (and also referenced by Ms. Olson at this instant Hearing,[35] and indeed, by Chairman Johnson in his Opening Remarks to this Hearing [36]). Surely the IRS has been aware of the practice since at least 2004! [37]

---

[31] Testimony of Steven T. Miller, instant Hearing, p. 4 (8 May 2012), *available at* 2012 TNT 90-57.

[32] This includes deceased children under the age of one year who would not have been claimed as dependents on their parents' prior tax returns.

[33] Statement of Jonathan Eric Agin, Esq., Hearing on the Accuracy and Uses of the Social Security Administration's Death Master File, House Committee on Ways and Means Subcommittee on Social Security (2 February 2012), <http://waysandmeans.house.gov/UploadedFiles/Agin_Testimony202ss.pdf>.

[34] Statement of Terry D. McClung, Jr., Hearing on the Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury, United States Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth (25 May 2011). <http://finance.senate.gov/imo/media/doc/Testimony%20of%20Terry%20McClung.pdf>.

[35] Testimony of Nina E. Olson, instant Hearing, p. 7 (8 May 2012), *available at* 2012 TNT 90-58.

[36] Chairman Sam Johnson, Opening Remarks, instant Hearing (8 May 2012).

[37] *See, e.g.* United States Attorney's Office, Press Release, 31 March 2004, *available on the Internet at* <http://www.justice.gov/tax/usaopress/2004/txdv04PSedore.html>.

In light of the IRS's prior known dysfunctions in tracking and processing the SSNs of individuals associated with taxpayers (as distinct from the taxpayer herself/himself),[38] Mr. Miller's statements can provide but sparse comfort to Messrs. McClung and Agin and their families, and to those apparently numerous families similarly situated. The IRS needs to establish the connection between the deceased dependent individual and the taxpayer who can rightfully claim the deceased individual as a dependent. And if indeed the IRS is in fact pursuing such measures but Mr. Miller's testimony did not clearly convey that fact, then Mr. Miller needs to clarify this to the Subcommittees and to the American public.

"Credible studies indicate that dates of birth are not the sin qua non of identity theft. The most common form of identity theft arises from credit card theft or check fraud, and ***the least common form arises from stolen social security numbers or other personal information***." [emphasis supplied].[39] If misappropriated SSNs are the ***least*** common form of identity theft, then why is it that such identity thefts are so disproportionately common in connection with tax fraud upon the IRS?

Do not blame the DMF, but look to the IRS's deficient data stewardship practices. Do not blame the mouse, but blame the hole!

C. The Supply and Demand of SSNs for Tax Fraud Purposes:

The proposals to block public access to the DMF are not at all encouraging when viewed through the prism of the economic supply and demand principles. SSNs are valuable commodities for which there is a demand.[40] Prison inmates have sold their own SSNs,[41] and indeed, deceased infants' parents have been known to sell their own departed children's SSNs for

---

[38] *See, e.g.* United States. v. Nielsen, 1 F.3d 855, 857 (9th Cir. 1993), *cert. denied*, 525 U.S. 827 (1998); Wallin v. Commissioner, 744 F.2d 674, 677 (9th Cir. 1984); United States v. Shafer, 1996 U.S. Dist. LEXIS 56165 (E.D. Pa. 1996); Grimland v. Commissioner, T.C. Memo 1993-367; In re Washington, 172 B.R. 415, 418 - 419 (Bankr. S.D. Ga. 1994).

[39] Texas Comptroller of Public Accounts v. Attorney General, 354 S.W.3d 336, 355 - 356 (Tex. 2010) (citing Herb Weisbaum, *Identity Theft Problem: The Facts Behind the Fear*, MSNBC (Oct. 21, 2010, 7:42 AM) < http://www.msnbc.msn.com/id/39763386/ns/business-consumer_news/>.

[40] In addition to commanding a monetary price, SSNs can be stolen and/or bartered. *See, e.g.* Fayton v. Goord, 17 A.D.3d 753, 792 N.Y.S.2d 259 (N.Y. App.Div., 3d Dep't 2005).

[41] *See, e.g.* N.Y. State Dept. of Taxation & Finance, News Release, *Seven Charged For Preparing False Tax Returns* (22 March 2011), *available on the Internet at* <http://www.tax.ny.gov/press/rel/2011/sweeppreparers032211.htm>.

cash [42] (though, given the dependency exemption to the personal Income Tax, [43] parents most likely to consummate such a sale have a significant likelihood of being illegal aliens or other nonparticipants in the voluntary compliance with the income tax laws).

