AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–708

TAX FRAUD BY IDENTITY THEFT, PART 2: STATUS, PROGRESS, AND POTENTIAL SOLUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

OF THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 20, 2012

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE

78–502—PDF WASHINGTON : 2012

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 FINANCE

MAX BAUCUS, Montana, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia
KENT CONRAD, North Dakota
JEFF BINGAMAN, New Mexico
JOHN F. KERRY, Massachusetts
RON WYDEN, Oregon
CHARLES E. SCHUMER, New York
DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
BILL NELSON, Florida
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland

ORRIN G. HATCH, Utah
CHUCK GRASSLEY, Iowa
OLYMPIA J. SNOWE, Maine
JON KYL, Arizona
MIKE CRAPO, Idaho
PAT ROBERTS, Kansas
MICHAEL B. ENZI, Wyoming
JOHN CORNYN, Texas
TOM COBURN, Oklahoma
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina

RUSSELL SULLIVAN, *Staff Director*
CHRIS CAMPBELL, *Republican Staff Director*

SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

BILL NELSON, Florida, *Chairman*

MAX BAUCUS, Montana
KENT CONRAD, North Dakota
JEFF BINGAMAN, New Mexico

MIKE CRAPO, Idaho
TOM COBURN, Oklahoma
RICHARD BURR, North Carolina

CONTENTS

OPENING STATEMENTS

	Page
Nelson, Hon. Bill, a U.S. Senator from Florida, chairman, Subcommittee on Fiscal Responsibility and Economic Growth, Committee on Finance	1
Burr, Hon. Richard, a U.S. Senator from North Carolina	4

WITNESSES

Miller, Steven T., Deputy Commissioner for Services and Enforcement, Internal Revenue Service, Department of the Treasury, Washington, DC	5
Cimino, Ronald A., Deputy Assistant Attorney General for Criminal Matters, Tax Division, Department of Justice, Washington, DC	7
Olson, Nina E., National Taxpayer Advocate, Internal Revenue Service, Department of the Treasury, Washington, DC	8
Augeri, Sal, detective, Criminal Intelligence Bureau, Tampa Police Department, Tampa, FL	19
McKay, Bernard F., vice president, global corporate affairs, Intuit, Inc., Washington, DC	21
Trusko, Kirsten, president and executive director, Network Branded Prepaid Card Association, Montvale, NJ	24

ALPHABETICAL LISTING AND APPENDIX MATERIAL

Augeri, Sal:	
Testimony	19
Prepared statement	31
Burr, Hon. Richard:	
Opening statement	4
Cimino, Ronald A.:	
Testimony	7
Prepared statement	34
Responses to questions from subcommittee members	44
McKay, Bernard F.:	
Testimony	21
Prepared statement	48
Miller, Steven T.:	
Testimony	5
Prepared statement	54
Nelson, Hon. Bill:	
Opening statement	1
Prepared statement with attachments	64
Olson, Nina E.:	
Testimony	8
Prepared statement with attachments	69
Trusko, Kirsten:	
Testimony	24
Prepared statement with attachments	94

COMMUNICATIONS

Federation of Genealogical Societies	111
International Association of Jewish Genealogical Societies (IAJGS)	116
Massachusetts Genealogical Council	124
Records Preservation and Access Committee (RPAC)	127
Ryesky, Kenneth H.	134

TAX FRAUD BY IDENTITY THEFT, PART 2: STATUS, PROGRESS, AND POTENTIAL SOLUTIONS

TUESDAY, MARCH 20, 2012

U.S. SENATE,
SUBCOMMITTEE ON FISCAL
RESPONSIBILITY AND ECONOMIC GROWTH,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Bill Nelson (chairman of the subcommittee) presiding.

Present: Senator Burr.

Also present: Democratic Staff: Ryan McCormick, Legislative Assistant. Republican Staff: Mike Quickel, Senior Policy Advisor.

OPENING STATEMENT OF HON. BILL NELSON, A U.S. SENATOR FROM FLORIDA, CHAIRMAN, SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH, COMMITTEE ON FINANCE

Senator NELSON. Good morning. Senator Crapo is under the weather with a bug that is going around. So he is going to miss all of this morning, and, hopefully, he will be well enough that he can get here when we have a number of votes that will be occurring on the floor of the Senate come 11:30.

I want to thank the witnesses who are here. I want to thank everybody who is interested in this topic, and it has generated quite a bit of interest.

And is it not interesting that all of a sudden police departments are seeing street crime drop, drug dealing drop, house burglaries drop? And when that happens, you know that something has happened.

Well, I think we have uncovered it, the police departments have uncovered it, and that is going to be the topic that we are going to discuss today, from two panels of witnesses, and get at this question of ID theft and how it is now involving the IRS.

This is a serious crime. A south Florida Federal prosecutor recently described it as an epidemic. People describe it as "cocaine on a card." And that south Florida prosecutor told the CBS affiliate in Miami that it is a lot of money, and people are having parties in their homes and training others on how to commit this crime.

There was a big training seminar, if you can believe it, on how to get people's Social Security numbers and then to use them. Well,

he is talking about thieves stealing people's ID to get tax refunds. And it is evident now that it is a crime that is skyrocketing, and it is across the country. We just happened to see it pop up first in Florida.

There have been hundreds of thousands of cases in which unsuspecting and law-abiding taxpayers are having their lives turned upside down by identity theft and then tax fraud. They have their tax refund stolen, and then they are delayed when the IRS sorts out the mess. And to the poor taxpayer, it is unfair and it is unjust.

I want to show you a chart. This chart is the amount of identity theft cases in the IRS which the IRS received between 2009 and 2011. It tripled. And the most recent data available from the IRS, through March 7, 2012, indicate that the agency is tracking nearly 300,000 identity theft cases.

Tax fraud through identity theft has become a street crime. Instead of stealing cars or selling illegal drugs, more and more criminals are looking with envy at the ease others have in taking other people's money through tax fraud. And it can be committed anonymously. All the fraudster has to do—and let us not sweeten up that word—all the criminal has to do is to file a false tax return electronically then have the tax refund loaded onto a prepaid debit card.

They never have to use a real physical address or even open a bank account. They do not have to use a crowbar or a gun or a knife. And the thief is nearly impossible to track down.

The CBS affiliate in Miami even found that software to enable these kinds of schemes is being made available online for free. It has gotten to the point where criminals are now getting organized to institutionalize tax fraud by teaching classes of 50 to 100 people on how to file fraudulent tax returns. And it is clear that the problem is not confined to one area of the country. It stretches from Miami up to Detroit, and all the way to the coast of California. And we saw a huge spike in Tampa.

Our local police, they are on the front lines trying to fight this battle, and they are the ones who originally notified us, as well as the victims, by saying, "What's going on here? Street crime is going down."

Last September at Florida's WFLA, there in Tampa, channel 8 reported that the police had arrested 47 individuals and recovered $130 million in stolen Federal tax refunds from an organized ring of criminals.

We are very grateful for our local police, because they are not letting the restraints, which we are going to talk about, of Federal inhibitions get in their way of going after these criminals.

Now, the IRS has made strides in modernizing their internal systems to flag potential cases of identity theft, and the Department of Justice has successfully prosecuted a number of these cases. But this crime—this particular crime—keeps growing.

According to the FTC, identity thieves are now using the Federal Treasury as their ATM of choice, with the agency citing tax fraud as the leading complaint filed by identity theft victims, as shown here. [*See* p. 67 in the appendix.]

Look at this. The dark gray column is credit card fraud. It is going down. Government benefits fraud, the white column, is going down. Tax or wage-related fraud is going up over the last 3 years. And so you can see that tax-related identity theft is rising, while credit card-related identity theft is declining.

So here we are in this era of government cuts. We are going to need to make sure that taxpayer dollars are safeguarded from theft and abuse, and we need to stop these thieves from stealing. And this may be as much as a $10-billion rip-off of the taxpayer per year.

I am grateful that the IRS has given serious attention to this issue, but the reality is that we are only starting to scratch the surface. And we are also here about the moral condition in this country, because when the police apprehended, in Tampa, a number of these criminals and talked to them, they did not think they had done anything wrong. They think that the fact that they did not use a crowbar or a knife or a gun or break into somebody's home or stop them at a stoplight in a bad part of town or sell some drugs, that doing this electronically through a laptop onto a debit card they thought was okay, with the taxpayer getting ripped off to the tune of maybe as much as $10 billion.

Well, we are here today not only to look in the past, but also try to figure out the possible solutions to this problem. I have introduced legislation, the Identity Theft and Tax Fraud Prevention Act. It is a start. The bill would give the IRS and identity theft victims the means to better detect and prevent this disastrous offense. And the IRS, to their great credit, has already implemented some of these reforms administratively.

The bill would strengthen penalties for tax fraud through identity theft and the improper disclosure of taxpayer information. It gives all ID theft victims a unique personal identification number to include on their tax return in order to prevent fraud and avoid tax refund delays.

It allows identity theft victims to opt out of the electronic filing and do paper filing. If it is done by paper, these guys—these criminals—cannot do it. But why should the taxpayer have to go through the laborious process of a paper filing? This is just one of the terrible consequences of what is going on.

The legislation secures the Social Security numbers of deceased Americans so that the fraudsters cannot use them to file fake tax returns.

I must say, the Commissioner of Social Security told me that he cannot administratively stop putting up dead people's Social Security numbers immediately. All we want him to do is to delay it. And if you have to get to a subset, delay children's on behalf of grieving parents, so that their child's Social Security number does not go up on the Web and then that grieving family becomes a victim on their tax return. He said he cannot do it. Senator Durbin and I vigorously disagree.

So we did the next best thing. We went to some of these genealogy websites. There are half a dozen major ones. And to their credit, a couple of them said that they will stop putting up the Social Security numbers, because that is another source of information for these criminals.

The bill further reallocates IRS resources for tax fraud prevention and detection, and it improves coordination between the IRS and local authorities, which has been a problem. Take, for example, the Tampa police. The Tampa police would like to have the ability of having the Federal Government, through the IRS, get into the act. They have to use existing statutes, State statutes, and the prosecutors to go after these criminals.

IRS, of course, is trying to protect the confidentiality, which they do so judiciously and wisely, and yet that is why we need a new law to give them the ability to share this information with local law enforcement so they can go after these criminals.

In the meantime, to the IRS's credit, what they have done is, if the taxpayer victim will give them a waiver, then they can share this information with the local police so the local police can go after these criminals.

The bill further extends the authority for the IRS to share this information with Federal and State prison authorities, and the IRS has already administratively shared that information with the prison authorities.

So, with those reforms fully enacted, I believe that we can bring this problem under control. We can protect victims. We can stop this taxpayer rip-off. And so I am really looking forward to this discussion.

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

Senator NELSON. Senator Burr, since Senator Crapo is under the weather, would you like to give an opening statement?

OPENING STATEMENT OF HON. RICHARD BURR, A U.S. SENATOR FROM NORTH CAROLINA

Senator BURR. Mr. Chairman, I would love to. And I want to thank you on behalf of the minority side for holding this hearing.

I think if we can answer one question that you raised, it is solved—stop thieves from stealing. I am afraid that is a little more difficult than it sounds. And I think my brethren from Louisiana would be disappointed to find out that we might secure Social Security numbers. It may reduce the vote total of Louisiana elections if we do that.

We are all concerned about tax fraud. It is occurring in our country, identity theft. The chair and I both know the cyber security threat that we are under, and that is part of the risk you take when you integrate the use of transfer by electronics the way that we do as a society. And we have a generation that banks and lives 100 percent of the time electronically.

The rapid growth of the Internet is welcome and it is useful. The genie is not going to go back in the bottle nor should it. However, criminals have long been using the Internet for fraud, and it is time for the government to catch up in the way that it ensures that we have the same capacity for rapid response as do criminals. It costs taxpayers money, it harms the privacy of citizens, and it threatens the military and industrial base through espionage in this country.

What is happening with the IRS is one more indication that the government is struggling to keep up with the pace of change and

the volume of attacks. Government cannot fix this problem alone. You can only chase a fleeting enemy so much. We have to change the battlefield. We need to actively involve the dynamic private sector.

The private sector is more nimble than government agencies, and it must be an essential partner in fighting back against extremely smart, often state-trained fraudsters who constantly morph their schemes to exploit our weaknesses.

The problem is also an indication of our current tax code. The simpler and fairer we make our tax code, the easier it will be for citizens to avoid overpayment of taxes.

I look forward to this important hearing. I look forward to learning more about how we can work with the private sector to close the security leak and the possible solutions in your legislation to the problem today.

I thank the chair.

Senator NELSON. Thank you, Senator.

Our first panel is Steven Miller, the Deputy Commissioner for Services and Enforcement of the IRS; Ronald Cimino, Deputy Assistant Attorney General for Criminal Matters in the Tax Division of the Department of Justice; and Nina Olson, the National Taxpayer Advocate for the people at-large from the IRS.

So I want to welcome you all. And in that order, if you will make about a 5-minute statement, your complete statement will be put in the record, and then Senator Burr and I will get into questions.

Mr. Miller?

STATEMENT OF STEVEN T. MILLER, DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT, INTERNAL REVENUE SERVICE, DEPARTMENT OF THE TREASURY, WASHINGTON, DC

Mr. MILLER. Thank you, Chairman Nelson, Senator Burr. My name is Steven Miller. I am the Deputy Commissioner, as you mentioned, at the Internal Revenue Service.

Over the past few years, identity theft has grown. It starts outside the tax system. And I should note, Mr. Chairman, that identity theft, as you mentioned, occurs in many places across the country, but does appear disproportionately in Florida.

The IRS is confronted with the same challenges as 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 refunds to ensure that all are correct. We have to balance the need to make payments in a timely manner with the need to ensure that claims are proper and that taxpayer rights are protected.

Let me begin by describing our efforts at up-front protection. In 2011, the IRS identified and prevented the issuance of over $14 billion in fraudulent refunds. A great deal of this was identity theft.

This year, we will stop even more returns. So far, we have identified almost 2 million returns for review. That number approaches the total for all of last year. Until we complete our review of these returns, we do not have a precise tally of how much is identity

theft, but it is likely that at least the majority of the above inventory is in that category.

As evidenced by the number of returns stopped, we have improved our up-front screening filters to stop false returns before a refund is issued.

We have done other changes as well. These changes include improvements to certain filters specific to identity theft but also in related areas, such as decedents, prisoners, returns held because the identity is previously suspected of having been taken, and returns rejected because somebody tried to file without the appropriate personal identification number.

More specific to this filing season, we have also done the following. Despite substantial cuts in our budget, we have added hundreds of staff in this area and intend to add hundreds more. We issued special identification numbers, the so-called PINs, to expedite filing for those taxpayers whose identities have been stolen. There are 250,000 of those PINs that have been sent out at this point.

We are also accelerating the matching of information returns so that we can help spot fraud up front. There are new procedures to allow us to match returns to lists of taxpayers' information that law enforcement officials believe may have been stolen. We have improved collaboration with software developers and others to determine how we can better partner to prevent theft. And we are working with the Social Security Administration on modifications to their practice of making the death master file public.

In addition, our criminal investigation division continues to increase its work in the area. In 2012, we will spend more than 400,000 hours of investigative work in this area, almost double that of 2011.

In my written testimony, you will see details of this work, including a description of a week-long sweep in January that led to over 900 criminal charges across 23 States. We will also begin a pilot shortly that will improve the process for local law enforcement to obtain tax return data vital to their local law enforcement purposes. 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 I have mentioned, we have added staff to resolve cases faster. And, of course, the PINs that I spoke about earlier are going to assist identity theft victims with getting through our systems and filing future returns. We have also trained 35,000 of our employees to identify and deal with identity theft situations.

Let me conclude. Our work here is critical. We see identity theft as affecting the way people view our agency. We cannot be lax in stopping fraud and in our treatment of those who have had their identities stolen.

I cannot tell you that we will beat this problem in one year, Mr. Chairman, but I can say our work in 2012 represents real progress. They are not the end of our efforts.

And, obviously, I will be more than happy to answer any questions.

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

Senator NELSON. Thank you, Mr. Miller.

Mr. Cimino, I mispronounced your name, and I apologize. And thank you for your work at the Justice Department going after tax fraud.

So, please, your comments as well.

STATEMENT OF RONALD A. CIMINO, DEPUTY ASSISTANT ATTORNEY GENERAL FOR CRIMINAL MATTERS, TAX DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. CIMINO. Chairman Nelson, Senator Burr, and members of the subcommittee, I would like to thank you for the opportunity to appear before you this morning to discuss the Department of Justice's efforts to combat tax fraud through identity theft.

The Department greatly appreciates the commitment the chairman, the subcommittee, and the staff have made to highlight this serious crime of tax fraud by identity theft.

Over the past few years, identity theft has become a major problem for Federal, State, and local law enforcement across the country. Combating identity theft is one of the Department's top priorities, as set forth in our current strategic plan. And, as the Attorney General has said, our core mission is to pursue justice for criminal acts, and that pursuit includes justice for the victims of the crime.

In criminal matters involving tax fraud by identity theft, the IRS investigates these matters and then refers them to the Department of Justice. Thereafter, the Tax Division supervises or directly prosecutes these matters.

The Tax Division prosecutors work closely with assistant United States attorneys across the country to develop and prosecute these tax refund crimes. The cases are prosecuted by both Tax Division prosecutors and assistant United States attorneys, either separately or jointly.

Federal task forces comprised of Federal, State, and local law enforcement personnel are often used. These task forces include representatives from the Federal Bureau of Investigation, the Secret Service, the Postal Inspection Service, IRS Criminal Investigation, as well as State and local law enforcement entities.

The close working relationship developed among task forces' partners enables the Department to share our knowledge and to leverage our resources in order to combat refund fraud.

In every one of these cases, Federal prosecutors strive to ensure that victims' rights are respected. While some prosecutions may only involve a single defendant or a small group of defendants, the majority of the cases involve large-scale identity theft schemes affecting many victims. Regardless of the number of the victims or the amount of the refund involved, the Department evaluates the overall merits of each case to ensure that the matter can be successfully prosecuted.

There are cases in various stages in which the Department is investigating and prosecuting perpetrators of tax fraud by identity theft. As described in my written testimony, there are statutory restrictions on my ability to comment on the specific facts of these cases. However, I can assure the subcommittee that the Department is vigorously prosecuting these cases.

Since the beginning of the 2012 fiscal year, Federal prosecutors have indicted more than 80 individuals and convicted 21, many of whom filed multiple false returns claiming stolen identities. Courts have also responded to the seriousness of these crimes by sentencing defendants to significant terms of incarceration; in one instance, imposing a sentence of more than 15 years.

As IRS Deputy Commissioner Miller has noted, stopping identity theft before it starts is critical. However, while prevention and early detection are always the first and best line of defense, the Department recognizes that prosecution is a critical and an effective tool when it comes to combating tax fraud.

The Department is committed to working with its Federal, State, and local law enforcement partners to combat identity theft. When we prosecute these cases, we send a clear message to those who are engaged in this conduct that they will be held accountable for their actions.

I would like to thank you again, Mr. Chairman, for the opportunity to appear before you, and I am happy to take any questions from you and the members of the committee.

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

Senator NELSON. And that is a true statement that prosecution deters these fellows, because it was not even the Department of Justice, it was the local prosecutors in Tampa who, once they got on it using State laws, which are limited tools—that is why we need to get to these—lo and behold, this crime went down, and the normal street crime, which is awful, the drugs, et cetera, then went back up.

So clearly, prosecuting is a deterrent to this specific crime.

Ms. Olson, you are the National Taxpayer Advocate. You are an independent voice for taxpayers in the IRS. Taxpayers are getting ripped off here, not to speak of the grief that they go through when their identity is stolen or the grief of a grieving parent whose child has just died and the child's identity is stolen and then used for a tax fraud refund. Please share with us.

STATEMENT OF NINA E. OLSON, NATIONAL TAXPAYER ADVOCATE, INTERNAL REVENUE SERVICE, DEPARTMENT OF THE TREASURY, WASHINGTON, DC

Ms. OLSON. Well, thank you, Chairman Nelson, Senator Burr, and members of the subcommittee. Thank you for inviting me to testify today about tax-related identity theft.

Since 2004, I have extensively written 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 have become identity theft victims.

The IRS has adopted many of my office's recommendations and made significant progress in this area with respect to the victims in recent years. Notwithstanding these efforts, however, identity theft continues to pose significant challenges for the IRS, and it has become an organized, large-scale operation.

My written testimony addresses this subject in considerable detail. I will highlight four points that I think deserve particular emphasis.

First, I am concerned that the Federal Government continues to facilitate tax-related identity theft by making public the death master file, a list of recently deceased individuals, including children, that includes their full name, SSN, date of birth, date of death, and county, State, and zip code 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 the death master file records in light of the Freedom of Information Act. For that reason, I strongly support legislation that would eliminate the uncertainty by making clear that public access to the DMF can and should be limited. However, I want to make clear that my legal staff believes the Social Security Administration has at least a reasonable basis for seeking to limit public access to the death master file. And, if legislation is not enacted, I encourage the SSA to act on its own.

Second, I am aware that some State and local law enforcement agencies would like more information to enable them to help combat identity theft and are seeking access to tax return information to do it. I have significant concerns about loosening taxpayer privacy protections and believe this is an area where we need to tread carefully.

But I think we may have a solution. I am very pleased that the IRS Office of Chief Counsel recently advised that, because a return filed by an identity thief may be considered return information of the victim, the victim may obtain a copy of the bad return, as well as other information pertaining to the bad return. The victim then may authorize the IRS to share all of this information with State and local law enforcement agencies.

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.

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 and to try to assist them. However, for the week ending March 16, the level of service on this unit's phone line was 13.7 percent, up slightly from 11.7 percent the week before, but meaning that only 1 out of every 7 calls was answered. And those callers who did get through had to wait on hold an average of 1 hour and 11 minutes. More support for this unit is clearly required.

Fourth and last, I want to squarely present a big picture issue that Congress and others will need to carefully consider if tax-related identity theft and other refund fraud continues. At the same time that 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 marginal improvements in both areas, the two goals are fundamentally at odds. Given the constantly evolving types of identity theft schemes, IRS identity theft filters will never be perfect. Therefore, we have to set our priority. If our overriding goal is to process tax returns and deliver tax refunds as quickly as possible for the vast majority of persons who file legitimate tax returns, it is inevitable that some iden-

tity thieves will get away with refund fraud, and some honest taxpayers will be harmed.

On the other hand, if we decide to 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 million 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 is no way around these tradeoffs.

Thank you, and I will be delighted to answer questions.

[The prepared statement of Ms. Olson appears in the appendix.]

Senator NELSON. Waiting for 1 hour on hold to get information or to report a case, I mean, that is just unconscionable. Who in this day is going to wait?

So that means it does not get reported.

Ms. OLSON. Right.

Senator NELSON. Unless it is worked out at the local level.

Ms. OLSON. These are taxpayers who have received a letter from us saying we are looking at your return and who have been stopped by our filters. And in that group of taxpayers are the legitimate taxpayers whose returns have also been stopped by our filters, and this unit is supposed to be dealing with those taxpayers.

I think we did not estimate well how many calls were going to come in, but, as well, with all of these things that are happening with identity theft and other refund fraud, there are only a certain number of employees to go around and, if you remove them from one area to answer the phone in another, taxpayers are harmed in that other area.

Senator NELSON. Senator Burr?

Senator BURR. Thank you, Mr. Chairman.

Ms. Olson, is there an obvious reason that the Social Security death list should be public?

Ms. OLSON. I think that the origin of the publicity came from the insurance industry that found getting the information about deceased individuals helped protect against insurance-related fraud, claims against policies where the person had not died or someone was posing as the person, the deceased person. I do not know whether you can pose as a deceased person.

And we think that narrowly crafted exceptions can be created to address these other areas of fraud. The courts over the years have recognized privacy interests in light of the Freedom of Information Act for family members of the deceased.

Senator BURR. But if we focused on those areas of our economy that might need that information and crafted legislation saying, "You have access, but you have to request it," so that Social Security is able to check out whether this is a credible source that is seeking it, you do not think that there is anybody left out there who would be harmed in any way for this not to be available?

Ms. OLSON. I think that is right. I think we are really talking about a delay. For taxes, we only need it delayed for 3 years, the date of death and 2 years after that, and then there are not really any tax issues pertaining to that number, by and large.

Senator BURR. Well, I think there is a big question as to whether that is beneficial to have it out there at any time.

Ms. OLSON. Right.

Senator BURR. Other than the economic reasons that it should be available.

Mr. Miller, let me ask you, does MasterCard or Visa or any other private sector company have this problem as big as the IRS has it; do you know?

Mr. MILLER. I do not know that, Senator. I would say there are differences, obviously, in terms of the ability to track transactions. For example, the credit card companies have a long number of trends of items that are being charged, where they are being charged, and that is a much easier trend to see than what we see on an annual basis.

There are an awful lot of people who move in a given year, more than 10 million. There are 40 million people who change jobs, and there are births and deaths in a year. It makes for a more difficult sort of analysis than a credit card company that has the ability to track on a monthly basis where people are spending.

Senator BURR. So let me ask you, is there a role for the private sector to play in partnership with the IRS to try to enhance the validity of the claims that are being made to you that these are actually real people?

Mr. MILLER. Absolutely. I think there are various ways that could happen. I think we are talking now to the software developers—you will be able to speak to them on the second panel—and the debit card providers as well. We are talking to the banks. We have relationships with over 70 banks now.

Banks have a very good ability to take a look to see what is going into their accounts, and they have know-your-customer rules that provide them with the ability to stop a lot of fraud.

They sent us back more than $290 million last year. I will bet we beat that by far this year. So we are working with banks.

