

**IDENTITY THEFT AND TAX FRAUD: GROWING
PROBLEMS FOR THE INTERNAL REVENUE
SERVICE, PART 4**

HEARING

BEFORE THE
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION,
EFFICIENCY AND FINANCIAL MANAGEMENT
OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

NOVEMBER 29, 2012

Serial No. 112-191

Printed for the use of the Committee on Oversight and Government Reform



Available via the World Wide Web: <http://www.fdsys.gov>
<http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

77-479 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 OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana	ELIJAH E. CUMMINGS, Maryland, <i>Ranking</i>
JOHN L. MICA, Florida	<i>Minority Member</i>
TODD RUSSELL PLATTS, Pennsylvania	EDOLPHUS TOWNS, New York
MICHAEL R. TURNER, Ohio	CAROLYN B. MALONEY, New York
PATRICK T. McHENRY, North Carolina	ELEANOR HOLMES NORTON, District of
JIM JORDAN, Ohio	Columbia
JASON CHAFFETZ, Utah	DENNIS J. KUCINICH, Ohio
CONNIE MACK, Florida	JOHN F. TIERNEY, Massachusetts
TIM WALBERG, Michigan	WM. LACY CLAY, Missouri
JAMES LANKFORD, Oklahoma	STEPHEN F. LYNCH, Massachusetts
JUSTIN AMASH, Michigan	JIM COOPER, Tennessee
ANN MARIE BUERKLE, New York	GERALD E. CONNOLLY, Virginia
PAUL A. GOSAR, Arizona	MIKE QUIGLEY, Illinois
RAÚL R. LABRADOR, Idaho	DANNY K. DAVIS, Illinois
PATRICK MEEHAN, Pennsylvania	BRUCE L. BRALEY, Iowa
SCOTT DESJARLAIS, Tennessee	PETER WELCH, Vermont
JOE WALSH, Illinois	JOHN A. YARMUTH, Kentucky
TREY GOWDY, South Carolina	CHRISTOPHER S. MURPHY, Connecticut
DENNIS A. ROSS, Florida	JACKIE SPEIER, California
BLAKE FARENTHOLD, Texas	
MIKE KELLY, Pennsylvania	
VACANCY	

LAWRENCE J. BRADY, *Staff Director*

JOHN D. CUADERES, *Deputy Staff Director*

ROBERT BORDEN, *General Counsel*

LINDA A. GOOD, *Chief Clerk*

DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND FINANCIAL MANAGEMENT

TODD RUSSELL PLATTS, Pennsylvania, *Chairman*

CONNIE MACK, Florida, <i>Vice Chairman</i>	EDOLPHUS TOWNS, New York, <i>Ranking</i>
JAMES LANKFORD, Oklahoma	<i>Minority Member</i>
JUSTIN AMASH, Michigan	JIM COOPER, Tennessee
PAUL A. GOSAR, Arizona	GERALD E. CONNOLLY, Virginia
FRANK C. GUINTA, New Hampshire	ELEANOR HOLMES NORTON, District of
BLAKE FARENTHOLD, Texas	Columbia

CONTENTS

Hearing held on November 29, 2012	Page 1
---	-----------

WITNESSES

Ms. Beth Tucker, Deputy Commissioner for Operations Support, Internal Revenue Service	
Oral Statement	6
Written Statement	9
The Honorable J. Russell George, Inspector General, Treasury Inspector General for Tax Administration	
Oral Statement	19
Written Statement	21
Ms. Nina E. Olson, National Taxpayer Advocate, Internal Revenue Service	
Oral Statement	37
Written Statement	39
Mr. James R. White, Director, Strategic Issues, U.S. Government Accountability Office	
Oral Statement	56
Written Statement	58

APPENDIX

The Honorable Todd Russell Platts, a Member of Congress from the State of Pennsylvania, Opening Statement	95
The Honorable Edolphus Towns, a Member of Congress from the State of New York, Opening Statement	97
Mr. Kenneth H. Ryesky, Esq., Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York, Statement for the Record	99

IDENTITY THEFT AND TAX FRAUD: GROWING PROBLEMS FOR THE INTERNAL REVENUE SERVICE, PART 4

Thursday, November 29, 2012

HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION,
EFFICIENCY AND FINANCIAL MANAGEMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:07 a.m., in Room 2247, Rayburn House Office Building, Hon. Todd Russell Platts [chairman of the subcommittee] presiding.

Present: Representatives Platts, Issa, Towns, Connolly.

Also Present: Representative Diaz-Balart.

Staff Present: Alexia Adrolina, Majority Assistant Clerk; Molly Boyl, Majority Parliamentarian; Steve Castor, Majority Chief Counsel, Investigations; John Cuaderes, Majority Deputy Staff Director; Linda Good, Majority Chief Clerk; Mark D. Marin, Majority Director of Oversight; Tegan Millspaw, Majority Professional Staff Member; Scott Schmidt, Majority Deputy Director of Digital Strategy and Press Secretary; Jaron Bourke, Minority Director of Administration; Beverly Britton Fraser, Minority Counsel; and Devon Hill, Minority Research Assistant.

Mr. PLATTS. Good morning. Today's hearing on Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service will come to order.

Before I begin my statement, I would like unanimous consent that our colleague from Florida, Mr. Diaz-Balart, will be allowed to participate in today's hearing. Without objection, so ordered.

Mario, we are delighted to have you here with us.

The purpose of today's hearing is to address the serious and rapidly growing problem of identity theft-related tax fraud. This is the fourth hearing the Subcommittee has had this Congress on this important issue, and it will continue our examination of how fraud is occurring and what can be done to stop it. We will review the IRS's actions to prevent and detect identity theft tax fraud, and evaluate what more can be done to reduce the problem and assist victims of this crime.

Identity theft-related tax fraud occurs when a fraudster uses stolen information to file a fraudulent tax return in the victim's name. If the victim has not filed a tax return yet, the fraudster can file a return and end up receiving a tax refund from the IRS. When

the legitimate taxpayer goes to file a tax return, it may be flagged by the IRS as a duplicate claim.

Many victims are unaware that their identities, and in many cases their tax refunds, have been stolen until they file their own return and are notified that someone else has already filed in their name. It can take months or, as we have learned, sometimes even years for these cases to be resolved and for a tax refund to the legitimate taxpayer be issued.

In the last few years, the number of incidents of identity theft-related tax fraud has drastically increased, from approximately 51,700 cases in 2008 to over 1 million cases in 2011. This number represents only the known cases of identity theft. The total number of incidents that go undetected is unknown, but the Treasury Inspector General for Tax Administration, Mr. George, who we are delighted to have with us here today, estimates that the number could be much higher. In TIGTA's review of tax returns filed in 2011, TIGTA identified an additional 1.5 million potentially fraudulent returns that were not detected by the IRS.

TIGTA and the Taxpayer Advocate have also raised concerns that victims of identity theft do not receive adequate assistance from the IRS. In June 2011, this Subcommittee heard from three witnesses who had been victims of identity theft and learned that their interactions with the IRS were often uninformative, frustrating, or discourteous. One witness stated that, "the way I feel I have been treated by the IRS system has made me a victim a second time." We want to certainly recognize that the IRS has made tremendous efforts to improve its assistance to victims, including creating a Taxpayer Protection Unit and providing better training to their employees. However, we also want to recognize that there are still significant issues to be addressed to ensure that victims get the assistance they need.

In addition to the impact on victims, identity theft-related tax fraud results in a significant loss to the United States Government and ultimately the American taxpayers. TIGTA estimates that the IRS could issue as much as \$21 billion in fraudulent tax refunds over the next five years as a direct result of identity theft.

The average amount of a fraudulent tax refund is only about \$3,400, so it is difficult, and almost impossible, for the IRS to devote the resources necessary to investigate every case. Some fraudsters manage to collect millions of dollars, though, through multiple refunds. Given the severity of the problem, we are committed to ensuring that we do better in deterring this type of fraud.

And while, Ranking Member Towns and I, this is our last hearing as Chairman and Ranking Member, and in the past we would say and perhaps we would be switching seats, but this time we are both leaving our seats as we both prepare to retire from Congress, but we know, with our great staff on both sides of the aisle, as well as our colleagues on this Subcommittee and full Committee, the attention to this issue will continue.

Another key problem is the lack of information the IRS has about identity theft-related tax fraud. The Government Accountability Office has raised concern that IRS needs better performance measures and data collection to help assess the effectiveness of its initiatives to stop fraud. IRS agreed with GAO's recommendation, but

there is still a shortage of information about this problem, and I know one of those challenges is resources available to commit to this responsibility.

IRS is also not utilizing all information that it currently possesses, according to TIGTA, including the case files of victims of identity theft. Once a case has been resolved, files are often deleted without IRS using this information to identify trends or study them for ways to detect and prevent future fraud.

We are pleased that the IRS has launched a number of pilot programs to better combat fraud and to improve on the issues that TIGTA has raised, as well as the Taxpayer Advocate, and we look forward to hearing about them here today. One of these improvements is a Personal Identification Number, or PIN, which is given to victims of identity theft. This PIN is used by the victims to identify their returns and add an extra level of security to their legitimate return.

IRS has also finished its first pilot of a program designed to share sensitive taxpayer information with local law enforcement officials in order to better investigate and prosecute fraud. IRS tested this pilot in Florida and, in October, the IRS expanded the pilot program to eight additional States, including my home State of Pennsylvania and Mr. Towns' home State of New York.

The IRS is working to stop the rise of identity theft-related tax fraud and to better detect and prevent fraud. We appreciate their efforts and have followed their work closely throughout this Congress. As I stated earlier, though, we also know we have more room for improvement, and we appreciate the continued focus on this important issue. Today we will hear from a panel of experts on how to both combat identity theft-related tax fraud and how to better assist the victims of this fraud. We look forward to their testimony.

We are certainly grateful for the written testimony that we have been provided, as well as the oral testimony you will give here today, and very much want to thank each of our witnesses not just for being here today, but for your focus on this issue, as well as numerous others that relate to tax code and the implementation of the tax code and how we can do so in a fair and efficient manner that ensures that the Federal Government receives its revenues prescribed by law, but also that we do right by the American taxpayers and, in this case, especially by innocent Americans who are victimized by criminals.

With that, I am honored to recognize the distinguished Ranking Member, my colleague from New York, Mr. Towns. And, Ed, before I do, just again, with this being our final hearing, whether it was when I chaired the Committee and you have been ranking member, or when you chaired it and I was ranking member, it has been an absolutely great privilege to have served with you in the broad sense, and especially here with this Subcommittee; and not just from a professional standpoint, but personally. I know that we are both leaving the House and going to be going our separate ways, but look forward to a continued friendship with you and we will look forward to future visits to Brooklyn and seeing how you are doing in your retirement as I move on to my next chapter as well.

With that, I recognize Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman. And let me say that a term and phrase that is used around here sometimes and people don't really mean it, they say my good friend. Well, I want you to know when I say my good friend to you, I really, really mean it, because it has been a pleasure working with you over the years. And, of course, I know you that will do well in whatever you decide to pursue in the future.

Identity theft and tax fraud are serious, and it is a growing problem. According to a July 2012 report from the Treasury Inspector General for Tax Administration, incidents of identity theft reported by the Internal Revenue Service have skyrocketed, from 51,702 in 2008 to over 1 million cases in 2011. Even though ID theft and the related tax fraud continue to escalate, the IRS has been working diligently to get ahead of the identity thieves. More fraud cases are being detected by IRS filters. As a result, billions of dollars have been kept from the hands of criminals. But more effort is required for us to stay ahead of the criminals and to help the victims.

One of the most important priorities we must address is the quality of assistance given to taxpayers victimized by tax refund fraud. The Inspector General puts it bluntly: The IRS is not providing effective assistance to taxpayers who report being victims of identity theft. This must change. It also appears that a better job has to be done tracking ID theft tax fraud cases so that a clear solution can be developed. And, most notably, we must increase the prosecution rates of fraudsters to serve as a deterrent to others.

Today's hearing is the fourth in a series held by this Subcommittee examining how the IRS handles the problems of identity theft and tax fraud. Our witnesses are all well versed in the issues we will examine today. Each of them has had a hand in identifying problems and crafting solutions to the current crisis, and I thank you for that and I look forward to your testimony this morning.

I have spent most of my 30 years in Congress pursuing initiatives that have resulted in a better, more efficient Federal Government. As you have heard from my colleague and the Chairman of this Committee, Mr. Platts and I have shared this commitment as we traded the chairmanship of this Committee over the years. Unfortunately, this will be our last hearing. I look to you and the returning members of this Committee to continue the hard work and the fight for a solution to this problem and all of the other issues that will make our great government a better one.

Mr. Chairman, it has been an honor and a great pleasure working with you. Whatever you decide to pursue, I wish you the best and I know you will have success. On that note, I yield back.

Mr. PLATTS. Thank you for the kind words and, as I said, the feeling is mutual, and you truly are my good friend as well.

Mr. TOWNS. Thank you.

Mr. PLATTS. With that, I am honored to yield to one of our colleagues from Florida who joined us here today, the gentleman who is not a member of the Committee, but I know has a keen interest in this issue for his constituents as well, Mr. Diaz-Balart.

Again, welcome, and I yield to you for an opening statement.

Mr. DIAZ-BALART. Thank you very much, Mr. Chairman. Let me first thank you and also Ranking Member Towns for holding an-

other hearing on this important issue and for inviting me to sit in and give a brief opening statement.

I do want to take this opportunity, Mr. Chairman, though, to mention that you have been really a spectacular leader on this issue and others, but specifically on this issue, and I know that I can speak for everyone in Congress and the American people when I say that you are going to be missed here, Mr. Chairman. Again, I want to thank you for your service, for your leadership.

I also want to take this opportunity to thank the Ranking Member. He has dedicated his life to public service and we are very grateful for that. So, to both of you, thank you for your invaluable service.

Mr. Chairman, as some of you know, as you clearly know, South Florida has been one of the most affected areas in the Country when it comes to IRS identity theft. I, myself, my office have had dozens of constituents who have reached out to us because their tax returns have been stolen, and as you mentioned, Mr. Chairman, they feel absolutely helpless. I have had numerous constituents who have also had their tax returns stolen more than once, in consecutive years; and imagine how they must feel. These are hardworking people who depend on, in many cases, their returns to pay basic bills, basic necessities.

So obviously we need to do more to help those victims and to prevent those crimes from taking place in the future. It has been one of my top priorities and I have worked closely with the IRS to try to help resolve this epidemic.

I also want to thank the IRS. You all have been exceedingly, exceedingly accessible not only to me, but to my staff; always been willing to come forward to discuss this issue and to try to let us know what you are working on, et cetera. So I want to thank you for being extremely accessible to us.

Mr. Chairman, they have made some great improvements over the last year, but obviously, as the Ranking Member and you have said, a lot more has to be done. I was really happy to learn about the Identity Theft Victim Disclosure Waiver pilot program that was implemented in Florida in April of this year. I let met with stakeholders down there, the State attorney's office and the State attorney herself, and they were really looking forward to getting this program going. And I have spoken to both the IRS and the local authorities about the success so far. It does seem to be helping State and local authorities to prosecute the individuals responsible for this heinous crime.

Now, while this program is a step in the right direction, as we have all said before, much more needs to be done. So far, most of what the IRS has implemented deals with dealing with the crime after it has occurred. That pilot program is one of those examples. And, again, while I appreciate that and I think they are having some success, I think more emphasis needs to be put and more focus needs to be put on preventing these crimes from happening in the first place. Obviously, the IRS needs to come up with detailed and up-to-date plans to prevent further tax return fraud, while also taking care of the taxpayers who have already fallen victim.

So it is my hope that this hearing will once again serve as a discussion on how we can improve our tax return system and to protect taxpayers' hard-earned money.

I once again want to thank you, Mr. Chairman, and the Ranking Member for holding this hearing, but for being leaders in this area. The taxpayers of our Country have a great debt of gratitude to you. And I hope, Mr. Chairman, that we are able to also hear about exactly how successful and some of the results from the South Florida pilot program.

With that, Mr. Chairman, I thank you very much for this opportunity, for allowing me to sit in, and I yield back.

Mr. PLATTS. The gentleman yields back, and more than glad to have you here with us, Mario, and, again, your efforts with your constituents. I think more and more of our colleagues are coming to realize the challenge of this issue as our offices are being contacted by those who have been victimized and all the more important of the work of the IRS and all involved to prevent this and, when it does occur, help those who have been victimized.

We will keep the record open for seven days for any other opening statements or extraneous material. We will now move to our panel of witnesses, and we are, again, very grateful for all four of you being here with us today.

First, Ms. Beth Tucker, Deputy Commissioner for Operations Support at the Internal Revenue Service; the Honorable J. Russell George, Inspector General at the Treasury Inspector General for Tax Administration; Nina Olson, National Taxpayer Advocate; and Mr. James White, Director of Strategic Issues at the United States Government Accountability Office.

Pursuant to our Committee rules, if I could ask all four of you to stand and raise your right hand as I swear you in.

Do you solemnly swear or affirm that the testimony you are about to give this Committee will be the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Mr. PLATTS. Thank you. You may be seated.

Let the record reflect that the witnesses all answered in the affirmative.

We are going to set the clock at five minutes because we do, again, appreciate the written testimony in greater detail. If you need to go over a little bit, that is not a problem. We will try to keep it as close to five as we can so we can get more time for exchange, Q and A, with you.

So, Ms. Tucker, if you would like to begin.

WITNESS STATEMENTS

STATEMENT OF BETH TUCKER

Ms. TUCKER. Chairman Platts, Ranking Member Towns, and Mr. Diaz-Balart, my name is Beth Tucker, and I am the Deputy Commissioner for Operations Support at the Internal Revenue Service. I appreciate the opportunity to update you on the actions we are taking at the IRS to combat refund fraud and help the victims of identity theft.

Let me also say, on a personal note, you probably don't hear this from witnesses at hearings a lot, but it is an honor to be here with you today for your final hearing, and I appreciate all the support you have given us at the IRS over the years.

Mr. PLATTS. Well, Ms. Tucker, it is a partnership with you, between the Committee, and I was going to joke that maybe you are glad that Ed and I are retiring so you can get rid of it.

Ms. TUCKER. No, sir, you won't hear that from me.

[Laughter.]

Mr. PLATTS. And I can honestly say that has never been conveyed by you and your staff and colleagues at IRS. It has been a great partnership, so thank you.

Ms. TUCKER. Over the past few years, the IRS has seen a significant increase in refund fraud schemes, particularly schemes involving identity theft. Identity theft, and the harm it inflicts on innocent taxpayers, is a problem that we take very seriously at IRS.

When it comes to identity theft, the IRS faces, unfortunately, the same challenges as every major financial institution. We are continually reviewing our processes and our policies to make sure we are doing everything possible to minimize identity theft, to help the victims, and to investigate the people committing these crimes.

There is a delicate balance here, as we all know. The IRS has a dual mission when it comes to refunds, particularly when they are generated, in whole or in part, by tax credits. When we develop controls to minimize fraud, we must always consider, as well, the need to distribute refunds in a timely manner and ensure that taxpayer rights are protected.

The IRS is committed to improving our efforts at blocking fraudulent refund claims before they are processed. We strive to screen our false returns at the earliest stage and we are getting results. During the first ten months of this calendar year, we protected approximately \$20 billion of revenue related to refund or to fraudulent returns, including identity theft. Let me share with you some of our up-front prevention efforts.

We did implement 13 new filters at last filing season to improve our ability to spot false refunds before they go out the door. We are also adding additional filters for the upcoming filing season, which I can discuss more later. We also issued identity protection PINs in 2012 to more than 250,000 taxpayers whose identities were stolen. The PIN authenticates a return filer as the legitimate taxpayer at the time of filing and also, of course, helps prevent the repeat of stolen identity that Mr. Diaz-Balart mentioned earlier. For the coming filing season, we expect to issue well over 600,000 PINs to taxpayers to aid in protection of their next return.

We have accelerated the matching of information returns to help identify bad returns earlier. We are also locking more accounts of deceased taxpayers whose Social Security Numbers have been used by these unscrupulous thieves so they can't be used again. We are also working more closely with law enforcement to match information they are providing us against information we have on file. We are also working closely with our partners across tax administration to identify other opportunities.

This effort is not over. We have talked about all of the things that IRS has done. We continue to find ways to improve our proc-

esses and our systems, and we look forward to talking with you today about those continuing efforts.

[Prepared statement of Ms. Tucker follows:]

**WRITTEN TESTIMONY OF
BETH TUCKER
DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND
FINANCIAL MANAGEMENT
ON IDENTITY THEFT
NOVEMBER 29, 2012**

INTRODUCTION AND SUMMARY

Chairman Platts, Ranking Member Towns and Members of the Subcommittee on Government Organization, Efficiency and Financial Management, my name is Beth Tucker and I am Deputy Commissioner for Operations Support at the Internal Revenue Service. I appreciate the opportunity to update you on the actions we are taking at the IRS to combat refund fraud and help victims of identity theft.

Over the past few years, the IRS has seen a significant increase in refund fraud schemes, particularly schemes involving identity theft. Identity theft – and the harm it inflicts on innocent taxpayers – is a problem that we take very seriously. We have a comprehensive identity theft strategy focusing on both fraud prevention and victim assistance.