If the DMF were no longer accessible, the many of the fraudsters who depend upon it as a supply source for SSNs would look to other sources, including those previously mentioned in this Commentary, and would be quite willing to pay a higher price for them as a component of the cost of doing business. This would mean, for example, that the errant employees who misappropriate their employers' databases would be operating in a market in which their nefarious services might command a higher price than in an environment such as the one which recently prevailed, where the DMF is freely accessible.

While some embargoes and restrictions on the DMF may well be appropriate, the potentially corruptive effects of the resulting supply and demand curves upon the business and commercial environment ought not be ignored. One must also take into account recent healthcare legislation which serves to increase the demand for healthcare, add additional bureaucracy to facilitate healthcare and its financing, and thereby create more data and databases which would be subject to expropriation by unscrupulous employees.

D. Moving towards Solutions:

America has gotten itself into a situation in which an individual's SSN is so key to his or her daily activities and existence in society that the misuse of a SSN wreaks havoc in a broad spectrum of life. That the data security standards legislated for health care information [44] were never applied to many if not most realms outside the healthcare field only complicates the situation. Therefore, protections and safeguards need to be in place in order to prevent identity theft, and to limit the damages caused when identity theft does occur. The IRS must do its part in its own house in such regard, and, as reflected in Ranking Member Lewis's remarks, [45] will need the cooperation and assistance of other branches and departments of the government in order to do so.

---

[42] *See, e.g.* FBI, Jacksonville Division, Press Release, "Duval County Man Pleads Guilty to Federal Charges of Aggravated Identity Theft and False Representation of a Social Security Number" (22 February 2011), *available on the Internet at* <http://www.fbi.gov/jacksonville/press-releases/2011/ja022211.htm>.

[43] I.R.C. §§ 151 - 153.

[44] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, Title II.

[45] Ranking Member John Lewis, Opening Statement, instant Hearing (8 May 2012), *available at* 2012 TNT 90-40.

Notwithstanding the differing (and often diametrically opposite) viewpoints of various constituencies, two matters are now indisputable:

(1) There are no simple or ideal solutions; and

(2) Doing nothing is not an option for the Congress.

There is no perfect solution, and any solutions concocted will inevitably displease one or more constituencies and cause complications in other areas.

The Commentator has no reason to question the integrity or goodwill of any of the witnesses at the instant Hearing or at any of the abovementioned related previous hearings; if anything, such attributes have been well proven and established. Nor does the Commentator have any quarrel with the qualifications or propriety of the line-up of witnesses; the constricting limitations inherent in the scope and diversity of the invited witness line-ups are easily remedied by the Subcommittees and their staffs inviting public submission of comments and according such comments serious regard.

Nevertheless, there is reason to fear that the Hearings might collectively function as a lynch mob against the public's (including the genealogical community's) interest in accessing the data in the DMF. There is concern that the targeting of the DMF is, perhaps, a convenient exercise in blame assignment so as to avoid the vexing issues inherent in crafting real solutions. As detailed above, the IRS's lax data stewardship practices facilitate the use of the information in the DMF to defraud the public fisc, and closing down the DMF to the public will not stop such depredations.

Ranking Member Becerra's Opening Statement states that "the question of the Death Master File -- the DMF -- also requires striking the right balance." [46] Mr. Black's testimony similarly speaks of "striking a balance between transparency that helps prevent fraud and protecting individuals from identity theft." [47] Striking a fair and appropriate balance needs to be the guiding principle in addressing the systemic problem.

Ms. Olson's dual-sided approach in (1) embargoing the release of info in the DMF for a period; and (2) delaying the sending of refund checks to taxpayers has much merit. Though, as acknowledged by Ms. Olson, her approach is not without downside, it can significantly stanch the raid on the public treasury, increase the likelihood of detection and prosecution, reduce the instances of legal and emotional distress inflicted upon the families of deceased identity theft victims, and boost the public confidence so critical to America's system of voluntary tax compliance.

---

[46] Ranking Member Xavier Becerra, Opening Statement, instant Hearing (8 May 2012), *available at* 2012 TNT 90-37.