Software developers we have made strides with, as well, in the past few months. We have worked with them to determine what is the information that they can utilize. During their tax filing process to spot fraud, we have also built a gateway for that information to flow into the IRS.

So we are working with both of those, and I do think there is quite a bit of leverage that could be done there.

Senator BURR. Mr. Cimino, how difficult is it to prosecute these cases?

Mr. CIMINO. The difficulty ranges, I think, with the wide differences in some of the crimes that we are investigating. Some of these are interstate organizations. Others are very local crimes.

We have had great assistance from local authorities, as the chair has said, providing information.

Senator BURR. I was going to ask you. We have actually embedded Department of Justice attorneys into the system out there helping prosecutors, have we not?

Mr. CIMINO. We have. Several things are occurring to try to deal with the most recent problems that we have seen. First of all, we are working as closely as we can with our IRS criminal investigators, and we have redoubled our efforts to offer resources from the

tax division to U.S. attorneys in terms of prosecutors and information about how these schemes are working in other jurisdictions.

Senator BURR. Let me ask you. This was actually a program that Deputy Attorney General Cole approved where attorneys who work for various litigation divisions of the Department of Justice, such as the antitrust and civil divisions, could be transferred to U.S. attorneys' offices throughout the country for a 6-month program.

In fiscal year 2012, under the program, attorneys were assigned to the U.S. attorney's offices throughout the country. Attorneys generally do not work on tax issues in this program.

I understand that the Department of Justice litigation division opted out of this program, but that the tax division did not opt out and that, of the 76 attorneys who applied for the program, 33 of them are working the criminal component of the tax division.

These are the same attorneys who handle identity theft prosecutions and are charged with stopping refund fraud, among other tax crimes. Thirty-three attorneys constitutes almost 15 percent of the entire criminal component of the tax division.

Considering that the identity theft refund fraud issue is an ongoing and active issue, do you think it is wise to divert a significant portion of the criminal component of the tax division to deal with a non-tax issue?

Mr. CIMINO. What we in the tax division did, Senator, is to place for 6 months our prosecutors and our civil litigators—they are actually both—of the numbers that you referred to, across the country.

In part, when this was done, some of them were working more on their own cases in the jurisdiction. We tried to establish, where we could, that the work that they were working on would continue with even closer ability.

In other instances, I think it will actually help U.S. attorney's offices to have prosecutors in their jurisdictions to work with and to coordinate with other assistant United States attorneys.

Senator BURR. Mr. Chairman, just one last question. I will open it to anybody who would like to answer it.

If fraud using a Social Security number had the additional penalty of disqualifying that individual from participation in Social Security for life, would it have an impact on how many people chose to participate in fraud using Social Security numbers?

Ms. OLSON. I do not know whether the people who are participating in this crime report their illegal income to Social Security so that they would be eligible for Social Security in the future. I do not know that people involved in this kind of crime think about the long-term consequences.

They might think about jail terms, but receiving Social Security may be really far off. So I do not know.

Senator BURR. I do not disagree with the chairman's statement that penalties need to increase.

Ms. OLSON. I agree with that.

Senator BURR. I doubt there are many who, when they turn 65, turn down the Social Security check that they are getting. It might be an interesting thing for you to think about and respond back if you think it would have a positive impact.

But I think we need to look outside the box if, in fact, we want to try to fulfill what the chairman said, and that is an active pre-

vention mechanism. It will take all the above, but it will also take a penalty structure that makes somebody think twice before they venture in.

I want to thank all three of you for your testimony.

Thank you, Mr. Chairman.

Senator NELSON. Thank you, Senator Burr.

Let us go through a few things. One hour and 6 minutes for IRS to answer a call. What do we need to do to improve that?

Mr. MILLER. Well, Mr. Chairman, we are going to have to add more people to that unit is the short answer. There are not that many calls coming in, but those that come in have to be answered faster than that. I quite agree.

Senator NELSON. In the case that we have been looking at, when a fraudster files first and then walks away with a stolen refund, and then the legitimate taxpayer files and he is second in line, should it not be relatively easy for the IRS to measure the revenue loss as a result of that?

So how much do you think has been stolen from the taxpayer?

Mr. MILLER. Mr. Chairman, I do not have that number available. We may—and we talked to staff about this—we may be able to approximate the number. It would be an interesting thing to do, because, as I mentioned, banks are returning money. We are retrieving checks. And so it would have to be netted in some fashion.

But of those cases that we have now determined who is the right person, we should be able to get you something in terms of the revenue that was related to the first checks that went out in those cases.

So we can come back to you on that, Mr. Chairman.

Senator NELSON. Well, in the case of Tampa, if it is over $130 million and it is just in a short period of time of one filing just in one community, you can imagine how, if you multiply that nationwide, what this thing could be.

I know the IRS does not endorse legislation, but what do you think about what we have filed as a way of trying to help you stop this crime?

Mr. MILLER. I would think, Mr. Chairman, we would welcome the opportunity to talk about it. I would group some of the provisions into three categories.

There are those, as you mentioned, that we support sufficiently, that we have sort of done something on already. For example, you have the liaison with the local law enforcement through our criminal investigation. That has happened right now, especially in Florida. At this point, we have approved that.

Senator NELSON. So you agree with that as long as you get a waiver from the aggrieved taxpayer.

Mr. MILLER. That is a second piece. The liaison with local law enforcement was one. The waiver aspect I would like to talk just a moment about, if I could.

It is true, as you mentioned, Mr. Chairman, that we are limited in what we can supply to local law enforcement. We can supply to State tax officials tax information for tax charges. That does not exist, obviously, in Florida. We do not have that ability. We are not permitted to give that to local law enforcement.

What you have mentioned and what Nina mentioned as well is, we do have the ability, we believe, to seek a waiver from the victim and make that bad return that clogged them up in the system available to local law enforcement.

So we are going to try to pilot something that would look like this. When local law enforcement pulls over someone in their car who has a batch of debit cards, has a batch of Social Security numbers, local law enforcement provides that batch of Social Security numbers to us. We will find some victims whom we know are the correct person from that list. We will then seek waivers on behalf of local law enforcement in order to provide a set of returns, probably not all of them, but a set of returns to local law enforcement so that they can pursue their local case.

I think that is what we will try to do with this. It is not a perfect sort of fix, but it is a workaround that will help with this problem.

Senator NELSON. It will not be a fix until you get statutory authority.

Mr. MILLER. It is not a substitute for our unfettered ability to share with local law enforcement. The balance here, Mr. Chairman, is that—and one can argue it either way.

There is a reason why we are limited in providing to local law enforcement in an unfettered manner. That is because we treat and Congress has treated tax return information as sacrosanct, as truly needing protection.

So we would have to talk about what sort of safeguards would be put in place were a change of law to occur.

Senator NELSON. Well, I do not want to get down in the weeds, but successful prosecution is down in the weeds, and if the local prosecutors only have the State statutes of theft and fraud, and they cannot get to the IRS return as evidence of that, then that is where the prosecutorial system of upholding the law breaks down. And so that is what we have to get at.

Mr. MILLER. I agree, Mr. Chairman. So the waiver is one way to get part of the way there. We are more than willing to talk about other changes.

I want to note one other aspect, and that is that the prisoner part of your bill, which we very much support, we actually no longer can share information with State and local prisons because that part of 6103 expired at the end of last year.

We need that extended, and the administration has a proposal that would even improve a little bit upon what you are suggesting, and we would love to talk to you about that as well.

Senator NELSON. Well, tell us about the success of 6103.

Mr. MILLER. The success. I can tell you about the success of the prisoner work that we have done.

Senator NELSON. That is correct.

Mr. MILLER. They are in abeyance, because the ability has stopped. But we had agreements with 22 States to share data with them.

For example, if they find that there—or if we find that one of the prisoners is engaged in this sort of theft, we were able to provide them with return information that would allow them to start on a disciplinary process with respect to those prisoners. That, we thought, was vital.

So that is the piece that expired at the end of last year that we truly could use help in extending.

Senator NELSON. And you cannot go after those prisoners anymore because of that expiration?

Mr. MILLER. We could prosecute each of the prisoners under filing false returns. It probably is a better way of doing it if we are able to work with the local prison authorities to engage and stop that going forward and create disciplinary action in the prison itself.

Senator NELSON. Why don't you share with everybody what the prisoners were doing?

Mr. MILLER. We are a few years into prisoner fraud. We have stopped so far this year about 135,000 returns filed from prisoners. They got into the refund fraud business a little ahead of the general gang activity that we are seeing in Florida and elsewhere at this point, but they are doing basically the same sorts of things.

Sometimes they are working with folks on the outside of the prison walls, sometimes inside, and sometimes it is strictly identity theft. Sometimes it is something different than that, where they are expanding on the earned income tax credit or other refundable credits to get more than they are otherwise entitled to.

Senator NELSON. And were they getting the identities, the Social Security numbers, through the same means, through the Internet?

Mr. MILLER. It will depend. And I wanted to mention that is one way of getting identities. One way is the death master file. There are numerous other ways.

In fact, I would think that in Florida, at this point, a larger problem is the theft from institutions. We see it across the country. We see thefts from schools. We see thefts from hospitals, doctors' offices.

Wherever a Social is being used, that is a target for theft, and that is the start of this process. We do really need to tighten down the protection of Socials outside of the Internal Revenue Service, frankly, as a good way to stop some of this.

Senator NELSON. What was the source of the numbers for the prisoners?

Mr. MILLER. It will depend, Mr. Chairman. Some of it, I am quite sure, could have been the death master file. Some of it probably was stolen from hospitals and supplied to them, some of it from fellow prisoners, quite frankly. So it probably was not one single item.

Senator NELSON. What do you think about the Social Security Commissioner who says basically that he is unwilling to take any steps to reign in his agency's practice of publicly disseminating the Social Security numbers of deceased persons?

Mr. MILLER. I will split that into two pieces, if I could, Mr. Chairman. First, we would love to see something done with respect to the death master file, and we are working with the Social Security Administration, and we are working with the administration more generally on what we can do about that.

I cannot speak to what the Social Security Commissioner has said or done.

Senator NELSON. Well, he says his hands are tied by the Freedom of Information Act.

Mr. MILLER. Then that is a legal question that is best answered by others than me.

Senator NELSON. Well, I disagree with him. But maybe that is another reason why we need this legislation passed.

In your testimony, you referred to a new procedure the IRS is developing to allow the local police access to falsified returns if the taxpayer, the true taxpayer, fills out that waiver.

Would you describe that again for everybody?

Mr. MILLER. Sure. That is actually, Mr. Chairman, what I was describing when I talked about the local law enforcement pulling over somebody with those Socials, supplying the IRS with the Socials, our looking at those Social Security numbers to see, do we know some true taxpayers in those categories? To the extent we find them, we reach out to those individuals, asking them, "Will you supply a waiver to local law enforcement of your 6103 rights so that we can get the information to them to prosecute?"

That is what we will be piloting, and I would hope we would start it, frankly, in the Tampa area.

Senator NELSON. Once your agency knows that a refund has been sent to a fraudster, so you know that is done, to what degree does the IRS work with the prepaid card companies and tax preparation software companies to track down this criminal?

Mr. MILLER. We would work with the debit card companies and the software developers more to prevent it than after the fact, although we could do either, actually. And, as I mentioned in my discussion with Senator Burr earlier, we have worked with the software companies to determine what information they do have as part of the filing process that they can utilize to sort of track the fraud.

There is a provision of the Internal Revenue Code that prohibits—and I am sure Mr. McKay can speak to this more intelligently than I can—but there is a provision of the Internal Revenue Code that limits the ability of software developers to utilize taxpayer information, for very good reasons. We do not want them utilizing that information for inappropriate commercial purposes.

But we have found, a month or two ago, that we think they can utilize some of that information to spot fraud. We have now built a gateway from the software companies to the Service to provide information on that.

We are trying to work with the debit card companies, as well, and we are not quite as far along in that endeavor.

Senator NELSON. Just so everybody understands, if you do not have an address and this fraudulent tax refund is going to a debit card, it is very, very hard to track down this criminal, because you do not have an identity unless, like the Tampa police, they stop them on the street and find all this stuff in their car, in a stop unrelated to the tax fraud.

Let me turn to you, Mr. Cimino. In Tampa, 47 arrests busted this tax-related identity theft ring. There has not been a single Federal indictment. Tell me about that.

Mr. CIMINO. Actually, Mr. Chairman, in Tampa, there has been a series of very successful prosecutions of identity theft by the U.S. Attorney for the Middle District of Florida. I alluded to them in my written testimony.

Senator NELSON. But not this kind of theft.

Mr. CIMINO. I believe that it is very similar, if it is not the exact thing that the chair is interested in. In the written submission, I talked about two cases that were part of this Federal and State task force in Tampa, which was called Rainmaker, where the U.S. attorneys were successful in convicting people in the midst of these refund schemes. And recently, the first person whom I mentioned in my testimony, Shawntrece Sims, was sentenced to a 9-year prison sentence for both tax fraud and mail fraud related to identity theft, just as we are talking about, the type that we are talking about.

Senator NELSON. Then I want to let the record show that you have had a successful prosecution.

Mr. CIMINO. Thank you.

Senator NELSON. Well, as a prosecutor, do you have enough tools in your toolbox to go after these crooks?

Mr. CIMINO. There is a wide variety of charges that our Federal prosecutors and tax prosecutors use. The charges range from those that are found in the Internal Revenue Code to those found in our regular criminal law.

I think the answer is, yes, we have the ability to charge these crimes and to prosecute them.

Senator NELSON. For the committee record, tell us the percentage of case referrals from the IRS that have led to prosecutions and convictions.

Mr. CIMINO. Recently, for the past fiscal year, Mr. Chairman, I think there were 200 individuals referred and approved for prosecution. Over the last 3 years, the number has continued to increase. I can, for the staff, following the hearing, give you more specific data on that.

Senator NELSON. All right. We would like that, and the record will be held open for that information.

[The information appears in the appendix on p. 44.]

Senator NELSON. In your testimony, you note that DOJ can formally deputize local law enforcement so that they can assist Federal law enforcement in the Federal tax investigation.

In the local law enforcement, they are only permitted to access information related to the Federal tax investigation, and those who participate in the investigation are not permitted to utilize the tax information in a State or local tax investigation or prosecution.

So what is the policy rationale for this firewall?

Mr. CIMINO. This is, as you and others have spoken about, a provision in the Internal Revenue Code that provides privacy rights to each of our taxpayers, section 6103.

The legislation, since 1976, struck a balance between the privacy rights of individuals and the genuine need of law enforcement, both Federal and State.

When there is a task force, as you mentioned, and individuals outside the Federal law enforcement agencies participate, there is a procedure where they can be deputized as U.S. marshals and then they work and have access to and use of this tax return information as others in the Federal system do. But they are subject to the same restrictions, and that is that it must be used for Federal law enforcement.

Senator NELSON. Ms. Olson, what do you think about the proposed legislation?

Ms. OLSON. Well, I think it is excellent. As noted in my testimony, I do caution about the 6103 exceptions. And I just have to say, as someone who has practiced in tax since 1975 and lived through what Congress did in 1976 to rein in the rampant exposure of tax return information all over the place in government, both Federal, State, and local, I really want us to be very careful.

One thing that I would suggest, if you are going to make a statutory exception for State and local government, is that you put limits on its re-disclosure and its reuse so it is being used for the specific purpose of these investigations and prosecutions and not filtering out to other activities. And the rationale behind that is that taxpayers—we think that confidentiality has some impact on their willingness to tell us all their information, because they know that others are not going to get a handle on it.

But otherwise, I think that the legislation is excellent.

Senator NELSON. In your testimony, in your written testimony, you mention about the Social Security numbers of deceased people. And you know about some of the genealogy websites that have since voluntarily redacted the Social Security numbers.

Now, the legislation would prevent the Social Security Administration from releasing the personal information of the deceased in the year of their death and the year following. So it would delay the publication of those numbers for a couple of years.

Do you think that if that change is enacted in law, it will make it harder for these thieves to perpetrate this tax fraud?

Ms. OLSON. I think in that area, it will. I would add one more year, because for surviving spouses, widows or widowers, they can file as married-filing jointly for 2 years, the year of the date of death and then the year after. So that really means 3 years: the date of death, the filing season for the date of death, and then the filing season for the year after.

So you really have 3 years to delay the release. And then at that point, the IRS can disable that Social Security number. If, for some reason, somebody comes in with a tax purpose, we would have to work that case individually, but we can handle that. And then we can just block any returns that come in and then, eventually, the criminals will learn that it is not a profitable avenue for committing fraud, because we can block it.

After that date, you could release the information, maybe redact all but the last four numbers still for the genealogists and things like that.

Senator NELSON. Thank you all. This has been most illuminating.

I want to call up the second panel, please.

Good morning. I want to thank our second panel. Sal Augeri is a detective with the Criminal Intelligence Bureau, Tampa Police Department.

By the way, have you seen Federal prosecutions in Tampa?

Mr. AUGERI. I have seen offers given to the defendants in which they have pled. Shawntrece Sims went to trial, and it was a successful prosecution.

Senator NELSON. All right.

Bernard McKay is chairman of the American Coalition for Taxpayer Rights and vice president of global corporate affairs for Intuit, the parent company for TurboTax.

Ms. Kirsten Trusko is president and executive director of the Network Branded Prepaid Card Association.

So, thank all of you for coming. Again, if you will give about a 5-minute statement, then we will get into some questions.

Mr. Augeri?

STATEMENT OF SAL AUGERI, DETECTIVE, CRIMINAL INTELLIGENCE BUREAU, TAMPA POLICE DEPARTMENT, TAMPA, FL

Mr. AUGERI. Good morning, Mr. Chairman. I am Detective Sal Augeri with the Tampa Police Department. And on behalf of Mayor Buckhorn, Chief Castor, and the city of Tampa, thank you. I would like to thank you for allowing me to testify this morning.

The IRS is facing a major crisis, and criminals are stealing hundreds of millions of dollars from hardworking taxpayers. When I first became a police officer with the city of Tampa 27 years ago, crack cocaine was just hitting the streets, and, within 2 years, it had become an epidemic and no community was immune.

Tax refund fraud mirrors the spread of crack cocaine. In late 2010, members of the Tampa Police Department became aware of the severity of this crime in our community. Reports of identity theft increased, as well as encounters with individuals and groups committing tax fraud.

Officers would conduct traffic stops and find individuals possessing various driver's licenses and identification cards in different names. Large numbers of tax return debit cards and ledgers containing hundreds of names and Social Security numbers were found. Officers found groups of individuals in motel rooms filing fraudulent tax returns on stolen laptop computers. And many of our narcotic operations turned up evidence of tax refund fraud.

Although tax fraud is not a local issue, citizens were coming to us for help, and we, in turn, contacted the IRS and quickly found they were of little assistance in these investigations.

The tax code prevents the IRS from sharing information with local law enforcement. In addition, we were advised that there was a $100,000 investigation-to-prosecution threshold that had to be met on the Federal level. Most of the cases we encountered were from $9,000 to $10,000 in fraudulent filings, although numerous cases surpass the threshold and reach into the millions.

Originally, suspects obtained the names and Social Security numbers of the deceased people from historical and genealogy websites. When that information became difficult to get, individuals who worked in assisted living facilities would obtain the necessary information on patients. Names were now being sold to the suspects from accomplices who worked in businesses, medical offices, schools, and anywhere that personal identification could be compromised.

In April of 2011, we learned that several agencies were trying to address the growing tax fraud issue. A task force was created, and the United States Secret Service took the lead. Members of the

United States Postal Service, Hillsborough County Sheriff's Office, and the Tampa Police Department joined forces.

In the Tampa Bay area at that time, tax refund fraud was completely out of control, and it was estimated to be in the hundreds of millions of dollars. The task force concentrated on known suspects committing the fraud, as well as collusive businesses cashing the fraudulent checks for as little as $.20 on the dollar.

On September 1, 2011, Operation Rainmaker took place with the issuance of five Federal search warrants targeting collusive businesses and suspects engaged in tax refund fraud, identity theft, and credit card fraud. Forty-seven arrests were made and several cars were seized, including a Mercedes, two Jaguars, a BMW, and a Bentley Rolls Royce.

Despite all of the arrests and the compelling cases made, there have been no Federal indictments. More disturbing, there is nothing to indicate that most of those arrested have slowed their tax fraud activities.

Due to the inability to obtain tax information, our investigations center on identity theft. In most instances, this is a very simple offense to investigate. But due to the lack of information-sharing, locating the victims was difficult and time-consuming.

In addition, we had to locate video of the suspect using the debit card that was issued in the name of the victim of the initial identity theft. Cases would take 3 to 6 months to investigate, and suspects were not charged with the actual initial crime of the tax refund fraud.

Only the IRS can levy this type of charge and that more serious penalty. Our local State attorney's office and the U.S. attorney's office have assisted us as much as possible.

Postal workers have been threatened concerning the delivery of fraudulent tax returns, and FedEx stopped delivery of Green Dot debit cards to Florida in 2011. Neighborhood residents have been threatened by thugs to stay away from their mailboxes.

The magnitude of the problem is staggering. In September of 2011, we arrested an individual who committed $9 million in tax refund fraud. He was initially arrested on the State charge, bonded out, and, to date, has not been indicted. We have no reason to believe he has stopped committing this crime.

The Postal Service has seized thousands of debit cards and U.S. Treasury checks. And, even if the debit cards had been seized by the Postal Service or blocked by the card companies, a paper check was generated by the Treasury and sent to the original address the cards had been destined to.

A temporary benefit from the tax fraud was our exaggerated reduction in crime in our city. We pride ourselves on our crime-fighting efforts, and we have been very successful over the years.

Since tax refund fraud was so simple, most of the criminals started to get involved with it. In the past few months, we have seen the dramatic increase in violent crime targeting those involved with committing tax fraud. And due to the large amounts of money the suspects have, they have been targeted for armed robberies and home invasions. An attempted homicide last week in Tampa is rumored to be the result of unpaid tax money between two individuals involved in this crime.

The tax return process was constructed for law-abiding citizens, with a focus on expedient returns. The process needs to be revamped. The IRS will tell you they have filters and flags in place to detect the fraud, but there are countless examples of the system failing. In the first few weeks of this tax season, we had four Tampa police officers who were victims of identity theft and then subsequent tax refund fraud.

Officer David Curtis, a Tampa police officer, killed in the line of duty in 2009, had his identity stolen shortly after his death. His wife, who was left with four young sons, had to navigate through that difficult process of straightening out and submitting her legitimate return.

We will not be able to investigate our way out of this problem, and I believe this issue can only be corrected by fixing the point of filing. Criminals committing this type of fraud have no reservations about stealing the government's money, and I believe that the legitimate American taxpayer would be outraged that their hard-earned dollars sent to the government were subsequently being sent out by the government to those criminals at an alarming rate.

And, therefore, we believe that the Federal Government needs to reexamine its method of accepting tax returns and the subsequent refunds issued to its citizens.

Thank you.

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

Senator NELSON. Detective, thank you for your service to our community and to our country.

Mr. AUGERI. Thank you.

Senator NELSON. Is it true, in Tampa, when you all arrested some of these people, that they actually thought that they were not committing a crime?

Mr. AUGERI. I do not know if it is so much they do not think that they are committing a crime. The majority of the people that we are involved with are already receiving Federal or State assistance to begin with, whether it is food stamps, medical, housing, and their impression is it is just more government money to be had.

Senator NELSON. And did they say that to you?

Mr. AUGERI. Yes, specifically, "The government's got deep pockets."

Senator NELSON. You gave the example of the difficulty that the widow of a Tampa police officer is having, trying to raise four sons and needing a refund. Do you recall how long it finally took her to get that straightened out?

Mr. AUGERI. I do not know the exact time, no, sir.

Senator NELSON. Well, let us go to Mr. McKay. Thank you for being here. Share with us your statement.

STATEMENT OF BERNARD F. McKAY, VICE PRESIDENT, GLOBAL CORPORATE AFFAIRS, INTUIT, INC., WASHINGTON, DC

Mr. MCKAY. Thank you, Chairman Nelson. My name is Bernie McKay. I am here today as chairman of the American Coalition for Taxpayer Rights. ACTR is a 10-member coalition of the largest companies in the tax preparation industry serving U.S. taxpayers, and includes tax preparation firms, software developers, and financial institutions.

The members of ACTR are committed to high quality services, transparency in pricing and service terms, and have a long history of assisting many millions of U.S. taxpayers in their annual voluntary compliance obligations under our complex Federal income tax system.

It is also this industry that answered the call of Congress back in 1998 to convert the U.S. income tax compliance method to a lower cost, more accurate, and faster return submission system, where 80 percent or more of all individual tax returns would be filed electronically instead of on paper.

This industry worked cooperatively and collaboratively with the Federal Government over a period of a little more than a decade to achieve consumer adoption of electronic filing as the preferred method of income tax compliance in this country.

The IRS and industry worked together to achieve this major objective, and, today, well in excess of 80 percent of all individual income tax returns are, indeed, filed electronically.

One of the ACTR member companies is Intuit, at which I am the global chief public policy officer and vice president for global corporate affairs. The other ACTR member companies include Refund Advantage, H&R Block, Jackson Hewitt, Liberty Tax, Republic Bank, Santa Barbara Tax Products Group, 2nd Story Software, TaxSlayer Software, and Universal Tax Systems–CCH.

All ACTR companies strictly adhere to IRS regulation 7216, which is the private sector corollary to the 6103 privacy statute you have been discussing this morning. All of our companies take the privacy and security of taxpayer data very seriously. All of our companies have business controls to detect and respond to suspicious activity, and to prevent and combat all types of tax fraud, which span all segments of the taxpayer services industry.