The IRS is confronted with the same challenges as every major financial institution in detecting and preventing identity theft. The landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information and using it for their gain. We are continually reviewing our processes and policies to ensure that we are doing everything possible to minimize the incidence of identity theft, to help those who are victimized by it, and to investigate those who are committing the crimes. There is a delicate balance here, though. 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 support important policy goals set by Congress, such as relieving poverty, encouraging work, and boosting the economy. When we develop and implement additional controls to minimize fraud, it is imperative that we consider the need to distribute refunds in a timely manner while also ensuring that taxpayer rights are protected.

The IRS encounters identity theft in several ways. First, identity thieves attempt to defraud the federal government of funds by filing fraudulent refund claims using another person's identifying information they have stolen from a wide variety of places. Second, innocent taxpayers are victimized because their refunds are delayed. In some situations, fraudulent filings may cause us to initiate an adverse enforcement action against the innocent taxpayer until we are able to confirm that someone else has used

his or her information. In others, the stolen identity may belong to a person who is not an active filer – for example, a deceased individual or a person without a filing requirement.

We continue to make improvements in both fraud prevention and victim assistance. This year, we have implemented new processes for handling returns and new filters to detect fraud, and will continue to make improvements going forward. We are collaborating with outside stakeholders to learn and educate and to share information, where appropriate; and we are committed to aggressively pursuing perpetrators of tax fraud to bring them to justice.

The IRS is working to speed up and further streamline identity theft case resolution so that innocent taxpayers will experience as little inconvenience as possible. We have committed more staff to work identity theft cases, and substantially increased training for employees who assist victims. Although identity thieves steal the information they use from sources outside the tax system, the IRS is sometimes the first to inform a victim that identity theft has occurred. Therefore, it is especially important that IRS employees understand what identity theft victims are experiencing and how to provide victims with information that will help them limit any non-tax-related negative effects of identity theft.

As I describe for you in greater detail our efforts to combat fraud, I urge you to keep in mind that the improvements the IRS is making would not be possible without the additional resources we have directed toward these programs. Even in this challenging budget environment, we have substantially increased our resources devoted to both preventing fraud and serving victims. The Administration's Fiscal Year (FY) 2013 Budget request includes important funding for additional enforcement and taxpayer service initiatives focused specifically on addressing refund fraud, including identity theft. As you will see, we have accomplished a lot, and we intend to do much more in the coming year.

PREVENTING FRAUD

During the first ten months of this calendar year, the IRS protected approximately \$20 billion of revenue related to fraudulent returns, including identity theft. The IRS is committed to improving its multi-faceted approach to blocking these fraudulent refund claims. To that end, we strive to operate in such a way that false returns are screened out at the earliest possible stage.

Stopping the Refund at the Door – Enhanced Return Processing

The IRS screens returns for fraud at multiple stages in the processing life-cycle. In 2008, we began placing an indicator on the accounts of taxpayers who have experienced identity theft. These indicators initially served two primary purposes: to speed up account reconciliation for the legitimate taxpayer, and to reduce the likelihood

that a taxpayer's information could be used for a fraudulent refund claim in subsequent years. As our identity theft indicator program has developed, we have leveraged it to put in place additional proactive tools that identify fraudulent returns at the point of filing.

Last year, we launched a pilot program to test the Identity Protection Personal Identification Number (IP PIN). The IP PIN is a unique identifier that authenticates a return filer as the legitimate taxpayer at the time the return is filed. For filing season 2012, the IRS issued IP PINs to approximately 250,000 taxpayers who had identity theft markers on their tax accounts. We verified the presence of this IP PIN at the time of filing, and rejected returns associated with a taxpayer's account where an IP PIN had been assigned but was missing. For the 2013 filing season, we have enhanced our programming to increase efficiency, and are expanding the IP PIN program to more than 600,000 taxpayers.

In 2011, we launched several new efforts focused on catching fraudulent refunds during the initial processing of returns, with identity theft being a key focus of these initiatives. As a result, we have made numerous improvements in catching fraud before refunds are issued:

- We implemented new identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds. For example, we designed and launched new filters that flag returns if certain characteristics are detected. While the development of effective filters is complex given the dynamic lives of legitimate taxpayers, these filters enable us to identify fraudulent returns even where a taxpayer's information has not been previously used for filing by an identity thief. These new filters specific to identity theft are only a small part of our overall program which includes a large percentage of identity theft cases over and above the new filters. These filters alone have caught over 490,000 questionable returns for review this calendar year. We continue to work this inventory, but thus far we have prevented the issuance of \$1.5 billion in erroneous refunds from these filters. We are adding even more identity theft filters for the 2013 filing season, to include filters that target multiple refunds into a single bank account or to a single address.
- We have accelerated the use of information returns in order to identify mismatches earlier. Moving this matching process forward in time has enhanced our ability to identify fraudulent tax returns before we process them. We will accelerate more types of information return data in 2013.
- We have implemented a variety of mechanisms to stop the growing use by criminals of deceased individuals' identity information to perpetrate fraud. During the first nine months of calendar year 2012, the IRS has stopped over 130,000 returns using these tools. Once we confirm the fraud, we lock these accounts so that no further misuse will occur. To date, we have locked over 97,000 accounts. Additionally, we are collaborating with the Social Security Administration and

other parts of the Administration on a potential legislative change to the practice of routine release of the Death Master File.

- We have developed procedures for handling information about identity theft victims received from law enforcement officials, who discover this information in the course of investigating identity theft schemes or other criminal activity. This data is extremely valuable. It can be used to flag taxpayer accounts and help us block returns filed by identity thieves who attempt to use the personal information of those taxpayers to file a fraudulent return. Our Criminal Investigation (CI) Division will use this data to identify links between criminal schemes, and will share this information when appropriate to ensure that victims' accounts are adjusted and protected from future identity fraud.
- We expanded the use of our list of prisoners to better stop the processing of problematic returns. In FY 2012, we stopped over 220,000 fraudulent returns filed by prisoners. This represents over \$2.5 billion in refunds stopped, a more than 10 percent increase over last fiscal year. The IRS has collaborated with the Bureau of Prisons and states that choose to partner with us to help identify prisoners who may be engaged in tax fraud, and we received additional help in 2011 with the passage of the United States-Korea Free Trade Agreement Implementation Act, which included language requiring federal and state prisons to provide information on the current prison population. Unfortunately, the authority allowing us to share return information with prisons expired at the end of 2011. The Administration's FY 2013 Budget contains a revenue proposal that would reinstate the provision authorizing the IRS to disclose return information with respect to individuals incarcerated in federal or state prisons who we determine may have filed or facilitated the filing of a false return.
- We are collaborating with software developers, banks, and other industries to determine how we can better partner to address identity theft and prevent federal monies from reaching the hands of identity thieves. For example, we established a cooperative agreement with more than 100 financial institutions to reject questionable deposits. The IRS also established relationships with representatives of the prepaid access card industry, which has security protocols designed to detect and prevent fraudulent use of the cards. In many cases, these companies may have the ability to identify potentially fraudulent tax refunds and freeze or cancel the cards. We continue to work with these sectors and will roll out improvements in 2013.

The IRS will continue to strengthen our efforts to catch identity theft and other fraud before erroneous refunds are issued. We will continue refining our filters aimed at detecting and preventing the processing of fraudulent returns, and develop new methodologies as needed. Additionally, we are considering new technologies for authenticating the identities of taxpayers at the time of filing as a future means of precluding tax-related identity theft.

Criminal Investigation Work

The investigative work done by CI is a major component of our efforts to combat tax-related identity theft. CI investigates and detects tax 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 future problems. CI recommends prosecution of refund fraud cases, including cases involving identity theft, to the Department of Justice.

In response to the growing threat that identity theft poses to tax administration, IRS established the Identity Theft Clearinghouse (ITC), a specialized unit within CI that became operational in January 2012, to work on identity theft leads. The ITC receives all refund fraud-related identity theft leads from 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 provide support to ongoing criminal investigations involving identity theft.

Investigations of tax fraud related to identity theft have increased significantly over the past three fiscal years, and the trend is continuing into FY 2013. In FY 2012, CI initiated 898 investigations involving identity theft, which is more than triple the number of investigations in FY 2011. Indictments in identity-theft related cases also increased significantly, totaling 494 in FY 2012, with 223 individuals sentenced and an average time to be served of 48 months. This compares with 165 indictments, 80 individuals sentenced, and a 44-month average sentence in FY 2011. Additionally, the direct investigative time spent by CI on identity theft cases has increased by 129 percent in FY 2012 over FY 2011.

In collaboration with the Department of Justice's Tax Division (DOJ-Tax) and local U.S. Attorneys' offices, the IRS conducted a highly successful coordinated identity theft enforcement sweep during filing season. This nationwide effort targeted 105 people in 23 states and included indictments, arrests, and the execution of search warrants involving the potential theft of thousands of identities. In total, 939 criminal charges were included in 69 indictments related to identity theft. That same week, IRS auditors and investigators conducted numerous compliance visits to money service businesses in a variety of locations across the country to help ensure that these businesses were not facilitating refund fraud and identity theft.

Our collaborative efforts extend to other federal agencies as well. For example, the IRS has worked with the U.S. Postal Inspection Service (Postal) to provide training updates on how to handle refund checks and prepaid access cards diverted as part of Postal's fraud detection process. We also issued updated guidance to other federal law enforcement agencies, including the Secret Service and the Federal Bureau of Investigation, on available methods for returning stolen refund amounts to the Department of the Treasury. We will expand upon these efforts in 2013.

The IRS continues to seek out additional methods to combat the proliferation of tax-related identity theft. In July 2012, the IRS expanded the number of charges that special agents investigate when identity theft matters arise in the context of fraudulent returns. The additional charges include: Forging Endorsements on Treasury Checks; Theft of Public Money; Fraud in Connection with Access Devices; Mail Fraud; and Wire Fraud.

Aiding in the fight against identity theft, in September 2012 DOJ-Tax issued Directive 144, Stolen Identity Refund Fraud (SIRF), to provide federal law enforcement officials with the ability to timely address a subset of identity theft cases. This directive specifically focuses on identity theft in the context of fraudulent tax refunds and provides for streamlined initiation of these investigations and prosecutions. CI subsequently responded by streamlining investigative and review processes to capitalize on these historic changes and will continue to move expeditiously on SIRF investigations.

State and local law enforcement agencies also play a critical role in fighting identity theft. CI regularly collaborates with these agencies, and this effort will only increase in the future. Over the past several years, CI has established or participated in at least 35 task forces and working groups around the country in an effort to leverage the resources and expertise of various law enforcement agencies to address identity theft-related crimes.

As part of this collaborative effort, the IRS is working to assist state and local law enforcement agencies in the efforts they are making to fight identity theft-related refund fraud. One way we have done this is by developing the Identity Theft Victim Disclosure Waiver Process, which was launched in Florida in April 2012. This program provides for the disclosure of federal tax returns and return information associated with the accounts of known and suspected victims of identity theft with the express written consent of those victims. Prior to disclosing any tax information, victims are required to sign a waiver authorizing the release of information to the designated state or local law enforcement official pursuing the investigation. In October 2012, we expanded this program to an additional eight states: Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania and Texas. We will continue to expand this initiative to include other states over time. As of October 31, 2012, the IRS has received over 972 waiver forms from roughly 55 participating law enforcement agencies.

Some of the IRS' recent successes involving identity theft include the following cases in which sentences were handed down over the last several months:

- On October 1, 2012, two North Carolina men were sentenced to a total of 155 months in prison and ordered to pay a total of \$466,153 in restitution for their involvement in an identity theft scheme. The individuals broke into a tax preparation office, stealing over 300 files containing the personal information of tax clients. Using this information, the individuals filed returns in the names of the clients and directed the tax refunds to either debit cards that were mailed to

addresses they controlled or to bank accounts that were opened using fraudulent and unauthorized information.

- On September 21, 2012, an Arizona woman was sentenced to 36 months in prison and ordered to pay \$386,938 in restitution on charges related to her involvement in a conspiracy to commit identity theft. The defendant utilized stolen identities to file 180 tax returns to falsely claim more than \$1,000,000 in tax refunds. The defendant concealed the fraud by filing the tax returns electronically using the unsecured wireless networks of neighbors, directing the refunds to prepaid debit card accounts obtained using false identities, and recruiting friends and associates to receive the prepaid debit cards by mail at various addresses.
- On September 19, 2012, three Alabama defendants were sentenced to 90 months in prison for conspiring to operate a sham tax business, utilizing stolen identities to falsely file over 190 tax returns and directing a total of \$1,458,600 in fraudulent refunds to a bank account they controlled.
- On September 13, 2012, an Alabama woman was sentenced to 64 months in prison and ordered to pay over \$1 million in restitution on several charges, including filing false claims and aggravated identity theft. The defendant and others were involved in filing at least 482 fraudulent tax returns using stolen identities. The returns sought over \$2 million in tax refunds and were filed through a tax preparation business, opened in another individual's name to conceal the defendant's involvement.
- On September 6, 2012, a Pennsylvania woman was sentenced to 68 months in prison and ordered to pay more than \$200,000 in restitution for her involvement in a conspiracy to steal over \$1 million in fraudulent tax refund checks from the United States mail. The defendant and others were involved in stealing identities and then causing false tax returns to be filed with the IRS.
- On September 5, 2012, a Florida man was sentenced to 57 months in prison for orchestrating a scheme in which approximately 486 fraudulent tax returns were filed utilizing compromised police and firefighter identities. The fraudulent returns requested the refunds to be loaded onto various prepaid debit cards, which the defendant would use to make cash withdrawals at various local banks.
- On September 4, 2012, a Florida man was sentenced to 40 months in prison for aggravated identity theft and related charges. The defendant had been involved in stealing identifying information from a medical center. It was estimated that approximately 1,100 photographs of patient records, containing their personal identifying information, were taken illegally by the defendant and sold to other unknown individuals.

- On August 30, 2012, nine individuals in Florida were sentenced to a total of 450 months in prison for their participation in a tax fraud conspiracy that included the preparation and filing of more than 350 false tax returns seeking \$2.4 million in refunds. The conspirators created the returns using taxpayer identification numbers and other personal identifying information stolen from both living and deceased individuals, as well as wholly fictitious information, such as fabricated names of employers and dependents.

ASSISTING TAXPAYERS

Improving our Processes

We realize the importance of resolving cases involving identity theft quickly and efficiently, allowing taxpayers victimized by identity theft to receive their refunds as soon as possible and preventing adverse enforcement actions from being taken against them. To that end, we continue to develop and implement new procedures to improve the service provided to identity theft victims. Despite significant FY 2012 budget decreases across taxpayer service and enforcement programs, we more than doubled the level of staffing resources dedicated to working identity theft cases between FY 2011 and FY 2012. As we enter the 2013 Filing Season, we now have over 3,000 employees working identity theft issues.

During FY 2012, the IRS reengineered our identity theft process to close cases more efficiently and accurately and to find ways to reduce customer burden. As a result, we have made a number of programming and procedural enhancements, enabling us to move faster to identify accounts with a high potential for identity theft. Cases generated as a result are reassigned for review more quickly than in the past. Other procedural enhancements are helping us to reduce delays in releasing refunds to the legitimate filer in cases where duplicate returns are filed.

We are also continually improving the way we track and report on the status of identity theft cases, which we believe will lead to quicker case resolution and provide innocent taxpayers with the most current account information and status of their refunds. Additionally, better tracking and reporting means that we can spot – and correct – any flaws in the system more quickly.

As mentioned above, the IRS is also working proactively to help ensure that identity theft victims do not encounter delays in filing future tax returns. Our establishment and expansion of the use of the IP PIN is an important development in this regard. The IP PIN is a promising innovation that can dramatically reduce the number of taxpayers caught up in delays.

Employee Training

The IRS runs one of the largest phone centers in the world, and we are dedicated to providing quality service with a high degree of accuracy to every taxpayer who contacts us. We realize, however, that taxpayers who contact us with identity theft problems present unique challenges to our telephone representatives, and we are committed to providing our assistors with the information they need to ensure these taxpayers receive quality, courteous service. As part of this effort, we conducted a thorough review in 2011 of the training we provide our employees to make sure that they have the tools they need to respond appropriately to those who have been victimized by identity theft.

As a result of this review, we provided our telephone assistors with updated training this past filing season to ensure they better understand the serious financial problems of identity theft victims and maintain the proper level of sensitivity when speaking with victims. Additionally, we broadened the scope of our training beyond telephone assistors to cover all IRS employees who might interact with identity theft victims. We developed a new training course that includes sensitivity training as well as training on the proper tools and techniques to use when handling identity theft cases. In all, 35,000 IRS employees received this training in preparation for filing season 2012. We have updated and enhanced this training for filing season 2013 and will be delivering it once again to our public contact employees.

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. As part of our outreach efforts, we overhauled and updated the identity protection training provided to tax practitioners at our annual Nationwide Tax Forums in 2011 and again in 2012. These annual events, held in several cities around the country, draw more than 16,000 practitioners, who attend to learn about key tax laws and issues. In addition, we 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 are also working closely with software developers to ensure that instructions regarding the use of an IP PIN are included in their products.

We have a far-reaching communications effort that uses both traditional and social media channels to relay information on identity protection issues. As part of this effort, we have produced new identity theft awareness videos for the IRS YouTube channel in English, Spanish, and American Sign Language, and we distributed identity protection information through IRS Twitter feeds and podcasts. 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 locate this information. We have issued a number of news releases and tax tips to help taxpayers and to highlight our continuing enforcement efforts. We plan to continue this sweeping communication effort in the upcoming filing season and beyond.

CONCLUSION

Mr. Chairman, 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 are victims of this crime. Fighting identity theft will be an ongoing battle for the IRS, and one where we will not let up. Our work here is critical. We cannot be lax either in stopping fraud or in assisting taxpayers who have had their identities stolen. Although we cannot stop all identity theft, our efforts in filing season 2012 provide a solid foundation upon which we will continue to build and improve. We have to act aggressively because we have a responsibility to preserve the public's faith in the essential fairness and integrity of our tax system. I would be happy to answer any questions that you may have.

Mr. PLATTS. Thank you, Ms. Tucker.
General George?

STATEMENT OF THE HONORABLE J. RUSSELL GEORGE

Mr. GEORGE. Thank you, Chairman Platts, Ranking Member Towns, Mr. Diaz-Balart. Thank you for the invitation to provide testimony on our recent work regarding identity theft.

As TIGTA has previously reported, the total impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents. The IRS is not providing effective assistance to taxpayers who report that they have been victims of identity theft. While the IRS is continuing to make changes to its processes to address these weaknesses, there is much work that still needs to be done.

My auditors analyzed tax year 2010 tax returns processed during the 2011 filing season and identified 1.5 million tax returns with tax refund issues totaling in excess of \$5 billion which the IRS did not identify as potentially fraudulent. If not addressed, the IRS could issue approximately \$21 billion in fraudulent tax returns resulting from identity theft over the next five years.

Incidents of identity theft affecting tax administration have continued to rise since calendar year 2011, when the IRS identified more than 1 million incidents of identity theft. As of October, the IRS identified over 1 million incidents thus far this year.

When the identity thief files the fraudulent tax return, the IRS does not yet know that an individual's identity could have been used more than once. Instances of duplicate tax returns cause the greatest burden to the legitimate taxpayers. Once the legitimate taxpayer files a return, the duplicate tax return is identified and the refund is held until the IRS can confirm the taxpayer's identity.

When reviewing returns for 2010, we identified more than 48,000 Social Security Numbers that were used multiple times on potentially fraudulent tax returns. We estimate that more than \$70 million in potentially fraudulent tax returns were paid to identity thieves who filed tax returns before the legitimate taxpayer filed theirs. This is in addition to the \$5.2 billion noted previously, which was related to taxpayers who do not appear to have a filing requirement.

The gaining of access to third-party income and withholding information at the time tax returns are processed is the single most important tool the IRS could use to detect and prevent identity theft resulting from the reporting of false income and withholding. Most of this information is not available until well after the tax return filing season begins.

As we reported both in 2008 and 2012, the IRS is not in compliance with direct deposit regulations that require tax refunds to be deposited to an account only in the name of the individual listed on the tax return. Direct deposit, which includes a debit card, provides thieves the ability to quickly receive fraudulent tax refunds. Of the approximately 1.5 million 2010 returns we identified, 1.2 million, about 82 percent, used direct deposit to obtain tax refunds totaling approximately \$4.5 billion. One bank account received 590 direct deposits totaling over \$900,000.

Our analysis of questionable tax year 2010 tax returns that appear to have been filed by an identity thief found that 2,274 children under the age of 14 had almost \$4 million in refunds issued. In addition, almost 1 million individuals whose income level does not require them to file a tax return had over \$3 billion in refunds issued.

In May of this year we reported that the IRS is not effectively providing assistance to taxpayers who report that they have been victims of identity theft. Identity theft cases can take more than one year to resolve, and communication between the IRS and victims is limited and confusing.

The growth of identity theft presents considerable challenges for tax administration. In fiscal year 2011, the IRS received approximately 438,000 identity theft cases and closed more than 300,000 cases. For fiscal year 2012, it received over 640,000 identity theft cases and closed almost 440,000 of them. As of October of this year, the IRS had over 370,000 identity theft cases in its inventory.