[47] Testimony of David F. Black, instant Hearing, p. 4 (8 May 2012), *available at* 2012 TNT 90-59.

That the IRS has not done enough to help identity theft victims is well recognized and beyond cavil; indeed, the week prior to the instant Hearing saw the release of a report by Mr. George's own agency detailing the failings of the IRS in that regard. [48] The rights of identity theft victims must be recognized. This includes the right to know the identity of the identity thief, and the right of civil redress against him or her.

Included in the balance that must be struck is the right of the public to know some if not all of the information in the DMF. Genealogical research is one of many such legitimate uses of such information, of which other representatives of the genealogical community will no doubt provide further details to the Subcommittees in the commentaries they surely will submit. [49]

This Commentary concededly contains some assertions and predictions which may be viewed by some as harsh, extreme, or even cynical. If this Commentary is published as part of the record and made readily transparent and accessible to the public without restriction, then, in future years, public officials and private individuals alike will be able to seek out the Commentator and tell him how erroneous -- or how correct -- subsequent events will have proven those assertions and predictions to be.

10 May 2012
Respectfully submitted,

Kenneth H. Ryesky, Esq.

---

[48] Treasury Inspector General for Tax Administration, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service*, Report No. 2012-40-050 (3 May 2012), *available on the Internet at* <http://www.treasury.gov/tigta/auditreports/2012reports/201240050fr.pdf>.

[49] The Commentator, while certainly in favor of transparency of the DMF, shall defer to those other commentators from the genealogy community and shall not now take up the cudgels for the genealogists' perspectives, other than to remind the Subcommittees that the perceived want of transparency in certain genealogical records has led to a highly visible political distraction in the news media in connection with the President of the United States and doubts, in the minds of some, of his Constitutional eligibility to serve as such.


NATIONAL GENEALOGICAL SOCIETY

3108 Columbia Pike, Suite 300
Arlington, VA 22204-4304

703- 525-0050 800- 473-0060
Fax 703-525-0052

**JOINT HEARING BEFORE THE HOUSE OF REPRESENTATIVES COMMITTEE ON WAYS AND MEANS, SUBCOMMITTEES ON OVERSIGHT AND SOCIAL SECURITY, MAY 8, 2012, ON IDENTITY THEFT AND TAX FRAUD, STATEMENT FOR THE RECORD FILED BY THE NATIONAL GENEALOGICAL SOCIETY**

I. INTRODUCTION

U.S. House of Representatives Committee on Ways and Means, Subcommittees on Oversight and Social Security held a Hearing on 8 May 2012 on Identity Theft and Tax Fraud. Public comments were solicited. We appreciate the opportunity to submit this statement on behalf of the National Genealogical Society.

II. BACKGROUND ON THE NATIONAL GENEALOGICAL SOCIETY AND CONTACT INFORMATION:

The National Genealogical Society (NGS) is a non-profit Virginia corporation, founded in 1903 and has approximately 9,100 individual members and 600 organizational subscribers which include regional, state, and local societies. Although our membership includes many professional genealogists, most of our members are people actively researching their own families. All officers and directors serve as volunteers and receive no compensation for performing their duties.

The mission of the National Genealogical Society is to serve and grow the genealogical community by providing education and training, fostering increased quality and standards, and promoting access to and preservation of genealogical records.

The genealogical community works together through The Records Preservation and Access Committee (RPAC), a joint committee which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS), and the International Association of Jewish Genealogical Societies (IAJGS) as voting members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), and the American Society of Genealogists (ASG) also serve as participating members. RPAC also includes participation from a few of the commercial providers of genealogical information. RPAC meets monthly to advise the genealogical community on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

Contact information: Janet A. Alpert, National Genealogical Society, 3108 Columbia Pike, Suite 300, Arlington, Virginia, 22204-4304, telephone 703-525-0050, fax 703-525-0052, and email janalpert@aol.com. Janet A. Alpert is a member of the National Genealogical Society board of directors, immediate past president, and served two terms as president from 1 October 2006 through 30 September 2010. She previously served one term as secretary from 2004 through 2006. Ms. Alpert has a Bachelor of Arts Degree in Political Science from the University of California, Santa Barbara, California, and a Masters in Business Administration from the

University of Connecticut. She retired in 2004 from a thirty-five year career in the title insurance industry, and now resides in Hilton Head Island, South Carolina. Ms. Alpert is an amateur genealogist who has been researching her family for over thirty years.