The IRS and industry have been working together cooperatively for many years. It is important to note the realities of the modern world and the widespread growth of identity theft as a global criminal phenomenon. Identity theft takes many forms and strikes at every type of commerce, in both bricks and mortar and web-based environments.

In the web-based world, it most routinely strikes at everyday e-mail, seeking to deceive individuals and businesses and to attempt to steal and misuse sensitive information of all kinds. It is increasingly the focus of significant domestic and international efforts to combat it on both a privacy and security level, involving both prevention and law enforcement.

ACTR supports and recognizes the central role that the IRS and the U.S. Department of Treasury play, assisted by the Department of Justice and local law enforcement, as part of their duty to protect the U.S. taxpayers from identity theft and fraudulent tax schemes.

The IRS has thousands of auditors and criminal investigators. It has subpoena power, and many other tools to prevent or address fraud, including critical information databases built over decades of experience that only it can access.

Notwithstanding the key role that IRS plays, industry recognizes it also has responsibility to detect and report suspicious activity and help prevent fraud. In fact, ACTR companies routinely report

suspicious activity to the IRS when they see it, although we lack the more complete picture that is obtained by the IRS when it analyzes multiple government databases so that they find criminal activity that they have known and seen patterns of before, and as new patterns are emerging.

Across the private sector, privacy and security protection, together with fraud prevention, are major focuses of continuous private investment and dedicated effort. An example of the type of fraud that private companies are seeing and reporting are instances where identity theft has occurred and a criminal group relentlessly submits return after return that utilizes real taxpayer stolen identities, correct Social Security numbers, dates of birth, and copies of an apparently correct W–2.

These groups are almost always using multiple tax preparation companies and modalities to insert numerous returns with the same data. Using information technology to identify such fraudulently filed returns is both lawful and appropriate and does not implicate any value of trust we in the industry have with our customers.

Last year, ACTR companies reported that hundreds of thousands of returns should be reviewed by the IRS due to suspicious activity, and our financial companies stopped payment of hundreds of millions of dollars in refunds and saved the U.S. Government millions of dollars in those public funds.

Mr. Chairman, let me turn for just a moment to the redoubled antifraud collaboration that is currently ongoing between the IRS and the private sector tax preparation industry.

In October 2011, the 10 members of the American Coalition for Taxpayer Rights proactively reached out to the IRS to determine how we might work together with the IRS to an even greater degree to assist in combating tax fraud. The response from the IRS has been positive and encouraging, and the IRS has been appropriately sensitive to the confidentiality and privacy issues that are implicated anytime taxpayer information and tax return information is involved.

Last fall, the members of the coalition met with Deputy Commissioner Steve Miller—who testified before you this morning—and many senior IRS staff and officials at their headquarters and mapped out a cooperative agenda for combating these challenges to the tax system. That is an ongoing work effort.

Over several meetings, the IRS and ACTR member companies designated personnel to participate in two fraud task force working groups, one group made up of tax preparation and software developer companies, which I lead for the industry, while the other group is made up of financial institutions, which are typically involved in the receipt and processing of income tax refunds.

This collaboration with IRS is an ongoing work effort, and it evolves over time as the IRS identifies appropriate ways in which we can help.

In conclusion, Mr. Chairman, the reality is that the increase in the incidence of identity theft and associated fraud is likely to continue across all forms and modalities of commerce, not just here in the United States, but abroad as well, as criminal groups gain greater technological capability.

Unfortunately, the financial attractiveness of tax systems here and abroad is also likely to continue as a target for such criminal activity. The increased focus by the IRS on prosecuting tax fraud has led to the discovery of organized criminal rings in places such as Florida, New York, and Belarus. These crime rings and their use of identity theft to perpetrate tax fraud violate various title 18 provisions and are rightly receiving increased attention by Federal, State, and municipal law enforcement.

ACTR and industry companies are fully cooperating with law enforcement as they seek to break these criminal rings. We recognize there is no silver bullet. Rather, fraud prevention is a multi-layered defense and a team effort that involves the IRS, law enforcement, taxpayers, and the private sector.

Mr. Chairman, ACTR wants to continue to be a part of the solution, and that is why we will continue to collaborate closely with the IRS for the benefit of the U.S. taxpayer to detect and combat tax fraud so that our real customers, the taxpayers, can continue to prepare and file their returns with ease, with peace of mind, and with security.

Thank you, Mr. Chairman.

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

Senator NELSON. Are you aware of conferences or seminars where people are taught to do this?

Mr. MCKAY. We have read and seen the same news reports. In addition, as the industry has cooperated with local law enforcement authorities, such as those in Tampa, we are hearing this from them as well.

Senator NELSON. All right. Let us ask the detective. Did any of this go on in Tampa, where they were actually doing seminars to teach them how to do this?

Mr. AUGERI. I think the generalization of the seminars was a little misconstrued. What it is is groups of individuals, you can be looking at five, six, 10, 15 people, getting together and discussing having issues getting their fraudulent returns sent through. And then each person would give their little input on how to correct that problem to get that submission in.

So they were actually working together in groups to beat the system.

Senator NELSON. All right. Ms. Trusko?

STATEMENT OF KIRSTEN TRUSKO, PRESIDENT AND EXECUTIVE DIRECTOR, NETWORK BRANDED PREPAID CARD ASSOCIATION, MONTVALE, NJ

Ms. TRUSKO. Chairman Nelson and members of the subcommittee, my name is Kirsten Trusko. I am the president of the Network Branded Prepaid Card Association and appreciate the opportunity to appear before you today on behalf of the NBPCA and its members, and to testify on the important topic of tax fraud through identity theft.

The NBPCA is a nonprofit trade association founded in 2005. Our membership includes the payment networks, card issuers, program managers, processors, and other third parties. Network branded prepaid cards bear the logo of the payment network—

American Express, Discover, MasterCard, or Visa—and are similar in use and function to credit and debit cards.

They give consumers a safe, secure, and convenient payment choice to satisfy a range of uses from everyday transactions, such as retail purchases and bill payment, to receipt of funds, like payroll, government benefits, and now, more commonly, tax refunds.

To obtain a card, the consumer may go to a branch or website of a financial institution or program manager or to a retail location to obtain a temporary prepaid card. These temporary cards are limited in functionality, as they do not provide cash access or permit additional value loads until the cardholder has provided verifiable personal information, as they do in opening an online bank account. Upon verification, a personalized card is issued, with an associated ABA bank routing number, and, like bank debit or credit cards, must be activated before it becomes fully functional.

It is important to note that the USA PATRIOT Act and the Bank Secrecy Act impose specific compliance requirements on issuers of general purpose reloadable cards, and, under recent FinCEN rules, providers and sellers of prepaid cards must maintain substantially similar compliance programs. This is outlined in detail in my written statement.

Issuers and providers of general purpose reloadable cards are required by law to collect four pieces of personal information from a prospective cardholder: name, street address, identification number, and date of birth. Identity is verified through some of the same services used by financial institutions to verify customer identity, and this process is the same as that used by a financial institution when a customer applies for a credit card or an online bank account.

If the identity of the prospective cardholder cannot be successfully verified, the account is not established.

The NBPCA recognizes that, like other consumer financial products, prepaid cards are susceptible to misuse. Fraudulent use of prepaid cards with tax refunds was flagged last year as a concern, which was a driver in the NBPCA's forming of the Prepaid Anti-Fraud Forum. This forum brings together prepaid fraud experts to establish industry-leading practices, collaborate with law enforcement, and host educational forums for industry and government.

Early this year, NBPCA's antifraud forum compiled a confidential handbook with tax refund fraud mitigation strategies for its members. To avoid tipping off potential fraudsters on methods used to mitigate the use of prepaid cards in tax refund fraud, my statement today is limited in specific details, but I am happy to share more detailed information with you in a confidential briefing.

Some key antifraud processes and fraud detection practices include watching for patterns of suspicious activity by the consumer, freezing accounts and filing suspicious activity reports when fraud is suspected, identifying hot zip codes and fraud trends across the country, using additional screening processes when incoming ACH loads are identified as being an income tax refund, and rejecting and returning suspicious ACH value loads. Industry efforts have so far resulted in over $1 billion of value loads to prepaid cards being returned to the IRS based on attempted fraudulent tax refunds.

In closing, as the subcommittee continues to examine this issue, the NBPCA would urge you to take into consideration the large number of legitimate filers who rely on prepaid products to receive their tax refunds quickly, safely, and cost-effectively. Any additional processes and procedures must be balanced against increasing the burden to the honest, hardworking taxpayers who are depending on the timely receipt of their tax refunds to pay bills or fulfill other family needs.

Before imposing any additional burden to the consumer, there are ways that industry and IRS can work more closely together to prevent fraudulent tax returns on prepaid cards with minimal impact on the millions of honest filers. I would be happy to discuss these in a closed forum.

Through our prepaid antifraud forum, the NBPCA remains committed to continuing our work with the IRS criminal investigation division, the Department of Justice, and the FBI to enable more effective information-sharing.

Thank you for the opportunity to appear before you today. The NBPCA stands ready to work with you, and I would be happy to answer any questions you may have.

[The prepared statement of Ms. Trusko appears in the appendix.]

Senator NELSON. Well, the balance that you suggested is, in fact, what we are trying to find here: how to stop the criminals and not inhibit the system in any way from the vast majority being able to get a refund in a timely manner.

Now, other than the things that you mentioned that your industry is doing, are there any identifiable markers in the software products that could help the IRS or law enforcement track down the criminals?

Ms. TRUSKO. There are ways that we could work together and collaborate even more closely together. The Prepaid Anti-Fraud Forum is a new group that was started June of last year, and, with the members of the Network Branded Prepaid Card Association, all of the cards are issued by financial institutions.

So I think as we collaborate further together on identifying what is already being used, what could be used more effectively, and identifying new ways to work together, we would welcome the discussion.

Senator NELSON. But as of this moment, you cannot suggest—and, of course, we will continue to collaborate.

Here is the problem. A refund comes to something that does not have an address, does not have an identification number, does not have anything. It is a prepaid debit card. Now, if it is detected because a false return has been filed and the victim suddenly figures it out, how can we help law enforcement to go after that criminal, whose only identity at this point is a debit card that is prepaid?

Ms. TRUSKO. So when the consumer opens—goes to open a prepaid debit card, they supply their name, their address, their ID number, and their date of birth.

Senator NELSON. Is that checked against some documentation?

Ms. TRUSKO. It is. It is the same documentation and check that would be used when opening an online bank account. So, if the fraudster gets through that to open the account, there are additional checks used to validate the accounts.

Senator NELSON. Mr. McKay, what do you think about tax software products having an identifiable marker?

Mr. MCKAY. Senator, one of the things that the IRS cannot do, and I would recommend probably you would not want any of us to do, is to publicly talk about particular trade craft methods and procedures that could tip off criminals and make it easier for them. But our coalition would be very happy to work collaboratively with you and your staff, as we are with the IRS, on looking at the ways that there can be increased prevention, as well as increased catching of fraud on the back end.

The interesting thing is the dichotomy as we talk about the Internet world. The reality is that IRS has more ability through its filters to catch potential fraud in an electronically filed return right up front before it goes into processing than ever existed for paper returns.

You have a Social Security match that the IRS makes that, if you do not pass that, the return gets rejected and sent back. There is an AGI match, where the taxpayer has to identify what their previous year's AGI was, which is a concept by itself that many taxpayers are not readily familiar with, and, to respond, the individual must actually have some real information about the prior year's return.

There is a PIN, much along the lines of what you suggest in your legislation, that is already part of the way electronic filing takes place up front now.

All of those filters exist today. While they are not foolproof—and there are returns that get through at the end that are a challenge on the processing end——

Senator NELSON. Let me stop you right there. How is there a PIN when, in fact, the PIN number that we have been talking about is something that, fortunately, the IRS has assigned the aggrieved taxpayer who has been ripped off?

Mr. MCKAY. Well, this is a different PIN for a different purpose, and this is a self-selected PIN that the taxpayer has to give another identifier for in order to get that PIN. And this PIN is part of the standard up-front electronic filing of the return itself.

And what I was suggesting is, simply, those filters never existed for paper. Any paper return that went through the mails was accepted and processed.

But that does not mean that there is anything about that to rest on and feel that that is sufficient. However, there is a foundation that electronic filing is built on, and some experience now over the last couple of decades with the IRS of being able to see where things could also be tightened on the back end.

So I think the collaborative work effort is now going to be critically important.

Senator NELSON. Detective, what was the year that the Tampa police officer was killed?

Mr. AUGERI. 2009.

Senator NELSON. And this is 2012. So this has gone on 3 years.

While we have been having this hearing, I just got an e-mail from Tampa Police Chief Castor that says that the widow, Kelly Curtis, still has not gotten this problem sorted out with the IRS. That has gone on 3 years.

Mr. AUGERI. I stand to be corrected. I am sorry. David Curtis was murdered in 2010. We had another officer killed in 2009.

Senator NELSON. 2010.

Mr. AUGERI. 2010.

Senator NELSON. Going on 2 years.

Mr. AUGERI. Correct.

Senator NELSON. Ms. Curtis still has not gotten this issue worked out. And you can imagine, with four children, she needs to get a refund, and here it has been 2 years and she still has not gotten it sorted out.

Now, this is why I wish the Deputy Commissioner of the IRS were still here, but I imagine he has turned on his television back in his office. And this is the kind of stuff that we are trying to get to, because taxpayers are being taken advantage of enormously. And in the case of this policeman's widow, 2 years have gone by and she still cannot get it straightened out.

Is it any wonder that people are frustrated?

Detective, my sense from your testimony is that these are not just isolated instances. These are organized networks, gangs or syndicates.

Mr. AUGERI. Yes. They are groups of people who network with other criminals, and the majority of the stuff we are seeing now has spread from Hillsborough County into the surrounding counties and then into the adjoining States of Georgia, Alabama, and Louisiana.

Senator NELSON. Mr. McKay, you spoke very well about how the software industry recognizes its shared responsibility to detect and report. Does Intuit, the maker of TurboTax, have a legal or moral obligation to verify the identity of individuals filing Federal tax returns with the use of these products?

Mr. MCKAY. Whether the company is Intuit or any of the other member companies in this coalition, the trust of the customer in their tax compliance process is the single-most important asset of the relationship with the company, of your reputation.

We have a responsibility in this industry, we have a responsibility as a company, to do everything in our power to help ensure that the taxpayer is safe, that the taxpayer is able to have confidence that their information remains confidential and private.

In fact, there is an interesting fact that is relevant here. There are many privacy statutes at the Federal level. But the toughest privacy law in the United States is what we know in the industry as IRS 7216. It is tougher than the privacy statute for banking, even for medical records.

So there is not just a moral obligation. There is a legal obligation. But it also goes to if, in fact, integrity is your brand and, if integrity is the service that you are selling and the basis of trust with your customer, there can be no more important obligation.

Senator NELSON. Detective, again, thank you for the dogged persistence of the Tampa Police Department in going after this. Since you all had this major bust of 47 people, describe how much it declined, for how long, and then when it started picking back up.

Mr. AUGERI. The decline that we saw in the actual suspects getting their hands on checks and debit cards came toward the end of 2011, and I just believe it was because of the time of the year,

that it was a little more difficult to get the returns through. It was during that time that we saw a spike in the armed robberies and the home invasions of people who were known to have large quantities of money.

This year, it has completely taken off again. The amount of cards that are coming in, the amount of addresses and personal identifiers we are coming across, is in the thousands.

Senator NELSON. Now, what is that? The amount of personal identifiers; what are you speaking of?

Mr. AUGERI. Officers make stops or, say, we do a search warrant on a narcotics house. Once you get in there, the specific crime you are in there for, you take care of that, but you come across these laptops and ledgers.

Senator NELSON. I see.

Mr. AUGERI. The debit cards, the medical records, and the amounts are staggering.

Senator NELSON. So somebody in the hospital is in collusion with these guys, getting them the medical records so they can rip off——

Mr. AUGERI. Yes.

Senator NELSON. Have you all been able to go and follow that trail and go back to whomever is ripping off the stuff in the hospital?

Mr. AUGERI. We try to backtrack. I can tell you this. It is very difficult. There is a State threshold that they want for the charge of the identity theft. Then, obviously, there is the Federal threshold. For a lot of those times, the criteria, we just cannot meet them. To actually get enough to charge somebody, especially in the State court, is pretty demanding.

We are used to handling the volume and, obviously, the Federal system just cannot handle that volume of suspects.

Senator NELSON. Of these ringleaders that you might bust on a completely different charge, is it typical what you testified, that they are driving around in Bentleys and Mercedes and walking around with all the so-called accoutrements of wealth?

Mr. AUGERI. Mr. Chairman, our criminals in Tampa, who are historically drug dealers, robbers, burglars, they are making money to the tune of $.5 million to $1 million, $2 million a year. And, when I first started looking at that, I thought it was an exaggeration, but when you dig into the cases, they obviously are at that dollar amount.

The vehicles they are driving, the interiors of their homes, property that they are buying outside of the city of Tampa—they like to hang out and congregate in the areas where they grew up, but because there is so much trouble there, they like to move to the outer parts of the county. And they never had that kind of money before.

Senator NELSON. Well, this has all been very illuminating, and I want to thank each of you for your involvement in this.

Let us see if we can maybe get this legislation moving that will give some additional tools to law enforcement and the IRS in trying to get at what has become an obvious criminal problem.

Thank you. The meeting is adjourned.

[Whereupon, at 11:50 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Statement of Detective Sal Augeri, Tampa Police Department

Before the Subcommittee on Fiscal Responsibility and Economic Growth Senate Finance Committee

Hearing on Tax Fraud by Identity Theft

March 20, 2012

The IRS is facing a crisis of epic proportion. Criminals are stealing hundreds of millions of dollars from the hard-working Tampa tax payers. And I'm only aware of what's going on here in Tampa. It won't be easy, but it must be fixed. To ignore this problem is reckless and a major disservice to Americans.

When I first became a Tampa police officer 27 years ago, crack cocaine was just hitting the streets. Within two years, it was an epidemic touching just about every person in every community. The tax refund fraud scams mirror the spread of crack cocaine here in Tampa.

In late 2010, members of the Tampa Police Department became aware of the gravity of the tax fraud issue in our community. There was an increase in reports of identity theft, as well as encounters with individuals and groups that were committing the tax fraud. Officers would conduct traffic stops and find individuals with various driver's licenses and identification cards in different names, large numbers of tax return debit cards, and journals containing names and social security numbers. Officers were also finding groups of individuals in motel rooms filing fraudulent tax returns on stolen laptop computers. Most of our narcotics operations turned up evidence of tax fraud.

Although tax fraud is not a local issue, most of our citizens came to us for help. We in turn contacted the IRS and found out in quick order that they were of little assistance in these investigations. As you are aware, the tax code prevents the IRS from sharing information with local law enforcement. In addition, we were advised that there was a $100,000 investigation/prosecution threshold. Most of the cases we encountered were for $9-$10,000 fraudulent filings, even though there were plenty of cases that reached this threshold and surpassed it, even reaching into the millions.

Originally, suspects obtained the names and social security numbers of deceased people from historical and genealogy websites. When that information ran dry, they turned to individuals who 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.

In April of 2011 we learned that several agencies were trying to address the growing tax fraud issue. In an effort to make an impact, a task force was created that included the Secret Service, Postal Inspectors, the Hillsborough County Sheriff's Office and the Tampa Police Department.

The issue of tax fraud was out of control by this time, estimated to be in the hundreds of millions of dollars in the Tampa Bay area alone. As a result we had to narrow our investigative efforts by focusing on a small group of individuals and businesses that were committing and profiting from tax fraud. The businesses targeted were cashing the fraudulent tax returns for, in some cases, as little as 20 cents on the dollar.

On September 1, 2011, "Operation Rainmaker" took place with the issuance of five Federal Search Warrants targeting businesses and suspects engaged in Tax Refund Fraud, Identity Theft and Credit Card Fraud. Several arrests were made at the state level for Identity Theft and Credit Card Fraud. There were 47 arrests made during this operation. Several cars were seized, including a Mercedes, Jaguar, BMW and a Bentley Rolls Royce. Despite all of those arrests and the compelling cases made, there have been no federal indictments to date. More disturbing is the fact that there is nothing to indicate that any of those arrested has slowed their tax fraud activities.

The inability to obtain tax information caused us to have to investigate the lesser offense of identity theft. In most instances this is a simple offense to investigate, but the lack of information sharing meant that locating the victim of identity theft was difficult if not impossible and required tedious and time-consuming subpoena processes. In addition, we had to have video of the suspect actually using the fraudulent identification. Each case required three to six months of investigating, and none of the suspects was charged with the actual crime they committed: tax fraud. Only the IRS can levy this charge, which carries a more serious penalty than our state charges. Our local State Attorney's Office and the U.S. Attorney's Office have assisted as much as possible.

Postal workers have been threatened concerning the delivery of fraudulent tax return checks, FedEx stopped delivering "Green Dot" tax return debit cards, and citizens have been threatened to stay away from their mailboxes.

For the sake of time, I will highlight two examples that may illustrate the magnitude of this problem. We arrested an individual in September that we know committed at least $9 million in tax fraud. This is the amount that we are aware of. To date he has not been indicted, and we have no reason to believe he has stopped committing this

crime. Another alarming example is a photograph of a room full of tax return debit cards that were seized by the Postal Service. I am talking about thousands of envelopes. These envelopes represented returns that the mail sorters could recognize as being fraudulent: multiple returns to the same address or returns going to abandoned houses. When showed this photograph, the IRS response was that the seizures made little difference, as a paper check was **automatically** sent if the debit cards were not cashed within 30 days.

A temporary benefit of tax fraud was an exaggerated reduction in crime in our city. We pride ourselves on making our city safe through continued crime reduction and have been very successful over the years. Since tax fraud was so simple, most criminals were getting involved. As a result, we saw an exaggerated drop in crime for a short period of time. In the past few months we have seen a dramatic increase in violent crime aimed at those committing tax fraud scams, and home invasions and robberies of those believed to have large amounts of "drop" or tax fraud money. We had a homicide some weeks back that is rumored to be the result of unpaid "drop" money. Tax fraud is viewed as a very lucrative crime to commit; there is relatively little risk of being caught (based on difficulty of investigations), a seemingly endless amount of available money, and the crimes usually don't involve violence.

The tax return process was constructed for law-abiding citizens, with a focus on expedient returns. It is time to revamp this process with a degree of focus on fraud. IRS will tell you that they have filters and flags in place to detect fraud. I can assure you, through countless examples, they do not work.

In the first few weeks of this tax season we had four Tampa Police Officers who were victims of Tax Refund Fraud and Identity Theft. Officer David Curtis, who was killed in the line of duty in 2009, had his identity stolen shortly after his death. His wife, who was left with four young sons, had to navigate the onerous process of straightening out that mess.

In my humble opinion, this problem needs to be fixed at the point of filing. To allow the money to be distributed and then try and investigate is a losing proposition. The one issue we all agree upon is that we are not going to investigate our way out of this problem.

Those who commit these crimes readily explain what they are doing and how they do it, feeling that there is nothing wrong with taking the government's money. They see this as a victimless crime. Nothing could be further from the truth. Try to explain that to the thousands of Americans who have gone through the nightmare of identity theft and the process of trying to right their financial life. Or try to explain to hardworking Americans that the hard-earned dollars they send to support our government are being sent to criminals at an alarming rate.

Department of Justice

STATEMENT OF

RONALD A. CIMINO
DEPUTY ASSISTANT ATTORNEY GENERAL
FOR
CRIMINAL MATTERS, TAX DIVISION,
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

SENATE FINANCE COMMITTEE
SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

CONCERNING

"THE SPREAD OF TAX THEFT BY IDENTITY THEFT"

MARCH 20, 2012

Deputy Assistant Attorney General for Criminal Matters
Tax Division, U.S. Department Of Justice
before the
Senate Finance Committee
Subcommittee on Fiscal Responsibility and Economic Growth
Concerning
The Spread of Tax Fraud by Identity Theft
March 20, 2012

Chairman Nelson, Ranking Member Crapo, and Members of the Subcommittee, thank you for the opportunity to appear before you this morning to discuss the Department of Justice's (Department) efforts to combat tax refund fraud arising from identity theft.

The Department greatly appreciates the commitment that the Chairman, the Subcommittee, and staff have made to highlight the serious crimes of identity theft and tax fraud. The Subcommittee's hearings on May 25, 2011, and this hearing today, bring attention to criminal behavior that threatens the fundamental integrity of our tax system. Although we stand ready to enforce the tax laws whenever and wherever necessary, enforcement is only one element of successful tax administration. Thanks to your efforts, taxpayers will have a greater understanding that they need to detect and report identity theft and tax fraud. Those who are engaged in designing and carrying out these tax fraud schemes will also be on notice that their crimes will be detected and prosecuted to the fullest extent of the law.

In conducting law enforcement investigations, the Department goes to great lengths to ensure that the government's inquiry is complete, and that testimony and evidence are gathered and fully analyzed outside of the public arena. Our policy of not disclosing non-public information about ongoing matters protects the rights of individuals who may be assisting in the investigation, the rights of those under investigation and criminal defendants, and the integrity of the investigation itself. Our ability to comment is also circumscribed by Federal Rule of Criminal Procedure 6(e), which protects the disclosure of grand jury information. In a tax case, the tax privacy statute, 26 U.S.C. § 6103, further limits the government's ability to disclose tax information. Therefore, my remarks today will be limited to information that is already available in the public record.