In January 2012, the IRS established a unit to manage identity theft cases during the 2012 filing season. Taxpayers found it difficult to reach employees in this unit. The unit received approximately 200,000 calls during fiscal year 2012, but was only able to answer about 73,000 of them.

In conclusion, the IRS has made some progress in this area; however, we at TIGTA remain concerned over the ever-increasing growth of identity theft and its impact on tax administration.

In closing, Mr. Chairman, Ranking Member Towns, I also want to just express my true appreciation for the cooperation and the attention that you and this Committee have put to this very important issue. You will be missed. Thank you.

[Prepared statement of Mr. George follows:]

**HEARING BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT ORGANIZATION, EFFICIENCY, AND
FINANCIAL MANAGEMENT
U.S. HOUSE OF REPRESENTATIVES**

**“Identity Theft and Tax Fraud: Growing Problems for the
Internal Revenue Service, Part IV”**



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

November 29, 2012

Washington, D.C.

TESTIMONY OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT ORGANIZATION, EFFICIENCY, AND FINANCIAL MANAGEMENT
U.S. HOUSE OF REPRESENTATIVES

"Identity Theft and Tax Fraud: Growing Problems for the
Internal Revenue Service, Part IV"

November 29, 2012

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, thank you for the invitation to provide testimony on the subject of identity theft and its impact on the Internal Revenue Service (IRS) in its function of administering the Nation's tax laws. Since I last testified before this Subcommittee on identity theft and tax fraud in April 2012,¹ my office, the Treasury Inspector General for Tax Administration (TIGTA), has issued two reports² on this subject. The first report, issued May 3, 2012, addressed the IRS's efforts to assist victims of identity theft, while the second, issued July 19, 2012, dealt with the IRS's efforts to find and prevent identity theft. My comments today will focus on those results and on the ongoing work we have underway to assess the IRS's progress on detecting and resolving identity-theft issues related to tax administration.

As we have reported, the total impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents, and the IRS is not providing effective assistance to taxpayers who report that they have been victims of identity theft. Although the IRS is continuing to make changes to its processes to increase its ability to detect, prevent, and track fraudulent tax returns and improve assistance to victims of identity theft, there is much work that still needs to be done.

Incidents of identity theft affecting tax administration have continued to rise since Calendar Year (CY) 2011, when the IRS identified more than one million incidents of identity theft that impacted our Nation's tax system. As of October 27, 2012, the IRS

¹ *Problems at the Internal Revenue Service: Closing the Tax Gap and Preventing Identity Theft*, Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency and Financial Management, 112th Cong. (Apr. 19, 2012) (statement of J. Russell George).

² TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 2012); TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

identified almost 1.2 million incidents during CY 2012. This figure includes approximately 186,000 incidents in which taxpayers contacted the IRS alleging that they were victims of identity theft,³ as well as more than one million incidents where the IRS detected the occurrence of potential identity theft.⁴

Detection and Prevention of Identity Theft

Despite the increased number of identity-theft incidents the IRS has found, the IRS is still challenged in detecting and preventing them. In July 2012, TIGTA reported that the impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents.⁵ Using the characteristics of confirmed identity theft, we analyzed Tax Year (TY) 2010 tax returns processed during the 2011 Filing Season and identified 1.5 million undetected tax returns with potentially fraudulent tax refunds totaling in excess of \$5 billion. If not addressed, we estimate that the IRS could issue approximately \$21 billion in fraudulent tax refunds resulting from identity theft over the next five years.

The primary characteristic shared by tax-related identity-theft cases is that the identity thief reports false income and withholding to generate a fraudulent tax refund. Without the falsely reported income, many of the deductions and/or credits used to inflate the fraudulent tax refund could not be claimed on the tax return. In addition, many individuals who are victims of identity theft may be unaware that their identity has been stolen to file fraudulent tax returns. These individuals are typically those who are not required to file a tax return. It is not until the legitimate individual files a tax return resulting in a duplicate filing under the same name and Social Security Number (SSN) that many individuals realize that they have become victims of identity theft.

When the identity thief files the fraudulent tax return, the IRS does not yet know that an individual's identity will be used more than once. Instances of duplicate tax returns cause the greatest burden to the legitimate taxpayer. Once the legitimate taxpayer files his or her tax return, the duplicate tax return is identified and the refund is held until the IRS can confirm the taxpayer's identity. For TY 2010, we identified more than 48,000 SSNs that were used multiple times, *i.e.*, one or more potentially fraudulent tax returns were associated with the multiple use of the SSN.⁶ We estimate that more

³ Taxpayers can be affected by more than one incident of identity theft. These incidents affected 154,139 taxpayers.

⁴ These incidents affected 804,527 taxpayers.

⁵ TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

⁶ This estimate includes only those tax returns filed on tax accounts that contain an Identity Theft Indicator added on or before December 31, 2011.

than \$70 million in potentially fraudulent tax refunds were paid to identity thieves who filed tax returns before the legitimate taxpayers filed theirs.⁷ This is in addition to the \$5.2 billion noted previously, which was related to taxpayers who do not appear to have a filing requirement.

Although the IRS is working toward finding ways to determine which tax returns are legitimate, it could do more to prevent identity thieves from electronically filing (e-filing) tax returns. Of the 1.5 million tax returns we identified, almost 1.4 million (91 percent) were e-filed. Before a tax return can be submitted electronically, the taxpayer must verify his or her identity with either the prior year's tax return Self-Select Personal Identification Number (PIN) or Adjusted Gross Income. However, we determined that this control can be circumvented.

If the taxpayer does not remember the prior year's Self-Select PIN or Adjusted Gross Income, he or she can go to IRS.gov, the IRS's public Internet website, to obtain an Electronic Filing PIN by providing personal information that the IRS matches against data on the prior year's tax return filed by the taxpayer. In the alternative, a taxpayer can call the IRS and follow automated prompts to receive an Electronic Filing PIN. For the 2013 Filing Season, the IRS plans to require additional personally identifiable information to be provided by the taxpayer. Nonetheless, authenticating taxpayers is a challenge whenever they call or write to the IRS requesting help with their tax account. The IRS has not adopted industry practices of shared secrets to authenticate taxpayers, such as security challenge questions (e.g., mother's maiden name or name of first pet).

Access to third-party income and withholding information at the time tax returns are processed is the single most important tool the IRS could use to detect and prevent identity-theft tax fraud resulting from the reporting of false income and withholding. Third-party reporting information would enable the IRS to identify the income as false and prevent the issuance of a fraudulent tax refund. However, most of this information is not available until well after tax return filing begins.

In addition, another important tool that could immediately help the IRS prevent identity theft-related tax fraud is the National Directory of New Hires.⁸ Legislation is needed to expand the IRS's authority to access the National Directory of New Hires wage information for use in identifying tax fraud. Currently, the IRS's use of this

⁷ This estimate is based only on the duplicate use of the primary SSN.

⁸ A Department of Health and Human Services national database of wage and employment information submitted by Federal agencies and State workforce agencies.

information is limited by law to just those tax returns with a claim for the Earned Income Tax Credit. The IRS included a request for expanded access in its annual budget submissions for Fiscal Years (FY) 2010, 2011, 2012, and has once again included a request in its FY 2013 budget submission.

Even with improved identification of tax returns with false wage and withholding being reported, verifying whether the returns are fraudulent will require resources. Using IRS estimates, it would cost approximately \$32 million to screen and verify the approximately 1.5 million tax returns that we identified as not having third-party information, which indicates that the return information could be false. However, the IRS can maximize the use of its limited resources by reviewing tax returns with the highest risk for refund fraud.

Without the necessary resources, it is unlikely that the IRS will be able to work the entire inventory of potentially fraudulent tax refunds it identifies. The IRS will only select those tax returns that it can verify the identity of the taxpayer and/or the income based on resources while allowing other fraudulent refunds to be issued. The net cost of not providing the necessary resources is substantial, given that the potential revenue loss to the Federal Government of these identity-theft-refund fraud cases is billions of dollars annually.

As we reported in July 2008⁹ and July 2012, the IRS is not in compliance with direct deposit regulations that require tax refunds to be deposited to an account only in the name of the individual listed on the tax return. Direct deposit, which now includes debit cards, provides the ability to quickly receive fraudulent tax refunds without the difficulty of having to negotiate a tax refund paper check. Of the approximately 1.5 million TY 2010 tax returns we identified, 1.2 million (82 percent) used direct deposit to obtain tax refunds totaling approximately \$4.5 billion. One bank account received 590 direct deposits totaling over \$900,000.

To improve the IRS's conformance with direct-deposit regulations and to help minimize fraud, we recommended that the IRS limit the number of tax refunds being sent to the same direct-deposit account. Limiting the number of tax refunds that can be deposited into the same account can minimize losses associated with fraud. While such a limit does not ensure that all direct deposits are in the name of the filer, it does help limit the potential or extent of fraud.

⁹ TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (Sept. 2008).

We also recommended and the IRS agreed to coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that tax refunds issued via direct deposit to either a bank account or a debit card account are made only to an account in the taxpayer's name. The IRS indicated that it will initiate discussions with the Financial Management Service to revisit this issue and reevaluate the feasibility of imposing such restrictions. Based on the discussions with the Financial Management Service, the IRS will determine whether such restrictions can be effectively implemented.

As I mentioned earlier, the IRS has continued to make changes to its processes to increase its ability to detect, prevent, and track fraudulent tax returns and improve assistance to victims of identity theft. During CY 2012, as of September 30, 2012, the IRS reports that it has stopped the issuance of \$9.3 billion in potentially fraudulent tax refunds associated with 1.4 million tax returns classified as involving identity theft. This represents a 49 percent increase in the number of fraudulent tax returns identified over the same period last year.

In addition, the IRS continued to expand its efforts to prevent the payment of fraudulent tax refunds by processing all individual tax returns through identity-theft screening filters. These filters look for known characteristics of identity-theft cases to detect false tax returns before they are processed and before any fraudulent tax refunds are issued. For example, the filters use Social Security benefit and withholding information from the Social Security Administration (SSA). This information is used to ensure that individuals reporting Social Security benefits and related withholding on tax returns received benefits from the SSA at the time the tax return is filed and before tax refunds are issued. Overall, this will help prevent the successful use of false Social Security benefits and withholding to obtain fraudulent refunds. We identified over 93,000 such tax returns in TY 2010 with fraudulent refunds issued totaling over \$230 million. The IRS reports that it identified and confirmed identity theft on over 31,000 tax returns claiming fraudulent Social Security benefits and withholding and stopped approximately \$169 million in fraudulent tax refunds in Processing Year 2012.

Tax returns detected by these new filters are held during processing until the IRS can verify the taxpayers' identity. IRS employees attempt to contact these individuals and request information to verify that the individual filing the tax return is the legitimate taxpayer. If the IRS cannot confirm the filer's identity, it halts processing of the tax return to prevent the issuance of a fraudulent tax refund. During CY 2012, as of September 30, 2012, the filters identified over 218,000 tax returns, stopping the issuance of approximately \$1.5 billion in fraudulent tax refunds.

In January 2012, the IRS created the Identity Theft Clearinghouse in response to a TIGTA recommendation. The Clearinghouse was created to accept refund-related identity-theft leads from IRS Criminal Investigation field offices. The Clearinghouse performs research and develops each lead for the field offices and provides support for ongoing criminal investigations involving identity theft. As of October 25, 2012, the Clearinghouse had received over 2,000 identity-theft leads for development. These leads have resulted in the development of 264 identity-theft investigations.

In April 2012, the IRS launched a pilot program designed to help law enforcement obtain tax-return data vital to their efforts in investigating and prosecuting cases of identity theft. State and local law enforcement officials with evidence of identity theft involving fraudulently filed tax returns are now able, through a disclosure consent from the victim, to obtain tax returns filed using the identity-theft victim's SSN. This program was initially piloted in the State of Florida and has since been expanded to eight additional States.¹⁰ As of September 30, 2012, the IRS has received 788 requests for information from State and local law enforcement.

The IRS is continuing to proactively lock¹¹ tax accounts to prevent the issuance of potentially fraudulent refunds. The IRS began a pilot program in Processing Year 2011, which locked taxpayers' accounts where the IRS Master File and SSA data showed a date of death. The IRS places a unique identity-theft indicator to lock the individual's tax account. This will systemically void tax returns filed on an individual's account if he or she is deceased. During CY 2012, as of September 30, 2012, the IRS had locked over 78,000 tax accounts and prevented approximately \$548,000 in fraudulent tax refunds claimed using deceased individuals' identities. Since the program began, the IRS has locked over 97,000 tax accounts of deceased individuals and has prevented the issuance of approximately \$2.3 million in fraudulent tax refunds.

The IRS has plans to expand its use of the tax account lock in CY 2013 to begin locking the accounts of minor children and taxpayers who do not have filing requirements. The IRS will place the same unique identity-theft indicator on these accounts, which will result in the systematic voiding of the tax return. This action should help to prevent additional identity-theft refund fraud. Our analysis of questionable TY 2010 tax returns that appeared to have been filed by an identity thief showed 2,274 children under the age of 14 had almost \$4 million in refunds issued. In addition, almost

¹⁰ Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania, and Texas.

¹¹ A specific transaction code used to prevent a taxpayer's identification number (TIN), either a Social Security Number or Individual Taxpayer Identification Number, from being used as the primary or secondary TIN on a current or subsequent year Federal income tax return.

one million individuals whose income level does not require them to file a tax return¹² had over \$3 billion in refunds issued.

To measure the success of the actions that the IRS took to combat identity theft in CY 2012, we are currently performing the same analysis we performed for TY 2010 tax returns.¹³ Using the characteristics of confirmed identity theft, we are analyzing TY 2011 tax returns processed during the 2012 Filing Season to determine whether we can identify any undetected tax returns with potentially fraudulent refunds resulting from identity theft.

IRS Assistance to Victims of Identity Theft

In May 2012, we reported that the IRS is not effectively providing assistance to taxpayers who report that they have been victims of identity theft, resulting in increased burden for those victims.¹⁴ Moreover, identity-theft cases can take more than one year to resolve and communication between the IRS and victims is limited and confusing. Victims are also asked multiple times to substantiate their identities. Furthermore, during the 2012 Filing Season, identity-theft tax returns were not prioritized during the standard tax return filing process.

The growth of identity theft presents considerable challenges to tax administration. In FY 2012, the IRS estimated that its inventory of more than 228,000 identity-theft cases that had been carried over from FY 2010 to 2011 would require 287 staff years to resolve.¹⁵ This inventory did not include 500,000 cases that were in the Duplicate Filing inventory,¹⁶ many of which were identity-theft cases.

In FY 2012, the IRS dedicated 400 additional employees to the Accounts Management function¹⁷ to work identity-theft cases. The Accounts Management function now has approximately 2,000 employees working these cases. However, the inventory of identity-theft cases has grown almost 50 percent from FY 2011 to 2012. In

¹² This category contains tax returns filed with income claimed for which there are no supporting income documents that would indicate the legitimate taxpayer was not required to file a tax return.

¹³ TIGTA, Audit No. 201140044, *Effectiveness of the Internal Revenue Service's Efforts to Identify and Prevent Fraudulent Tax Refunds Resulting from Identity Theft* (Follow-Up), report planned for April 2013.

¹⁴ TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 2012).

¹⁵ One staff year is approximately 2,080 hours.

¹⁶ A duplicate tax return condition occurs when a tax return posts to a taxpayer's account that already contains a tax return. The duplicate tax return becomes part of an inventory of duplicate tax return cases that require an IRS employee to work and resolve.

¹⁷ The function that works the majority of identity-theft cases involving individual duplicate tax returns.

FY 2011, the function received approximately 438,000 identity-theft cases and closed more than 300,000 cases. For FY 2012, the function received over 640,000 identity-theft cases and closed almost 440,000 cases. As of October 1, 2012, the Accounts Management function had over 370,000 identity-theft cases in its inventory.

Most identity-theft cases are complex and can present considerable challenges throughout the resolution process. For example, it can be difficult to determine who the legitimate taxpayer is or if the case is actually a case of identity theft. Taxpayers sometimes transpose digits in SSNs, but do not respond to IRS requests for information to resolve the case. As a result, the IRS may not be able to determine who the legitimate taxpayer is. With other cases we have reviewed, taxpayers claimed to be victims of identity theft after the IRS had questioned deductions or credits or proposed examination adjustments. There have been instances in which the SSA has issued to taxpayers the same SSN.

As previously mentioned, resources have not been sufficient to work identity-theft cases dealing with refund fraud and continue to be a concern. IRS employees who work the majority of identity-theft cases are telephone assistors who also respond to taxpayers' calls to the IRS's toll-free telephone lines. TIGTA is concerned that demanding telephone schedules and a large identity-theft inventory make it difficult for assistors to prioritize identity-theft cases. Nevertheless, because of limited resources and the high taxpayer demand for telephone assistance, assistors who work identity-theft cases also work the telephones on Mondays (and any Tuesday following a Monday holiday).

Furthermore, telephone assistors are not examiners and are not trained to conduct examinations, which require skills and tools beyond those possessed by the assistors. Instead, assistors are trained to communicate with taxpayers and know the tax laws and related IRS operational procedures. Identity-theft cases can be complex and often present considerable challenges throughout the resolution process. We recommended that the IRS provide additional training for assistors, to include the importance of documenting case actions and histories.

The IRS responded that it has improved training and provided training to all IRS employees who work identity-theft cases. TIGTA is currently evaluating whether the IRS has provided additional training to the assistors.¹⁸ The IRS is currently testing new

¹⁸ TIGTA, Audit No. 201240041, *Effectiveness of Assistance Provided to Victims of Identity Theft* (Follow-Up), report planned for August 2013.

procedures for processing and working identity-theft cases. Interviews with more than 20 assistors showed that many believed the training was not adequate and that the new procedures are still constantly being revised and updated, which is creating confusion for the assistor and the taxpayer alike.

However, the IRS has implemented new tools and job aids for the assistors to use when attempting to resolve identity-theft cases, including an Identity Theft Case Building Guide and Identity Theft Tracking Indicator Assistant. Some assistors stated that they believe these tools have been helpful when working identity-theft cases.

The management information system that telephone assistors use to control and work cases can add to the taxpayer's burden. For instance, one victim may have multiple cases opened and multiple assistors working his or her identity-theft issue. A review of 17 taxpayers' identity-theft cases showed 58 different cases had been opened and multiple assistors worked their cases. Victims become further frustrated when they are asked numerous times to prove their identities, even though they have previously followed IRS instructions and sent in Identity Theft Affidavits and copies of identification with their tax returns.

The IRS sends the victims duplicate letters at different times, wasting agency resources and possibly confusing the victims. For example, the IRS sends taxpayers two different letters advising them that their identity-theft case is resolved. Assistors working an identity-theft case send a letter to a taxpayer when they have completed actions taken on the case. A second letter is systemically generated two to 12 weeks later advising the taxpayer again that their case has been resolved. Neither letter advises when the taxpayer should expect to receive his or her tax refund.

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

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

Currently, victims are not notified when the IRS receives their tax returns and affidavits reporting suspected identity theft. We recommended that the IRS ensure that taxpayers are notified when the IRS has received their identifying documents and/or it has opened their identity-theft cases. The IRS also needs to analyze the letters sent to taxpayers regarding identity theft to ensure that those letters are relevant, provide sufficient information, and are consistent, clear, and complete.

The IRS agreed with these recommendations and began implementing new procedures to notify taxpayers when their documentation is received. The IRS is also reviewing its suite of identity-theft letters to determine if the information contained therein is accurate and applicable to the taxpayer's identity-theft circumstance. However, these corrective actions are not expected to be fully implemented until September 2013.

Taxpayers could also be further burdened if the address on the tax return filed by the identity thief is false. If the identity thief changes the address on the tax return, the IRS does not know that the address change is inappropriate and will update its account record for the legitimate taxpayer. For example, many taxpayers do not notify the IRS when they move, but just use their new/current address when they file their tax returns. When the IRS processes a tax return with an address different from the one that it has on file, it systemically updates the taxpayer's account with the new address. It does not notify the taxpayer that his or her account has been changed with the new address.

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

This situation can also create disclosure issues. For example, if the legitimate taxpayer's prior-year tax return has been selected for an examination, the examination notice will be sent to the address of record – the address the identity thief used on the fraudulent tax return. The identity-theft victim is now at risk that his or her personal and tax information will be disclosed to an unauthorized third party (whoever resides at that address). In response to our report, the IRS stated that in January 2012, it expanded its identity-theft indicator codes that annotate the taxpayer's account when there is a claim of identity theft. We will be testing the effectiveness of the new identity-indicator codes during our current audits.

The IRS has taken steps in FY 2012 to improve assistance for taxpayers who learn that another taxpayer has filed a tax return using his or her identity. For example, the IRS reorganized to establish an Identity Theft Program Specialized Group within each of the business units and/or functions where dedicated employees work the identity-theft portion of the case. It has also revised processes to shorten the time it takes the IRS to work identity-theft cases and has refined codes to better detect and track identity-theft workloads.

The IRS has updated tax-return processing procedures to include a special processing code that recognizes the presence of identity-theft documentation on a paper-filed tax return. This will allow certain identity-theft victims' tax returns identified during the 2013 Filing Season to be forwarded and assigned to an assistor, rather than continuing through the standard duplicate tax return procedures. This should significantly reduce the time a taxpayer must wait to have his or her identity-theft case resolved.