III. OVERVIEW OF THE ISSUES

The Social Security Administration's Death Master File (DMF) is a publicly available resource of great value to both family history researchers and professional genealogists. Genealogists use a commercial version of the product called the Social Security Death Index (SSDI). The SSDI has been available to the public since the Consent Judgment, Perholtz v. Ross, No. Civ. 78-2385, Dist. D. C. (April 3, 1980).

Genealogy is different than the other social sciences where researchers draw their conclusions from a broad overview of the available records. Genealogists study specific individuals—their ancestors. Therefore if a genealogist does not have access to the records about the ancestor they are researching, their work may come to an abrupt halt.

I am writing on behalf of the National Genealogical Society, its members, and organizational subscribers about why family history researchers and professional genealogists need access to the Social Security Death Index (SSDI).

1. Many genealogists begin researching their family because there is a part of their family they never knew. The estrangement may have occurred because of adoption, divorce, abandonment, death, or other reasons. Regardless of the cause, learning about an unknown branch of the family helps the healing process. The SSDI has been an essential tool for genealogists looking for relatives who were born in the 19th and 20th centuries and is one of the few nationwide resources to connect their living memory to the historical set of records that allow people to begin their genealogical research.

   From the earliest settlements in America, we have been people on the move, generally migrating west in search of cheaper land and better opportunities. Since Vital Records are kept by state, without the SSDI, no national index will be available to determine where people might have moved. Information contained in the SSDI includes the state where the social security number was initially issued and the social security number, which helps genealogists determine if this is the actual person they are researching. After finding the person in the SSDI, the researcher often writes to the Social Security Administration, OEO FOIA Workgroup, PO Box 33022, Baltimore, Maryland 21290-3022 for a copy of the original Social Security application form, called the SS-5. The SS-5 contains valuable information for family history researchers including full name at birth including maiden name, date and place of birth, current address, and full name of father and mother. The SS-5 is necessary if you are researching someone with a common name, to make sure you identify the correct parents. The researcher pays a fee of $27 for a copy of the SS-5, and a fee of $29.00 if we do not have the Social Security number.

2. Another use of the SSDI is to find the date of death and death location of the person you are researching so you can look for an obituary. Many recent obituaries are available online, but many older obituaries are on microfilm and obtained by writing the local library for a copy. Librarians cannot do an extensive search, but can usually find an obituary if they have the death date. An obituary normally identifies living and deceased relatives, the married names of daughters, and the current cities of residence which is essential information.

3. A third use of the SSDI is to find siblings and cousins when a family carries a disease which can be inherited. In these instances time is of the essence. The first step is to find the aunts or uncles, or great aunts or uncles in the SSDI, and then follow the procedure in (III. 2.) above to locate an obituary. Finding and notifying distant cousins can mean the difference between early detection and treatment versus possible death.

   Each year since 2004, the Surgeon General (see http://www.surgeongeneral.gov) has declared Thanksgiving to be "National Family History Day." When families are together over the holidays or at other gatherings, the Surgeon General encourages families to discuss and write down the health problems that appear to run in their family and to share the information with their family doctor. The Health and Human Services website http://www.hhs.gov/familyhistory/ provides a "My Family Health Portrait" tool for families to record their health history information.

   Diseases residing in estranged branches of the family as described in paragraph III.1. above are sometimes the silent killers. Parents of adopted children are given the health history of the biological parents. However, since the biological parents are often under the age of thirty-years old, sometimes there are few health risks disclosed. If you could ask those same parents about their health history fifty years later, after their parents have died, the answer would be more complete. Therefore it is important for people who are adopted to first identify and then reach out to their biological parents and siblings after they reach adulthood.

4. Professional genealogists need access to the SSDI to continue their livelihood. You can learn more about the Association of Professional Genealogists (APG) which has over 2,000 members in the United States at http://www.apgen.org/about/index.html. In addition to helping clients discover their family history, many professional genealogists have important specialties.
   a. Some professional genealogists work in the field of forensic genealogy. Working with the military they help find the families of servicemen lost in previous military conflicts to assist in the repatriation of the remains.
   b. Others work with county coroners to identify the relatives of unclaimed persons.
   c. Some genealogy clients include attorneys who need to find missing heirs to settle estate cases.
   d. Genealogists who are researching a genetically inherited disease in their family where time is of the essence in locating extended family members why who may have inherited a gene and need to be tested and treated as quickly as possible.

e. Other genealogists specialize in finding the living biological parents or siblings of someone who was adopted.