At some point in our lives too many of us have experienced, or will experience, the stressful moment when we realize that a credit card or our identification is lost or stolen. If we are fortunate, the only cost we suffer is the inconvenience of obtaining new accounts and identification. However, for victims of identity theft, the economic and personal consequences are much more severe and often long-term. As the victims who testified before the Subcommittee's hearing on May 25 eloquently recounted, in addition to suffering the original theft of their identity, the crime against them was

compounded when the stolen information was then used to steal the federal tax refund to which they were legally entitled. Further, when a stolen identity is used to commit tax refund fraud, all Americans are impacted by the loss to the federal fisc.

In recognition of the importance of the problem, the Department and the IRS have devoted significant resources to the successful prosecution of a number of individuals who have engaged in identity theft and tax fraud. While the schemes used to steal identities vary, in many instances the stolen identity was used to access an unwitting victim's legitimate tax refund. Depending on the facts of a particular case, we can bring a variety of charges, including aggravated identity theft, filing a false claim for refund and conspiracy. While each prosecution may only involve a single defendant or a small group of defendants, in the majority of cases the number of incidents and victims is significantly greater.

In the last several years, the Department has successfully prosecuted a variety of cases in which a stolen identity was used to commit tax refund fraud. Here are some recent examples of successful prosecutions of refund fraud involving identity theft:

- In December 2011, Shawntrece Sims, a Tampa, Florida resident, was sentenced to nine years in prison for a tax and mail fraud scheme. Sims

admitted to obtaining social security numbers of other individuals and using this information to file false tax returns. In many cases, the individuals were not aware that their identifying information was being used and in other cases, the individuals were deceased. Sims was ordered to pay $672,887 in restitution to the government.

- In November 2011, Roger Snells, also of Tampa Florida, was sentenced to 54 months in prison for tax fraud and aggravated identity theft. Snells admitted to using identifying information of deceased individuals to electronically file fraudulent tax returns with the IRS. This case was part of Operation Rainmaker, a coordinated effort by the United States Attorney's Office, the U.S. Secret Service, U.S. Postal Inspection Service, IRS Criminal Investigation, the FBI, and the Tampa Police Department.
- In January 2012, Marsha Elmore, an Alabama tax return preparer, was sentenced to 184 months in prison for filing false claims, wire fraud, and aggravated identity theft. Elmore admitted to steal tax refunds by filing false tax returns using stolen identities, including names, Social Security numbers, and dates of birth. She was ordered to pay over $1 million in restitution to the IRS.

- In December 2011, Janika Fernae Bates, a resident of Millbrook, Alabama, was sentenced to 94 months in prison following her conviction at trial on charges of aggravated identity theft, wire fraud, and conspiracy to make false claims for tax refunds. The evidence at trial established that Bates obtained names and Social Security numbers of student loan borrowers from electronic databases of a former employer.

Our success in prosecuting these and many other cases is the direct result of the close cooperation among the Tax Division, the United States Attorneys' offices, and the IRS. The Tax Division supervises most federal tax prosecutions. Tax Division prosecutors work closely with IRS Criminal Investigations Special Agents to develop and prosecute a wide array of tax crimes, including tax refund fraud arising from identity theft. Tax Division prosecutors also routinely provide tax expertise to United States Attorneys' offices across the country. These close working relationships enable the Department and the IRS to share knowledge and leverage resources in order to combat refund fraud across the country.

The ability of the IRS to share tax information with the Department and others is governed by 26 U.S.C. § 6103. Section 6103(a) requires officers and

employees of the United States to keep tax returns and return information confidential, and prohibits them from disclosing such information, except as specifically authorized by the Internal Revenue Code. Thus, absent a specific exception, tax information received by the IRS must remain confidential and cannot be disclosed. To the extent that an exception applies and the IRS is able to disclose the information to another officer or employee of the United States, the recipient is also subject to the confidentiality requirements of section 6103. In recognition of the Department's role in prosecuting and litigating tax cases, Congress included specific exceptions to permit the IRS to disclose information to the Department for use by employees who are personally engaged in a proceeding involving tax administration. To safeguard taxpayer privacy, in most instances specific taxpayer information may not be disclosed by the IRS to the Department unless and until a matter is specifically referred to the Department. The successful enforcement efforts I mentioned earlier were possible because of the proper sharing of taxpayer information as authorized by section 6103.

At past hearings before Congress, questions have been asked about how local law enforcement could play a role in investigating and prosecuting identity theft and federal tax refund fraud. Given the unique ability of local law enforcement to understand what is going on in their community, at first

glance the idea has obvious appeal. In many instances, the Department has partnered with local law enforcement to successfully combat a wide variety of crimes. For example, in certain cases the Department may formally deputize local law enforcement so they can assist federal law enforcement in a federal tax investigation. However, in these cases local law enforcement is only permitted to access information related to the federal tax investigation, and those who participate in the investigation are not permitted to utilize the tax information in a state or local non-tax investigation or prosecution. While a statutory exception does authorize disclosure to State tax officials and state and local law enforcement who are charged with the administration of State tax laws, this exception would not permit disclosing tax information to local law enforcement who are pursuing non-tax state charges such as identity theft or fraud.

Since its enactment in 1976, section 6103 has served to protect the personal and financial information provided by American taxpayers to the IRS. The statute plays a critical role in fostering the notion that in exchange for voluntary compliance with their reporting and payment obligations, taxpayers can expect that, absent a specific exception authorizing disclosure, their information will remain confidential. The Department and the IRS go to great lengths to ensure that all of its employees understand and fulfill their

obligations to safeguard taxpayer information as required by the Internal Revenue Code.

In crafting limited exceptions to section 6103, Congress sought to balance individual privacy interests with the legitimate needs of tax administration and enforcement. This balance is not an easy one, as clearly demonstrated by the issues that we are discussing today. Given their training and experience in federal tax enforcement, Department prosecutors and IRS investigators are uniquely suited to carrying out the statutory mandate to strike the proper balance between respecting taxpayer privacy and ensuring compliance with the law. The joint efforts of the Department and the IRS demonstrate that vigorous tax enforcement can be accomplished while respecting taxpayer privacy rights. However, care and consideration should be given to expanding access to taxpayer information to a wide array of agencies and individuals who may not have the same training and experience as federal officials. Expanding the circle too far or too fast might unintentionally erode the safeguards that Congress has enacted in section 6103.

While prevention and early detection are always the first and best line of defense, the Department recognizes that prosecution is also a critical and effective tool when it comes to combating identity theft and tax fraud. It is an

unfortunate truth that there will always be a small but persistent segment of society who will seize on any opportunity to make "a quick buck" at the expense of others. While the Department will never be able to fully eradicate crimes such as identity theft and tax fraud, our persistence, dedication, and success in prosecuting these cases sends a clear message to those who engage in this conduct that they will be held accountable for their actions.

Thank you again, Mr. Chairman, for the opportunity to appear this morning. The Department is interested in properly balancing the privacy interests of taxpayers and the genuine needs of local and state law enforcement. We welcome the opportunity to work with this Committee toward that end. I am happy to take any questions that you or the other Members of the Subcommittee may have.

Senate Finance Committee
Subcommittee on Fiscal Responsibility & Economic Growth
"Tax Fraud by Identity Theft; Part 2: Status, Progress, and Potential Solutions"
March 20, 2012

Questions for the Record for Ronald A. Cimino
Deputy Assistant Attorney General for Criminal Matters, Tax Division
U.S. Department of Justice

From Senator Nelson

1. **Over the last two years, what percentage of identity theft-related case referrals from the IRS led to prosecutions?**

   Response: According to the IRS statistics, in fiscal year 2010, IRS - Criminal Investigation referred for prosecution 147 matters involving stolen identity refund fraud. The number of matters referred involving stolen identity refund fraud increased to 218 in fiscal year 2011. After evaluation and review, these matters were authorized for prosecution or forwarded to the US Attorneys for limited additional investigation. No matters were declined.

2. **What percentage led to convictions?**

   Response: Of those matters that have been indicted by Tax Division attorneys, the conviction rate of completed criminal litigation by trial verdict or the entry of a guilty plea is 100%. In addition, the sentences that have been secured in these stolen identity refund fraud cases have reflected the seriousness with which the Department and the courts take these crimes. For example, in one recent case the defendant was sentenced to 334 months of incarceration.

3. **What reasons would most likely lead the Department of Justice not to prosecute a tax-related identity theft referral from the IRS?**

   Response: In every criminal matter referred to the Tax Division by the IRS, the Department evaluates numerous factors to determine whether a matter can be successfully prosecuted. Cases of stolen identity refund fraud are evaluated in the same manner and we apply the same standards. United States Attorneys Manual 6-4.211, 9-27.220. The reason why the Tax Division would decline prosecution would be because the case did not meet our normal review standards, which require a reasonable probability

of conviction based on sufficient admissible evidence to prove all elements of the offense charged.

4. **To what extent is your office involved in the authorization of applications for disclosure of tax returns and tax return information under section 6103(i) (1) of the Internal Revenue Code?**

   Response: The Tax Division normally receives returns and return information related to matters referred from the Internal Revenue Service for civil or criminal proceedings under 26 USC § 6103(h). These are referrals for matters involving "tax administration."

   Other components of the Department of Justice may independently secure information from the Internal Revenue Service pursuant to 26 USC § 6103(i). These requests frequently involve securing an ex-parte order from a federal judge and involve matters of federal criminal law not involving tax administration. Occasionally, the Tax Division provides informal supplemental guidance to such components on the procedure and guidance found in the United States Attorneys Manual 6-4.205[4]. We do not, however, actually authorize any application for disclosure in this area. Pursuant to section 6103(i)(1), the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any United States Attorney, any special prosecutor appointed under 28 U.S.C § 593, or any attorney in charge or a criminal division organized crime strike force may authorize an application for an ex parte order. Section 6103(i) orders are often utilized by the United States Attorneys in drug and criminal fraud cases. The statute empowers a United States Attorney to authorize the application for an order but does not permit the authority to be further delegated. Prosecutors in receipt of information pursuant to section 6103(i) must follow the same stringent safeguarding requirements applicable to all information disclosed under the statute. An application pursuant to section 6103(i) must establish (1) reasonable cause to believe that a specific non-tax criminal violation has occurred, (2) reasonable cause to believe that the return or return information is or may be relevant to a matter relating to the commission of a crime, (3) that the return or return information will be used solely for the criminal investigation of the referenced crime, and (4) that such information cannot be reasonably obtained from another source. 26 U.S.C § 6103(i)(1)(B)(i)-(iii).

5. **What is your experience and view with respect to this disclosure provision and its effectiveness? Does it strike a sound balance between the need for disclosure and the need to safeguard taxpayer privacy?**

   Response: We believe that 26 USC §6103(i) provides a workable manner for US Attorneys to access tax information for use in non-tax federal criminal prosecutions. The Department provides written guidance and training to Assistant United States Attorneys on accessing, using, and safeguarding this information.

6. **In your view, could this provision be an appropriate model for a similar statutory exception with respect to state and local criminal investigations?**

   Response: Responsibility for the development of policy and legislative initiatives under 26 U.S.C. § 6103 is vested in the Department of Treasury, Office of Tax Policy.

7. **Could the Department of Justice provide technical assistance with respect to drafting a provision that allows for limited information sharing in limited circumstances with state and local law enforcement for use in criminal investigations?**

   Response: The Department is interested in properly balancing the privacy interests of taxpayers and the genuine needs of state and local law enforcement. We are happy to work with others involved in tax administration and with the Subcommittee to achieve that goal.

From Senator Burr

1. **Mr. Cimino, I asked you the following question at the recent subcommittee hearing**:

   Deputy Attorney General Cole approved a program where attorneys working for various litigation divisions of the Justice Department, such as the antitrust and civil divisions, could be transferred to U.S. Attorneys' offices throughout the country for a six-month program in fiscal year 2012. Under the program, attorneys were assigned to U.S. Attorney's Offices throughout the country. Attorneys generally do not work on tax issues in this program. I understand that most DOJ litigation divisions opted out of this program, but that the Tax Division did not opt out. I also understand that of the 76 attorneys that applied to the program, 33 of them work in the criminal component of the Tax Division. These are the same attorneys who handle identity theft prosecutions and are charged with stopping refund fraud, among other tax crimes. 33 attorneys constitutes almost 15 percent of the entire criminal component of the Tax Division. Considering that the identity theft refund fraud issue is such an ongoing and active issue, do you think it is wise to divert a significant portion of the criminal component of the Tax Division to deal with non-tax issues?

   You gave the following answer:

   "What we in the Tax Division did, Senator, is to place for six months our Tax Division prosecutors and our civil litigators across the country—they're actually both, of the numbers you referred to. In part, when this was done, some of them are working more on their own cases in the jurisdiction. We tried to establish where we could the work that they were working on would continue with even closer ability. In other instances, I think

it will actually help U.S. Attorneys' Offices to have prosecutors in their jurisdiction to work with and coordinate with other Assistant United States Attorneys."

In fact, my understanding is that the numbers I was referring to—33 applicants from the criminal component of the Tax Division—were accurate. If you include civil litigators from the Tax Division, I understand that the total number of applicants to the program from the Tax Division was 46. Out of the 33 attorneys from the Tax Division that applied for the program, how many of those 33 are working on identity theft tax refund prosecutions while they are working at U.S. Attorneys' Offices throughout the country? I am attaching an email from the Tax Division that shows that the vast majority of assignments that Tax Division attorneys would be working on at U.S. Attorneys' Offices would not even be related to tax issues. How does sending a large portion of the criminal component of the Tax Division out to U.S. Attorneys' Offices to generally work on non-tax issues help in dealing with the ongoing problem of identity theft tax refund crimes? What is the rationale behind the allocation of Tax Division attorneys? It appears that attorneys select what opportunities they wish to apply for and that this is not a coordinated DOJ effort to address other specific crime priorities.

Response: The Tax Division responded to a Department-wide request to provide criminal prosecutors and civil litigators to US Attorney Offices for a six-month detail. The Department's decision to provide details to United States Attorneys' Offices enables Department resources to be effectively deployed across the country, while strengthening working relationships between the litigating divisions and United States Attorneys' Offices. In response to the Department request 23 prosecutors and 14 civil attorneys from the Tax Division were detailed. Prior to this detail, Tax Division prosecutors routinely worked both independently and as co-counsel with Assistant United States Attorneys in criminal tax investigations and prosecutions of all types. A number of our detailed prosecutors are exclusively handling tax matters, including stolen identity refund fraud cases, and others are providing technical assistance and expertise to their colleagues while prosecuting white collar crime. The Tax Division's commitment to combating stolen identity refund fraud and other tax crimes will only benefit from the exchange of skills and closer working relationships fostered by the six-month detail program.

Statement of
Bernard F. McKay, Chair
American Coalition for Taxpayer Rights (ACTR)

Before the

U.S. Senate Committee on Finance
Subcommittee on Fiscal Responsibility and Economic Growth

Tuesday, March 20, 2012
10:00 a.m.

Chairman Nelson, Ranking Member Crapo, and other Members of the Subcommittee, thank you for inviting me here today.

My name is Bernie McKay. I am here today as the Chairman of the American Coalition for Taxpayer Rights (ACTR). ACTR is a 10-member coalition of the largest companies in the tax preparation industry serving U.S. taxpayers, and includes tax preparation firms, software developers and financial institutions. The members of ACTR are committed to providing high quality services, transparency in pricing and service terms, and have a long history of assisting many millions of U.S. taxpayers in their annual Voluntary Compliance obligations under our complex Federal income tax system.

It is also this industry that answered the call of Congress in 1998 to convert U.S. income tax compliance to a lower cost, more accurate and faster return submission system where 80% of all individual tax returns would be filed electronically instead of on paper. This industry worked cooperatively and collaboratively with the Federal Government over a period of a little more than a decade to achieve consumer adoption of electronic filing as the preferred method of income tax compliance in this country. The IRS and industry worked *together* to achieve this major objective and today well in excess of 80% of all individual Federal income tax returns are indeed filed electronically.

There are many differences between the U.S. system of income taxation and those of other countries around the world. But it is the U.S. tax system, for all its flaws, that is citizen-centric. It is based entirely on the principle of engaging and empowering citizens directly in their own tax compliance as a central, independent duty of their citizenship. As a result, the United States enjoys one of if not the highest rate of tax compliance of any nation in the world. U.S. taxpayers are served by a combination of private sector and public sector expert resources who are dedicated to supporting the taxpayer in fulfilling their annual Voluntary Compliance obligation accurately, completely and efficiently, year in and year out.

Annually, the nearly 140 million U.S. individual taxpayers who file taxes have a variety of options for their compliance, ranging from old fashioned pen and paper, to Do-It-Yourself ("DIY") software which they can access online from a home computer or mobile device, to non-profit programs, such as IRS VITA, to no-cost public-private partnerships like IRS Free File, to storefront tax services located in their own city, town or neighborhood, to accountant tax professionals operating small businesses in communities all across the country. On an annual

basis millions of taxpayers move back and forth between these product and service segments based upon their personal circumstances and individual and family tax filing needs.

One of the ACTR association member companies is Intuit, at which I am the Global Chief Public Policy Officer and Vice President of Corporate Affairs. I have been with Intuit for nearly 15 years. Prior to joining Intuit I served in capacities in both the technology industry and in government. My company, Intuit, began in Silicon Valley 28 years ago and offers software and financial products and services that serve small businesses and consumers alike. Our tax software products serve both accounting professionals and Do-it-Yourself taxpayers, and the nature of this highly competitive industry is that each year our customers come from all the aforementioned segments as taxpayers annually choose their method of tax compliance.

The other ACTR association member companies provide tax-related products and services in all of the competitive service segments that comprise this dynamic and innovative industry. The other ACTR member companies include:

Fort Knox Financial Services Corp., d/b/a Refund Advantage
H&R Block, Inc.
Jackson Hewitt Tax Services, Inc.
JTH Tax, Inc. (Liberty Tax Service)
Republic Bank & Trust Company
Santa Barbara Tax Products Group
2nd Story Software, Inc.
TaxSlayer
Universal Tax Systems, Inc., d/b/a CCH Small Firm Services

Because of who we are in this industry and the type of information our customers entrust with us, all ACTR companies strictly adhere to IRS Code Section 7216 and take the privacy and the security of taxpayer data very seriously. All of our companies have business controls to detect and respond to suspicious activity, and prevent fraud. To combat all types of tax fraud, which spans all of the market segments noted above, the IRS and industry have been working together cooperatively for many years. I will describe how that cooperation has been further enhanced over the past year.

It is also important to note the realities of the modern world in the widespread growth of Identity Theft as a global criminal phenomenon. Identity Theft takes many forms and strikes at every type of commerce, in both bricks and mortar and Web-based environments. In the Web-

based world it most routinely strikes at everyday email, seeking to deceive individuals and businesses to attempt to steal and misuse sensitive information of all kinds. It is increasingly the focus of signficant domestic and international efforts to combat it on both a privacy and security level, involving both prevention and law enforcement. Unfortunately, one of the many places where Identity Theft and associated fraud have struck is in tax systems, at home and abroad.

Government Role and Responsibility For Preventing Fraud

ACTR supports and recognizes the central role that the IRS and the U.S. Department of Treasury play, assisted by the U.S. Department of Justice, and on occasion by local law enforcement, as part of their duty to protect the U.S. taxpayers from identity theft and fraudulent tax schemes. The IRS has thousands of auditors and criminal investigators, it has subpoena power, and many other tools to prevent or address fraud, including critical information databases built over decades of experience that only it can access. The IRS, for example, has access to all past and current year tax return information and information reporting.

IRS also has access to a host of federal, state and local databases, including the Social Security Administration database of Social Security numbers, prisoner listings and new hires. Attempts to defraud IRS can and are defeated every day by filters utilizing closely held methods to ensure the tax return is really from a taxpayer who deserves a refund. Criminal conspiracies of varying sophistication can only be investigated and rooted out by government investigation, even when such a case begins with a referral of suspicious activity identified by industry.

Private Sector Companies' Approach To Fraud Reporting

Notwithstanding the key role that IRS plays, industry recognizes it has a "shared responsibility" to detect and report suspicious activity and prevent fraud. In fact, ACTR companies routinely report suspicious activity to the IRS when they see it, although we lack the more complete picture that is obtained by IRS when it analyzes multiple data indices against government databases, known criminal activity, and the like. The companies that make up our industy association have for many years reported information to IRS regarding returns or refunds that are suspicious because of indicia of potential fraud. Across the private sector, privacy and

security protection, together with fraud prevention, are major focuses of continuous investment and dedicated effort.

An example of the type of fraud that private companies are seeing and reporting are instances where identify theft has occurred, and a criminal group relentlessly submits return after return that utilize real taxpayers stolen identities, the correct SSN, date of birth, and a copy of an apparently correct W2. These groups almost always use multiple tax preparation companies to insert numerous returns with the same data. Using information technology to identify such fraudulently filed returns is both lawful and appropriate, and does not implicate any value of trust we in industry have with our customers.

Last year ACTR companies reported that hundreds of thousands of returns should be reviewed due to suspicious activity, and our financial companies stopped payment of hundreds of millions in refunds and saved the U.S. Government millions of dollars in refunds. However, fraud is a constantly evolving criminal activity, domestically and around the world. Given the reports of increasing criminal schemes, the ACTR association began a collaborative effort to improve our help to the government in its ongoing quest to combat tax fraud.

The Anti-Fraud Work Underway Between IRS And Industry

Mr. Chairman, let me turn for a few minutes to the anti-fraud collaboration that is currently ongoing between the IRS and the private-sector tax preparation industry. In October 2011, the 10 members of the American Coalition for Taxpayers Rights proactively reached out to the IRS to determine how we might work together with IRS to assist in combating tax fraud. The response from IRS has been positive and encouraging, and IRS has been appropriately sensitive to the confidentiality and privacy issues that are implicated any time taxpayer information is involved. For example, government cannot tell industry on most occasions how and to what degree the referral information we provided was useful in ferreting out fraud. Likewise, government cannot disclose details of the closely held tools and filters it has at its disposal to identify and capture fraudulent activity.

Last fall, the members of our Coalition met with IRS Deputy Commissioner Steve Miller and many senior IRS staff at IRS headquarters, and mapped out a cooperative agenda for combatting these challenges to the tax system. Our conversation was very positive and

productive. From the perspective of our members, we wanted to know what more we could do to assist IRS in detecting, identifying and combating fraud -- and suspected fraud. Given the ensuing tax filing season, however, I think both sides -- the IRS and ACTR companies -- recognized that much of our collaboration would be undertaken with an eye toward the future. Subsequently, IRS and ACTR representatives met again in Washington for continuing dialogue.

At subsequent meetings, the IRS and ACTR-member companies designated personnel to participate in two fraud task force working groups -- one made up of tax preparation and tax software companies (which I lead for industry), and the other made up of financial institutions, which are typically involved in the receipt and processing of income tax refunds. This collaboration is ongoing and it evolves as the IRS identifies appropriate ways in which we can help.

Conclusion

The reality is that the increase in the incidence of identity theft and associated fraud is likely to continue across all forms and modalities of commerce here in the United States and abroad as criminal groups gain greater technological capability around the world. And unfortunately, the financial attractiveness of tax systems is also likely to continue as a target for such criminal activity. The threat is already complex and will constantly be changing. The increased focus by the IRS on prosecuting tax fraud has led to the discovery of organized criminal rings in places such as Tampa, New York, and Belarus; these crime rings and their use of identity theft to perpetrate tax fraud violate various Title 18 provisions, and are rightly receiving increased attention by federal, state and municipal law enforcement.

ACTR and industry companies are fully cooperating with law enforcement as they seek to break these criminal rings. We recognize there is no silver bullet. Rather, fraud prevention requires a multi-layered defense, and a team effort that includes the IRS, law enforcement, taxpayers and private industry. Mr. Chairman, ACTR wants to continue to be part of the solution, and that is why we will continue to collaborate closely with IRS for the benefit of the U.S. taxpayer to detect and combat tax fraud so that our real customers, the U.S. taxpayer, can continue to prepare and file their returns with ease, peace of mind, and security.

WRITTEN TESTIMONY OF
STEVEN T. MILLER
DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT
INTERNAL REVENUE SERVICE
BEFORE THE
SENATE COMMITTEE ON FINANCE
SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH
ON IDENTITY THEFT
MARCH 20, 2012

INTRODUCTION AND SUMMARY

Chairman Nelson, Ranking Member Crapo and Members of the Subcommittee on Fiscal Responsibility and Economic Growth, 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. Since 2008, the IRS has identified more than 460,000 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 March 9, 2012, we have stopped 215,000 questionable returns with $1.15 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 stopped roughly as much so far this filing season as we stopped 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, but 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 this 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. So far this filing season, 66,000 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 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 135,000 questionable returns this filing season. For the fiscal year, we have prevented almost $800 million in refunds representing an 80% increase in 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.

- 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 258 cases and recommended 150 cases for prosecution. Indictments in identity theft cases total 167, with 49 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. We are, however, developing a procedure by which we will be able to share falsified returns with local law enforcement by way of obtaining a privacy waiver from the innocent taxpayer. 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 in the 2012 filing season and beyond.

Some of the recent successes involving identity theft include the following cases in which sentences were handed down during December-February:

- 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 great 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 460,000 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.

Sen. Bill Nelson opening statement
March 20, 2012

Hearing of the Finance Subcommittee on Fiscal Responsibility and Economic Growth
"Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions"

Welcome, ranking Member Crapo, witnesses, and those joining us today. Thank you for being here.

We're here today to talk about a serious crime that a South Florida federal prosecutor recently described as an "an epidemic."

"People describe it as cocaine on a card." That's what the prosecutor told a CBS affiliate in Miami. He also said, it's a lot of money and people are "having parties in their homes and training others on how to commit this crime."

Surprisingly, he's not talking about drugs.

What then?

Would you believe he's talking about id-thieves stealing people's tax refunds ?

That's right. And it's evident now that this is a crime that's skyrocketing across the country – and particularly in Florida – over the past year.