To further assist victims in the filing of their tax returns, the IRS issues Identity Protection Personal Identification Numbers (IP PIN) to these individuals. The IP PIN will indicate that the taxpayer has previously provided the IRS with information that validates his or her identity and that the IRS is satisfied that the taxpayer is the valid holder of the SSN. Tax returns that are filed on accounts with an IP PIN that has been correctly entered at the time of filing will be processed as the valid tax return using standard processing procedures, including issuing any refunds, if applicable. A new IP PIN will be issued each year before the start of the new filing season, for as long as the taxpayer remains at risk of identity theft. For the 2012 Filing Season, the IRS sent 252,000 individuals an IP PIN. It plans to issue about 500,000 IP PINs for the 2013 Filing Season.

Finally, in January 2012, the IRS established a Taxpayer Protection Unit to manage work arising from the identity-theft indicators and filters used to detect tax returns affected by identity theft – both to stop the identity thief's tax return from being processed and to ensure that the legitimate taxpayer's tax return is processed. During the 2012 Filing Season, taxpayers found it difficult to reach employees in this unit. The unit received approximately 200,000 calls during FY 2012, but was only able to answer about 73,000. The average wait time for taxpayers was 33 minutes. For the 2013 Filing Season, the IRS will direct these telephone calls to its Accounts Management function where about 230 employees have been trained to respond to these calls.

We are currently evaluating whether the IRS is effectively implementing corrective actions to our prior report to improve assistance to victims of identity theft.¹⁹ An initial review of 16 identity-theft cases²⁰ worked by the Accounts Management function shows that for eight of the 16 cases, IRS processes stopped refunds from being issued to the apparent identity thieves. The time it took to process the 16 cases to resolve the identity-theft cases ranged from 47 days to 735 days, or an average of 242 days.

Criminal Investigations of Identity Theft

When the crime of identity theft occurs within TIGTA's jurisdiction, TIGTA's Office of Investigations initiates an investigation. Identity theft not only has a negative impact on the economy but the damage it causes to its victims can be personally, professionally, and financially devastating. When individuals steal identities and file fraudulent tax returns to obtain refunds before the legitimate taxpayers file, the crime is simple tax fraud and falls within the programmatic responsibility of IRS Criminal Investigation. There are, however, other variations of tax-related identity theft that fall within TIGTA's jurisdiction and have a significant impact on taxpayers.

TIGTA focuses its limited investigative resources on investigating identity theft that involves any type of IRS employee involvement, the misuse of client information by tax preparers, or the impersonation of the IRS through phishing schemes²¹ and other means.

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

For example, IRS employee George L. Albright was sentenced on August 15, 2012, to 24-months and one-day of imprisonment, followed by one-year of supervised release, for committing aggravated identity theft and making false claims. Albright was also ordered to pay restitution to his victims in the amount of \$9,669 and a court

¹⁹ TIGTA, Audit No. 201240041, *Effectiveness of Assistance Provided to Victims of Identity Theft* (Follow-Up), report planned for June 2013.

²⁰ Auditors plan to review a statistical sample of 138 identity-theft cases from a population of 78,477 identity-theft accounts with specific identity-theft indicators that were entered by the Accounts Management function accounts for the period of August 1, 2011 through July 31, 2012.

²¹ Phishing is a fraudulent attempt, usually made through e-mail, to steal an individual's personal information.

assessment of \$200. During the course of his employment with the IRS, Albright used his position to access Federal tax records to obtain the names, SSNs, and dates of birth of taxpayers to electronically file nine fraudulent Federal tax returns that were sent to the IRS. He requested refunds on these returns and then directed payments totaling \$10,954 to be electronically deposited into bank accounts that he controlled. Albright ultimately received refunds from eight of the nine fraudulent returns totaling \$9,669.²²

Tax preparers who steal and disclose any taxpayer's Federal tax information as part of an identity-theft scheme cause serious harm to taxpayers. The following case highlights the work of our criminal investigators who investigated a tax preparer who stole the personal identifiers of several individuals and unlawfully disclosed the information to others to fraudulently obtain tax refunds.

Neil Thomsen worked as a tax preparer from January 2002 to June 2008. In 2010, Thomsen used the personal identifiers of other individuals to file false income tax returns and obtain refunds from the IRS. Thomsen had obtained most of the personal identifiers from his prior employment as a tax preparer and from other employment positions he held. He disclosed this information to co-conspirators so they could also file false income tax returns and obtain refunds from the IRS. Thomsen and his co-conspirators ultimately defrauded or attempted to defraud the IRS out of at least \$560,000 in tax refunds.²³

Impersonation of the IRS as part of an identity-theft scheme takes many forms. Criminals involved in these schemes use creative ways to obtain victims' personally identifiable information to commit fraud. Phishing, which usually involves mass solicitation of potential victims through e-mail or other forms of electronic communication, is a widespread method used by criminals to steal another's identity. Often scammers send e-mails claiming to be from the IRS. These phishing e-mails contain a "hook" that induces the victim to take some overt action.

For example, victims may be told that they are due a refund, their tax payment was rejected, or that they owe taxes on lottery winnings and need to click on a link which opens an attachment or directs them to a website where they are prompted to enter their personal identifiers, Federal tax information, and credit card information. Victims also may be told that they are under investigation by the IRS and need to respond immediately by clicking on a link which, again, opens an attachment or directs

²² M.D. Tenn. Judgment filed Aug. 15, 2012; M.D. Tenn. Plea Agr. filed May 18, 2012

²³ S.D. Cal. Superseding Ind. filed June 19, 2012.

them to a website where they are prompted to enter their personal information to verify the status of their tax matter.

The following case is an example of a phishing scheme where several individuals were deceived into divulging their personal identifiers and banking information to identity thieves who then defrauded them of over \$1 million.

Christian Amaukwu was sentenced to a total of 30-months of imprisonment and five-years of supervised release for Aggravated Identity Theft and Conspiracy to Commit Wire Fraud. He was also ordered to pay \$1,741,822 restitution to his victims and a \$200 assessment.

Amaukwu and his co-conspirators operated a scheme to defraud numerous individuals through Internet solicitations, stealing more than \$1 million and the identities of those individuals. Amaukwu and his co-conspirators obtained massive e-mail distribution lists containing thousands of e-mail addresses and sent unsolicited e-mails falsely informing victims that they had won a lottery or had inherited money from a distant relative. Follow-up e-mails instructed the victims to provide personal and bank account information to receive their lottery winnings or inheritance. Subsequent e-mails to victims falsely indicated that a Government or a quasi-governmental agency, such as the IRS or the United Nations, would not pay the money due to them because advance payment of taxes and other fees was required. The e-mails solicited the victims to wire money to pay the taxes and other fees to designated bank accounts controlled by Amaukwu and his co-conspirators.

If the victims were unable to pay the taxes and fees, Amaukwu and his co-conspirators offered to loan them the money. Victims were convinced to open online bank accounts and provide the necessary login information. Using this information, Amaukwu and his co-conspirators stole money from various bank accounts, transferred that stolen money to the victims' accounts, and instructed the victims to wire the money to foreign bank accounts controlled by Amaukwu and his co-conspirators as payment for taxes and other fees on their purported lottery winnings or inheritance. The victims never received any lottery winnings, inheritance, or other money in connection with the scheme.²⁴

While phishing schemes may range in their technical complexity, most share a common trait: They involve computers located outside the United States. Despite the

²⁴ E.D.N.Y. Judgment, filed Aug. 9, 2012; E.D.N.Y. Response to Defendant's Sentencing Letter filed Dec. 19, 2011; E.D.N.Y. Superseding Info. filed May 10, 2011.

significant investigative challenges this poses, TIGTA's Office of Investigations has been successful in working with law enforcement personnel in foreign countries to identify the perpetrators and obtain prosecutions.

Identity thieves may also impersonate IRS employees or misuse the IRS seal to induce unsuspecting taxpayers to disclose their personal identifiers and financial information for the purpose of committing identity theft. The following case is an example of how an IRS employee was impersonated to facilitate a fraud scheme.

Jared Brewton, posing as an IRS "Audit Group Representative," sent letters to various employers demanding that they send him the names, contact information, dates of birth, and SSNs of their employees. He then prepared and filed false Federal tax returns with the IRS in the names of various taxpayers without their knowledge or consent. The tax returns contained W-2 information such as income and withholding that was falsely and fraudulently inflated. As a result, Brewton received fraudulently-procured tax refunds in the names of those taxpayers and used the refunds to purchase personal items. Brewton pled guilty to false impersonation of an officer and employee of the United States; identity theft; subscribing to false and fraudulent U.S. individual income tax returns; and false, fictitious or fraudulent claims.²⁵

In conclusion, the IRS has undertaken important steps and initiatives to prevent the occurrence of identity theft and associated tax fraud. It has made some progress in addressing the rapidly growing challenge of identity theft. Nevertheless, we at TIGTA remain concerned about the ever-increasing growth of identity theft and its impact on tax administration. We plan to provide continuing audit coverage of IRS efforts to prevent tax fraud-related identity theft and provide effective assistance to those taxpayers who have been victimized. In addition, we will continue to conduct criminal investigations of identity-theft violations involving IRS employees, tax return preparers, and individuals impersonating the IRS.

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, thank you for the opportunity to update you on our work on this critical tax administration issue and to share my views.

²⁵ S.D.N.Y. Crim. Indict. filed Jan. 25, 2012.; S.D.N.Y. Minute Entry filed July 11, 2012.

Mr. PLATTS. Thank you, General George. You, in your previous life as a staff director of this Subcommittee with Mr. Horn, set a great model for Mr. Towns and me to follow, so we are honored to have been allowed to kind of carry that torch for the last several years.

Ms. Olson?

STATEMENT OF NINA OLSON

Ms. OLSON. Chairman Platts, Ranking Member Towns, Congressman Diaz-Balart, and members of the Subcommittee, thank you for inviting me to testify at your second hearing this year which I have testified on the subject of tax-related identity theft.

Since 2004, I have written extensively about the impact of identity theft on taxpayers and tax administration, and I have worked closely with the IRS to improve its efforts to assist taxpayers who become identity theft victims. The IRS has adopted many of my office's recommendations and made significant progress in this area in recent years. Notwithstanding these efforts, the IRS continues to struggle to keep up with the increase in identity theft schemes and their evolving nature, and I remain concerned that the IRS is not doing a good enough job of working with and assisting the victims of this crime.

At the end of September, the IRS had nearly 650,000 identity theft cases in its inventory. The IRS did not have a reliable way to track the cycle time of all of its cases yet, but at least one major category of cases had an average cycle time of over six months and the IRS issued instructions to its employees to advise identity theft victims it would generally take about six months to resolve their cases. After I objected and urged the IRS to move more quickly, it rescinded the instruction to provide taxpayers with a six-month case resolution estimate, but it is not clear yet whether the IRS will do substantially better than that time frame.

The impact these delays have on victims is significant. About 80 percent of taxpayers each year are due a refund, and the average refund amount is about \$3,000. While an identity theft case is pending, the victim generally does not receive the refund. Particularly for low income taxpayers, for whom the refund may constitute 25 percent or more of their annual income, this delay imposes an enormous hardship. In addition, once a taxpayer's Social Security Number has been compromised, the taxpayer is at much greater risk of becoming a victim in future years.

The IRS has implemented measures to protect victims in future years by issuing them a Personal Identification Number that they may use in filing their returns, but with a six month cycle time to resolve cases, many victims will go into the following filing season with their cases unresolved and, therefore, be at greater risk of being victimized again, or at least having their refund held up a second time.

Even when the IRS closes a case, because the IRS looks at each year and each issue one at a time, victims find themselves dealing with the IRS year after year, through no fault of their own, just to resolve collection and audit issues caused by identity theft. In fact, more than 20 functional areas of the IRS deal with different

aspects of identity theft, and taxpayers with multiple issues have often had to deal with multiple functions.

I have repeatedly urged the IRS to establish a single point of contact for taxpayers to work through, and former Commissioner Shulman committed to that in a hearing before the Senate Finance Committee in April 2008. Specifically, he said in his testimony that a new unit known as the Identity Protection Specialized Unit, or the IPSU, “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. We believe this unit will assist taxpayers whenever the need arises in dealing with identity theft.”

Yet, today the IRS is moving backward, toward a decentralized approach, creating specialized identity theft units within 21 separate functional areas. The specifics of the new procedures are still under development, and if the IRS maintains the IPSU as the single point of contact or traffic cop for all taxpayers, the specialization within each unit could be a net plus.

But if, as seems likely, the IRS reduces the role of the IPSU and directs taxpayers to deal directly with the 21 specialized units, I am deeply concerned we will revert back to where we were in 2008, with large numbers of taxpayers that have cross-functional issues unable to get their problems resolved without multiple contacts, with multiple functions, and that would, in my opinion, be a disaster for the victims.

All this does not paint a pretty picture, but there is good news. The IRS now recognizes that tax-related identity theft is a major threat to tax administration, and the agency’s senior leadership, including Deputy Commissioner Tucker, is making this a priority and is devoting considerable resources to addressing it. Among its achievements, the IRS has made considerable improvements to its identity theft filters to try to identify and stop more identity theft returns before they are processed, and it appears to be having some success.

Mr. Chairman and Ranking Member Towns, I want to thank you for your continuing interest in this issue, and wish you well in your retirement. I pledge to you that I and my office will continue to work with taxpayers and the IRS and this Committee to try to get this problem under control and ensure that victim assistance improvements.

[Prepared statement of Ms. Olson follows:]

Chairman Platts, Ranking Member Towns, and distinguished Members of the Subcommittee:

Thank you for inviting me to testify today about the subject of identity theft-related tax fraud.¹ I have had the opportunity to address the impact of this subject on taxpayers and to tax administration in four other congressional hearings this year.² A month from now, I will submit my 2012 Annual Report to Congress, where I will again discuss identity theft and refund fraud, and describe in detail my continuing concerns with the IRS's approach to victim assistance.

My first of many experiences with identity theft took place when I was the founder and Executive Director of The Community Tax Law Project (CTLP), the first independent nonprofit low income taxpayer clinic in the country.³ CTLP provides *pro bono* legal representation to low income taxpayers throughout Virginia.⁴ In 1993, a legally resident agricultural worker came to CTLP with Internal Revenue Service (IRS) assessments for additional tax purportedly attributable to unreported wages. My client and I spent the next four years proving to the IRS that it was impossible for him to be working and physically present at three different locations at the same instant. Because the identity thieves – several co-workers on a job from years before – continued to work under my client's name and Social Security number (SSN), we had to prove *each year* to the IRS that my client did not earn the unreported income. At that time, the IRS did not have

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 *Identity Theft and Income Tax Preparation Fraud*, Hearing Before the H. Comm. on the Judiciary, Subcomm. on Crime, Terrorism, and Homeland Security, 112th Cong. (June 28, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Identity Theft and Tax Fraud*, Hearing Before the H. Comm. on Ways and Means, Subcomm. on Oversight and Social Security, 112th Cong. (May 8, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Tax Compliance and Tax-Fraud Prevention*, Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency, and Financial Management, 112th Cong. (Apr. 19, 2012) (statement of Nina E. Olson, National Taxpayer Advocate); *Tax Fraud by Identity Theft Part 2: Status, Progress, and Potential Solutions*, Hearing Before the S. Comm. on Finance, Subcomm. on Fiscal Responsibility and Economic Growth, 112th Cong. (Mar. 20, 2012) (statement of Nina E. Olson, National Taxpayer Advocate).

³ See generally Internal Revenue Code (IRC) § 7526. The Low Income Taxpayer Clinic (LITC) program serves individuals whose incomes are below a certain level and require assistance in dealing with the IRS. LITCs are independent from the IRS and most LITCs can provide representation before the IRS or in court on audits, tax collection disputes, and other issues for free or for a nominal fee. IRC § 7526 authorizes the IRS to award matching grants of up to \$100,000 per year to qualifying clinics that represent low income taxpayers involved in controversies with the IRS, or that provide education and outreach on the rights and responsibilities of U.S. taxpayers who speak English as a second language.

⁴ See www.ctlp.org.

any system to flag my client's account and avoid tormenting and burdening him each year.

My experiences as a tax lawyer representing clients in identity theft and other cases have served as a guide in my role as the National Taxpayer Advocate, the "voice of the taxpayer" inside the IRS. The Taxpayer Advocate Service (TAS) is unique in the IRS in that we work our taxpayers' cases from beginning to end. We are also charged, by statute, to make administrative and legislative recommendations to mitigate the problems taxpayers experience with the IRS.⁵ As a result, many TAS employees have developed expertise in identity theft over the years.

To its credit, the IRS has adopted many of my office's recommendations to help victims of identity theft and refund fraud. Certainly, identity theft-related tax fraud is not a problem the IRS can fully solve. But I believe that the IRS can do considerably more to assist victims of identity theft.

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

1. The IRS has made significant improvements in its identity theft procedures over the years, but significant challenges remain.
2. The IRS and TAS continue to see unprecedented levels of identity theft casework.
3. Identity theft cases are quite complex, often involving multiple issues and impacting multiple tax years.
4. With the IRS moving away from a centralized approach to identity-theft victim assistance, more taxpayers may fall through the cracks.
5. Even after determining the legitimate owner of an SSN, the IRS does not promptly update the address on the account in question with the address of the identity theft victim, leaving the victim susceptible to further victimization and increasing the likelihood that the victim will not receive legally significant notices.
6. While the identity protection personal identification number (IP PIN) program provides additional security, it covers only part of the identity theft victim population.
7. TAS works closely with the Criminal Investigation division to ensure that identity theft victims receive the attention and assistance they require.
8. The Social Security Administration should restrict access to the Death Master File.

⁵ See IRC § 7803(c)(2)(A)(iii) & (iv).

I. The IRS Has Made Significant Improvements in Its Identity Theft Procedures Over the Years, but Significant Challenges Remain

When I first started writing about tax-related identity theft in 2004, the IRS literally had no procedures for its employees to follow when taxpayers claimed to be victims of identity theft. Since then, the IRS has established a program office in charge of developing procedures to assist victims of identity theft (now known as the Office of Privacy, Governmental Liaison, and Disclosure, or PGLD). PGLD has adopted many of the recommendations my office has made over the years, some of which I describe below. While the IRS needs to do more, I want to acknowledge the significant progress it has made over the past few years.

Determination of SSN ownership

Just a few years ago, if a taxpayer claimed that another person had used his or her SSN to file a tax return, the IRS would send the case to the Social Security Administration (SSA) to determine the true owner of the SSN, a process that would routinely take two years.⁶ In my 2005 Annual Report, I recommended that the IRS train and empower its employees to make determinations of the true SSN owner without involving the SSA. Today, the IRS not only allows its employees to determine SSN ownership based on documentation, but it uses data mining to speed up the process even more. I view this as a significant advance and applaud the IRS for this change.

"Fencing off" of wages

When someone who is not authorized to work in this country seeks employment, he or she must still generally provide a valid SSN to the employer. Often, the undocumented worker will provide to the employer an SSN belonging to another individual. Because the tax code requires taxpayers to report all income "from whatever source derived," these undocumented workers are required to obtain an individual taxpayer identification number (ITIN) and file a tax return using that number.⁷ The problem is that the wages are reported on a Form W-2 with someone else's SSN. In the past, a mismatch between an ITIN on a tax return and an SSN on a Form W-2 created problems for the unsuspecting owner of the SSN, who would receive a notice from the IRS that he or she underreported income. I have urged the IRS to develop procedures that will protect victims of identity theft from having to spend unnecessary time and effort proving that they did not earn the wages reported under their SSNs.⁸ Today, the IRS has

⁶ See IRM 21.6.2.4.4.2 (Oct. 1, 2012).

⁷ See IRC § 61(a).

⁸ See National Taxpayer Advocate 2005 Annual Report to Congress 185.

procedures to dissociate the wages from the SSN and associate the wages with the ITIN holder's account.⁹

Identity theft affidavit

Initially, the IRS did not have its own identity theft affidavit, and it required victims to complete and submit the Federal Trade Commission (FTC) identity theft affidavit. However, the FTC affidavit contained this statement emblazoned in red ink and capital letters: "DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY." Faced with contradictory instructions from the IRS and FTC, identity theft victims were understandably confused about the purpose and use of the affidavit. In 2007, I recommended that the IRS create its own identity theft affidavit.¹⁰ The IRS has now developed its own ID theft affidavit (Form 14039), which the victim signs under penalty of perjury.

Standardized documentation requirements

An identity theft case frequently involves more than one IRS function. In the past, identity theft victims were required to present different sets of documents to establish their identity with a particular IRS function. It was a burdensome requirement for identity theft victims, who would often correspond with multiple IRS functions during the course of their case resolution. In 2005, I recommended that the IRS establish standardized documentation requirements for taxpayers to substantiate their claim of identity theft and for taxpayers to provide this documentation just once.¹¹ In 2007, the IRS adopted this recommendation, and procedures are now detailed in the Internal Revenue Manual.¹²

Electronic indicator

In my 2005 Annual Report, I recommended that the IRS consider using an electronic indicator on its master files to mark the accounts of taxpayers who have verified that they have been victims of identity theft. Such an indicator would alert IRS personnel in other departments that this taxpayer might have special needs based on the circumstances and relieve the taxpayer of the burden of proving again that he or she was a victim of identity theft. Use of an indicator would also raise awareness that this taxpayer may have identity theft-related issues in future filing seasons. Today, the IRS uses a transaction code to mark the accounts of taxpayers who have established that they are victims of identity theft. Such an indicator not only enables the IRS to protect the victims' accounts from future identity theft, but it also allows the IRS to track the number of identity theft cases and the amount of time it takes to close them.