IV. SOLUTIONS AVAILABLE TO REDUCE TAX FRAUD FROM IDENTITY THEFT

Genealogists are also opposed to identity theft and support efforts to stop it. We support many of the recommendations made at the hearing by J. Russell George, Treasury Inspector for Tax Administration. The Internal Revenue Service (IRS) has recently initiated a number of screening procedures to prevent tax fraud and more can be achieved with implementation of the following:

1. Legislation is needed to provide the IRS with broader access to the National Directory of New Hires wage information which is explained on page 4 of Mr. George's testimony.
2. The IRS has been hamstrung by budget cuts and subsequent reductions of staff. The House of Representatives needs to provide the IRS with more funds to screen and verify approximately 1.5 million income tax returns which do not have third-party information to support the reported income. On page 5 of his testimony, Mr. George estimates an additional $31.8 million for such screening and verifying could help reduce the estimated $5.2 billion annual loss to the Federal Government from tax fraud.
3. The IRS needs to adopt common industry practices for authentication such as security challenge questions as proposed by Mr. George on page 6 of his testimony.
4. Treasury, IRS, and the banking industry need to develop procedures so direct deposit income tax refunds are made only to accounts in the tax payer's name as described by Mr. George on pages 6–8 of his testimony.
5. The National Taxpayer Advocate's report for 2011 specifically highlights the benefits of the IRS Issued Identity Protection PINs and suggests that taxpayers should be allowed to turn off their ability to file tax returns electronically. Tax fraud committed on deceased individuals can be prevented if an executor has the ability to turn off electronic filing.
6. The SSNs of parents should be required when filing a tax return for any minor. If the minor dies, the IRS could have a procedure to flag any filings without the parents' social security numbers, again preventing attempts at fraud.

V. TAX FRAUD REQUIRES A COMPREHENSIVE SOLUTION

The hearing on 8 May 2012 revealed many causes of tax fraud which require a more comprehensive solution than closing public access to the Death Master File (DMF). The Death Master File is a major deterrent to fraud which is used by many industries including small business owners, financial institutions, and life insurance companies. Why risk even greater chance of fraud by changing a system that works for the purposes for which it was designed. Why create additional administrative procedures that burden small businesses and local merchants by requiring them to qualify and sign up for access to the Death Master File.

While we advocate all genealogists should have immediate access to the SSDI, the National Genealogical Society would support the two year delay in access as proposed is S 1543—and if necessary the third year that National Taxpayer Advocate Nina Olson advocated during her oral testimony during the March 20th hearing. This support is with the caveat that certain genealogists are to be eligible for certification for immediate access. These genealogists include: forensic genealogists, heir researchers, and those researching individual genetically inherited diseases whose work is described in (III.4.a–d) above.

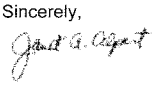
Although these genealogists may be working with other professionals who are certified for access, genealogists are usually self-employed contractors who do not have access to the business databases of the companies who contract with them. It has also been suggested that professional genealogists could use LexisNexis for their research in lieu of the SSDI. Subscriptions to LexisNexis are cost prohibitive for these small business self-employed professionals.

We recommend that the Department of Commerce certify those genealogists with government or legal contracts doing work as forensic genealogists or heir researchers and other certified or accredited genealogists. The Records Access and Preservation Committee (RPAC), described in the "II Background" on page 1, is willing to work with the subcommittee in determining who would qualify.

If the House Committee on Ways and Means is serious about finding solutions to tax fraud, they need to invite witnesses from the business and genealogical communities to testify. One business which has studied identity theft is ID Analytics. A summary of their 2011 study can be found at http://www.idanalytics.com/news-and-events/news-releases/2012/4-23-2012.php. Clearly identity theft is much broader than the use of the DMF by genealogists. The genealogical community represented through the Records Preservation and Access Committee described on page 1 of this testimony, is eager to provide a qualified industry witness upon request.

The National Genealogical Society appreciates the opportunity to present our positions to the subcommittees.

Sincerely,



Janet A. Alpert
Immediate Past President of the
National Genealogical Society and
NGS Representative on RPAC