There are hundreds of thousands of cases out there now in which unsuspecting and law-abiding taxpayers are having their lives turned upside down by identity theft and tax fraud. Having their refunds stolen, and then delayed while the IRS sorts out the mess, is unfair and unjust.

As this chart shows, the amount of identity theft cases the IRS received between 2009 and 2011 nearly tripled.

The most recent data available from the IRS, which is through March 7, 2012, indicates that agency is tracking nearly 300,000 identity theft cases.

Tax fraud through identity theft has become an ordinary street crime. Instead of stealing cars or selling illegal drugs, more and more criminals are looking with envy at the ease to which tax fraud can be committed anonymously. All the fraudster has to do is file a false return electronically, and then have the tax refund loaded onto a prepaid debit card. They never have to use a real physical address or even open a bank account, so the thief is nearly impossible to track down.

The CBS affiliate in Miami even found that software to enable these kinds of schemes are available online for free. It's gotten to a point where criminals are now getting organized to

institutionalize tax fraud by teaching classes of 50 to 100 people at a time on how to file fraudulent returns.

It's clear this problem is not confined to one area of the country. It stretches from the shores of Miami, up to Detroit, and all the way to the coast of California.

Our local police are on the front lines of this battle, and can be a great resource at a time when the Federal government is undergoing a budget squeeze. Last September, as Tampa's WFLA reported, police there arrested 47 individuals and recovered $130 million in stolen federal tax refunds from an organized ring of criminals. I am grateful that our local police are not letting the restraints of federal inhibitions stop them from going after these criminals.

The IRS has made strides in modernizing their internal systems to flag potential cases of identity theft-related tax fraud. And the Department of Justice has successfully prosecuted a number of these cases.

But this crime keeps growing. According to the Federal Trade Commission, identity thieves are now using the Federal treasury as their ATM of choice, with the agency citing tax fraud as the leading complaint filed by identity theft victims, as shown in this chart. As you can see, tax-related identity theft is rising while credit card-related identity theft is declining.

With much-needed government services facing serious cuts, we need to make sure taxpayer dollars are safeguarded from theft and abuse. We need to stop these thieves from stealing from taxpayers.

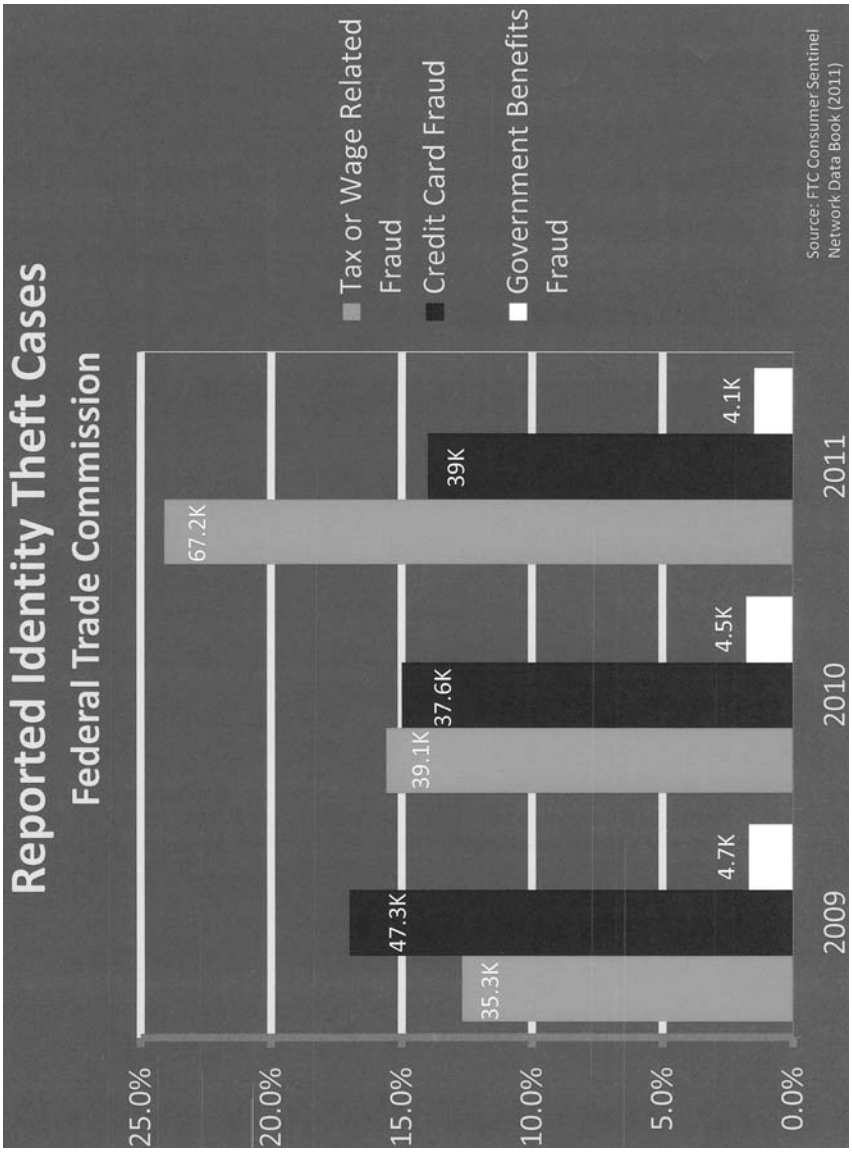
I am grateful that the IRS has given serious attention to this issue, but the reality is we are only starting to scratch the surface. We are here today to not just look back on the past and review what's been done, but also to look toward the future and figure out possible solutions to this problem.

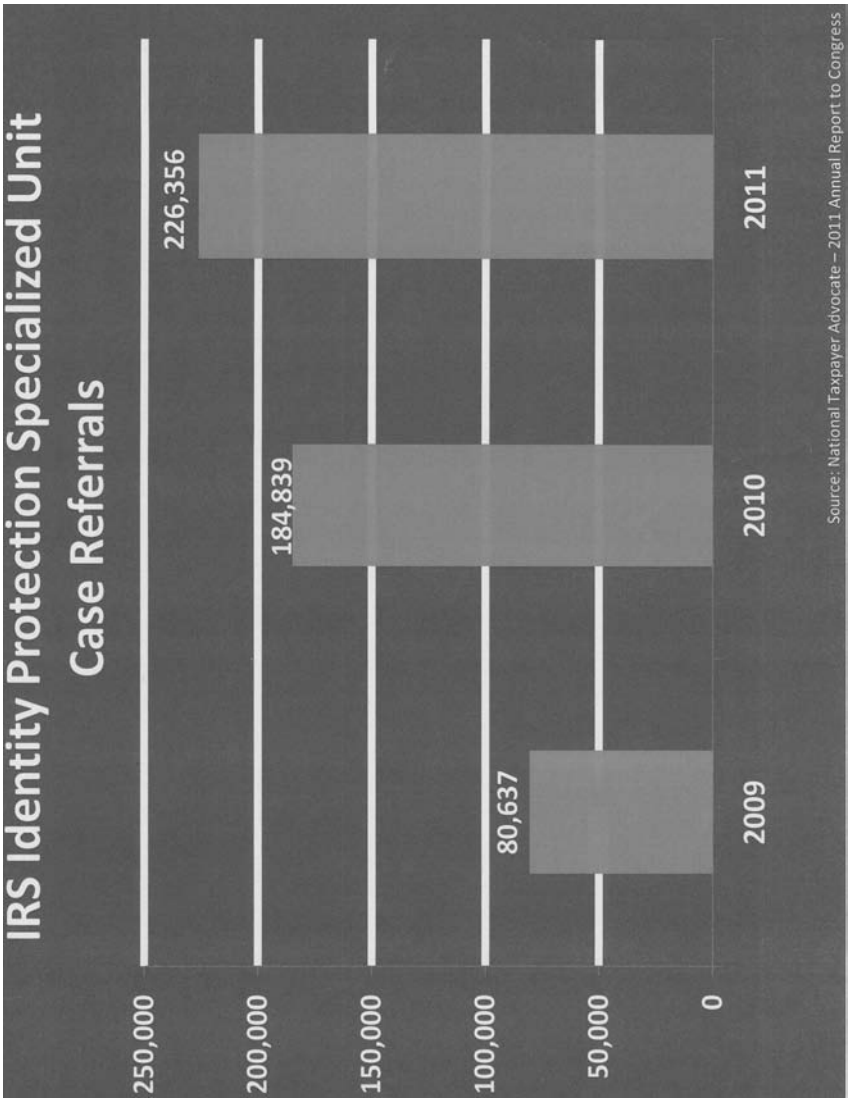
I have introduced comprehensive legislation, the Identity Theft and Tax Fraud Prevention Act. The bill would give the IRS and identity-theft victims the means to better detect and prevent this disastrous offense. I am pleased that the IRS has already implemented some of these reforms. Specifically, the bill:

- Strengthens penalties for tax fraud through identity theft and the improper disclosure of taxpayer information;
- Gives all ID theft victims a unique personal identification number (PIN) to include on their tax return to prevent fraud and avoid tax refund delays;
- Allows identity-theft victims to "opt out" of the electronic filing of their federal tax returns;
- Secures the Social Security numbers of deceased Americans so that fraudsters cannot use them to file fake tax returns;
- Reallocates IRS resources for tax fraud prevention and detection;
- Improves coordination, cooperation, and communication between the IRS and local authorities in criminal investigations; and

- Permanently extends the authority for the IRS to share information with federal and state prison authorities.

With these reforms fully enacted, I believe we can begin to bring this problem under control. We can protect victims and save taxpayer dollars. I look forward to hearing from our witnesses today. Senator Crapo?


Reported Identity Theft Cases
Federal Trade Commission
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
35.3K
47.3K
4.7K
39.1K
37.6K
4.5K
67.2K
39K
4.1K
2009
2010
2011
Tax or Wage Related Fraud
Credit Card Fraud
Government Benefits Fraud
Source: FTC Consumer Sentinel Network Data Book (2011)


IRS Identity Protection Specialized Unit
Case Referrals
250,000
200,000
150,000
100,000
50,000
0
80,637
184,839
226,356
2009
2010
2011
Source: National Taxpayer Advocate – 2011 Annual Report to Congress

WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

TAX FRAUD BY IDENTITY THEFT, PART 2:

STATUS, PROGRESS, AND POTENTIAL SOLUTIONS

BEFORE THE

SUBCOMMITTEE ON FISCAL RESPONSIBILITY

AND ECONOMIC GROWTH

COMMITTEE ON FINANCE

UNITED STATES SENATE

MARCH 20, 2012

Chairman Nelson, Ranking Member Crapo, and distinguished Members of the Subcommittee:

Thank you for inviting me to testify today about the subject of identity theft.[1] 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. Since 2004, I have written extensively about the impact of identity theft on taxpayers and tax administration and have worked closely with the IRS to improve its efforts to assist taxpayers who are identity theft victims.[2] The IRS has made significant progress in this area in recent years, including adopting many of my office's recommendations. Notwithstanding these efforts, it is clear that combating identity theft continues to pose significant challenges for the IRS.

In my testimony today, I will make the following points:

1. The IRS continues to see unprecedented levels of identity theft casework.

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

3. The IRS should continue working with the Social Security Administration to restrict access to the Death Master File.

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

---

[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*); *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, Subcommittee 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).

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

6. Recent identity theft process improvements require fine-tuning.

7. The IRS has had ample time to develop procedures to assist victims of return preparer fraud and should finalize procedures promptly.

I. The IRS Continues to See Unprecedented Levels of Identity Theft Casework.

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.[3] Identity theft wreaks havoc on our tax system in many different ways. Victims of identity theft 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 could otherwise be shifted to taxpayer service or compliance initiatives.

The IRS has begun to utilize data analysis to develop automated identity theft filters. Programmers can perform data mining to detect trends based on a variety of factors and develop customized filters to isolate suspicious claims for refunds. While such tools make it easier for the IRS to identify such schemes, the IRS is fighting an uphill battle. It seems that new schemes are hatched each week, and while the IRS can scramble to adjust its filters, it will generally be in a reactive mode.

News reports suggest some very organized groups have chosen tax-related identity theft as the crime du jour.[4] Identity theft has become a large-scale operation – it is no longer just the work of one person stealing a few numbers and trying to get refunds, nor

---

[3] 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 tax identification 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 for this testimony.

[4] According to one report, suspects are teaching classes of 50 to 100 people at a time on how to file fraudulent returns. *See* 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/.

is it just someone trying to work under someone else's number. The greatest source of harm today is with "boiler room" operations involving the theft of massive lists of numbers. Apparently, there are networks of criminals who not only share stolen personal information, but also present seminars about how to use this information to file bogus returns.[5] In response to the increase in criminal activity in this area, the IRS's Criminal Investigation division (CI) in fiscal year (FY) 2011 initiated 276 fraud cases related to identity theft, with 81 convictions – up from 224 investigations and 40 convictions in FY 2010.[6]

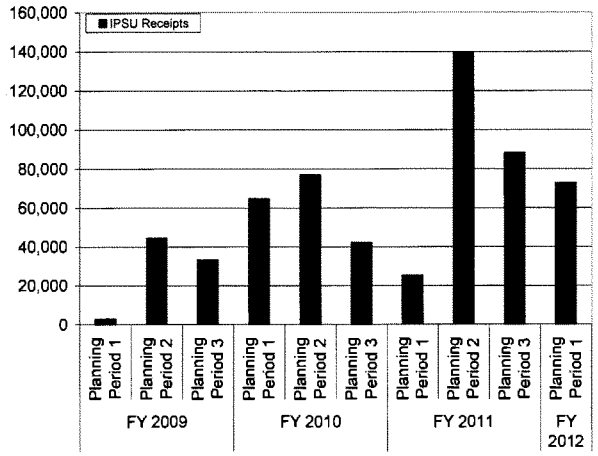
The Identity Protection Specialized Unit (IPSU), the centralized IRS organization that assists identity theft victims, is also experiencing unprecedented levels of case receipts. As the chart below shows, IPSU receipts increased substantially over the two previous years.

---

[5] *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/.

[6] Data obtained from the IRS Criminal Investigation division's Research function (Mar. 13, 2012).

Chart 1: IPSU Paper Inventory Receipts, FY 2009 to FY 2012 by Planning Period[7]

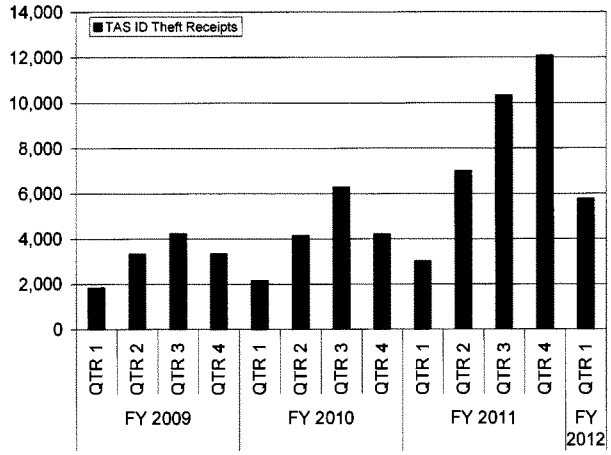


The Taxpayer Advocate Service (TAS) has experienced similar increases in identity theft cases. TAS had a 97 percent increase in identity theft receipts in FY 2011 over FY 2010, on top of a 23 percent rise from FY 2009 to FY 2010. The upward trend in identity theft receipts has continued in FY 2012. In the first quarter of FY 2012, TAS received 5,762 identity theft cases, a 91 percent increase over the same period in FY 2011.[8] The increase in TAS identity theft casework reflects the impact of both the increase in identity theft incidents and the IRS's inability to address the victims' tax issues promptly.

[7] 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.

[8] Data provided by TAS Technical Analysis and Guidance (Mar. 12, 2012).

Chart 2: TAS Stolen Identity Case Receipts, FY 2009 to FY 2012 by Quarter[9]



The IRS has more identity theft cases than those that show up in IPSU inventory and TAS Stolen Identity receipts. The most recent IRS data show nearly 300,000 identity theft cases servicewide.[10] In addition, there will be fallout from the newly implemented identity theft filters, which stopped approximately 140,000 tax refunds from going out in the 2012 filing season (just through February 22).[11] The IRS notifies the impacted taxpayers by letter that there was a problem processing the return and instructs them to call the new Taxpayer Protection Unit (TPU) to provide more information to have their returns processed. These cases are not included in the IPSU or TAS counts. The TPU will also handle lists of SSNs involved in identity theft schemes referred by the Criminal Investigation division and other law enforcement agencies. Once the TPU reviews these lists, verified identity theft victims will receive the appropriate identity theft marker on their accounts.

Notwithstanding the IRS's verification of the identity of the victim, the fact that the SSN was misused once means it could be misused again. Thus, the taxpayer will be required to include a special personal identification number (PIN) when e-filing in future years. For verified identify theft accounts, the IRS undertakes certain protective measures, including processing future tax returns associated with a marked account through a

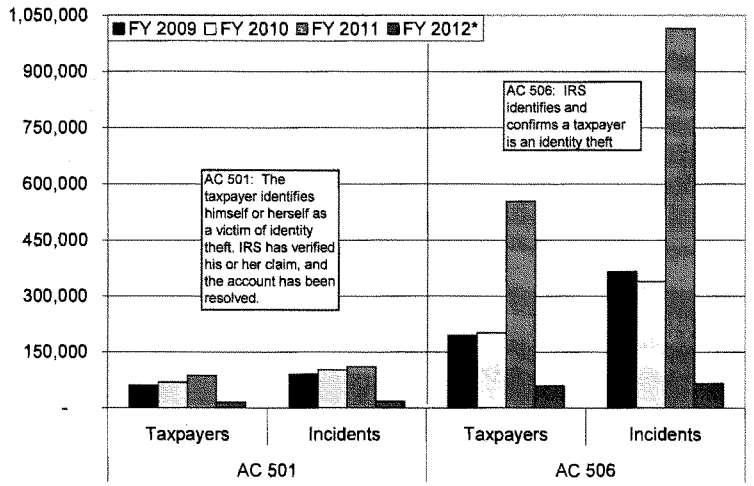
[9] Taxpayer Advocate Management Information System (TAMIS), FY 2009, FY 2010, FY 2011.

[10] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[11] Through Feb. 22, 2012. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

series of business rules designed to filter out suspicious returns. Consequently, not only does the IRS face a growing number of new identity theft cases each year, but the overall number of taxpayers impacted by identity theft continues to rise as well.

Chart 3: Accounts with Identity Theft Indicators, FY 2009 to FY 2012 Q1[12]



I am pleased to report that the IRS has accepted many of my office's recommendations for improving identity theft procedures. At various times, I have advocated for the following improvements, each of which has been adopted in some capacity:

- Development of an electronic indicator to mark accounts of verified identity theft victims;
- Creation of an IRS identity theft affidavit form;
- Adoption of a standardized list of acceptable documents to substantiate identity theft;
- Establishment of a centralized unit to provide assistance to identity theft victims;
- Provision for a global account review prior to closing an identity theft victim's account to ensure that all related issues have been resolved; and

[12] Office of Privacy, Government Liaison, and Disclosure, Incident Tracking Reports.

- Issuance of an identity protection PIN to verified taxpayers that would enable their electronically filed returns to bypass the identity theft business rules.

Despite these significant improvements, more can be done to combat, or even prevent, identity theft and other refund fraud.

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

Before I discuss possible process improvements, I want to take a moment to provide 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.[13] 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.[14]

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

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 to filter out questionable refund claims. 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.[15] The IRS estimates that EFDS has an 89 percent accuracy rate, meaning that upwards of 100,000 legitimate taxpayers are

---

[13] 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).

[14] 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.

[15] 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.

expected to be caught up in these filters.[16] In my 2011 Annual Report to Congress, I discuss in depth my concerns with the IRS's delay in processing the refunds of such legitimate taxpayers.[17]

While it is important for the IRS to develop procedures 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 tax 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 that the majority of refund requests can be processed within days of filing.[18] 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 can develop automated filters to try to screen out as many suspicious refund claims as possible, it is unrealistic to expect the IRS to detect and deny all such claims given its resource and time constraints. 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 sure 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 the full arsenal of information reporting databases – including complete data on wages and withholding, interest income, dividends, capital gains, and partnership income – and could better detect and resolve discrepancies and questionable returns.

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 of filing their return. 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. Such a population may have made substantive decisions depending upon the availability of cash 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

---

[16] National Taxpayer Advocate 2011 Annual Report to Congress 28.

[17] *Id.* at 28-47.

[18] 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 is currently able to manage, then Congress would need to authorize significantly more funding for the IRS. 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.[19] 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 in which to conduct the necessary wage and withholding verification. Absent that, overall taxpayer service and compliance will suffer as the IRS directs resources from other IRS activities to combat identity theft.

III. The IRS Should Continue Working with the Social Security Administration to Restrict Access to the Death Master File.

In a relatively new tactic, some identity thieves are filing tax returns that claim the personal or dependency exemption and various tax credits for deceased individuals. Identity thieves have found that SSNs and other personal information of the deceased are easily accessible. Perhaps surprisingly, the federal government itself is one source of this information. The Social Security Administration (SSA) maintains a "Death Master File" (DMF) containing the full name, SSN, date of birth, date of death, and the county, state, and ZIP code of the last address on record of decedents.[20] DMF data is updated weekly and made available to the public. Today, anyone can quickly find a number of websites (including genealogy sites) that publish DMF information free or for a nominal fee.[21]

The SSA created the DMF database in 1980 in the aftermath of a consent judgment it entered into with an individual who had sought some of this information under the

---

[19] 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.

[20] *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).

[21] *See* Boston Herald, *Sandwich Parents Are Twice Robbed* (Nov. 27, 2011); Scripps Howard News Service, *ID Thieves Cashing in on Dead Children's Information* (Nov. 3, 2011). Recently, several genealogy websites have voluntarily agreed to curtail the availability of DMF information. Ancestry.com announced in December 2011 that it will no longer display SSNs for anyone who has passed away within the past ten years, and RootsWeb.com, a genealogy site affiliated with Ancestry.com, states that it will not share information from the DMF "due to sensitivities around the information in this database." *See* Scripps Howard News Service, *Genealogy Sites Remove Social Security Numbers of Deceased* (Dec. 15, 2011), *available at* http://www.abcactionnews.com/dpp/news/national/genealogy-sites-remove-social-security-numbers-of-deceased.

Freedom of Information Act (FOIA).[22] FOIA generally provides that any person has a right to obtain access to certain federal agency records.[23] In crafting FOIA, Congress recognized the importance of allowing citizen access to government information. The core purpose of FOIA is to allow the public to learn what the government is up to.[24] Congress also understood the government's need to keep some information confidential, including private information about individuals who might be mentioned in federal files, and it thus included nine exemptions in the law.[25]

Personal privacy interests are protected by two exemptions within FOIA. Section 552(b)(6) protects information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." Section 552(b)(7)(C) relates to information compiled for law enforcement purposes and protects personal information when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

The challenge for the courts has been balancing the public's interest in the release of records in question against the privacy interest of the individuals involved. In 1989, the Supreme Court reiterated that the purpose of FOIA is to enable citizens to find out "what their government is up to" and clarified that this purpose "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."[26] The DMF contains personal records of more than 80 million deceased individuals, but these records do not reveal much, if anything, about the SSA's own conduct.[27]

An additional challenge for the courts has been assessing the privacy interest of the deceased. FOIA contains an exemption for records or information compiled for law enforcement purposes, but only to the extent production could reasonably be expected to constitute an unwarranted invasion of personal privacy (hereinafter referred to as "Exemption 7(C)").[28] While the death of the subject of personal information diminishes

---

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

[23] *See* 5 USC § 552.

[24] *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978) (citations omitted). In contrast, see *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 773 (1989) (withholding criminal "rap sheets" compiled by the FBI; they reveal nothing about agency operations); *NARA v. Favish*, 541 U.S. 157, 169, *reh'g denied*, 541 U.S. 1057 (2004) (withholding photographs of body of publicly notable individual; they reveal nothing about agency operations).

[25] *See* 5 USC § 552(b).

[26] *Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 772-73 (1989).

[27] We acknowledge that there may be some value in accessing the DMF to gain insight into the SSA. For example, an individual may suspect that the SSA's death records are grossly inaccurate. By accessing the DMF, an individual could attempt to show that the SSA's method of recordkeeping is seriously flawed. However, one could make such a finding with only partial access to the DMF or if access was delayed a couple of years.

[28] 5 U.S.C. § 552(b)(7)(C).

to some extent the privacy interest in that information, courts have held that it does not extinguish that interest.[29] In *Accuracy in Media, Inc. v. Nat'l Park Service*, the U.S. Court of Appeals for the District of Columbia "squarely rejected the proposition that FOIA's protection of personal privacy ends upon the death of the individual depicted."[30]

In 2004, the Supreme Court recognized that surviving family members also enjoy a privacy interest that must be considered when analyzing the release of agency records as it relates to Exemption 7(C). It unanimously held that the surviving family members of former Deputy White House Counsel Vince Foster had a protectable privacy interest in his death-scene photographs.[31] Other courts have also applied FOIA exemptions to withhold decedent information on the basis of survivor privacy.[32]

It is my understanding the SSA has determined there are no exemptions from FOIA that support the nondisclosure of the DMF, and it may seek a legislative remedy. I strongly support legislation to limit public access to the DMF. At the same time, I recognize the difficulty of passing legislation, and if Congress does not act, I believe the SSA has sufficient legal authority to limit public access to the DMF even without a statutory change.