⁹ See IRM 4.19.3.15.1.3, *Withholding and ITIN Filers* (Oct. 2, 2012).

¹⁰ See National Taxpayer Advocate 2007 Annual Report to Congress 115.

¹¹ See National Taxpayer Advocate 2005 Annual Report to Congress 185.

¹² See IRM 10.5.3.2.7 (July 9, 2012).

Centralized ID theft unit

In 2007, I recommended that the IRS develop a dedicated, centralized unit to handle all identity theft cases. In 2008, the IRS established the Identity Protection Specialized Unit (IPSU) to assist identity theft victims. As I describe more fully later in this testimony, I have concerns about the limited role of the IPSU. I believe the IPSU should serve as the single point of contact with the identity theft victim and serve as the "traffic cop" to help the taxpayer navigate the various IRS functions that may touch the identity theft case.

Despite these improvements, the IRS still faces significant challenges in handling identity theft cases. The increasing levels of identity theft cases have driven the IRS to move away from a central overseer of this casework, increasing the risk that more taxpayers will fall through the cracks or come to TAS for help. The IRS still does not provide adequate taxpayer service to victims of identity theft, waiting too long to update the address of the legitimate owner of the SSN, and unnecessarily increasing the risk of continued harm to the victim and revenue loss to the government. The federal government, through the release of the Death Master File, still makes available to the public at large, including identity thieves, taxpayers' personally identifying information.

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

As I have written in my Annual Reports to Congress since 2004, 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.¹³ In general, tax-related identity theft occurs when an individual intentionally uses the SSN of another person to file a false tax return with the intention of obtaining an unauthorized refund.¹⁴ Identity theft wreaks havoc on our tax system in many ways. Victims not only must deal with the aftermath of an emotionally draining crime, but may also have to deal with the IRS for

¹³ 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*).

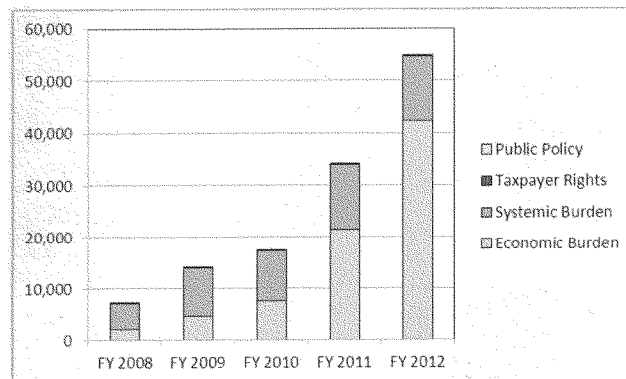
¹⁴ We refer to this type of tax-related identity theft as "refund-related" identity theft. In "employment-related" identity theft, an individual files a tax return reporting his actual wages using his or her own taxpayer identifying number (usually an Individual Taxpayer Identification Number or ITIN), but uses another individual's SSN in order to obtain employment, and consequently, the wages are reported to the IRS under the SSN. Unlike in 1993, when I first represented a client in an identity theft case, the IRS now has procedures in place to minimize the tax administration impact to the victim in these employment-related identity theft situations. Accordingly, I will focus on refund-related identity theft in this testimony.

years to untangle the resulting tax account problems. Identity theft also impacts the public fisc, as Treasury funds are diverted to pay out improper refunds claimed by opportunistic perpetrators. In addition, identity theft takes a significant toll on the IRS, tying up limited resources that could otherwise go toward improving taxpayer service or compliance initiatives.

Today, identity theft can be an organized, large-scale criminal operation. The most recent IRS data show nearly 650,000 identity theft cases in inventory servicerwide.¹⁵ I would love to be able to report on the upward trend of identity theft cases IRS-wide from the past several years, but the IRS does not have this data. Until this year, the IRS had no ability to track identity theft case inventory, much less monitor the time it takes to resolve such cases.

I firmly believe that the failure of the IRS to take prompt action on my office's recommendations in the early years – when the volume of identity theft cases was relatively modest – has led to the crisis we have today. When established IRS procedures do not work as intended, taxpayers turn to the Taxpayer Advocate Service for assistance. The volume of identity theft cases in TAS has risen each year since the IRS established the IPSU, from about 7,100 in FY 2008 to nearly 55,000 in FY 2012, an increase of more than 650 percent.¹⁶

FIGURE 1, TAS Stolen Identity Case Receipts, FY 2008 to FY 2012¹⁷



¹⁵ IRS, Identity Theft Advisory Council, *Identity Theft Status Update* (Oct. 24, 2012). As of September 30, 2012, there were 646,950 identity theft cases servicerwide.

¹⁶ Data obtained from TAMIS on Oct. 16, 2012. TAS received 7,147 identity theft cases in FY 2008, compared to 54,748 in FY 2012, a 666.0 percent increase.

¹⁷ Data obtained from TAMIS on Oct. 16, 2012. TAS received 54,748 identity theft cases in FY 2012, out of 219,666 cases overall (24.9 percent).

In FY 2012, identity theft cases constituted 25 percent of TAS's receipts, more than any other issue in our inventory. Moreover, identity theft has been the top issue in TAS case receipts for the last two fiscal years.

III. Identity Theft Cases Are Quite Complex, Often Involving Multiple Issues and Impacting Multiple Tax Years

When TAS case advocates receive a case, they assign Primary and (one or more) Secondary Issue Codes to the case, indicating what issues are involved and, by inference, what other IRS functions TAS must work with to resolve all the tax issues completely before closing the case. The vast majority of TAS identity theft cases encompass multiple issues and tax years, as shown in the table below.

FIGURE 2, FY 2012 TAS Identity Theft Closures by Secondary Issue¹⁸

Top Ten Secondary Issues	Closed Cases	Avg. Case Age (Days)
Unspecified ¹⁹	13,306	95
020 - Expedite Refund Requests	9,216	98
310 - Processing Original Returns	5,582	109
045 - Pre-Refund Wage Verify Hold	5,529	86
315 - Unpostable/Reject	3,190	74
330 - Processing Amended Returns	1,046	112
090 - Other Refund Inquiries	974	115
040 - Returned/Stopped Refunds	848	92
410 - Multiple/Mixed TIN	813	132
060 - IRS Offset	669	139
670 - Closed Automated Underreporter	603	133
All Other Secondary Issues	4,846	132
Total	46,622	101

Each case that comes in to TAS is assigned to a case advocate, who identifies potential related issues and keeps the case open until all related issues are resolved. For example, if a taxpayer has a problem with an unpostable return, TAS would need to interact with the Submission Processing function. If the case issues relate to wage or withholding verification, TAS would coordinate with the Accounts Management Taxpayer Assurance Program function. With levy or offset issues, TAS may need to

¹⁸ Data obtained from TAMIS on Oct. 16, 2012.

¹⁹ Pursuant to TAS guidance, identity theft cases, by definition, have at least one secondary issue. However, a portion of TAS identity theft cases did not specify a secondary issue code, which is an error.

deal with the Collection function. Any given case could involve several tax years with any combination of these issues.

In contrast, the vast majority of the IRS's identity theft cases are being worked by Accounts Management (AM). AM does not look back at the taxpayer's filing history to conduct a global account review and address all related issues, but focuses on the issue before it. I believe that because the IRS does not take the holistic approach to case resolution that TAS employs, the IRS vastly underestimates the complexity of the typical identity theft case. I am concerned that the IRS is making strategic decisions based on a distorted view of how difficult it can be to fully unwind an identity theft case.

IV. With the IRS Moving Away from a Centralized Approach to Identity Theft Victim Assistance, More Taxpayers May Fall Through the Cracks

In former Commissioner Shulman's first month in office in 2008, he testified before the Senate Finance Committee on identity theft. At this hearing and through his responses to follow-up questions, the Commissioner described his vision for addressing the issue. In describing the IPSU, the Commissioner 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.... We have found that over time, identity theft cases can be handled by approximately 24 functional areas of the IRS, including customer service, tax return processing, and compliance, and we believe this unit will assist taxpayers whenever the need arises in dealing with identity theft.²⁰

The National Taxpayer Advocate generally agrees with the approach outlined by the Commissioner in 2008 – a single point of contact, seamless assistance, and prompt resolution. However, it is clear that the promises made by the Commissioner are not being fulfilled. Not only has the IRS failed to achieve the goals expressed by the Commissioner in 2008, but it is moving backward. The IRS is heading toward a *decentralized* approach to aiding identity theft victims, who are unlikely to describe the assistance they receive as “quick” or “efficient.” In short, it is replacing the 24 units the Commissioner identified as a problem in 2008 with 21 units today – a far cry from the single point of contact envisioned by the Commissioner.

In 2011, the IRS convened a task force to evaluate its victim assistance strategy. In the view of many participants, the external consulting firm leading this task force came in with the pre-conceived notion that the IRS should move away from centralized victim assistance and toward a specialized approach. It was based on a recommendation from this task force that the IRS leadership decided to create a specialized unit within each of its 21

²⁰ See *Identity Theft in Tax Administration*, Hearing Before the Senate Committee on Finance, 110th Cong. (Apr. 10, 2008) (statement of Doug Shulman, IRS Commissioner).

individual departments (or functions) to work on identity theft cases.²¹ Under this approach, identity theft cases would be assigned to specially trained employees in each function. If an identity theft case involves multiple issues, the case may be transferred to a specialized unit in a different function to address the additional issue(s).²²

The IRS maintains that transfers will be the exception rather than the rule, but based upon TAS's experience with identity theft cases over the years, it is foreseeable that transfers between functions will become commonplace. Since the IRS does not track all issues raised in an identity theft case and instead takes a piecemeal approach to victim assistance, and because no one employee has been responsible for all aspects of the case, the IRS has no data on the complexity of the cases. Thus, the IRS is designing its procedures based on flawed assumptions.

In 2012, each function was asked to develop procedures for its embedded identity theft unit. PGLD has been compiling and reviewing such procedures to ensure some level of consistency. Although TAS asked to review these procedures – and the procedures for when a taxpayer's case should be moved from one embedded unit to another – before these embedded units became operational in October 2012, we were not afforded this opportunity in all instances. At least three of these embedded specialized units began work without having their procedures reviewed by TAS.²³

I agree that, when properly designed, specialized units within various IRS functions staffed with employees who are familiar and skilled with identity theft issues should improve the speed and quality of identity theft case handling. However, I also firmly believe that the IRS needs a centralized body (such as the IPSU) to serve as the "traffic cop." As noted earlier, identity theft cases are often complex, requiring adjustments by multiple IRS departments.²⁴ Without a case coordinator, the risk that cases requiring involvement from multiple functions will get "stuck" or fall through the cracks is high. The IPSU has already been serving in this capacity for four years. Under the new, specialized approach to identity theft victim assistance, it is unclear what the role of the IPSU will be. In my view,

²¹ IRS, *Identity Theft Assessment and Action Group (ITAAG) Future State Vision and Supporting Recommendations* 44 (Oct. 11, 2011).

²² To transfer a case to another unit, the function must submit a transfer request to the office of Privacy, Governmental Liaison, and Disclosure, which is currently developing a transfer matrix to facilitate such transfer requests.

²³ Two centralized compliance teams were created to complete the identity theft post-function adjustment work; Examination no longer refers identity theft post-function adjustment work to Accounts Management. All Large Business & International (LB&I) and Small Business/Self-Employed (SB/SE) compliance referrals will be routed to the Designated Identity Theft Adjustment (DITA) team located in Philadelphia. All Wage and Investment (W&I) referrals will be routed to the Compliance Post Adjustment Teams (CPAT) located in Austin and Fresno. The CPAT and DITA units stood up in April 2012, but TAS did not receive procedures until October 2012. Submission Processing's embedded unit became operational in October 2012, without first sharing its procedures with TAS.

²⁴ An IRS task force found that up to 28 different functions may touch an identity theft case. IRS, *Identity Theft Assessment and Action Group (ITAAG) Future State Vision and Supporting Recommendations* 7 (Oct. 11, 2011).

the IPSU should remain the single point of contact for victims, tracking each case from start to finish as it moves from one specialized unit to another. Each function should have a liaison and service level agreement with the IPSU and be held accountable for meeting established deadlines for taking actions.²⁵

In addition, the IPSU should continue to serve an important role in this process by conducting a global account review on all identity theft cases. To provide the best service, the IPSU should conduct two global account reviews – an initial one to identify all related issues prior to transferring the case to the appropriate specialized units, and a final global review to ensure that all issues have been resolved prior to closing any identity theft case. Despite its “specialized” moniker, the IPSU should actually operate as a hub in a centralized environment to ensure a “seamless” experience for the victim.²⁶

V. Even After Determining the Legitimate Owner of an SSN, the IRS Does Not Promptly Update the Address on the Account in Question with the Address of the Identity Theft Victim, Leaving the Victim Susceptible to Further Victimization and Increasing the Likelihood That the Victim Will Not Receive Legally Significant Notices

Identity thieves typically file early in the tax filing season, well in advance of the true owner of the SSN. The IRS often has no way of knowing that the first return received is from an identity thief. As a result, the IRS will process the return and its systems will automatically update the last known address on the taxpayer’s account with the address provided by the perpetrator. This address becomes the address of record where notices are sent for all open years, including years for which the identity theft has not filed returns.²⁷

When the true owner of the SSN contacts the IRS, he or she will be asked to provide several documents to substantiate his or her identity and address. While the IRS takes this information and corroborates the identity and address of the identity theft victim, it

²⁵ A service level agreement (SLA) outlines the procedures and responsibilities for the processing of casework when the authority to complete certain case actions rests outside of one organization, operating division, or function. The SLA defines roles and responsibilities, and includes procedures for elevating disagreements. TAS established SLAs with each OD/function for the processing of TAS Operations Assistance Requests (OARs). The SLAs identify timeframes for acknowledging and assigning OARs, procedures for handling disagreements over actions requested or timeframes for completing actions.

²⁶ From the outset, the National Taxpayer Advocate has inquired about the role of the IPSU in the new specialized environment. After months of nonresponsiveness, the IRS finally created a team to look at the IPSU and invited TAS to participate. However, the “IPSU re-engineering” team that TAS was invited to join appears to have no real decision-making authority with respect to the IPSU’s interaction with the embedded specialized units.

²⁷ Treas. Reg. § 301.6212–2(a) generally provides that a taxpayer’s last known address is the one that appears on the taxpayer’s most recently filed and properly processed return.

does not update the address on the account until after the case is fully resolved.²⁸ This decision to delay updating the address has a detrimental impact on taxpayer rights, as the identity theft victim may not receive IRS notices with legal significance – such as a statutory notice of deficiency or a collection due process notice.²⁹ The fact that the IRS has had the correct address of the taxpayer from the beginning of the case, yet chooses not to update the address until the close of the case (typically in excess of six months³⁰) illustrates how difficult it is for the IRS to keep taxpayer rights in the forefront.

VI. While the Identity Protection Personal Identification Number (IP PIN) Program Provides Additional Security, It Covers Only Part of the Identity Theft Victim Population

For the 2012 filing season, the IRS introduced a number of identity theft-related process improvements. For example, to provide a greater level of security for taxpayers, the IRS issued identity protection personal identification numbers or IP PINs to about 250,000 victims whose identities and addresses it has verified.³¹ An IP PIN is a unique code that the taxpayer must use, along with his or her taxpayer identification number, to file electronically and bypass certain filters. Letters went out in December 2011, instructing the victims to use the IP PINs to file their 2011 returns. If the taxpayer attempts to e-file without that number, the IRS will not accept the e-filed return and the taxpayer will need to file a paper return, which will delay processing.

For the 2013 filing season, the IRS plans to expand the IP PIN program to more than 500,000 participants. I support expansion to as many verified identity theft victims as possible, provided the IRS can validate their current addresses. In general, the IRS does not issue IP PINs until after the victim's account is fully resolved. I have pushed the IRS to begin protecting the identity theft victim as soon as the SSN owner and address are verified. Tying the IP PINs to the *closing* of the identity theft case unnecessarily delays this protection.

Last month, I expressed concern to the Wage & Investment Division (W&I) management that the nearly 22,000 taxpayers with stolen identity cases in TAS

²⁸ See, e.g., IRM 10.5.3.2.9, *Closing Identity Theft Issues* (July 9, 2012). See also e-mail dated Nov. 14, 2012, from a tax practitioner (alerting me of this harmful IRS practice).

²⁹ Rev. Proc. 2010-16, 2010-19 I.R.B. 664, explaining how the IRS is informed of a change of address, identifies 20 Code sections that require notices and documents to be sent to the taxpayer's last known address, including the IRC § 6212(b) notice of deficiency, the IRC § 6320(a)(2)(C) notice and opportunity for hearing upon filing of notice of lien, and the IRC § 6330(a)(2)(C) notice and opportunity for hearing before levy. If the taxpayer does not respond to a valid statutory notice of deficiency, IRC § 6213(c) requires the IRS to assess the tax. The taxpayer can no longer obtain judicial review without first paying the tax. A taxpayer who does not respond to a valid IRC § 6330 or § 6320 notice loses not only the right to an administrative hearing, but also the right to pre-enforcement judicial review.

³⁰ The IRS monitored tax-related identity theft cases for an average of 196 days.

³¹ The IRS issued 251,568 IP PINs. IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Aug. 23, 2012).

inventory would not receive the benefit of the protections afforded by the IP PIN for the 2013 filing season, which means their accounts would be unprotected from fraudulent filings and they would be forced to file their legitimate returns on paper.³² The W&I Accounts Management unit shared this concern and worked quickly with TAS to develop a work-around solution. For identity theft cases that have been through the Electronic Fraud Detection System, the IRS will place one indicator on the account to signify the true SSN owner and a different indicator on the account to signify the non-SSN owner.

While I am pleased to report that these taxpayers will be eligible to receive the IP PIN for use in the 2013 filing season and appreciate AM working with us, I am disappointed that it took a last-minute fire drill to accomplish this result. The IRS had ample opportunity to verify the taxpayer addresses and input a marker making the verified taxpayer eligible to receive an IP PIN. Until the IRS changes its procedures to place the IP PIN marker on accounts upon verification rather than closure, the IRS will continue to waste resources on one-off adjustments and work-arounds.

VII. TAS Works Closely with the Criminal Investigation Division to Ensure Identity Theft Victims Receive the Attention and Assistance They Require

For many perpetrators, tax return fraud may be viewed as a low-risk, high-reward venture. News reports suggest some very organized groups have chosen tax-related identity theft as the crime du jour.³³ Identity theft has become a large-scale operation, with "boiler room" operations involving the theft of massive lists of SSNs. Apparently, there are networks of criminals who not only share stolen personal information, but even present seminars about how to use this information to file bogus returns.³⁴ Such brazen behavior suggests that identity thieves are not worried about criminal prosecution.

I am pleased to report that the IRS's Criminal Investigation division (CI) doubled the number of convictions against identity thieves in FY 2011. CI initiated 276 fraud cases related to identity theft, with 81 convictions – up from 224 investigations and 40 convictions in FY 2010.³⁵ To respond more nimbly to identity theft situations, CI now

³² As of October 16, 2012, there were 21,908 open stolen identity cases in TAS.

³³ 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/>.

³⁴ 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/>.

³⁵ Data obtained from the IRS Criminal Investigation division's research function (Mar. 13, 2012).

has a designated liaison for identity theft in each of its major offices, but more action is required.

My office has worked closely with CI over the last few years to make sure that where CI has identified a scheme and has lists of victims' SSNs, this information is quickly transferred to the civil side of the IRS so the victims are notified and identity theft markers are placed on their accounts. We have coordinated with CI and the Department of Justice on certain cases to ensure victims receive notification and are informed about avenues for assistance at the IRS. Only through detection, prosecution, and victim assistance will we be able to comprehensively address the rise of tax-related identity theft.

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

I am concerned that the federal government continues to facilitate tax-related identity theft by making public the Death Master File (DMF), a list of recently deceased individuals that includes their full name, SSN, date of birth, date of death, and the county, state, and ZIP code of the last address on record.³⁶ The SSA characterizes release of this information as "legally mandated,"³⁷ but the extent to which courts currently would require dissemination of death data under the Freedom of Information Act (FOIA)³⁸ has not been tested. To eliminate uncertainty, I have recommended that Congress pass legislation to clarify that public access to the DMF can and should be limited.³⁹

The public availability of the DMF facilitates tax-related identity theft in a variety of ways. For example, a parent generally is entitled to claim a deceased minor child as a dependent on the tax return that covers the child's year of death. If an identity thief obtains information about the child from the DMF and uses it to claim the dependent on a fraudulent return before the legitimate taxpayer files, the IRS will stop the second (legitimate taxpayer's) return and freeze the refund. The legitimate taxpayer then may face an extended delay in obtaining the refund, potentially causing an economic hardship, and will bear the emotionally laden burden of persuading the IRS that the deceased child was really his or hers.⁴⁰ Legislation could relieve survivors of this burden by simply delaying release of the information for several years.

³⁶ 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).

³⁷ *Social Security and Death Information 1*, Hearing Before H. Comm. on Ways & Means, Subcomm. on Soc. Security (statement of Michael J. Astrue, Commissioner of Social Security) (Feb. 2, 2012).

³⁸ FOIA generally provides that any person has a right to obtain access to certain federal agency records. See 5 U.S.C. § 552.

³⁹ See National Taxpayer Advocate 2011 Annual Report to Congress 519-523 (Legislative Recommendation: *Restrict Access to the Death Master File*).

⁴⁰ The full impact to families is demonstrated by a recent case described by a Low Income Taxpayer Clinic (LITC) to TAS in its interim grant report. A young woman was murdered, leaving her young children

In light of the practical difficulties of passing legislation, however, I also urge the SSA to reevaluate whether it has the legal authority to place limits on the disclosure of DMF information administratively. In the 1980s, the SSA created the DMF, now issued weekly, after an individual filed suit in the U.S. District Court for the District of Columbia seeking certain data fields pursuant to FOIA and the court entered a consent judgment in the case pursuant to an agreement reached by the parties.⁴¹ While the 1980 consent judgment may have seemed reasonable at the time, the factual and legal landscape has changed considerably over the past three decades.

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

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

In general, agencies receiving FOIA requests for personal information must balance (1) the public interest served by release of the requested information against (2) the privacy interests of individuals to whom the information pertains.⁴²

In 1989, the Supreme Court reiterated that the public's FOIA interest lies in learning "what their government is up to."⁴³ The Court continued:

to be raised by their grandmother. The deceased woman was a wage earner and entitled to a sizeable refund for the tax year in which she was murdered. The grandmother sought assistance from the LITC after the daughter's income tax return for that tax year was returned to her by the IRS with a request for Form 56, *Notice Concerning Fiduciary Relationship*. After obtaining an order from Probate Court naming the grandmother as personal representative of the estate, the return was resubmitted. The LITC then discovered that an earlier return had been e-filed by an identity thief using the deceased woman's name and SSN and claiming a refund based on fictitious income. The LITC assisted the grandmother in filing an identity theft affidavit. The case was referred to the IRS's IPSU to which the LITC was required to submit additional evidence of the grandmother's identity and claims. The grandmother finally received her daughter's refund more than a year after the original return was due.

⁴¹ See *Perholtz v. Ross*, Civil Action Nos. 78-2385, 78-2386 (D.D.C. Apr. 11, 1980).

⁴² See, e.g., *Department of Defense v. Federal Labor Relations Authority*, 510 U.S. 487, 497 (1994); *Department of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. 749, 773 (1989). This balancing applies to information described in FOIA Exemption 6, 5 U.S.C. § 552(b)(6) ("personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"), which would encompass files like the DMF. See *Department of State v. Washington Post Co.*, 456 U.S. 595, 599-603 (1982); see also *Judicial Watch, Inc. v. Food & Drug Administration*, 449 F.3d 141, 152 (D.C. Cir. 2006).

⁴³ *Department of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. at 773 (quotation omitted).

Official information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct.⁴⁴

Following the Supreme Court's reasoning, the Court of Appeals for the D.C. Circuit rejected a request for a list of names and addresses of retired or disabled federal employees, concluding that release of the information could "subject the listed annuitants 'to an unwanted barrage of mailings and personal solicitations,'" and that such a "fusillade" was more than a *de minimis* assault on privacy.⁴⁵

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

the death of the subject of personal information does diminish to some extent the privacy interest in that information, though it by no means extinguishes that interest; one's own and one's relations' interests in privacy ordinarily extend beyond one's death.⁴⁶

The courts have reiterated that decedents and their surviving relatives possess privacy rights in numerous cases.⁴⁷ In the decided cases, the privacy interest at issue generally has consisted exclusively of emotional trauma. Where there is tax-related identity theft, the privacy interest is much stronger because there is a financial as well as an emotional impact. For example, a parent who has lost a child to Sudden Infant Death Syndrome and then discovers an identity thief has used the DMF to claim his child as a dependent must not only devote time trying to prove to the IRS that he was the legitimate parent, but he must also deal with the financial burden of having his tax return (and refund) frozen.

⁴⁴ *Id.* See also *National Archives & Records Administration v. Favish*, 541 U.S. 157, 171 (2004) (quotation omitted) ("FOIA is often explained as a means for citizens to know 'what the Government is up to'").

⁴⁵ *National Association of Retired Federal Employees v. Horner*, 879 F.2d 873, 876 (D.C. Cir. 1989) (quotation omitted), *cert. denied*, 494 U.S. 1078 (1990).

⁴⁶ *Schrecker v. Department of Justice*, 254 F.3d 162, 166 (D.C. Cir. 2001) (citations omitted), *reiterated on appeal following remand*, 349 F.3d 657, 661 (D.C. Cir. 2003).

⁴⁷ See, e.g., *National Archives & Records Administration v. Favish*, 541 U.S. at 170 ("FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images."); *Accuracy in Media, Inc. v. National Park Service*, 194 F.3d 120, 123 (D.C. Cir. 1999) (noting that the D.C. Circuit "has squarely rejected the proposition that FOIA's protection of personal privacy ends upon the death of the individual depicted"); *Campbell v. Department of Justice*, 164 F.3d 20, 33 (D.C. Cir. 1998) ("The court must also account for the fact that certain reputational interests and family-related privacy expectations survive death."); *New York Times v. National Aeronautics & Space Administration*, 782 F. Supp. 628 (D.D.C. 1991) (concluding that NASA was not required to release audio tapes of the final minutes aboard the Challenger space shuttle).

Consider two legitimate uses of DMF information. One is by pension funds that use the information to terminate benefits as of the date of a beneficiary's death. The other is by genealogists who use DMF information to help them build a family tree. While both uses are reasonable, neither fits within the core purpose of FOIA of alerting the citizenry about "what their government is up to." The D.C. Circuit has held that where disclosure does not serve the core purpose of FOIA, no public interest exists, and any personal privacy interest, however modest, is sufficient to tip the balance in favor of nondisclosure.⁴⁸ Even if a court were to decide that the DMF does serve a core FOIA purpose, it would balance the public and privacy interests and could easily conclude that the privacy interests predominate.

Thus, if legislation is not forthcoming, I urge the SSA to reconsider its legal analysis and take steps to restrict access to the DMF.⁴⁹

IX. Conclusion

As I have stated, my office is unique in that my case advocates work every case from beginning to end, allowing us to make observations about the complexity of identity theft cases and pinpoint areas where IRS procedures are insufficient to fully resolve the problems. Each year, my office makes numerous recommendations to improve IRS identity theft victim assistance procedures. We have seen the IRS adopt many of our recommendations, often after initially resisting them. I first started focusing on this issue in 2004, when the IRS's identity theft caseload was at a more manageable level. By waiting years to adopt our recommendations, the IRS has put itself in a difficult position today, when the volume of cases is overwhelming. I urge the IRS to take advantage of TAS's vast experience dealing with identity theft cases and work together with TAS in developing its identity theft victim assistance strategy.

That said, identity theft-related tax fraud will continue to pose significant challenges for the IRS, as opportunistic thieves will always try to game the system. From their perspective, the potential rewards of committing tax-related identity theft may be worth the risk. We can do more both to reduce the rewards (by continuing to implement targeted filters) and to increase the risk (by actively pursuing criminal penalties against those who are caught). But in making the tax system less attractive to such criminal activity, we must do our best to avoid imposing additional burdens on legitimate taxpayers.

⁴⁸ *National Association of Retired Federal Employees v. Horner*, 879 F.2d at 879.

⁴⁹ The SSA may be able to restrict access to the DMF without even asking the court to modify its consent judgment in *Perholtz v. Ross*, Civil Action Nos. 78-2385, 78-2386 (D.D.C. Apr. 11, 1980). By its terms, the consent judgment applies only to requests for updated information submitted by Mr. Perholtz himself, is limited to one request per year, and covers only a decedent's "social security number, surname and (as available) date of death." Our understanding is that Mr. Perholtz has not submitted requests for updated information in recent years, that the SSA is now making DMF information available weekly, and that the SSA is making public considerably more information than the three data fields described.

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 perpetrators will get away with refund fraud and some honest taxpayers will suffer harm. If we place a greater value on protecting taxpayers against identity theft and the Treasury against fraudulent refund claims, we may need to make a substantial shift in the way the IRS does business. Specifically, we may need to ask all taxpayers to wait longer to receive their tax refunds, or we may need to increase IRS staffing significantly. Under current circumstances, I have come to the conclusion that it is simply not possible for the IRS both to process legitimate returns rapidly and to combat refund fraud effectively at the same time.

Mr. PLATTS. Thank you, Ms. Olson.
Mr. White?

STATEMENT OF JAMES R. WHITE

Mr. WHITE. Chairman Platts, Ranking Member Towns, and Congressman Diaz-Balart, I am pleased to be here to discuss identity theft-based refund fraud. The problem appears to be growing. IRS reported over 600,000 incidents of identity theft that affected taxpayers in 2012 and another 400,000-plus in one scheme using stolen identities of Puerto Rican citizens.

First some background. Typically, the identity theft takes place outside of IRS and IRS may be unaware of resulting tax fraud attempts until well after they occur. There are two basic types of identity theft tax fraud. One is refund fraud, where the thief files a tax return using the name and Social Security Number of the innocent victim and claims a refund. If successful, money is stolen from the U.S. Treasury.

The other is employment fraud, where the thief uses a stolen ID to obtain a job. The thief's employer reports the wages to IRS and it appears that the innocent victim is under-reporting income. I will focus on refund fraud.

My major point today is that the full extent and nature of identity theft refund fraud is not well understood. This is not a surprise because of the hidden nature of the crime and the continually changing tactics of the thieves. However, without good information on the extent and nature of the fraud, it is hard for IRS to craft a response and congressional oversight is complicated.

Here is some of what IRS does not know.

One, the total number of fraudulent returns. IRS counts the refund fraud attempts it identifies, but does not have an estimate of fraud it failed to detect. Identifying a fraud attempt when the thief files with the name and Social Security Number that match is a challenge. IRS may not know of the fraud until the legitimate taxpayer files and IRS realizes it has two returns with the same name and Social Security Number. However, identifying fraud can be complicated. Some honest taxpayers mistakenly file duplicate returns.

Two, cost of fraudulent returns. IRS counts the amount it recovers from fraudulent returns of all types; it does not label recoveries by specific fraud type. We do know that significant amounts of fraudulent returns of all types are returned to IRS by banks and other entities. Between January and September of 2012, IRS reported that \$754 million was returned.

Three, identity of the thieves. Unless IRS pursues a criminal investigation, it generally does not know the identity of the thief. The only information on the fraudulent tax return is the identity of the innocent victim. Criminal investigation officials at IRS told us they focus their resources on the most egregious identity theft cases. In 2012, they initiated 898 ID theft cases, more than doubling the investigative time spent in 2011. But this is small compared to the number of fraud incidents.

Four, fraud, whether the fraud is part of a broader scheme. Identifying schemes where one thief uses numerous taxpayer identities

depends on IRS analysts noticing patterns that connect cases. As a result, some schemes may go undetected.

Five, characteristics of ID theft returns. IRS officials told us that their current processes limit their ability to systematically track many of the characteristics of ID theft-related returns, such as whether it was paper or electronic, or whether the refund was a check, direct deposit, or debit card.

The dearth of information about the extent and nature of ID theft-related refund fraud highlights the importance of a recommendation we made to IRS in our 2009 report, namely, that IRS measure the effectiveness of its new identity theft initiatives. IRS implemented our recommendation and has since taken a number of actions, including placing new indicators on taxpayers' accounts, giving PIN numbers to past victims, and shifting resources to victim resolution.

This year, IRS took another step to consolidate and track existing information about ID theft tax fraud with its new Identity Theft Global Report. While not a direct attack on the problem itself, the Report is useful. It provides IRS management and others with up-to-date, consistent information. Because it is so new, IRS officials said they are working to improve the Report.

We agree that improvements are possible. Based on a selective assessment that we did before this hearing, we recommended adding additional information about data definition, sources, and limitations. This would give IRS managers and others who use the Report a clearer picture of the current state of the ID theft refund problem and IRS's efforts to combat it.

Despite IRS's efforts, the evidence shows ID theft is growing. Making headway will require continued innovation and strategies to combat the fraud, but such innovation depends on making continued improvements in measuring and assessing the outcome of current strategies.

Mr. Chairman and Ranking Member, this concludes my statement, and I would be pleased to answer any questions. I also want to echo what the other witnesses said about your retirements. I really appreciate, coming from GAO, your willingness to dig into the facts on a very challenging issue.

[Prepared statement of Mr. White follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Government
Organization, Efficiency and Financial
Management, Committee on Oversight and
Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
November 29, 2012

IDENTITY THEFT

Total Extent of Refund Fraud Using Stolen Identities is Unknown

Statement of James R. White, Director
Strategic Issues



GAO-13-132T



Highlights of GAO-13-132T, testimony before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Identity theft is a growing and evolving problem that imposes a financial and emotional toll on its victims. As of September 30, 2012, IRS had identified almost 642,000 incidents of identity theft that impacted tax administration in 2012 alone, a large increase over prior years. A taxpayer may have his or her tax refund delayed if an identity thief files a fraudulent tax return seeking a refund using a legitimate taxpayer's identity information.

GAO was asked to describe identity theft issues at IRS and limits to what is known about the extent of identity theft. GAO updated its analysis on identity theft with current data on identity theft cases and interviewed IRS officials. GAO also reviewed past GAO reports to identify key attributes of successful performance measures and compare information provided by the Global Report.

What GAO Recommends

To improve information available to IRS management and Congress, GAO recommends that IRS update the Global Report to provide definitions and data sources, where such information is missing; document procedures used to compile and validate the data; and describe limitations of the data presented.

IRS officials agreed with our recommendations. Based on their comment, we revised language in the report to clarify that, like other forms of fraud, IRS conducts criminal investigations only in the most serious identity theft-related refund fraud cases.

View GAO-13-132T. For more information, contact James R. White at (202) 512-9110 or whitej@gao.gov.

November 29, 2012

IDENTITY THEFT

Total Extent of Refund Fraud Using Stolen Identities is Unknown

What GAO Found

Understanding the extent and nature of identity theft-related refund fraud is important to crafting a response to it, but Internal Revenue Service (IRS) managers recognize that they do not have a complete picture. Program officials said that one of the challenges they face in combating this type of fraud is its changing nature and how it is concealed. While perfect knowledge about cases and who is committing the crime will never be attained, the better IRS understands the problem, the better it can respond and the better Congress can oversee IRS's efforts. IRS officials described several areas where the extent and nature of identity theft is unknown.

- *Total number and cost of fraudulent returns.* IRS does not know the full extent of the occurrence of identity theft. Officials said that they count the refund fraud cases that IRS identifies but that they do not estimate the number of identity theft cases that go undetected.
- *Identity of the thieves.* Unless IRS pursues a criminal investigation, IRS generally does not know the real identity of the thieves.
- *Whether a fraudulent return is an individual attempt or part of a broader scheme.* Identifying new schemes or significant cases, such as one thief using numerous taxpayer identities, depends on analysts noticing patterns or other indications that a few cases may be part of a larger scheme. As a result, some schemes or cases involving multiple taxpayers may go undetected.
- *Characteristics of known identity theft returns.* IRS officials told us that the agency does not systematically track characteristics of known identity theft returns, including the type of return preparation (e.g., paid preparer or software), whether the return is filed electronically or on paper, or how the individual claimed a refund (e.g., check, direct deposit, or debit card).

While much remains unknown about identity theft, IRS has taken steps to organize what it knows in a newly developed Refund Fraud and Identity Theft Global Report (Global Report). The Global Report consolidates and tracks information about identity theft incidents and IRS detection and resolution efforts from multiple sources within IRS. The report provides information to IRS senior management and a standard source of information for responding to data requests from external entities. GAO's selected review of the Global Report against key attributes of successful performance measures found that it had many of the attributes useful for program monitoring, but also had some areas where additional information or clarification would make the report more helpful. Updating the Global Report to provide information on definitions, data sources, and limitations such as the unknown number of undetected fraudulent returns, could help ensure users have a more complete picture of the data and its strengths and limitations. The quality of the report will also be enhanced by the institution of process controls to help ensure consistency in how the data in the report are compiled, verified and validated.



United States Government Accountability Office
Washington, DC 20548

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee:

I am pleased to be here to discuss the growing problem of identity theft and the Internal Revenue Service's (IRS) efforts to resolve, detect, and prevent identity theft-based refund fraud (identity theft).¹ My testimony today will discuss identity theft issues at IRS and will assess limits to what is known about the extent of identity theft. As discussed at a previous hearing before this committee, identity theft imposes a financial and emotional toll on its victims. A taxpayer may have his or her tax refund delayed if an identity thief files a fraudulent tax return seeking a refund using a legitimate taxpayer's identity information. As of September 30, 2012, IRS had identified almost 642,000 incidents of identity theft that impacted tax administration in 2012 alone, a large increase over prior years. This figure does not include incidents related to the "Operation Mass Mail" scheme in which identity thieves use the stolen identities of Puerto Rican citizens.² As of September 30, 2012, IRS reported around 436,000 incidents occurred in 2012 related to this scheme.

My testimony is based in part on our previous 2009 and 2011 reports.³ Our past work has found that IRS's ability to detect current identity theft incidents is limited and the number of incidents that go undetected is not known. In response to our recommendation that IRS should establish performance measures and collect data suitable for assessing the effectiveness of its identity theft initiatives, IRS agreed and implemented data collection and reporting procedures that help IRS evaluate more completely the effectiveness of its programs and identity opportunities for

¹Taxpayers can also be affected by employment fraud, which occurs when an identity thief uses a taxpayer's name and Social Security number to obtain a job. For additional information on employment fraud see GAO, *Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers*, GAO-11-674T (Washington, D.C.: May 25, 2011).

²IRS officials told us they do not classify Operation Mass Mail incidents as impacting tax administration since the fraudulent return usually does not harm an innocent taxpayer, as most of these cases involve individuals who do not have a filing requirement.

³GAO, *Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers*, GAO-11-721T (Washington, D.C.: June 2, 2011); GAO-11-674T; and *Tax Administration: IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness*, GAO-09-882 (Washington, D.C.: Sept. 8, 2009).

improvement.⁴ However, there continues to be gaps in what IRS knows about the extent of identity theft.

For this testimony we updated our analysis with current data on identity theft cases and interviewed IRS officials in the Wage and Investment Division (W&I); Criminal Investigation (CI); and the Office of Privacy, Government Liaison and Disclosure (PGLD). We also reviewed our past reports to identify key attributes of successful performance measures and compared information provided by IRS's Refund Fraud and Identity Theft Global Report. To determine the reliability of IRS data on identity theft, we discussed data quality-control procedures with agency officials, reviewed relevant documentation, and tested data for obvious errors. We determined that the data were sufficiently reliable for the purposes of this report.

Our prior reports and this November 2012 update were conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We discussed the information in this statement with IRS officials, and they concurred with our findings, conclusions, and recommendations.

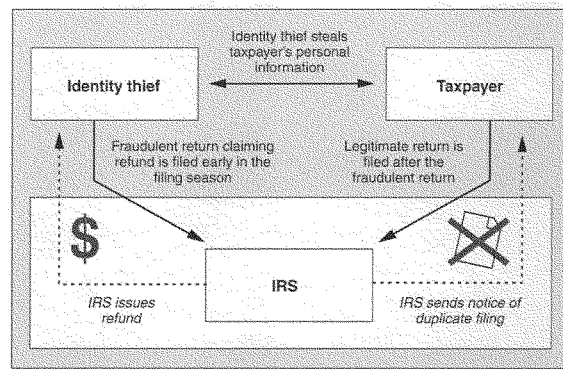
Identity Theft Issues at IRS

Identity thieves can obtain a legitimate taxpayer's name and Social Security number (SSN) in a variety of ways. They can obtain identity information by hacking into a computer system or paper files at one of the many entities that use names and SSNs in their records (e.g., employers, schools, or financial institutions). Thieves can trick the taxpayer into revealing such information, or they can steal it from the taxpayer. Armed with the stolen identity, the thief can then file a fraudulent tax return seeking a refund. The thief typically files a return claiming a refund early in the filing season, before the legitimate taxpayer files. If IRS determines the name and SSN on the tax return appear valid (IRS checks all returns to see if filers' names and SSNs match before issuing refunds) and it passes through IRS's other filters, IRS will issue the refund to the thief.

⁴GAO-09-882.

IRS often becomes aware of a problem after the legitimate taxpayer files a return. At that time, IRS discovers that two returns have been filed using the same name and SSN, as shown in figure 1. The legitimate taxpayer's refund is delayed while IRS spends time determining who is legitimate.

Figure 1: Notional Example of Identity Theft-Based Refund Fraud



Source: GAO.

As we have previously reported, IRS has taken multiple steps to detect, resolve, and prevent identity theft-based refund fraud.⁵ IRS developed new filtering processes in 2012 to detect identity theft based on the characteristics of incoming tax returns that do not rely on a duplicate filing or self-identification by filers. Identity theft indicators—also known as account flags—are a key tool used to resolve and detect identity theft. Identity theft indicators speed resolution by making a taxpayer's identity theft problems visible to all IRS personnel with account access. In some cases, IRS uses its identity theft indicators to screen tax returns filed in the names of known identity theft victims. If a return fails the screening, it is subject to additional IRS manual review, including contacting

⁵GAO-11-721T, GAO-11-674T, and GAO-09-882.

employers to verify that the income reported on the tax return was legitimate.