Since the 1980 *Perholtz* consent judgment, significant FOIA case law has developed that articulates strong arguments, and may be relied upon, to withhold the DMF under existing FOIA exemptions.[33] Given that (1) the type of information the DMF holds does not reveal much about "what the government is up to," (2) there is significant risk identity thieves can misuse the information contained in the DMF to claim improper tax benefits, and (3) the victims' families may suffer emotional and financial harm as they deal with the aftermath of identity theft and a death in the family, I believe that a court, after conducting the requisite balancing test under FOIA, might well allow the SSA to shield some DMF information from disclosure.

---

[29] *Schrecker v. Dep't 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).

[30] *See, e.g., Accuracy in Media, Inc. v. Nat'l Park Serv.*, 194 F.3d 120, 123 (D.C. Cir. 1999) (relating to photos of the death scene of White House official Vince Foster).

[31] *National Archives & Records Admin. v. Favish*, 541 U.S. 157, 168 (2004) (finding that "well-established cultural tradition acknowledging a family's control over the body and death images of the deceased has long been recognized at common law").

[32] *Hale v. DOJ*, 973 F.2d 894 (10th Cir. 1992) (families have a privacy interest in the photographs of a deceased victim under FOIA Exemption 7(C)); *Badhwar v. U.S. Dept. of the Air Force*, 829 F.2d 182, 185-86 (D.C. Cir. 1987) (observing privacy interest of families of deceased pilots in withholding autopsy reports "of a kind that would shock the sensibilities of surviving kin"); *New York Times v. NASA.*, 920 F.2d 1002, 1005 (D.C. Cir. 1990) (*en banc*) (audio tapes of the foundering of the space shuttle Challenger withheld).

[33] We recognize that, in light of the consent judgment, SSA may not be in a position to unilaterally change its position. Rather, we believe the changes in facts and law may merit the filing of a motion to alter the consent judgment to allow SSNs to be released in truncated form.

I recognize that there are many legitimate users of DMF information, and we should not restrict access any more than necessary to thwart tax-related identity theft. Perhaps the SSA can explore whether DMF data could be released with partial redaction of the SSN. Alternatively, the SSA may consider releasing unredacted DMF data on a delayed basis. Withholding DMF data for three years, for example, would frustrate the ability of identity thieves to file a purported tax return before the IRS locks down the SSN. (Because there may be legitimate tax filings with a decedent's SSN in the year of death and the year or two following death, the IRS is not able to "retire" an SSN immediately.) In my view, the damage to tax administration and the federal fisc caused by identity theft outweighs the incremental value of prompt release.

IV. 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.[34]

The Internal Revenue Code (IRC) contains significant protections for the confidentiality of tax 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; etc.[35] For example, information furnished to the IRS on a Form W-2 constitutes return information.

Section 6103(i)(2) authorizes the disclosure of return information (other than "taxpayer return information"[36]) in response to requests from federal agencies for use in criminal investigations. The head of the federal agency (or the Inspector General thereof)[37] 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

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

[35] IRC § 6103(b)(2).

[36] "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).

[37] If the request is being made by the Department of Justice, multiple individuals can make the written request for the information. *See* IRC § 6103(i)(2)(A).

which the United States or such agency is or may be a party.[38] Section 6103(i)(3)(A) authorizes the IRS to disclose return information (other than "taxpayer return information"[39]), 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.

There is no corresponding exception in IRC § 6103 that allows for the release of identity theft information to *state or local* agencies.[40] 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 may develop procedures that would facilitate 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 do not believe that such an expansion of this statute is appropriate. I believe that 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 recently advised that under IRC § 6103(i)(3), the IRS may share the "bad return" and other return information of an identity thief with other federal agencies. In addition, the Office of Chief Counsel has advised that because a return filed by an identity thief may be considered return information of the victim, an identity theft victim may obtain from the IRS a copy of the "bad return" and other return information associated with the processing of the "bad return" filed by the alleged thief. Further, the Office of Chief Counsel has concluded that under IRC § 6103(c)[41], an identity theft victim may 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 is working to develop procedures regarding how this information related to the "bad return" may be shared. For example, the IRS could

---

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

[39] *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). In the typical "bad return" case, however, the thief's identity, if discovered, will almost always come from other than taxpayer return information.

[40] 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.

[41] IRC § 6103(c) provides that the IRS can disclose returns and return information to any person or persons the taxpayer designates in a request for, or consent to, such disclosure. Treas. Reg. § 301.6103(c)-1 contains the requirements for such disclosures.

request taxpayer consent to release tax return information directly to state and local law enforcement. However, I am concerned that once the information is in the hands of state and local law enforcement, there is no restriction on redisclosure under the current law. I propose that Congress modify 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 redisclosure of such information.[42]

V. 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 IPSU unit 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."[43] 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 attempts to coordinate with up to 27 other functions within the IRS to obtain relief for the victim.[44] 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 don't get stuck in one function or another along the way. 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 victim's account every 60 days.[45] In other cases, the unit uses Identity Theft Assistance Requests (ITARs) to ask other IRS functions to take specific actions.[46]

While the procedures call for the receiving functions to give ITARs priority treatment, there are no "teeth" to ensure that this happens.[47] Unlike TAS, which can issue a Taxpayer

---

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

[43] *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.

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

[45] Internal Revenue Manual (IRM) 21.9.2.4.3(7) (Oct. 1, 2011).

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

[47] 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.

Assistance Order (TAO)[48] 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.

In 2011, the IRS made a decision to adopt a specialized approach to assisting identity theft victims. Under this approach, each impacted IRS function will create a specialized unit that will be trained on identity theft account resolution and work solely on identity theft cases. Because these specialized employees will see a lot of identity theft cases, they will quickly become familiar with patterns and recognize the needs of victims.

While I agree that this approach will have benefits, I firmly believe that 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 the risk that cases requiring involvement from multiple IRS functions will get "stuck" or fall through the cracks is high without a case coordinator. The IPSU should continue to serve an important role in this process by conducting a global account review and by then tracking each identity theft case from start to finish as it moves from one specialized function to another.

VI. Recent Identity Theft Process Improvements Require Fine-Tuning.

Identity Theft Personal Identification Numbers Rolled Out with Mixed Results

For the 2012 filing season, the IRS introduced a number of identity theft-related process improvements. Some were designed to provide greater protection for previously verified identity theft victims. Others were intended to help the IRS detect identity theft patterns using advanced data analysis. I believe these initiatives were well intentioned, but I have some concerns about their implementation.

In order to provide a greater level of security for taxpayers, the IRS issued identity protection personal identification numbers (IP PINs) to about 250,000 victims whose identities and addresses have been verified.[49] Letters went out in December 2011, instructing the victims that they must use the IP PIN to file their 2011 returns. If the taxpayer attempts to e-file without that number, the IRS will not accept it and the taxpayer will need to file a paper return, which will delay processing.

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."

[48] *See* IRC § 7811.

[49] The IRS issued 251,568 IP PINs. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

It is my understanding that over 9,000 letters containing the IP PINs were returned undeliverable, meaning that these taxpayers are unaware they cannot file their returns electronically.[50] In addition, as of February 23, approximately 15,000 taxpayers have contacted the IRS to request replacement IP PINs.[51] Through March 6, only 69 taxpayers have come to TAS for assistance with obtaining replacement IP PINs, but I anticipate that more taxpayers will be coming to TAS in the coming weeks, as they begin to realize they will not be able to electronically file without this six-digit code.

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

The IRS also designed and implemented several identity theft filters this filing season that are intended to weed out suspicious returns based on a variety of factors. The good news is that the IRS can identify these patterns relatively quickly and adjust the filters accordingly. The bad news is that there is a lot of work involved to resolve the downstream consequences of these actions. Significantly, the IRS must be able to answer phone calls from legitimate taxpayers who have been caught up in these filters.

When the IRS proposed these filters, I was consulted and I consented to them on the condition that the IRS develop procedures to address legitimate returns that happen to have the characteristics of a fabricated return. I was assured there would be a mechanism for filtered tax returns to be retrieved and quickly processed, and that a dedicated Taxpayer Protection Unit would take calls from taxpayers who receive notices after being caught by the identity theft filters.

Although the IRS has established this TPU, I am disheartened to learn that the level of service on the phone line for the TPU was 11.7 percent for the week ending March 9, with an average speed of answer exceeding 3,990 seconds.[52] Let me repeat this in layman's terms – about nine out of ten calls to the "Taxpayer Protection" line did not get through, and those that did get through had to wait on hold an average of an hour and six minutes! It seems not only that the IRS misjudged the number of customer service representatives that are needed to staff this line, but also that the identity theft filters have picked up more

---

[50] 9,137 letters containing IP PINs were undeliverable. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[51] 15,011 taxpayers have requested replacement IP PINs as of February 23, 2012. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[52] 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 Data Dictionary, *available at* http://cfo.fin.irs.gov/AssistReview/docs/FY%202009%20MD&A%20Data%20Dictionary%2008-04-09.doc (last visited Mar. 12, 2012).

returns than were anticipated. The IRS leadership has assured me this problem has been identified and resolved, and that additional resources have been allocated to ramp up TPU staffing. 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.

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 a laptop. As noted earlier, 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. If the current level of service on the phones is at 11.7 percent, can we realistically expect this unit to devote much attention to referral lists?

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

As I mentioned earlier, the IRS is making efforts to improve its tracking and reporting of identity theft cases. Each function that works an identity theft case will be required to input an identity theft marker on a purported identity theft 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 identity 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 only thing the IRS has done is to flag the account as a potential identity theft account.

I have requested 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.

VII. The IRS Has Had Ample Time to Develop Procedures to Assist Victims of Return Preparer Fraud and Should Finalize Procedures Promptly.

TAS has received a significant number of cases involving tax return preparer refund fraud. These preparers alter taxpayers' tax returns by inflating income, deductions, credits, or withholding without their clients' knowledge or consent. In one egregious instance involving several returns prepared by one person – and despite agreement by the IRS that the returns it processed were not the returns signed by the taxpayers – the Local Taxpayer Advocate could not persuade the IRS Accounts Management function to make the proper account adjustments to remove the fabricated income or credits.

The Local Taxpayer Advocate issued four Taxpayer Assistance Orders to Accounts Management in December 2010. After Accounts Management refused to comply, these TAOs were elevated 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 make appropriate adjustments to the victims' accounts. It was not until last week that the IRS finally made the requested adjustments to the taxpayers' accounts.

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.[53] 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. In this Proposed TAD, I cited two published opinions from the IRS Office of Chief Counsel which conclude that a return altered by a preparer *after* the taxpayer has verified the accuracy of the return is a nullity (*i.e.*, not a valid return).[54]

After receiving an unsatisfactory IRS response to concerns raised about this matter in the Proposed TAD and my 2011 Annual Report to Congress, I issued a TAD to the W&I Commissioner and the Small Business/Self-Employed Commissioner on January 12, 2012.[55] While both have acknowledged their intent to comply with the substance of the

---

[53] 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).

[54] *See* IRS Office of Chief Counsel Memorandum, *Tax Return Preparer's Alteration of a Return*, PMTA 2011-20 (June 27, 2011); IRS Office of Chief Counsel Memorandum, *Horse's Tax Service*, PMTA 2011-13 (May 12, 2003).

[55] *See* National Taxpayer Advocate 2011 Annual Report to Congress 59-60; 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) (attached).

TAD, they appealed the TAD solely in an effort to extend the timeframes within which to comply with the directed actions.

It has been 15 months since TAS first raised this issue in a series of TAOs issued to Accounts Management. I have no idea why the IRS needs more time to develop guidance to its employees with respect to an area of return preparer fraud that is growing, that is closely related to identity theft, and that 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.

VIII. Conclusion.

Identity theft poses significant challenges for the IRS. There will always be opportunistic thieves who 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). But it 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. The *status quo* simply will not suffice if we expect the IRS both to process legitimate returns rapidly and to combat identity theft effectively.

THE OFFICE OF THE TAXPAYER ADVOCATE OPERATES INDEPENDENTLY OF ANY OTHER IRS OFFICE AND REPORTS DIRECTLY TO CONGRESS THROUGH THE NATIONAL TAXPAYER ADVOCATE

Response Due:
February 2, 2012

January 12, 2012

MEMORANDUM FOR PEGGY BOGADI, COMMISSIONER,
WAGE AND INVESTMENT DIVISION
FARIS FINK, COMMISSIONER,
SMALL BUSINESS/SELF EMPLOYED DIVISION

FROM: Nina E. Olson
National Taxpayer Advocate

SUBJECT: 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*)

TAXPAYER ADVOCATE DIRECTIVE

I am issuing this Taxpayer Advocate Directive (TAD) to direct the Commissioner, Wage and Investment (W&I) and the Commissioner, Small Business/Self Employed Division to:

1) within 14 days of the date of this TAD, issue guidance directing employees to cease any collection actions on liabilities assessed against taxpayers in connection with a refund or portion of a refund that the taxpayer never received due to return preparer fraud;

2) within 45 days of the date of this TAD, in consultation with the National Taxpayer Advocate, issue interim guidance to establish procedures to abate assessments and correct refund amounts where the IRS is holding a taxpayer liable for repayment of a refund or portion of a refund that the taxpayer never received due to return preparer fraud; and

3) within 90 days of the date of this TAD, in consultation with the National Taxpayer Advocate, revise the Internal Revenue Manual (IRM) to provide guidance on abating assessments or correcting refund amounts where the IRS is holding a taxpayer liable for repayment of a refund or portion of a refund that the taxpayer never received due to return preparer fraud.

Thus, W&I must develop procedures to ensure that the accounts of taxpayers victimized by return preparers reflect the correct information.

I. Authority

This directive is being issued pursuant to Delegation Order No. 13-3, which grants the National Taxpayer Advocate 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.[1] This authority may not be redelegated.

II. Issue

TAS has received multiple cases and been notified of several schemes by other Business Operating Divisions involving return preparer refund fraud. These preparers altered taxpayers' tax returns without their knowledge or consent by inflating income, deductions, credits, or withholding after the taxpayers approved the return for filing. The taxpayers generally received refunds from the preparers in the amount the preparer advised each taxpayer that he or she should receive;[2] many taxpayers became aware of the preparer's fraudulent activity only upon hearing from the IRS when the IRS attempted to collect the excess refund amount.

Here is a basic example to illustrate the actions of the preparer:

> Taxpayer A provides her tax return preparer with her W-2 and relevant information. The preparer completes Form 1040, reflecting a zero income tax liability, and indicating Taxpayer A is entitled to a $350 refund. After

---

[1] Internal Revenue Manual (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).

[2] In some cases, the preparer provided only his or her bank account information to the IRS, and then upon receipt of the refund, wire-transferred the amount the taxpayer was expecting into the taxpayer's bank account (*i.e.*, the amount shown on the correct return). In other cases, the preparer provided the taxpayer's bank account and the preparer's bank account on Form 8888, *Allocation of Refund (Including Savings Bond Purchases)*, which allows the IRS to direct-deposit a taxpayer's refund into up to three different accounts.

Taxpayer A approves the return and is provided a printed copy of that return, the preparer electronically files a different return with the IRS.

Taxpayer A is not aware that the preparer altered the return before he electronically filed it by inflating income and the credit for income tax withholding; the preparer reported an income tax liability of $500 and withholding of $3850, thereby increasing the refund to $3,350. Unbeknownst to Taxpayer A, the return preparer designated two bank accounts into which the $3,350 refund is split: the expected refund of $350 is direct-deposited into Taxpayer A's account, and the balance of $3,000 is direct-deposited into the preparer's own account. Thus, Taxpayer A has received the refund to which she thought she was entitled, based on the copy of the return she approved and the preparer provided to her.

The IRS selects Taxpayer A's return for examination the following year. The IRS disallows Taxpayer A's excess withholding and proposes a deficiency of $3,000 (plus penalty and interest).

The Office of Chief Counsel has advised the IRS that a return altered by a preparer without the taxpayer's consent is not a valid return, and consequently, the taxpayer should submit his or her true original return upon discovering the fraudulent actions of the preparer.[3] Moreover, the Office of Chief Counsel has advised the IRS to adjust the taxpayer's account to remove all entries attributable to the purported return filed by the preparer.[4] The IRS has failed to provide guidance to its employees about the proper accounting entries needed to adjust the taxpayers' accounts.

III. History

On June 13, 2011, I issued a Proposed TAD directing the Commissioner of Wage and Investment to 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 in order to obtain a fraudulent refund. The W&I Commissioner did not respond to the Proposed TAD by the requested date of June 23, 2011, or the extended due date of July 7, 2011, and no guidance has yet been issued, nearly seven months after issuance of the Proposed TAD.

On August 16, 2011, I elevated four Taxpayer Assistance Orders (TAOs) to the Deputy Commissioner for Services and Enforcement, ordering the IRS to correct the accounts of four victims of preparer refund fraud. In elevating the TAOs, I

---

[3] PMTA 2011-20, *Tax Return Preparer's Alteration of a Return* (June 27, 2011); PMTA 2011-13, *Horse's Tax Service* (May 12, 2003).
[4] IRS, Office of Chief Counsel, POSTN-145098-08, *Refunds Improperly Directed to a Preparer* (Dec. 17, 2008).

outlined two possible processes that W&I could use to ensure the tax accounts of victimized taxpayers were accurately updated and taxpayers were not held liable for the amounts fraudulently obtained by the preparers:

> 1. The fraudulent portion can be written off using a process similar to the Identity Theft procedures outlined in IRM 21.9.1.9.1.2.4, *Identity Theft CAT 7 Bad Return Posted/Good Return Posted – Lost Refund – Process* (May 25, 2011).
> 2. Alternatively, an IRS-issued identifying number (IRSN) can be established with the address of the servicing campus, and the fraudulent portion can be moved to that account using the process outlined in IRM 21.5.2.4.23.10, *Moving Refunds* (Jan. 27, 2011).

On September 2, 2011, the Deputy Commissioner for Services and Enforcement agreed in writing to comply with the TAOs, take steps to provide relief to the taxpayers, and develop procedures to address similarly-situated taxpayers. To date, the IRS has not developed guidance to address this situation in a systemic manner.

IV. Conclusion

For these reasons and the reasons outlined in the National Taxpayer Advocate 2011 Annual Report to Congress (see attached Most Serious Problem: *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS*), I am issuing a TAD to protect the rights of taxpayers and prevent undue burden. In light of the significant harm taxpayers are suffering as a result of the IRS's inability to develop a process for providing relief to these taxpayers over the last two years, I direct the IRS to:

1) Cease any collection actions on liabilities assessed against taxpayers in connection with a refund or portion of a refund that the taxpayer never received due to return preparer fraud within ten days of this directive;
2) Issue an interim guidance memorandum, developed in consultation with the National Taxpayer Advocate, within 45 days of this directive; and
3) Revise the IRM within 90 days of this directive to instruct IRS employees how to correct the taxpayers' accounts to reflect the removal of the inflated refund received by the return preparer.

The two processes identified above are suggestions; I welcome any other processes the IRS chooses to implement, so long as those processes are developed and guidance issued expeditiously to ensure that the accounts of taxpayers victimized by return preparers reflect the correct information.

Attachments:

(1) Proposed Taxpayer Advocate Directive 2011-1 (*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*) (June 13, 2011)

(2) National Taxpayer Advocate 2011 Annual Report to Congress (Most Serious Problem: *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS*)

cc: Steve Miller, Deputy Commissioner, Services and Enforcement

Statement of

Kirsten Trusko
President and Executive Director

of the
Network Branded Prepaid Card Association

Before the

Subcommittee on Fiscal Responsibility & Economic Growth

Senate Finance Committee

Hearing on Tax Fraud through Identity Theft

March 20, 2012

Chairman Nelson, Ranking Member Crapo, and members of the Subcommittee, I appreciate the opportunity to appear before you today on behalf of the Network Branded Prepaid Card Association (NBPCA) and its members. My name is Kirsten Trusko and I am NBPCA's President and Executive Director. I have served in this position for going on three years. Prior to joining the NBPCA, I co-founded and lead the prepaid card and consumer driven healthcare management consulting and technology practices for a top 5 global consulting firm.

The NBPCA is a non-profit trade association founded in 2005 representing a diverse group of organizations that take part in delivering network branded prepaid cards to consumers, businesses and governments. Our membership includes financial institutions, card organizations, processors, program managers, marketing and incentive companies, card distributors, law and media firms and touches a vast majority of the network branded prepaid cards.

Overview of Network Branded Prepaid Cards

Network branded prepaid cards comprise a diverse group of extraordinarily popular products that serve a vital public need. Network branded prepaid cards bear the logo of a payment network (American Express, Discover, MasterCard or Visa), and work similar to credit and debit cards. Prepaid cards are issued by banks or licensed money service businesses. Prepaid cards allow for customized payment solutions for a range of payment situations that in the past were unwieldy and expensive. Card issuers can leverage the flexibility of network branded prepaid cards to create solutions that address many common consumer needs, offering a safe, easy-to-use alternative to paper-based products such as checks, cash, and even vouchers.

There are several parties involved in bringing prepaid cards to market. They include: (1) the payment networks, (2) the banks or licensed money service businesses which issue the prepaid cards, (3) the program managers which assist the issuing bank in setting up, marketing and operating the card program, (4) the processors which process the card programs on behalf of the issuers and program managers, and (5) the retailers and other third parties who distribute the cards to businesses and to consumers.

General Purpose Reloadable Cards

The general purpose reloadable (GPR) card is one of the most flexible prepaid products. GPR cards are typically purchased by a consumer for their personal use to pay for point-of-sale purchases, pay bills, and/or access cash at ATMs. GPR cards may be purchased online or in retail locations from a variety of providers. Funds may be loaded onto the card by the consumer at retail locations offering prepaid card reload services or by direct deposit of wages or benefits.

Convenient access to these prepaid cards with pricing that is often lower than other financial tools have been key drivers of their popularity among consumers. The cards are available in more than 200,000 retail locations and bank branches. The wide availability of the cards is particularly appealing to the 60 million Americans who are unbanked or underbanked, who have limited or no access to bank branches in their neighborhoods or cannot qualify for checking accounts.

How GPR Cards are Obtained

GPR cards are typically obtained in one of two ways. A potential cardholder may go to a web site of one of the many financial institutions or program managers which

offer GPR cards. Alternatively, the consumer may go to a retail location or check cashing service to obtain a temporary prepaid card. In the retail environment, the customer would hand over to the retailer funds for the purchase of the card and the initial amount to be loaded to the card. The retailer will then send a message to the processor of the temporary card indicating that the card had been purchased and the amount on the initial value load. The processor then activates the temporary card for the value of the initial load.

These temporary cards are essentially limited-functionality cards, with value loads that generally do not exceed $500, and do not provide cash access or permit the card to be reloaded until the purchaser has provided personal information to the program manager or processor, and that information is then verified. Once the information has been verified, the program manager or processor sends a fully functional personalized prepaid card to the purchaser. Once the fully functional card is received by the cardholder, and the cardholder activates the card, the card is reloadable by the cardholder. The cardholder is provided an ABA routing number and an account number which is associated with the prepaid card account, which the cardholder can provide to employers or other parties, including government agencies, for purposes of direct depositing wages, government benefits or tax refunds to the cardholder's prepaid card account.

Bank Secrecy Act (BSA)

GPR cards are issued by regulated banking institutions or by other highly regulated organizations, such as state-licensed and FinCEN-registered money service businesses (MSBs). Issuers of prepaid cards are subject to examination, review and

supervision by either state banking or other departmental regulators, federal banking regulators, the Internal Revenue Service or a combination of all of these agencies.

Banks which issue GPR cards are legally required by the USA PATRIOT Act and the BSA to have an effective anti-money laundering (AML) compliance program that addresses customer due diligence, suspicious activity monitoring, currency transaction reporting and OFAC screening, as well as other BSA reporting and recordkeeping requirements.

Additionally, under a recent final rule issued by FinCEN addressing prepaid access, providers and sellers of GPR cards are classified as MSBs and are required to maintain effective BSA compliance programs that address customer due diligence, suspicious activity monitoring, currency transaction reporting and OFAC screening, as well as other BSA reporting and recordkeeping requirements.

Under the BSA, both the issuer and provider of a GPR card have the obligation to implement risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the issuer and or provider to form a reasonable belief that they know the true identity of each customer. These procedures must be based on the assessment by the issuer and provider of the relevant risks, including those presented by the various types of accounts maintained by the issuer, the various methods of opening accounts provided by the issuer and provider, the various types of identifying information available, and the issuer's/provider's size, location, and customer base.

As part of their BSA compliance programs, issuers and providers of GPR cards must collect the following four pieces of personal information from a prospective

cardholder: (1) name, (2) street address, (3) identification number, and (4) date of birth. This information is collected by the program manager or processor when the purchaser either acquires the card online or contacts them to convert the temporary card to a fully functional card. After this information is collected, as required by the BSA, the program manager or processor will use non-documentary verification systems in an attempt to verify the prospective cardholder using the information provided. The applicant is verified using one or more identity verification services which are used by financial institutions or brokerages to verify customer identity. The process used to verify identity is the same as is used by a financial institution when a consumer applies for a credit card or online bank account. The process may be automated, manual or a combination of manual and automated processes, depending on the program manager and processor. If the information is successfully verified, the cardholder is approved for a fully functional GPR card. If the information is not successfully verified, the program manager or processor will either decline to establish the account or require the prospective cardholder to provide additional information, such as a copy of a government-issued identification card, prior to approval of the cardholder. If the program manager or processor cannot successfully verify the identity of the prospective cardholder, the account is not established.

Identity Theft

As is the case with the providers of credit cards and other financial products, issuers and program managers of prepaid cards are faced with fraudsters who attempt to establish prepaid card accounts using stolen identities. The process of preventing fraud starts well before the fraudster tries to load the funds to a prepaid card—the

original identity theft has occurred in the fraudster's efforts to gain the tax refund in the first place. The prepaid card is just the acceptance method.