IRS uses the Identity Protection Personal Identification Number (IP PIN)—a single-use identification number sent to victims of identity theft that have validated their identities with IRS—to prevent refund fraud. When screening returns for possible identity theft, IRS excludes returns with an IP PIN, which helps avoid the possibility of a “false positive” and a delayed tax refund. If a taxpayer was issued an IP PIN and does not use it when filing electronically, IRS rejects the electronically filed return and prompts the taxpayer to file on paper. Taxpayers that do not use an IP PIN or enter an incorrect IP PIN filing on paper experience processing delays as IRS verifies the taxpayers’ identity. As of June 30th, IRS reported providing more than 251,500 IP PINs to taxpayers in 2012 and of those, 150,506 taxpayers filed using an IP PIN. Of filers that filed using an IP PIN, 8.6 percent (12,936) used an invalid IP PIN. IRS officials told us their review of a sample of these cases found that the majority of the invalid IP PINs were due to transposition or keying errors. Details on other IRS actions can be found in our previous reports.

Other steps taken in 2012 include temporarily reallocating hundreds of staff from other business units to resolve duplicate filing cases and issue refunds to legitimate taxpayers. Officials in IRS’s accounts management function told us that in October 2012 there were more than 1,700 staff working to resolve identity theft cases. Also, in April 2012, IRS began the Law Enforcement Assistance Pilot Program in Florida to help state and local law enforcement agencies obtain tax return data vital to local identity theft investigations. The pilot allows taxpayers to give their permission for IRS to provide state and local law enforcement with the returns submitted using their SSN in certain cases. IRS expanded the pilot to eight additional states in October 2012.⁶ As of September 2012, 49 state and local agencies participated in the pilot. We did not independently assess IRS’s 2012 efforts.

⁶As discussed in more detail in our 2009 report, GAO-09-882, IRS has limited authorities to share identity theft information with other federal, state, and local agencies. Tax returns and other information submitted to, and in some cases generated by, IRS are confidential and protected from disclosure, except as specifically authorized by statute. 26 U.S.C. § 6103.

Much Remains Unknown about the Extent and Nature of Identity Theft

The full extent and nature of identity theft-based refund fraud is not known, but IRS data indicate that it is a large and growing problem. The data show that in the first 9 months of 2012, the number of known tax-related identity theft incidents has already more than doubled over 2011 (see table 1).

Table 1: Tax-Related Identity Theft Incidents Identified by IRS, 2008 to 2012

	Incidents
2008	47,730
2009	165,524
2010	147,680 ^a
2011	242,142
2012 ^b	641,690

Source: IRS.

Notes: These figures include incidents affecting tax administration, where (1) a taxpayer identifies the identity theft and substantiates his or her identity with the IRS using documentation or (2) IRS identifies the identity theft. These figures do not include incidents related to the "Operation Mass Mail" scheme. The number of incidents in 2008, 2009, and 2010 differ from what we reported in GAO-11-721T and GAO-11-674T. IRS officials told us they believe the differences in 2008 and 2009 are likely due to indicators that were reversed at a later date. Officials noted that the 2010 data they previously provided erroneously included some Operation Mass Mail incidents.

^aIRS officials told us that the decline in incidents from 2009 to 2010 does not reflect a true decrease in the number of identity theft occurring, and that the decline is likely due to CI transitioning much of its identity theft work to the Accounts Management Taxpayer Assurance Program.

^bThe 2012 data are as of September 2012.

Understanding the extent and nature of identity theft-related refund fraud is important to crafting a response to it. Program officials said that one of the challenges they face in combating this type of fraud is its changing nature. The officials said that when they discover and shut down one vulnerability, thieves often change tactics. The hidden nature of the crime means it is not reasonable to expect perfect knowledge about cases and who is committing the crime. However, the better IRS managers' understanding of the problem, the better they can respond and the better Congress can oversee IRS's efforts.

IRS officials described several areas where the extent and nature of identity theft is unknown.

- *Total number and cost of fraudulent returns.* IRS does not know the full extent of the occurrence of identity theft. Officials said that they count the refund fraud cases that IRS identifies but that they do not estimate the number of identity theft cases that go undetected. IRS officials explained that "we don't know what we don't know," because

if a fraudulent return goes through IRS's identity theft models and other programs, they are unable to tell if they failed to detect the fraudulent return. Officials explained that it is very difficult to detect a fraudulent return when an identity thief uses a correct SSN and has enough identifying information to make the return "look" like it came from the legitimate tax filer. The tax return appears to be legitimate as it has been filed with a name and SSN that match. Detecting identity theft can also be challenging because some legitimate filers mistakenly file duplicate returns. For example, IRS officials told us that in some cases, taxpayers intending to amend their return are confused and file a second Form 1040. In such a case, IRS has to investigate whether the duplicate filing is due to taxpayer confusion or identity theft.

IRS captures data on the amount of money it recovers from all types of fraudulent returns, but it does not distinguish whether the type of fraud was identity theft or some other type of fraud. In some cases, external entities, such as banks or other agencies, may notify IRS of potential refund fraud, including suspected identity theft-based refund fraud. IRS reported it had received information from 116 banks and external leads on more than 193,000 accounts between January 1 and September 30, 2012, for all types of refund fraud. IRS reported that banks and other external entities returned almost \$754 million dollars during this period. These cases are ones where fraudulent returns passed through IRS processes and refunds were issued. W&I officials told us they analyze data from such cases to identify characteristics of the fraudulent returns to improve their screening for identity theft and other types of refund fraud. The officials told us that the procedure for banks to notify IRS of suspected refund fraud is not new, but more financial institutions have now begun doing so.

- *Identity of the thieves.* Unless IRS pursues a criminal investigation, IRS generally does not know the real identity of the thieves. An investigation is necessary because the only identity information IRS has on the fraudulent tax return is that of the identity theft victim, not the thief. Officials responsible for processing returns said that they do not have the sort of information that would be needed to even begin such an investigation.

CI has substantially increased efforts to criminally investigate identity theft cases in fiscal year 2012; however, as with other forms of fraud, CI focuses its investigative resources on the most serious cases. The number of identity theft investigations opened and time spent

investigating identity theft cases have increased from fiscal year 2010 to fiscal year 2012, as shown in table 2. Although identity theft is one of CI's investigative priorities, the number of investigations initiated is substantially less than the number of identity theft incidents confirmed by IRS in 2012. CI officials told us that while other IRS functions share leads with CI, not all of these leads meet CI's criteria for developing a case for prosecution. CI officials told us they generally focus their investigative resources on the most egregious and significant identity theft cases, as measured by volume and refund amounts.

Table 2: Selected Criminal Investigation Statistics for Identity Theft Cases, Fiscal Year 2008 to 2012

	Fiscal year				
	2008	2009	2010	2011	2012
Subject criminal investigations initiated	108	187	224	276	898
Direct investigative time (hours)	130,800	148,900	191,700	225,100	516,400
Direct investigative time (percentage of total)	3%	4%	5%	6%	13%

Source: IRS.

Notes: Fiscal year 2012 data are as of October 2, 2012, and are from the Criminal Investigation Management Information System. Fiscal years 2008 through 2011 data are as of October 4, 2011. We rounded the last two rows of the table.

- *Whether a fraudulent return is an individual attempt or part of a broader scheme.* W&I and CI officials told us the two units work closely to utilize the information they obtain from identity theft cases. They use this information to improve their measures to identify new identity theft-based refund attempts and to identify especially significant or egregious cases to consider for possible criminal investigations. When either W&I's analysis of identity theft cases or CI investigations lead to the identification of new schemes, that information is reported to the Return Integrity and Correspondence Services unit so it can strengthen its identity theft filters. Identifying new schemes or significant cases, such as one identity thief using numerous taxpayer identities, depends on analysts noticing patterns or other indications that a few cases may be part of a larger scheme. As a result, some schemes or cases involving multiple taxpayers may go undetected.

-
- *Characteristics of known identity theft returns.* IRS officials told us that the agency does not systematically track characteristics of known identity theft returns, including the type of return preparation (e.g. paid preparer or software), whether the return is filed electronically or on paper, or how the individual claimed a refund (e.g. check, direct deposit, or debit card). They added that the form in which a refund is claimed would be particularly hard to track using the current processes. Officials noted that they can identify the Internet protocol address of computers used to electronically file returns, which is helpful in detecting potential identity theft.

While much remains unknown about identity theft, IRS has taken steps to collect program data on its identity theft detection and resolution efforts. IRS developed the internal Refund Fraud and Identity Theft Global Report (Global Report) in July 2012 to consolidate and track existing information about identity theft incidents from multiple sources within IRS. IRS officials said that the information in the report is not new, but that they saw the need for consistency in identity theft-related information drawn from several data sources. The report is used to provide information to IRS senior management and the Identity Theft Advisory Council⁷ on identity theft metrics and to provide a standard source of information for responding to data requests from external entities, according to PGLD officials.

Officials also stated that because the Global Report is new, they are working to improve its quality. In a selective review of the Global Report, we found that it had many of the attributes we have previously found to be useful for program monitoring.⁸ For example, the report covers key program activities and generally provides names, definitions, and data sources. However, we also found some areas where additional

⁷The Identity Theft Advisory Council is part of the governance process to address IRS's service-wide identity theft efforts and is made up of representatives from various IRS functions. The primary objectives of the Identity Theft Advisory Council are to promote a collaborative vehicle for addressing and overseeing enterprise-wide identity theft matters and to monitor and report on the status of related identity theft initiatives.

⁸GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143 (Washington, D.C., Nov. 22, 2002) identifies linkage, clarity, measurable targets, objectivity, reliability, core program activities, limited overlap, and government-wide priorities as key attributes of successful performance measures. Because of the limited time to conduct our analysis for this testimony, we focused on only a few of these attributes that were relevant to the Global Report.

information or clarification of information currently in the report could make it more useful, as explained in table 3.

Table 3: Overview of Our Selective Assessment of the Global Report Program Data

Attribute	Definition	Potentially adverse consequences of not meeting attribute	GAO assessment
Core program activities	Measures cover the activities that an entity is expected to perform to support the intent of the program.	Not enough information available in core program areas to managers and stakeholders.	Performance metrics provided in the Global Report cover key efforts used by IRS to resolve, detect, and prevent identity theft. These include identity theft filters used to screen tax returns, the IP PIN program, leads provided by banks, CI investigations, and the Law Enforcement Assistance Pilot Program. The Global Report also provides information on how many days identity theft cases remain open, on average. However, some key data are not included, such as the known amount of funds distributed to identity thieves.
Clarity	Measure is clearly stated and the name and definition are consistent with the methodology used to calculate it.	Data could be confusing and misleading to users.	IRS generally provides names, definitions, data sources, and the frequency of data updates in the Global Report; however, it does not include such information for all data elements. For example, the Global Report does not define its level of service measurement, a measure that reflects the success rate of taxpayers who call the toll-free lines seeking assistance. Also, the Global Report's data dictionary does not list any known limitations in the data, such as the unknown number of fraudulent returns that went undetected. IRS officials noted that they are working to include additional information in future report iterations.
Reliability ^a	Measure produces the same result under similar conditions.	Reported performance data is inconsistent and adds uncertainty.	PGLD officials reported they manually key in data they receive from other IRS offices into the report. Because the report is new, PGLD staff found inconsistencies in the report. They are reviewing the report to improve the report's accuracy and ensure figures are not double counted. Officials told us they are developing documentation on how they collect and verify data. They are also planning on automating the report so that it will no longer require manual compilation. Developing process controls—such as documentation of procedures used to compile, verify, and validate the data—could reduce the risk that significant data mistakes occur. ^b

Source: GAO analysis.

Notes: We selected three key attributes discussed in GAO-03-143 that were relevant to the Global Report. All attributes are not equal and failure to have a particular attribute does not necessarily indicate that there is a weakness in that area or that the measure is not useful; rather, it may indicate an opportunity for further refinement.

^aWe did not perform a full assessment of the reliability of all data presented in the Global Report. We limited our data reliability assessment to data presented earlier in our report and found it sufficiently reliable for describing the number of identity theft incidents IRS detected.

^bVerification is the process of checking or testing performance information to assess types of errors, such as errors in keying data. Validation is an effort to ensure that data are free of systematic error or bias and that what is intended to be measured is actually measured.

The Global Report is a useful step towards providing IRS management and other entities with up-to-date, consistent information about identity theft-based refund fraud and IRS efforts to address it. However, it could be improved with the inclusion of additional information about data limitations, definitions, data sources, and the frequency of data updates in some areas. With such additional information, IRS management or other entities that use the report would have a clearer picture of not only what is known about identity theft-based refund fraud, but the strengths and limitations of the available information. The quality of the report will also be enhanced by the institution of process controls to help ensure consistency in how the data in the report are compiled, verified, and validated.

Conclusions

Identity theft-related tax fraud is a terrible problem for the victims and a growing problem for tax administration. For this reason, legislators, government officials, and the public want to know about IRS efforts to address identity theft. The nature of identity theft-related tax fraud means that it will be very difficult, if not impossible, to develop a complete picture of the extent and nature of the problem, which in turn makes it difficult to assess IRS's progress in combating it. While not a direct attack on the problem itself, IRS's new Global Report could be a useful management tool. It is a recognition of the fact that IRS is devoting significant resources to the identity theft problem and that consolidated and more consistent program information could assist in management oversight and decision making. In reading the report, we identified some improvements that could help users better understand the information provided.

Recommendations for Executive Action

To improve the identity theft information available to IRS management and Congress, we recommend that the Acting Commissioner of Internal Revenue update the Refund Fraud and Identity Theft Global Report to:

- provide definitions, data sources, and the frequency of data updates for data elements where such information is missing;
- document procedures used to compile and validate data; and
- describe limitations of the data presented.

Agency Comments and Our Evaluation

IRS officials provided oral comments in response to our draft findings, conclusions, and recommendations. The Director of PGLD stated that she agreed with our recommendations and plans on implementing our recommendations to improve the information provided in the Global Report. The Director of CI, Refund Crimes said that the discussion of CI's investigation of identity theft could be interpreted to suggest that CI is expected to work every case of identity theft. We revised language in the report to emphasize that, like other forms of fraud, CI focuses its identity theft-related refund fraud investigations on the most serious cases.

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

Contacts and Acknowledgements

For further information on this testimony, please contact James R. White at (202) 512-9110 or whitej@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. In addition to the individual named above, David Lewis, Assistant Director; Shannon Finnegan, Analyst-in-Charge; Michele Fejfar; Sarah McGrath; Donna Miller; Amy Radovich; and Sabrina Streagle made key contributions to this report.

Mr. PLATTS. Well, thank you, Mr. White. And I know from Mr. Towns and all of us concerned about this issue, while we are leaving office, the two of us, we know that you and your colleagues in your various agencies and offices will continue to stay on top of this issue and make improvements in the coming year.

I am going to yield myself five minutes for questions. I have a good number of issues I want to address, but maybe starting with a specific issue relating to the filters. I know we are not going to talk about it in detail here as part of a public hearing because we don't want to let the bad guys know what we are looking for so that they can then try to get around that.

I want, Ms. Tucker, to allow you to address some of the comments that were made, starting with the issue of bank accounts. It is my understanding that the IRS is not in compliance today of only making deposits into bank accounts with the same name. In the testimony we heard today with General George, he referenced one bank account receiving 590 direct deposits totaling over \$900,000. So I guess first is, are we still not in full compliance with only making direct deposits into accounts with the same name? And are the filters that are new going to be helping to target this type of issue?

Ms. TUCKER. Let me start by maybe talking about some of the enhancements in the filters, and then we will get onto the direct deposit issue.

So I think, the numbers that I alluded to earlier and my colleagues on the panel have talked about, IRS and the actions we have taken have shown progress in being able to detect identity theft and prevent bad refunds from going out, so the numbers speak for themselves in that we have stopped \$20 billion in refund fraud this year, as compared to 14 last year. And then specific to these new identity theft filters that we put into play this last filing season, and these are filters specific to identity theft, there was approximately 480,000 returns that were blocked and connected to that \$1.5 billion in refund fraud.

These filters, as we talked about, are constantly being revised to help us focus on different characteristics to different geographic locations where we are seeing spikes in identity theft, etcetera.

The other issue as it relates to deposit of refunds, and as my colleague, Mr. George, will say, we don't necessarily always agree 100 percent on all of our interactions. The direct deposit issue is complicated from the standpoint that a taxpayer that has a legitimate power of attorney can ask IRS to deposit their refund to the account of their legitimate power of attorney, and I think Mr. George would agree with that.

The other thing, obviously, too, is a lot of times you could have a dependent child who is filing a legitimate tax return that perhaps does not have their own bank account. Also, we believe that that is a legitimate deposit.

Now, that said, this coming filing season we do have what we believe is a very important progress to report in this area that I think Mr. George would agree with, and one of the filters we will be using will flag accounts where a deposit is going to a duplicate account. So, for example, the first return comes in and the deposit goes to X bank account. Subsequent returns that are filed that

show a refund going to that account will be flagged for us to take a look at.

Mr. Chairman, as you and I have talked about a little bit, this gets into the balancing act too, because we do know that there are situations where it is a legitimate refund going into that account again, so the balance is going to be how we quickly analyze that and then don't keep that refund from not getting to the legitimate person timely.

Mr. PLATTS. Certainly understanding that balance of timely refunds, but when we have cases where 590, obviously the system has not been working. Those examples that you gave, where there is a power of attorney, is it correct to say technically speaking the law would not allow that deposit because the name is not the same on the account?

Ms. TUCKER. No. I will defer to Mr. George. I believe that it would because we do have the power of attorney and the taxpayer saying that they would allow that to go to the other account.

Mr. PLATTS. And as maybe also relates to that child. Not that it shouldn't, but my point would be that it is an extenuating circumstance, so the fact that it would take a little extra time to allow those to be processed to make sure they are valid, along with the fact that we are trying to protect identity theft against it, is a reasonable delay.

Ms. TUCKER. I believe that the way that we have looked at these additional filters for this coming filing season, once again, goes back to the balancing act, that to detect and prevent fraud, there could be some delays for legitimate taxpayers as we do our validation.

Mr. PLATTS. Maybe a final follow-up before I yield to Mr. Towns. On the direct deposits, of the cases that you, not the ones that are potentially the \$1.5 million that Mr. George's office has identified, but the ones that you have identified, do we know what percentage of those were direct deposits today?

Ms. TUCKER. No, I don't believe I have that information.

Mr. PLATTS. Because that is one of those filter issues that how you look at it. My guesstimate, and it is more based on no exact data, but that you are going to find direct deposit or the debit cards are going to be the norm, especially the debit cards because it is easier to get them and don't always require a photo ID, as now you are going to have to show at a bank.

So that type of data collection, that goes to, I think, Mr. White's testimony. I am not sure what needs to be done in your system, but to be able to be able to pull out that type of data to then assess what is a typical case that has been identified as fraud and what are other parameters.

And I think, Mr. White, that is what your testimony, I know in your written testimony, addressed, that because we don't have that data yet, it makes it harder for you to be able to respond to better prevent, not just after the fact, but up front.

Ms. OLSON. Mr. Platts, if I might intercept something here. Several years ago we identified this very issue about the name mismatch for a different reason, when sometimes taxpayers inadvertently switch the numbers of their accounts for a direct deposit and the dollars were going into that account, and then we couldn't re-

trieve it back from that account and the IRS wouldn't issue a new refund to the taxpayers.

And we learned that historically the IRS did have arrangements with the banks in which they did do a mismatch, and I could never identify the exact reason why it was discontinued maybe about a decade ago. I heard different stories: one that the banks didn't want to do it anymore or that, because of different programming, we weren't able to have that exchange. But it was done, so I know it is possible to do.

Mr. PLATTS. Okay. Thank you.

Mr. GEORGE. This is just not necessarily in their defense, but this is a government-wide issue; whenever taxpayers or any citizen receives a benefit from the Federal Government this issue exists.

Now, the Financial Management Service, which is a component of the Department of the Treasury, could help the IRS and other federal agencies develop procedures to help allay this problem. And I don't know whether Ms. Tucker is in a position to elaborate on their discussions, but it was my understanding that they were reaching out.

Mr. PLATTS. That is kind of an ongoing dialogue you are having.

Ms. TUCKER. Correct.

Mr. PLATTS. Right?

Ms. TUCKER. Correct. And I appreciate Mr. George for bringing that up just for clarification. I mean, the actual issuance takes place with FMS and I know that they are looking into the debit card issue.

Mr. PLATTS. Thank you.

I yield to the gentleman from New York for purpose of questions.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Let me begin, Ms. Tucker, with a question. We talk about the budget deficit and all of that. I am wondering do you have enough employees to be able to do the kind of things that are being asked of you to do? I know it is a sensitive question. I really realize that.

Ms. TUCKER. I think probably every time any of us from IRS come before a committee, we talk about the delicate balancing act in executing our duties. We are at a place right now with the IRS, our overall staffing levels are down fairly significantly. We just wrapped up a fairly tough budget year, and because of that we haven't been hiring in the numbers to replace attrition that we have in past years.