Industry Efforts

The NBPCA acknowledges that, like any payment system, prepaid cards are susceptible to abuse and misuse and, in particular, the use of prepaid cards in connection with tax return fraud was identified as a significant problem during the prior tax return processing season. Once this problem was identified, members of the NBPCA acted aggressively to address this problem.

Prepaid Anti-Fraud Forum

In 2011, the NBPCA formed the Prepaid Anti-Fraud Forum (PAFF). PAFF brings together leading practitioners, and collaborates with law enforcement, establishes leading practices, and hosts educational forums for members to learn from guest experts. To combat tax fraud the PAFF solicited input from industry participants and, prior to the beginning of this tax return processing season, compiled a confidential handbook discussing various fraud mitigation strategies. This confidential handbook has been shared with issuers, program managers and processors of prepaid cards. Although this statement necessarily omits greater detail, to avoid tipping off potential fraudsters on methods being implemented to mitigate the use of prepaid cards in tax refund fraud, the anti-fraud practices can be broken down into four high-level categories:

1. Fraud detection and processing at the application stage;

2. Fraud detection and processing at the post-application stage;

3. Fraud detection and processing at the ACH deposit stage; and

4. Additional questions triggered by suspected fraudulent ACHs.

As part of these processes, among other actions, industry participants are:

a. Watching for patterns of suspicious activity when activating the GPR card.

b. Identifying "hot" ZIP codes and fraud trends in various regions of the country.

c. Undertaking transaction monitoring and suspicious activity monitoring.

d. Undertaking additional processes when incoming ACH loads are identified as being an income tax refund.

e. Rejecting and returning ACH value loads to Treasury when there is a suspicion that the transaction may be the result of fraud.

f. Freezing accounts when fraud is suspected.

g. Filing suspicious activity reports when fraud is suspected, which reports are available to law enforcement and the IRS.

h. Working with the IRS, Department of Justice, and FBI when new fraud trends are identified.

i. Working with victims of identity theft, including supplying to the consumer all the information they have available on the ID theft, all records including those of the account opening, and any transactions on the account.

j. Assisting federal and local law enforcement in investigations of suspected tax refund fraud.

The industry efforts have so far resulted in over $1Billion of value loads to prepaid cards being returned to the IRS based on attempted fraudulent tax refunds.

The PAFF is developing a close working relationship with the IRS Criminal Investigation Division, the Department of Justice, and the FBI to enable more effective information sharing to prevent the use of prepaid cards in tax refund fraud.

IRS Efforts

As the IRS implements additional processes to prevent tax refund fraud, we would caution that such processes must take into consideration the large number of legitimate filers who rely on prepaid products to receive their tax refunds. The fraud-prevention benefits of additional processes and procedures must be balanced against the burdens borne by the unbanked taxpayers who are depending on the timely receipt of their tax refunds. Such processes should be implemented in a manner reasonably anticipated to takes into account the risks presented and the numerous safeguards already implemented by the industry.

Thank you for the opportunity to appear before you today . The NBPCA stands ready to work with you and I would be happy to answer any questions you may have.

Network Branded Prepaid Card Association

Educate. Advocate. Protect. Promote.

About NBPCA

- Nonprofit, inter-industry trade association
- Focus is Network branded (open-loop) prepaid cards
- Young – in our 6th year
- Membership representing companies touching >70% of the market's cards

NBPCA Mission

- Provide a fact-based voice to media, government and consumers
- Set a high industry bar through Code of Conduct and Best Practices
- Develop and share consumer education, and partner with others to deliver this training broadly across constituent groups

NBPCA Role

- Provide a highly interactive and participatory forum for thought leadership and collaboration to drive industry consensus and success
- Serve as the collective voice of industry and a trusted, credible point of factual information to industry, government, media and consumer groups

Network Branded Prepaid Card Association

NBPCA: What We Do

- Educate: Consumers, government, media on the types of uses and unique applications for network branded prepaid
- Advocate: Actively seek meetings and opportunities for interaction with people and entities of influence
- Protect: Preserve ability to offer a competitive product set
- Promote: Assertively highlight the unique benefits provided by network branded prepaid products to consumers, government, media, and businesses

NBPCA: Core Principles in Serving Consumers

- ***Choice. Access. Transparency. Education***

Network Branded Prepaid Card

Benefits to Constituents

- **Consumers.** Convenience, Financial Flexibility, Control, Security.
- **Corporations/ Government.** Process improvements, cost reductions, control, new markets, efficiency.
- **Merchants.** Increased spend, cost reduction, new consumers, efficiency.
- **Issuers.** New markets, risk mitigation, reduction in paper processing.

Payment Card Models

Pay Before	Pay Now	Pay Later
Prepaid products draw funds from a pre-funded card account which can be funded from a variety of sources.	Debit products draw funds from a checking account.	Credit products draw funds from a credit line.

Closed Loop

Typically accepted by a single merchant/group of merchants. Examples include dept. store gift, phone, and transit cards. Also called "retailer-branded" or "proprietary" prepaid cards.

Network Branded

Carry acceptance mark of a national/international payment network such as Visa, MasterCard, American Express, or Discover. Some ATM/EFT networks also offer prepaid card products. Functionality depends on card application.

Many Prepaid Card Types

Applications by card type	Closed Loop	Open Loop
Gift (Consumer funded)		✓
Money Remittance (Consumer Funded)		✓
Campus	✓	✓
Travel		✓
Telecom	✓	
FSA/HRA/HSA (Corporate Funded)		✓
Payroll (Corporate funded)		✓
Relocation (Corporate Funded)		✓
FSA/HRA/HSA (Corporate Funded)		✓
Employee & Partner Incentive	✓	✓
Consumer Incentive (Corporate Funded)	✓	✓
Benefits (Corporate Funded)	✓	✓
Court Ordered Payments		✓
Social Security/Unemployment (Government)		✓
Temporary Assistance for Needy Families, and Food Stamps (Government Funded)	✓	✓

What is Prepaid – "Open Loop", "General Purpose Reloadable" (GPR)

Open Loop – General Purpose Reloadable

Network Branded

- Visa
- Discover
- American Express
- MasterCard

Controls

- Cardholders Identified
- Transaction Monitoring
- Deposit and Spend Records
- Error Resolution

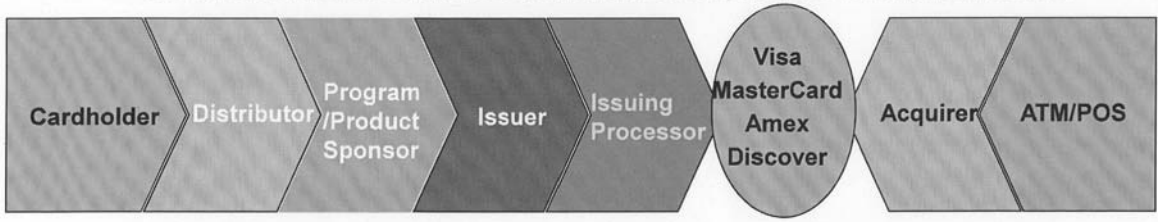
Bank Issued

- Underlying account
- FDIC Insured
- CIP Required
- AML Program

Features

- Reloadable
- ATM Withdrawals
- Direct Deposit
- Bill Pay
- Account Management Tools

Roles* of Participants in Prepaid Programs



- Cardholder – Loads the funds
- Distributor – retailer or bank / FI or program manager online
- Program/Product Sponsor – bank issuer or bank issuing partner that manages the programs
- Issuer –Institution responsible for "issuing" the cards
- Issuing Processor – card processor
- Networks – AMEX, Discover, MasterCard and Visa, PIN Networks
- Acquirer – facilitates processing with ATM and POS
- ATM/POS – provides cardholder with access to funds at ATM, cash advance in a branch or via POS (retail, web, telephone, etc)

* Roles to be covered in greater detail in later panel

Funding Sources and Sample Applications

Consumer-Funded	Corporate-Funded	Government-Funded
Consumers purchase a card for their own use or to provide a friend or relative: ▪Gift ▪Travel ▪Youth/Teen ▪General Purpose Reloadable	***Virtually unlimited opportunity for business to create new solutions to enhance their customers' lives:*** ▪Payroll ▪Incentive/Rebate ▪Insurance/Disaster ▪Employee Benefits - Health Care - Wellness - Transit	***Cards mitigate distribution costs, systemic fraud, and provide better service to recipients:*** ▪Unemployment ▪Child Support ▪TANF ▪Disaster Assistance ▪Redress Payments

COMMUNICATIONS

The U.S. Senate

Committee on Finance
Subcommittee on Fiscal Responsibility and Economic Growth

P. O. Box 200940

Austin TX 78720-0940

Statement for the Record

Hearing on Tax Fraud by Identity Theft, Part 2:

Status, Progress, and Potential Solutions

Submitted by

Patricia A. Oxley, President

March 20, 2012

Chairman Nelson, Ranking Member Crapo, and distinguished Members of the Subcommittee:

Thank you for the invitation to submit this Statement for the Record on behalf of the Federation of Genealogical Societies to supplement the record of the hearing held by the Subcommittee on the 20th of March 2012.

I serve as the President of the Federation of Genealogical Societies and as a member of the Records Preservation and Access Committee more fully described below.

The Federation of Genealogical Societies was founded in 1976 and represents the members of hundreds of genealogical societies. We have member societies in all 50 states, the District of Columbia, the Virgin Islands, Canada, Ireland, and the United Kingdom.

Be assured that the genealogical community shares the objective of protecting Americans against fraud and of addressing deficiencies in the current operation of the Social Security Administration's Death Master File. This hearing marks a valuable opportunity to express our views to Congress on this important subject and we commend the committee for adding it to their agenda.

Identity Thieves Have Long Targeted Infants

We have all been outraged by reports of identity thieves filing fraudulent tax refund claims using the SSNs of recently deceased infants & adults. Although the specific techniques and technologies may have changed, having a scoundrel target deceased infants is not new.

In the 1970s and early 1980s, the technique followed by those with sinister intent employed this pattern:

(1) The thief would visit the Babyland Section of a local cemetery and find the name and birth date of a deceased child roughly comparable with their own.

(2) The thief would approach the vital records custodian to request a duplicate birth certificate using that name and birth date.

(3) If issued, the duplicate birth certificate would then be used to apply for a driver's license and other purposes to create an identity in the deceased child's name that could then be used for purposes as benign as facilitating underage drinking but ranging to major thefts by making substantial credits purchases.

What Response Worked

The most effective response developed by the vital records community to this abuse was to verify the appropriateness of the request for a duplicate birth certificate by first checking their files of death certificates to ensure that the subject of the requested birth certificate was not found

there. If found, the duplicate birth certificate would only be issued if prominently annotated to reflect the fact that the person was deceased.

Inter-state compacts with adjoining jurisdictions allowed the vital records custodians of the birth records to screen the death records of neighboring states before responding to a fraudulent request. Efforts continue to expand the ability to access the death records of a broader range of states to be used to thwart this form of abuse.

As a society, we did not choose to restrict access to cemeteries.

What Is the Problem?

Death records have particular utility in the prevention of fraud or theft. Little judgment is required to decide not to extend credit to a person authoritatively reported to be dead. Significant barriers to continued economic activity should arise when an individual's SSN appears on the Death Master File. Other than using that SSN for tax credits or refund calculations on a tax return filed for the year of death and a limited interval thereafter, I am unaware of any other valid economic activity. A SSN listed on the Death Master File should no longer be recognized as valid and usable.

That reality places a particular burden on those creating such a record to get it right and a requirement to correct any mistakes as quickly as possible.

In recent years, identity thieves have recognized this vulnerability in the IRS processing of tax returns claiming a tax refund, aggravated by an objective to process refunds to taxpayers as expeditiously as possible.

Thieves may have abused online access to the Death Master File or its commercial form, the Social Security Death Index in order to identify the SSNs of recently deceased infants and adults.

The real problem is that the Internal Revenue Service and others, who should be using the Death Master File/Security Security Death Index for the purpose for which it was created, are struggling to adapt filters to identify possibly fraudulent tax returns and to mobilize the resources necessary to resolve questionable refund claims so found. Once the IRS has done so, this vulnerability should be closed.

About the Records Preservation and Access Committee

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), the American Society of Genealogists (ASG), and industry representatives also serve as participating members. RPAC

meets monthly, and more often if needed, to advise the genealogical and historical communities, as well as other interested parties, on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

RPAC Recommendations to the Congress and the Genealogical Community

After careful consideration of a variety of appropriate responses to this particularly despicable form of identity theft and the various legislative proposals it has prompted, we are prepared to recommend the following coordinated position. This week we plan to submit statements for the record of this hearing on behalf of RPAC, FGS, NGS and IAJGS. All RPAC leaders' statements for the record submitted to the Senate Subcommittee will state that:

> While we advocate all genealogists should have immediate access to the SSDI, we would support the two year delay in access as proposed in S 1534- 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.

To the extent that we might acknowledge that most genealogists in most cases could tolerate a brief delay in having access to the information reflected in the Death Master File, we must emphasize that there are cases in which anything less than immediate access could have significant adverse consequences. Historically, access to this information has not differentiated among the types of researchers nor case-specific circumstances which means that we do not currently have a well-defined mechanism in place which discriminates among classes of potential researchers.

The last sentence of the coordinated language represents our attempt to begin the process of gathering input from our colleagues in the broader genealogical community and seek to develop a workable definition addressing urgency. This past week we have initiated this dialogue. We will seek input from and the support of the broader genealogical community as quickly as possible.

We are unaware of any rationale that would justify delaying general access beyond the two or three year period during which the reported SSN would still have IRS implications. Please note that even the justification for this brief delay disappears once the IRS has closed this vulnerability through the development of workable filters and procedures/resources for resolving questionable returns.

We stand ready to work with all concerned parties to address this challenging issue and can best be reached at access@fgs.org .

Summary

(1) The most effective response to identity thieves' abuse of vulnerabilities in the online tax refund system is for the IRS to develop filters using the Death Master File for the purpose for which it was originally created, namely, fraud prevention.
(2) We recommend against limiting or delaying access to the Death Master File/Social Security Death Index. Should legislators deem it appropriate to delay access for the brief period of time necessary for the IRS to develop appropriate filters, the genealogical community could support such limitations if a mechanism can be worked out to allow those researchers with more urgent requirements immediate access.
(3) We stand ready to assist in developing appropriate safeguards.

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. SENATE FINANCE COMMITTEE, SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH, TAX FRAUD BY IDENTITY THEFT, PART 2: STATUS, PROGRESS, AND POTENTIAL SOLUTIONS, WRITTEN COMMENTS ON PROVISIONS RELATING TO SOCIAL SECURITY ADMINISTRATION'S DEATH MASTER FILE, ALSO KNOWN COMMERCIALLY AS THE SOCIAL SECURITY DEATH INDEX.

I. INTRODUCTION:

The U.S. Senate Finance Committee Subcommittee on Fiscal Responsibility and Economic Growth held a Hearing on 20 March 2012, on Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions 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 vital 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).

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

Officers
Michael Goldstein, Jerusalem, Israel, President@iajgs.org
Jan Meisels Allen, Agoura Hills, CA, USA, Vicepresident@iajgs.org
Joel Spector, Cherry Hill, NJ, USA, Secretary@iajgs.org
Paul Silverstone, New York, NY, USA, Treasurer@iajgs.org
Immediate Past President
Anne Feder Lee, Honolulu, HI, USA, Anne@iajgs.org

Directors-at-large
Nolan Altman, Oceanside, NY, USA, Nolan@iajgs.org
Daniel Horowitz, Kfar Saba, Israel, Daniel@iajgs.org
Kahlile Mehr, Bountiful, UT, USA, Kahlile@iajgs.org
Mark Nicholls, Edgeware Middlesex, UK Mark@iajgs.org
Jay Sage, Newton Center, MA, USA Jay@iajgs.org
Jackye Sullins, Carlsbad, CA, USA, Jackye@iajgs.org

Thank you for the opportunity to present the IAJGS concerns regarding the Subcommittee's proposed reduction 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 Subcommittee's 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 which proposes 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 for their own gain.

Rarely has it been documented that an individual's identity is violated by access to vital records or the SSDI. Rather, the violations occur due to computer breaches from government and private enterprises. 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"[1]. Many of these computer breaches have been well documented in the press.[2]

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. 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. 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 his oral statement during the March 20th hearing, Detective Sol Augeri stated once the genealogical websites withdrew the SSDI from public access, identity theft did not abate, rather, 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 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.[3] As tbe SSDI 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.

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.[4] 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-and if necessary the third year that National Taxpayer Advocate Nina Olson advocated during her oral testimony during the March 20th hearing, with the caveat that certain genealogists are to be eligible for certification for immediate access. These genealogists include:

1. Forensic genealogists. These are genealogists who work, for example 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; and
2. Heir researchers who are working to prove or disprove that someone is eligible as part of a deceased's estate or Native American tribal funds;
3. 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.

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, 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 [5]. 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[6].

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 [7].

> "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*[8]

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 [9].

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

It is a positive outcome that the IRS has undertaken activities that are more preventive. 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 and it defies credulity that this has not already been adopted by the IRS. The difference between data security and data stewardship is excellently described in Kenneth Ryesky's statement to the Subcommittee relative to the March 20th hearing. 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.". [10]

"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. 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 subcommittee through legislation can adopt the suggestion by National Taxpayer Advocate Olson in her written and oral statements for the March 20th hearing, that the identity theft victim be able to receive the "bad return" 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 [11]. 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 this Subcommittee's 25 May 2011 Hearing,[12] together with the testimony of Mr. Agin at the House Ways & Means Committee's 2 February 2012 Hearing, [13] 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 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 [14](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 [15] 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;

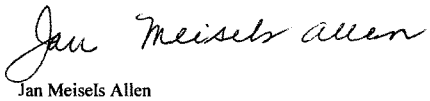
- Genealogists have legitimate, professional and life saving reasons to have immediate access to the SSDI; and

- Proactive measures are needed to prevent identity theft and vigorously pursue and punish the **TRUE** identity thieves,

IAJGS respectfully and vehemently encourages the Subcommittee 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 Subcommittee's attention the many services the genealogy community performs for local, state, and federal government offices. We look forward to working with the Subcommittee and staff to find an accommodation that provides genealogists with immediate and reasonable access to the SSDI.

Respectfully submitted,



Jan Meisels Allen
IAJGS Vice President
Chairperson, IAJGS Public Records Access Monitoring Committee

[1] 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 Vieraitis, L.M. (2009) *34*(3), 329-349.

[3] 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;

[4] 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

[5] Mayo Clinic staff: "Medical History: Compiling your medical family tree,"
http://www.mayoclinic.com/health/medical-history/HQ01707;

[6] https://familyhistory.hhs.gov/fhh-web/home.action

[7] http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA

[8] 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.

[9] http://www.aarp.org/relationships/genealogy/info-06-2011/genealogy-tips.html
http://www.familiesforforgottenheroes.org/Genealogist.htm

[10] 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.

[11] http://www.youtube.com/watch?v=gpgTFO7nMBk

[12] 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.

[13] 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.

[14] 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.

[15] 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.

1 SECTION 1. (1) The Commissioner of the Social Security Administration shall arrange and
2 permanently preserve the social security numbers of dependent children with the associated
3 social security numbers of their legal parents or guardians for all applications registered.
4 (2) The Commissioner of Social Security may release the indices and data files described in
5 paragraph (1) to the Internal Revenue Service. The Internal Revenue Service having obtained
6 the index pursuant to this paragraph may not release any portion of its contents to any other
7 party or government agencies.
8 (3) The Internal Revenue Service or other government agency may not sell or release Social
9 Security indices prepared and maintained by the Social Security Administration except as
10 authorized by law.
11 (4) In addition to the indices prepared pursuant to paragraph (1), the Commissioner of
12 Social Security shall prepare separate non-comprehensive electronic indices of all deceased
13 individuals with Social Security numbers that shall be made available for public inspection.
14 (5) For purposes of this bill, the following definitions apply:
15 (a) "Data files" means computerized data compiled from Social Security Applications
16 registered with the Social Security Administration.
17 (b) "Person" means any individual, firm, corporation, partnership, limited liability
18 company, joint venture, or association.
19 (c) "Personal identifying information" means first name, middle name, last name,
20 mother's maiden name, and father's surname, and a social security number that is
21 contained in the file.
22 (d) "Financial institution" means any commercial bank, trust company, savings and
23 loan company, insurance company, or person engaged in the business of lending money.
24 (e) "Commercial or non-profit company" means any company or not-for-profit organiza-
25 tion engaged in sharing information about deceased individuals for the pursuit of heir
26 searches, genetic research, blood quantum research, genealogy or family history research,
27 or other legal uses of the information as authorized by law.
28 (6) The Social Security Death Master File as presently constituted will be made available
29 for a reasonable fee to financial institutions, commercial companies, non-profit organizations
30 and educational institutions as authorized by law.
31 (7) Any person who, in violation of this section, uses, sells, shares, or discloses any informa-
32 tion provided pursuant to this section, or who uses information provided pursuant to this
33 section in a manner other than as authorized pursuant to this section, may be subject to the
34 assessment of a civil penalty by the Internal Revenue Service in the amount of $_____. The
35 penalty provided in this section shall not be construed as restricting any remedy, criminal,
36 provisional, or otherwise, provided by law for the benefit of the agency or any person.
37 (8) The Social Security Administration and the Internal Revenue Service shall adopt any
38 regulations necessary to implement this section.

MASSACHUSETTS
GENEALOGICAL
COUNCIL

info@massgencouncil.org P.O. Box 5393, Cochituate, MA 01778 www.massgencouncil.org

2 April 2012

Senate Committee on Finance
Attn. Editorial and Document Section
Rm. SD-219
Dirksen Senate Office Bldg.
Washington, DC 20510-6200

To: US Senator Bill Nelson (D-FL), Chair: US Senate Finance Committee, Subcommittee on Fiscal Responsibility & Economic Growth

From: Massachusetts Genealogical Council, Polly FitzGerald Kimmitt, CG[SM], President

Re: Testimony for hearing on "Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions," regarding the **Identity Theft and Tax Fraud Prevention Act (S.1534)**, held Tuesday, March 20, 2012, 10:00 AM, 215 Dirksen Senate Office Building.

The **Massachusetts Genealogical Council (MGC)** is an umbrella organization representing more than 36,000 members of genealogical and historical societies who utilize current and historical records to determine kinship. Whether residents of the Commonwealth or descendants of early Massachusetts settlers now living in all fifty states, we wish the Social Security Death Master File (DMF) to remain un-redacted and accessible to the public.

Senate Bill 1534 goes a long way in curbing tax fraud by correcting some of the more egregious problems within the IRS and in law enforcement practices, particularly in Florida, where the bulk of the abuse takes place. The one measure that will hinder rather than help this effort is removal of access to the Death Master File.

While we are in agreement that there are significant problems within the Social Security Administration, the Internal Revenue Service, and local law enforcement, we need to ensure that legislation proposed to rectify this problem will not have dangerous, if unintended, consequences.

As a tool for research in the genealogical field, the Death Master File is used to determine kinship in myriad ways, just a few of which follow.

• In 2009, Congress mandated that the US military hire genealogists to determine and locate next of kin of servicemen lost in previous conflicts. Genealogical case workers find next of kin and DNA donors in each serviceman's family to aid with identification of repatriated remains. The Death Master File is absolutely critical to this research.

• Unclaimed Persons, a group of over 400 volunteer genealogical case workers, assists medical examiners and coroners across the county in finding next of kin for unclaimed remains being stored in their facilities. Like other governmental agencies, coroners are overworked, understaffed and handling large case loads. Unclaimed Persons volunteers locate next of kin of the deceased so that remains can be released instead of remaining in the government's possession for an indeterminate amount of time.

• Attorneys and financial institutions employ the services of genealogists in probate, tax and heir-search cases. Again, the DMF is critical to this research.

• Physicians use the DMF to locate family members who can supply necessary information to help with diagnoses. Many lives have been saved through donations of blood and bone marrow possible only from family members. People with hidden genetic diseases can be alerted early enough to start preventive care which can add years to lives.

We are in full agreement that we must do everything we can to stop criminals from perpetrating tax fraud via identity theft. It is vital to recognize that the Death Master file was actually made public in order to curb this abuse. It is **precisely** where any American citizen or business should go to check for bogus use of social security numbers. Any bill that attempts to curb identify theft and correct errors within the SSA must *not* contravene the original reason for the creation of the DMF: to provide a check on identities and assure that the social security numbers of deceased individuals are not being used fraudulently.

And let us remember that the DMF should only contain numbers of deceased individuals. The fact that the SSA incorrectly reports deaths of living individuals shows a need to correct practices *within* the SSA, not completely remove access to the DMF. If we look at the facts we see that the amount of fraud using social security numbers of deceased Americans is minute in comparison with the amount via living Americans erroneously introduced into the system either by SSA negligence or criminal fraud. Removing the DMF just eliminates one way for the public to verify a number, a right which was granted to all Americans by the Federal courts in 1978 as a result of a lawsuit filed by Mr. Ronald Perholtz based on the Freedom of Information Act.

If we are to solve this problem it is essential to first critically examine several points.

1. Countless professions and industries across the nation are heavily reliant on the DMF: health care providers, the military, financial institutions, attorneys, insurance agencies, universities, funeral directors, credit agencies, and especially governmental agencies. While access would probably be granted to some, the use of the DMF is now inextricably woven into business

practices across the country. How will the decision be made as to who is allowed access? Who is qualified to make these decisions? Any attempt to discern eligibility to the DMF will inevitably result in resources being spent unnecessarily.

2. Tax fraud involving the use of the social security numbers of the deceased results from a lack of communication between governmental agencies. These cases could be eliminated if the IRS and law enforcement were to incorporate use of the DMF themselves. There is no excuse for the IRS failing to perform the same simple fraud checks the rest of us do.

3. Rather than enact legislation guaranteed to hamper commercial practices across the country, it is preferable to look to within the Social Security Administration itself to correct sloppy procedures that have led to improperly reporting the deaths of living individuals. Improper functioning within the SSA is not a reason to close off access to this tool.

4. The Death Master File is overwhelmingly used as a means to verify identity, not steal it. It is an essential tool for maintaining an open society. In a democratic nation it is our duty to safeguard the right of all individuals to have access to public records, even when there is the chance that those records could be abused. When the records remain open, the fraud is easier to expose.

Millions of genealogists would be greatly impacted if legislation restricting access to the DMF were to be enacted. While the Massachusetts Genealogical Council would have preferred to give live testimony at the invitation-only March 20th hearing, we submit this written testimony in the hope that our members' voices will be heard. We offer the assistance of our organization to the Senate Committee on Finance Subcommittee on Fiscal Responsibility & Economic Growth in safeguarding the security of all Americans with Social Security numbers while promoting open access to public records.

Sincerely, Polly Kimmitt

Polly FitzGerald Kimmitt, CG℠

President
Massachusetts Genealogical Council P.O. Box 5393
Cochituate, MA 01778 508-842-8850
president@massgencouncil.org

Certified Genealogist and CG are service marks of the Board for Certification of Genealogists®, used under license by the Board's associates after periodic evaluation.

The U.S Senate

Committee on Finance
Subcommittee on Fiscal Responsibility & Economic Growth

Records Preservation & Access Committee
Federation of Genealogical Societies, National Genealogical Society,
International Association of Jewish Genealogical Societies

P.O. Box 200940

Austin TX 78720-0940

Statement for the Record

Hearing on Tax Fraud by Identity Theft:

Status, Progress, and Potential Solutions

Submitted by

Frederick E. Moss, JD, LL.M.

March 20, 2012

Chairman Nelson, Ranking Member Crapo, and distinguished Members of the Subcommittee:

Thank you for the invitation to submit this Statement for the Record on behalf of the genealogical community through its Records Preservation and Access Committee to supplement the record of the hearing held by the Subcommittee on the 20th of March 2012.

I serve as the legal advisor to the Federation of Genealogical Societies and as a member of the Records Preservation and Access Committee more fully described below.

Be assured that the genealogical community shares the objective of protecting Americans against fraud and of addressing deficiencies in the current operation of the Social Security Administration's Death Master File. This hearing marks a valuable opportunity to express our views to Congress on this important subject and we commend the committee for adding it to their agenda.

Egregious Identity Theft Cases Can Be Stopped Using Existing Resources

We have all been outraged by reports of identity thieves filing fraudulent tax refund claims using the SSNs of recently deceased infants & adults. Our strongest message is that the means to stop this particular form of identity theft exists now, without waiting for any additional legislation.

The Internal Revenue Service could curtail such claims almost immediately if tax refund claims were screened against the SSA's Death Master File & matching cases identified for special processing. If thieves are using the publicly available Social Security Death Index (the commercial version of the Death Master File) as their source for the Social Security numbers of recently deceased infants, were the IRS to use the same source, this particular vulnerability could be closed immediately with minimal adverse impact on legitimate users. This filter, together with other viable and easily implemented safeguards, could actually expedite the processing of such claims.

The testimony of Mr. Steven T. Miller, Deputy Commissioner for Services and Enforcement, IRS, suggests that they are, in fact, developing filters and procedures to intercept fraudulent refund claims. Their immediate challenge seems to be that the number of questionable returns identified this filing season is much larger than anyone might have anticipated and greatly exceeds the available resources needed to resolve them in a timely fashion.

This resources challenge was reinforced by the testimony of Ms. Nina E. Olson, The National Taxpayer Advocate, as she highlighted the fact that only one in seven calls to the identity protection specialized unit (most, likely from legitimate taxpayers) were answered, and then only after a wait on hold exceeding an hour. In her 2011 Annual Report to the Congress, Ms. Olson has also endorsed the use of IRS- issued Identity Protection PINs and allowing taxpayers to turn OFF the ability to file tax returns electronically using specified SSNs. These techniques have the potential to help greatly reduce the vulnerability of legitimate taxpayers to the predations of identity thieves. See pp. 61-62.

The resounding message we heard from the Operation Rainmaker press conference convened by the Tampa Chief of Police last Fall, was that the online tax refund system is unacceptably vulnerable, has been corrupted, and that there are identity thieves fully aware and anxious to exploit the weaknesses in that system. http://www.tampabay.com/news/publicsafety/crime/49-accused-of-tax-fraud-and-identity-theft/1189406

There is no need to wait for legislation to stop this travesty and protect families of deceased infants and adults. What is required is for the IRS to use the SSA's Master Death File for the fraud prevention purposes for which it was originally created. The US Treasury should not function as an ATM for identity thieves.

Most Effective Response--Target the Criminal

There have been scattered news reports announcing arrests in identity theft and identity fraud cases but not nearly enough to send a message to potential perpetrators that it is a serious crime and that we intend to catch those who engage in it. Deterrence requires that the community of identity thieves be made significantly aware of numerous actual prosecutions with significant sentences.

Effective prosecution of identity theft cases has been achieved most frequently as the result of extensive collaboration between local, state, and federal law enforcement agencies. The "Cash Back" Task Force first involved the Tampa Police Department and the county sheriff's office, and then was expanded to include the U.S. Secret Service and U.S. Postal Inspection Service. A police officer who had been one of the victims expressed frustration at the extent to which IRS had been prohibited from cooperating with the task force investigation.

This and other successful investigations have revealed the existence of significant barriers to communications between the IRS and law enforcement agencies. The Congress could appropriately examine whether existing privacy guidance has gone so far in shielding "taxpayer" information from non-tax collector governmental officials that it, in fact, undermines the integrity of the system.

Most of these offenders have been charged under existing laws for theft, money laundering, racketeering and related offenses. We would defer to federal prosecutors as to the utility of defining a new tax fraud offense more specifically targeting these facts but that approach should get sympathetic consideration. Claiming the unrelated deceased child of another as a dependent for tax refund claims might be considered an "aggravating" factor increasing the punishment under the federal sentencing guidelines.

Historical role of DMF/SSDI

The Social Security Death Index (SSDI) has been freely available on the internet for well over a decade with relatively few instances surfacing of it being abused. The effect of a person's name and social security number appearing on the SSDI was to officially declare that the person was dead and that SSN was effectively "burned." Few opportunities existed that afforded thieves the opportunity to exploit the identity of a deceased person.

In recent years, identity thieves have, however, discovered vulnerabilities in the on-line IRS filing system that allowed them to file fraudulent tax returns with relative anonymity claiming refunds and credits flowing from the stolen identities of recently deceased infants and adults.

The 2010 IRS filing season demonstrated that thieves were well aware of these vulnerabilities and determined to exploit them.

The testimony presented at this hearing that revealed the extent that the filters were identifying questionable returns during the early months of the 2011 filing season confirm that it is possible to thwart this particular scam. It is reasonable to expect that as this revenue stream is closed off, and a relatively few particularly egregious cases are aggressively prosecuted; identity thieves will soon shift their attention to other schemes.

This may already be occurring. We noted with alarm the testimony of Detective Sal Augeri of the Tampa Police Department, suggesting that once the most freely available version of the SSDI found at the RootsWeb.com site was moved behind the Ancestry.com pay wall, the thieves in the Tampa area are turning to institutional sources such as schools, assisted-living facilities, medical offices and other such entities in order to compromise SSN's of both the living and the dead.

Living or Dead—Privacy Concerns Differ

The public is constantly admonished to safeguard their social security numbers, and appropriately so. With a name, birth date, and SSN, it is possible for a thief to assume the identity of a potential target for a variety of nefarious reasons. Thus, thieves have applied for credit, opened new accounts, diverted existing accounts, offered the false identity when arrested, and an array of other schemes limited only by their imagination. Those seeking unauthorized employment, potential terrorists, money launderers, etc. frequently acquire or generate the SSNs of others to achieve their purposes.

The calculus dramatically changes when the targeted identity is authoritatively reported to be dead, as when their death is reported on the DMF/SSDI. The world is on notice that that SSN should no longer be active. Since the SSDI became publically available it has proven to be one of our most effective fraud prevention devices and to serve a variety of legitimate purposes.

Genealogists/Researchers Are NOT Identity Thieves

It is difficult for anyone who claims the slightest thread of decency to imagine the mindset of a thief who would desecrate the memory of a deceased infant in this despicable way.

It is impossible for me to imagine that any person sincerely pursuing information on their own ancestors, or assisting others to do so, would ever consider participating in such a scheme. I would be amazed if those arrested in the Tampa investigation could name their four grandparents, or any of their great-grandparents.

Public Access to the Death Master File

In a hearing addressing this same topic, held on February 2, 2012 before a subcommittee of the House Ways and Means Committee, Congressman Marchant posed a question raised by a constituent (and "millions like her") when he asked how we could be careful in what we do so that the people who are harmed are protected but those vitally interested in their ancestry can still access accurate information.

An extract of this exchange can be viewed at: http://youtu.be/HuSVZvMmN5A . The full hearing is available at:
http://waysandmeans.granicus.com/MediaPlayer.php?view_id=2&clip_id=133

While we strongly dispute his assertion that the information researchers get from the SSDI can be readily found in other sources, we followed with great interest Social Security Commissioner Astrue's progress report on the Office of Management and Budget's efforts to arrive at a coordinated administration position concerning appropriate public access to the Death Master File. His observation was that the issues are more complex than they might at first appear and that an attempt to rush a decision would almost surely get it wrong. We support a thorough review of these issues and would urge decision makers not to leap to solutions before the problems have been carefully defined and options developed.

What has clearly been missing from the process so far has been input from actual genealogists. It is impossible to "balance" competing interests if representatives of one side cannot "add weight" to their side of the balance scale. If given an appropriate opportunity to make the case, we are confident that public access to the DMF for legitimate genealogical purposes can be justified.

The Records Preservation and Access Committee is prepared to assist in providing that input by coordinating the appearance of highly qualified, well-recognized representatives prepared to provide information to assist decision-makers in the Executive and Legislative branches in making well-informed decisions.

Interests of the Genealogical Community

The interests of the genealogical community are not hard to understand. Access to records or the lack thereof, is the pivotal issue for genealogists. Without documentation, our family histories are more legend than history. Recent genetic advances have given additional significance to well-documented medical family histories. You can expect to hear expressions of concern from across the genealogical community whenever they may have reason to believe their access to these records is being threatened.

About the Records Preservation and Access Committee

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), the American Society of Genealogists (ASG), and industry representatives also serve as participating members. RPAC meets monthly, and more often if needed, to advise the genealogical and historical communities, as well as other interested parties, on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

Pending Legislative Initiatives

A number of Legislative proposals and options being considered within the Administration would go a step further and attempt to prevent the theft by taking additional preventative measures. These involve proposals that would delay publication of the SSNs of recently deceased persons for varying periods of time or total denying public access to the DMF/SSDI.

H.R.3475: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3475ih/pdf/BILLS-112hr3475ih.pdf

SB 1534 : http://www.gpo.gov/fdsys/pkg/BILLS-112s1534is/pdf/BILLS-112s1534is.pdf

HR 3482: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3482ih/pdf/BILLS-112hr3482ih.pdf

HR 3215 : http://www.gpo.gov/fdsys/pkg/BILLS-112hr3215ih/pdf/BILLS-112hr3215ih.pdf

We understand that an inter-agency task force operating under the auspices of the Office of Management and Budget is reviewing the issue of the circumstances under which the Death Master File should be made available to the public.

In our opinion, this approach aims at the wrong target. Even if the Social Security Death Index were totally taken down, it would have minimal impact on closing the vulnerabilities in the online tax refund system. It would, however, dramatically impact the ability of law-abiding citizens to use it for the myriad of legitimate purposes for which it was created.

We urge the broader use of this resource. Clearly financial institutions could reduce fraudulent loans to identity thieves claiming to be persons who are deceased and already reported on SSDI. State Pension Programs need a mechanism giving them notice that a pensioner has died in another jurisdiction in order to know that their entitlement to benefits has changed. Credit card companies should be careful in changing the mailing address on statements without satisfying themselves that the "cardholder" does not appear on SSDI and that the request is legitimate. Those administering medical trials need to monitor the mortality of the participants. We hear of new purposes for which this resource is used every day.

There are real costs associated with limiting access to public records. While these costs may be difficult to quantify, they clearly become more onerous the longer access to vital information is delayed or denied.

Any delay or redaction undermines the utility of the Death Master File in achieving the fraud prevention purposes for which it was created.

Furthermore, I submit that the filters currently being developed and employed have the potential of slamming the door on this particular form of fraud. Thieves will move on. By the time additional legislation could be put in place, the only users likely to be affected will be legitimate, law-abiding citizens. The unintended consequences of these measures will almost certainly exceed any possible benefit. We are in danger of re-fighting the last war.

We prefer continued appropriate access to the information that has been available from this resource. Given the choice of having it removed completely from internet access or having some limitations placed on its use (or the completeness/timeliness of the information therein) our choice is obvious.

RPAC Recommendations to the Congress and the Genealogical Community

After careful consideration of a variety of appropriate responses to this particularly despicable form of identity theft and the various legislative proposals it has prompted, we are prepared to recommend the following coordinated position. This week we plan to submit statements for the record of this hearing on behalf of RPAC, FGS, NGS and IAJGS. All RPAC leaders' statements for the record submitted to the Senate Subcommittee will state that:

> While we advocate all genealogists should have immediate access to the SSDI, we would support the two year delay in access as proposed in S 1534- 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.

I understand that the FGS statement will address in more detail the need for immediate access by those genealogists working in specified areas. We stand ready to work with all concerned parties to address this challenging issue and can best be reached at access@fgs.org.

Summary

We offer two main points:

(1) Our strongest message is that the means to stop this particular form of identity theft exists now, without waiting for any additional legislation.
(2) As existing policy regarding public access to the Death Master File is reviewed, we urge that input from actual genealogists be sought. The members of the Records Preservation and Access Committee stand ready to assist in arranging for that input to both the Executive and Legislative branches.

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:

I. INTRODUCTION:

The Senate Finance Committee, Subcommittee on Fiscal Responsibility and Economic Growth, held a Hearing on 2 February 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]

Mr. Ryesky also engages in genealogical research, and has thereby facilitated the reconnection of relations within his own family approximately six decades following the cut-off of communications imposed by the repressive policies of the Soviet Union. He has also used his genealogical research skills to locate missing persons in probate proceedings. Mr. Ryesky is a member of the Jewish Genealogical Society.

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

---

[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>.

The same article, *Tax Simplification: So Necessary and So Elusive*, 2 PIERCE L. REV. 93 (2004), is reputed internationally, including citation in 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>.

necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

III. COMMENTARY ON THE ISSUES:

A. Overview:

The Subcommittee has taken interest in the problem of tax fraud in conjunction with identity theft, having held a hearing regarding the matter on 25 May 2011, and has followed up on that hearing with the instant 20 March 2012 Hearing. Moreover, the House Committee on Ways and Means Subcommittee on Social Security also held a hearing to address similar matters on 2 February 2012.

On 5 February 2012 the Commentator submitted a Statement for the Record of the aforementioned Ways and Means hearing, [2] in order to avail Ways and Means his perspective from his personal and professional backgrounds in both tax administration and genealogic research. That 5 February 2012 Statement is incorporated by reference into this instant Statement and is not now reprised at length verbatim; the purpose of this instant Statement is to provide further details on specific relevant issues, again from the Commentator's perspective gained through personal and professional involvement in both genealogy and tax administration.

B. Data Security and Data Stewardship:

The concept of data security is commonly viewed in terms of policies to restrict access to data. While the restriction of access is certainly a vital if not indispensable element of data security, there also need to be procedures and policies for verifying, processing and utilizing the data. This issue is distinct from the issue of who does or does not have access to the data. The concept of data stewardship encompasses far more that the concept of data security. [3]

---

[2] A copy of the 5 February 2012 Statement has been posted on the website of the Records Preservation & Access Committee, a committee formed by the various genealogical societies, <http://www.fgs.org/rpac/wp-content/uploads/2012/02/wm-ssdmf-comments-2012.pdf>.

The Commentator is informed that staffers from the office of Subcommittee Chair Nelson have also been availed copies of his 5 February 2012 Statement for the Record to Ways & Means. E-mail from Jan Meisels Allen [vicepresident@iajgs.org] to Ryan McCormick [ryan_mccormick@billnelson.senate.gov] and David Goldfarb [david_goldfarb@billnelson.senate.gov] (26 March 2012).

[3] *See, e.g. Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Record*, Nat'l Center for Education Statistics, SLDS Technical Brief, NCES 2011-602 (Brief 2, November 2010), available on the Internet at <http://nces.ed.gov/pubs2011/2011602.pdf>; Sara Rosenbaum, Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access, 45 Health Services Research, no. 5, Part II, 1442 (October 2010).

The misadventures related by Mr. McClung in his testimony at this Subcommittee's 25 May 2011 Hearing, [4] together with those related by Mr. Agin at the House Ways & Means Committee's 2 February 2012 Hearing, [5] serve as exemplars to illustrate the distinctions between data security and data stewardship. If data's security is evaluated solely upon how well the access to the data is restricted, then the IRS comes through with flying colors in its data security practices. Neither Mr. McClung nor Mr. Agin were (or, apparently, have since been) given access to adequate information regarding the identities of the scoundrels who misappropriated their respective deceased children's identity, nor what measures the IRS has taken and intends to take against those fraudsters.

On the other hand, the IRS's stewardship over its data has proven to be a miserable failure. The social security numbers (SSNs) were not verified, even though the means to verify the numbers should have been readily available to the IRS. This has resulted in a fraud not only upon the IRS, but upon the McClung and Agin families as well. Had the SSNs of the deceased dependents been verified, they would have been flagged as not being claimed on a return filed by the deceased dependents' parent, and the fraud perpetuated upon the government (and upon the McClung and Agin families) might have been prevented.

As Messrs McClung and Agin have painfully learned (through no fault of their own), data security practices alone do not constitute sound stewardship of taxpayer personal data. And, as reflected in the testimony of several witnesses, the McClung and Agin cases are in no way unique.

C. The IRS's Resolution Process:

If the word of higher management officials at the IRS is taken at face value, they certainly understand and appreciate the gravity of identity theft in the commission of tax fraud. Mr. Miller's testimony at the instant Hearing reflects this, as does the prior testimony of Ms. Tucker at the 25 May 2011 Hearing.

Such conceptual clarity on the personal level, however, has yet to fully percolate down to the operational level. As described by Mr. McClung (and to a lesser extent by Mr. Agin), in dealing with cases of the same SSN on two separate tax return filings, the IRS has heretofore passively postured itself more as a disinterested bailee seeking to correct a typographical error so that it can properly process its paperwork, rather than as an aggrieved co-victim of an egregious

---

[4] 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>.

[5] 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>.

crime who seeks justice. As recounted by Mr. McClung, the IRS, initially at least, depended upon the person who submitted the fraudulent return to make the correction, instead of giving the aggrieved identity theft victim any meaningful opportunity to substantiate his or her position.

This stands in contradistinction to the U. S. Postal Service's resolution of disputes regarding who should be entitled to receive mail addressed to a given location, whereby each party is given opportunity to explain why he or she is entitled to receive the mail, instead of waiting for one party to concede that he or she is not entitled to the mail. [6]

D. Vaccination or Quarantine:

It is well established and proven that vaccination against diseases such as measles, smallpox or polio is a far, far more effective prevention strategy than trying to quarantine and sequester from society those afflicted with active cases of such diseases. Similarly, preventing public access to the Social Security Death Master File (or its alternative incarnation, the Social Security Death Index) would in no way end the current identity theft tax fraud epidemic.

SSNs are available from many, many other sources. Mr. Cimino's testimony mentions cases which include a professional tax return preparer obtaining SSNs from her client database, and an ex employee who had accessed her former private sector employer's database. Det. Augeri's testimony mentions employees of assisted living facilities accessing SSNs. SSNs are to be found on many internet sites; not only those sites of shady provenance, but also perfectly legitimate governmental websites. Indeed, names, addresses, full Social Security Numbers and dates of birth are posted on the websites of certain state agencies of Chairman Nelson's home State of Florida, and on the website of at least one judiciary body in Ranking Member Crapo's home state of Idaho. [7]

And nearly two years ago, one of the Commentator's students retrieved a report about the Commentator from a proprietary online database to which the student had access as a perquisite for his business. The report contained the Commentator's SSN, date of birth, and other personal information. The foregoing exercise was done in the classroom, during class time, with the Commentator's consent in order to demonstrate to the class the ease with which identity theft can be committed.

While some restrictions on the Social Security Death Master File(DMF) may well be appropriate, its sudden disappearance would not prevent the use of identity theft in tax fraud. The fraudsters have plenty of other available SSN sources. The IRS would still receive

---

[6] 39 C.F.R. Part 965; *see also* Matter of Apostolidis and Apostolidis, (28 May 2010), P.S. Docket No. MD 10-75 (28 May 2010) <http://about.usps.com/who-we-are/judicial/admin-decisions/2010/md-10-75-id.htm>; Matter of Daniel Sager, Esq. and Joanne Savage, Esq., P.S. Docket No. MD 10-189 (13 January 2011) <http://about.usps.com/who-we-are/judicial/admin-decisions/2011/md-10-189-id.htm>.

[7] Particulars are not now set forth in this public document; the Commentator would be pleased to provide such particulars directly to the Senators or their staffs.

fraudulent tax returns with stolen identities and, if the IRS makes no improvements in its operational attitudes and procedures, would still subject law-abiding and compliant tax return filers to experiences similar to those suffered by Messrs. McClung and Agin and their families. Moreover, as more fully detailed by other commentators' submissions, the DMF is a valuable tool for individuals and businesses to use in order to prevent identity theft.

Clearly, then, the IRS needs to significantly upgrade its data stewardship practices.

E. The Aggrieved Taxpayer Identity Theft Victim's Right to Know:

I.R.C. § 6103, the Internal Revenue Code's implementation of the Freedom of Information Act, authorizes the IRS to release information tax return and taxpayer information to various persons under various circumstances. I.R.C. § 6103(e) provides for disclosure to persons having material interest in such information, but nowhere in that verbose subsection is disclosure authorized to innocent victims of identity theft whose identity (or the identity of their bona fide dependent) has been expropriated to perpetuate a tax fraud upon the government. Messrs McClung and Agin each implicitly if not explicitly expressed frustration , anger and disgust at not being informed of their assailants.

It would seem that the identity of such wrongdoers should be made available to their victims. Even in non-criminal, nonlethal and nontraumatic instances where a driver mistakenly causes his or her vehicle to strike an unattended parked car, the owner of the struck vehicle is entitled to the negligent driver's name, address, license number, automobile registration data and vehicle identification number, and the serial number of the insurance policy. While personal data such as the fraudster's Social Security Number may well be inappropriate for disclosure to the victim, [8] particulars such as the wrongdoer's name, whereabouts, and whether and to what extent the IRS has taken any action against such individuals (or contemplates such action) would be quite appropriate for disclosure if such disclosure would not materially compromise law enforcement activity.

G. Genealogical Research:

The Commentator's Statement for the 2 February 2012 Ways and Means Hearing succinctly mentions various important matters that depend upon sound genealogic research; other submissions for that Hearing give greater detail, as likely will other submissions for this instant 20 March 2012 Finance Committee Hearing. The Commentator shall not now belabor the matter, other than to (A) state that he shares the view that genealogical research is important and needs to be facilitated by governmental policy; and (B) remind the Subcommittee that the

[8] While there is a certain poetic justice in openly disclosing to the public and the national media the Social Security Numbers of the fraudsters such as those who expropriated the identity of Messrs McClung and Agin's deceased children, this would be antithetical to the rule of law. It is noted, however, that even the mere contemplation by individual members of the public of such self-help vigilantism is an indicium that the government is failing miserably in discharging its obligations to the public.

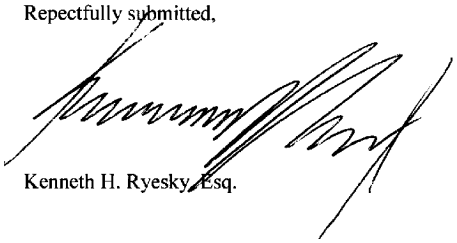
perceived lack of transparency in certain genealogical recordkeeping and disclosure practices has recently led to what amounts to a high profile political distraction on account of questions, in the minds of some, regarding the qualification and eligibility of the President of the United States to hold such an office.

H. Conclusion:

There is a pressing need to prevent identity theft, and that need is all the more salient when the identity theft is used in connection with tax fraud. The IRS (and the state taxation authorities) and other administrative agencies, the law enforcement bodies, prosecutors, courts and the private sector all need to rethink many of their current data stewardship practices and paradigms.

Amidst this all, it must be remembered that the information in the Social Security Death Master File (DMF) is a valuable public resource with legitimate purposes and uses, including, as further detailed by this Commentator and others in connection with this and/or other Hearings, the prevention of identity theft. Barring all non-governmental accessibility to the DMF would, contrary to the stated intentions of those who advocate such dire restrictions, actually facilitate the identity thief's nefarious scheme. While some embargoes or qualifications on the public availability of SSNs in the DMF may well be appropriate and warranted, it would be a grave and costly mistake to totally restrict access to the information in the DMF.

20 March 2012
Repectfully submitted,



Kenneth H. Ryesky, Esq.