So as our staffing levels have gone down, to deal with this heinous issue of identity theft, we have increased our staffing significantly over the past year. In fact, we have doubled it. We have, going into this upcoming filing season, 3,000 IRS employees solely dedicated to identity theft. And when you look at the fact that our overall staffing levels have declined during this tight budget time, the reality is that staffing has to come from somewhere else.

At the same time we have put additional staffing against identity theft, we also, to help get to the very issue that I know has been on your all's mind about assistance to taxpayers, we have trained 35,000 IRS employees in identification of identity theft and what they can do, even if their job is in an unrelated area to the 3,000 we have specifically dedicated to try to help and steer victims of identity theft to the proper channel.

So it is a concern for us that we have all of these initiatives that we have in play trying to get in front of identity theft, but the reality is once that victim has had this perpetrated against them, a lot of times it is that personal IRS touch that they need to help work through resolution of their account.

Mr. TOWNS. Thank you very much. Sometimes I think we don't look at things in the total way. The fact is that if you had more workers, then maybe some of the things we are talking about wouldn't exist. At the same time, more revenue would be coming in and life would be much better for people. So that is the reason why I raised it. But I know that it is a sensitive issue in terms of deficit and all of that, but I think the point is that I think that we need to spend some time making the case that this is the right way to go, this is the right thing to do.

Mr. George, you used a statement that I just can't let go. You said that much more work needs to be done. Could you be more specific?

Mr. GEORGE. Yes, sir. It relates to what you just discussed with Ms. Tucker in terms of resources. Again, in their defense, it is a zero sum game. Unless they are given additional resources, they have to take people from one function and apply them to another. And, again, as it relates to customer service and identity theft, many of the individuals within the IRS who attempt to assist people with their problems also handle routine telephone calls from other taxpayers who do not have, necessarily, identity theft problems, and these people are assigned on an as-needed basis, and I think once a week, and then many times the victims will be dealing with multiple representatives who are not familiar with their particular case, so they have to start the entire process all over again, from proving they are who they say they are and then explaining the situation that they find themselves in.

Now, again, to their credit, we reported in May of 2012 that the IRS case resolution of an identity theft issue was over 414 days. Now, our most recent review has shown that the average has fallen to 247 days during the review of an initial sample that we took a look at, with cases open still from 47 days to still over 735 days.

So, again, it is getting better, but as you, I am sure, are certain when you deal with your constituents, if you are being told that it is going to take six months to a year to get your tax refund, to get this matter cleared up, it is very frustrating, sir.

Mr. TOWNS. And I think about the fact that there were 200,000 calls. There are 127,000 that are not being answered. I mean, that is disturbing.

Yes, Mr. White?

Mr. WHITE. I agree with my colleagues about what has been said about the tradeoffs and resources here, but one thing to note is that despite the increase in resources that IRS has devoted to the problem and the initiatives they put in place, the problem continues to grow and get worse. So despite the efforts, they are not keeping up with the problem. And resolving cases after the theft has occurred and after the fraud has occurred is very labor-intensive. So that will be a huge hit to the budget.

The trick here is figuring out a way to prevent the fraud in the first place. That means doing more research up front, experi-

menting with better filters to try to prevent the fraud, and that way you avoid this very expensive process and very time consuming, lengthy process that is a terrible process for the victims, the innocent victims. But you can avoid that with the up-front prevention.

Mr. TOWNS. Thank you, Mr. Chairman.

Mr. PLATTS. I thank the gentleman.

Yield to the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you so much, Mr. Chairman. Again, before I begin, I want to thank you for your service here in the Congress. This is, I believe, your very last hearing?

Mr. PLATTS. Our final one. We have been just trying to groom you, so—

[Laughter.]

Mr. PLATTS. I know you are a ranking member on a different subcommittee, but this one is well served to have you move over.

Mr. CONNOLLY. Well, thank you, but apparently the Chairman of the Committee is just abolishing these subcommittees left and right, so I don't know.

Also, Mr. Towns, I am sorry to see you go, as well. You have been a great mentor and friend, and your leadership and commitment to trying to make this a better government, a more efficient government, the two of you have worked so well together and you have been a model, I think, for others. I wish them would emulate. But I personally am really going to miss both of you. Thank you so much for your leadership.

And thanks to our panel. Let me sort of start, for me, over a little bit on identity theft and IRS. Anybody, maybe Mr. George, but do I have it right that in a four-year period, formally recognized incidents of identity theft with respect to IRS went from 51,000, almost 52,000 in 2008 to 1.2 million this year?

Mr. GEORGE. Well, and we believe that is an understatement.

Mr. CONNOLLY. Understatement.

Mr. GEORGE. Exactly.

Mr. CONNOLLY. So we now have an exponential explosion in this problem.

Mr. GEORGE. Correct.

Mr. CONNOLLY. In four years.

Mr. GEORGE. Correct.

Mr. CONNOLLY. Is that correct?

Mr. GEORGE. That is correct.

Mr. CONNOLLY. Why do you think that is?

Mr. GEORGE. Sir, people are nimble and they will use their ingenuity when it comes to taking advantage of a federal program, a state program, a non-governmental opportunity, if they think they can get away with it.

Mr. CONNOLLY. Well, apparently they think they can.

Mr. GEORGE. And they are.

Mr. CONNOLLY. Now, you mentioned that at one point—first of all, the Ranking Member indicated 200,000 phone calls not even responded to.

Mr. GEORGE. Yes.

Mr. CONNOLLY. You mentioned that if we get around to responding to it, it is going to take you, well, at least recently, over 400 days, over a year.

Mr. GEORGE. The IRS, unfortunately, did not devote the amount of resources initially to this. And in all honesty——

Mr. CONNOLLY. Well, don't go there in resources just yet.

Mr. GEORGE. Okay.

Mr. CONNOLLY. I am going to come back to that.

Mr. GEORGE. Okay.

Mr. CONNOLLY. I just want to make sure I get the facts straight in my head. So here we are with that kind of statistic. Before we get to resources, maybe we have to pay attention to this problem. And anyone reasonably looking at this, let's say somebody of evil intent or someone who just has trouble not yielding to temptation. Maybe not a bad person, but gee, the odds are pretty good I can get away with it.

Mr. GEORGE. Yes. And keep in mind this is not only a domestic problem, this is an international problem.

Mr. CONNOLLY. Right. So, in a sense, the IRS has now become like a bank. Remember the famous bank robber who said why do you rob banks, because that is where the money is? I mean, this is where the money is. And if I understand it correctly, if we don't sort of change this trajectory, over the next five years the estimated loss due to identity theft alone is \$21 billion. Is that correct?

Mr. GEORGE. And, again, that is, in our view, a conservative estimate.

Mr. CONNOLLY. A conservative estimate.

Mr. GEORGE. Yes.

Mr. CONNOLLY. My, my, my. Okay. Now, I guess I want to understand to what extent, though, are we part of the problem here in Congress. It is easy to have a panel and beat up on IRS for why aren't you doing more, why didn't you catch on to this earlier, why aren't you answering the phone calls, and all that.

Ms. OLSON. Sir, could I intercede on that question?

Mr. CONNOLLY. Yes.

Ms. OLSON. I would just like to point out that one of the major sources of the availability of Social Security information and numbers is the death master file from the Social Security Administration, which is made public, sold by the Federal Government and is posted very quickly after a decedent, you know, after someone dies and contains all sorts of personal information.

Mr. CONNOLLY. Right.

Ms. OLSON. I was just meeting with low income taxpayer clinics yesterday in Cleveland. One of the clinics that had reported to me earlier that they had represented a taxpayer whose daughter had been murdered and the death master file dutifully reported her death, it was made public on one of the genealogy websites, and she spent over a year trying to clear up the last return of her deceased murdered daughter.

I think that there is legislation that has been introduced in both houses to restrict the access of this data, and I think until we do that, the Federal Government is perpetuating identity theft. And we do believe, my personal opinion is that the Social Security Administration can restrict access to that without Congress acting.

People might not like that, they might sue, but I think that FOIA law, the case law now under FOIA recognizes the kinds of exceptions to protect personal information.

Mr. CONNOLLY. I wasn't even thinking of that kind of example, but what a great point, Ms. Olson. Thank you. I mean, here we are, obviously unintentionally, but nonetheless contributing to the problem ourselves in terms of data release, data requirements, and so forth.

And I thank you for that intervention, but I was actually going to go at the resource question. So in the last few years what has happened to IRS's budget? We have been beefing it up, right? We have been adding agents, we have been giving you a lot more money because we recognize this problem and we want to solve it with you? That is what we have done here in Congress, right?

Ms. TUCKER. So, let me talk to the numbers. So for 2012, the year that was, we had a 2.5 percent reduction in the IRS budget from 2011.

Mr. CONNOLLY. And what kind of reduction did you have from 2010 to 2011?

Ms. TUCKER. We were also down. I don't have the number off the top of my head, but the number for last year, the equivalent for us with the increase in our overhead costs for our facilities, etcetera, was roughly a \$350 million reduction in our budget for 2012.

Mr. CONNOLLY. A \$350 million reduction? Is that what you said, Ms. Tucker?

Ms. TUCKER. Yes, sir.

Mr. CONNOLLY. Now, I am over my time, forgive me, Mr. Chairman, but I praised you.

[Laughter.]

Mr. CONNOLLY. And you really are a great chairman.

[Laughter.]

Mr. CONNOLLY. Is there sort of a back-of-the-envelope ratio of every dollar we invest in an IRS agent we collect X?

Ms. TUCKER. Yes, sir. It is actually a very good return on investment.

Mr. CONNOLLY. Well, what is that, Ms. Tucker?

Ms. TUCKER. Let's see. I think, Mr. George, you have reported on this.

Mr. GEORGE. One to 12.

Ms. TUCKER. Do you see how I like for my colleagues to help me out? So a very, very good return on investment.

Mr. CONNOLLY. Would \$200 for every \$1 we invest roughly be in that ballpark?

Ms. OLSON. Depending on how you look at it, sir. It is either \$4 for every dollar you invest or \$12 for every dollar you invest.

Mr. CONNOLLY. But in terms of tax enforcement, what happens?

Ms. OLSON. Well, that is the tax enforcement number. I think it is 250 to 1, if you look at all revenue that is collected by the IRS.

Mr. CONNOLLY. All right. So let's be conservative, four to one. So here is a Country struggling with its debt, breaking out in sweat over the fiscal cliff. This Subcommittee, our Chairman and Ranking Member have pointed out, for example, revenue left on the table every year. And, if I recall correctly, that number is roughly \$135

billion of either unassessed but owed, or uncollected and assessed. Roughly right?

Ms. TUCKER. Yes, sir. The thing that we talked about earlier is our overall staffing is down because we have constrained the back-filling behind attrition, and as we have talked about, we believe a dollar invested with the IRS is a good investment because we are the funding arm for this Country.

Mr. CONNOLLY. Ms. Tucker, I just want to say I don't know how we, with a straight face, in Congress can decry this kind of problem that is a legitimate problem. I mean, my gosh, it has exploded. And to protect our public we need to do something. We need to invest in the IRS so it can do something. And that doesn't even begin to address the rate of return for every dollar we invest in terms of new revenue owed that can help us reduce the debt and maintain strategic investments, because we don't like government, some of us, apparently.

We don't like the IRS, an obvious symbol and instrument of government. So we are willing to decry a debt, but not do anything about it when there is an answer that is readily at hand. It doesn't solve everything, but if you are right about \$135 billion on the table every year, let's roughly say that is true, if we could make a dent, \$135 billion a year times 10 years is \$1.35 trillion. That exceeds the sequestration amount entirely.

We could do something. We could make a dent in that if we invested in you. But we are not willing to do it for ideological reasons, and that hurts the Country.

With that, I yield back, after Mr. George has the last word, if the Chairman will indulge.

Mr. GEORGE. Well, thank you. Thank you both.

I just want to make it clear, though, there is no question that additional resources would allow the IRS to do more. That said, access to additional information would also assist the IRS in doing its job, without necessarily requiring additional resources. For example, the Department of Health and Human Services has what is known as the National Directory of New Hires. The IRS has some access to it, but it is limited. If this access were expanded, which would require statutory changes, it would allow the IRS to be able to better match the withholding and income information provided by a taxpayer to ensure that it is accurate.

Most recently, the IRS gained access to the Social Security Administration's database that deals with 1099s, which has assisted it in helping to stem tax cheats in the Social Security arena.

But I carry around with me a little card, and I think my colleagues are probably bored hearing me say this at every hearing, and I beg your indulgence. This third-party information. There is a very high correlation between tax compliance and third-party information reporting on income and withholding. The IRS estimates that individuals whose wages are subject to withholding report 99 percent of their wages for tax purposes. Self-employed individuals who operate non-farm businesses are estimated to report only 68 percent of their income for tax purposes. But the most striking number is self-employed individuals operating businesses on a cash basis report just 19 percent of their income.

So if Congress, and, again, it is not this Committee's jurisdiction, I realize that, but would require additional third-party reporting, I think, and this goes to the tax gap issue also, not just theft or identity theft, but it is just a global problem.

Mr. PLATTS. Well, Mr. George, as you reflect, it is not our jurisdiction, but it is an opportunity for us to help educate our colleagues because of the data we gather through this Committee, and an example of this is Mr. Connolly and Mr. Towns and I, back, after our April hearing, had done a letter to the appropriator saying we need to give you more resources because of the conversation you just had with Mr. Connolly that it is a good investment and it is going to be a good return for taxpayers and it is going to mean we would have further victims to then have to assist.

So while a number of these issues are outside of our jurisdiction, we have sought to try to educate, and I know with the April hearing, when we had similar data that we heard, that we did pass it on to our appropriator chairman and ranking member to say look at this. Now we have a CR, so who knows what the final appropriation is going to be for the coming year or the current year, really, but we have tried to make our appropriator colleagues aware of this, that this is a good investment; that if we want to help do right by the taxpayers, invest in your services.

Ms. TUCKER. If I might, because I think Mr. George did bring up something that I want to make sure we don't give the impression that because our staffing is down, we are waiting to take aggressive and significant actions. The third-party data issue is something that we have been focused on at IRS for many years, and specific to the issue we are talking about now, identity theft, some of the filters that we are using, and we are using successfully, and I agree with everything that has been said today, prevention is key here because the numbers that we have talked about and the assistance that the victims of this heinous crime are dealing with, that is where the pain points are.

We are doing some, I think, very innovative testing, using third-party data earlier, and I think you have all heard former Commissioner Shulman talk about an initiative that we are looking at at IRS called Real Time, and that really, I think, gets to the heart of the matter, too. If we do have basic information documents available to us to match quickly, when that return comes in the door, that does stem a tremendous amount of this fraud that we are seeing perpetrated on innocent taxpayers. So that is something that we will be doing some additional testing on this upcoming filing season, to look at how we can get information documents into IRS more quickly and then use our data analytics, use the computing capabilities we have to stem additional identity theft more quickly.

Mr. PLATTS. And incur that focus on prevention, protect taxpayers, and avoid victims. And then, also, that is again protecting taxpayers because of the amount of time you have to then spending the victims after they have been victimized. So prevention, and that actually brings me to kind of a follow-on to where I had asked in the first round. And I don't know if you have this data available, but it goes to the data collection issue and trying to identify what is more common to this type of fraud, these identity theft frauds.

And two in particular, two issues, is, Mr. White, in your testimony, I think it is, you talk about a typical type of case if they file early. Is there any data now as far as, again, the ones that we know were identity theft, what percentage were filed, say, prior to February 1? My guess is it is a large percentage, but I have never seen any numbers. It is one of the questions I kind of keep asking, I guess.

So do we have data now of how many of these cases that we know were identity theft were filed prior to, say, February 1 or February 15th? And I say February 1 because most employees are just getting their returns. And while they may file quickly in February, they probably don't file before February 1.

And then also a similar question is how many or what percentage are e-file? Because I think in the 1.5 million that, Mr. George, your office identifies potential, you estimate, I think, about 91 percent of that 1.5 were e-file.

Mr. GEORGE. It is 1.4.

Mr. PLATTS. So 1.4, 91 percent of that 1.4. So of the ones that we know were identity theft, do we know what percent were e-file?

Ms. TUCKER. So just a couple of things, if you will indulge me on the background here. Here is the difficulty in, I think, extrapolating the electronic filing number. The reality is well over 80 percent of all tax returns are filed electronically now, so I know there has been some discussion about is electronic filing the cause of this. Electronic filing is secure; it reduces cost to the Government for processing tax returns. I think we have talked with this Committee before about good government, and the reality is the paper return processing is extraordinarily expensive and the electronic filing is pennies on the dollar.

Mr. PLATTS. And, Ms. Tucker, I am not suggesting we want to ever move away from it. I raise this specific issue as part of the big picture, meaning if we know what percentage, if 99 percent were e-file, combine that with the second part of my question, and 95 percent were filed prior to January 31st, you start combining all those different filters or flags, that you get a pretty exact, if we get anybody that files e-file prior to February 1st with a change of address, with this, they are going to get bumped out.

Ms. TUCKER. Unfortunately, we had some conversation about this. The vast majority of early filers, legitimate early filers are refund filers, because folks that have worked hard all year are ready to come in the door, especially simple return filers, W-2 filers, folks that maybe have limited amount of interest income. So to slow down every return that comes in early simply because it is an electronically filed return with a refund on it and has a change of address.

Mr. PLATTS. Again, you are limiting, I am using those as examples.

Ms. TUCKER. Right.

Mr. PLATTS. But do we have that data to even try to do that?

Ms. TUCKER. Yes, we do know that we see early filing and refund perpetrators tend to go hand-in-hand. I don't have a number off the top of my head; we can go back and look at that for you.

Mr. PLATTS. Like the February 1. I would be interested if they are that percentage. What percentage, again, of the ones that you

know were identity theft from the previous year, what percent were filed prior to February 1.

Ms. TUCKER. So the other thing that I think is really critical here, the 13 filters that we put into play last filing season, coupled with two very, very important filters that we will have in place this filing season I think are going to get to the heart of some of this.

Mr. PLATTS. And I don't want you to share those.

Ms. TUCKER. Well, but we have talked about these two additional filters that I think are critically important. One is that the deposit to the bank accounts, even though understanding that we can catch some legitimate taxpayers up in that; and then the second being returns that are filed using the same address, because we know that that has been a hole that some of these perpetrators have run to, and again underscoring the fact that there are legitimate taxpayers filing from the same location, whether it is a blended family living at one address or someone that legitimately is using a paid return preparer.

The other thing that I would say, and I don't want to sound like a broken record, we are caught in the balancing act of a surge of filing early in the filing season from legitimate taxpayers who are looking to get their refund in a timely manner, and being able to nimbly use all of these different filters and the resources we have to try to screen the good from the bad, and it is a tough balancing act, Mr. Chairman.

Mr. PLATTS. Absolutely.

Ms. OLSON. If I may insert here to sort of second something that Ms. Tucker is saying. In many tax administrations around the world, and I have put this in earlier testimony for this Subcommittee, they hold off issuing refunds until they have received all of the tax returns. They have a tax return filing period and people submit the tax returns and the agency has a period of time within which to go through and identify discrepancies, which could be simple errors, could be two people claiming the same child, could be identity theft, all sorts of things. And then they are able to check that before they issue a dollar out.

That really is, if you really want to solve not just identity theft, but a whole bunch of other issues, including dealing with dependency exemptions, earned income credit, child credit, etcetera, that really is the global solution. It is a very radical solution for the United States because we have a culture in which we have grown up expecting these refunds as soon as we have filed, and then at the same time we have all these pressures about protecting bad refunds from going out.

And I really think that in the context of comprehensive tax reform, which you all have to do, we need to also think about the administrative side of it and really think about the savings of sort of shifting that balance a little bit.

Mr. GEORGE. If I may, Mr. Chairman, this goes also to a point that Mr. Connolly made, access to timely information, it is almost like the bad guys are racing to file false returns before the legitimate taxpayer can, and the dilemma that the IRS has is that legally employers have until March to submit the withholding and income information, and yet taxpayers can start filing as early as January 1st, or whenever they receive their W-2s.

So this is something if the IRS or if Congress were able to push to ensure that employers submit their information early or concurrent with the information they provide to the employee, that would assist the IRS in ensuring that no one is gaming the system and claiming more withholdings than they are entitled to.

Mr. PLATTS. Mr. White?

Mr. WHITE. Mr. Chairman, there is no doubt that some of these long-term solutions would be big steps towards dealing with the problem. There are some things, though, on the short-run that may not be as big a step, but that can be done. The key in the short-run is for IRS to get smarter. It is not just a matter of resources, but to get smarter about prevention. They are doing a lot with the filters, and so on, to move in that direction, but I do think that more can be done.

And this gets back to the point you were making earlier, I think, about the importance of research to understand what is going on, more systematic research on cases that get through the filters to understand how they got through, and then use the findings from that research to design new filters, new approaches. And IRS is doing some of that, but I think that is an area where even more might be able to be done even in the short-run.

Mr. PLATTS. And that is really my point. Using the example of the February 1 filing or the e-filing is that issue of analyzing to make sure that we have the hundreds of thousands of cases now, you know, from the previous year to say these got through, some factor, what were those common characteristics that we can try to respond to.

Ms. TUCKER. So if I might, and I think to Mr. White's point, even during a time of diminishing resources, we have made a significant investment in IRS in the Office of Compliance Analytics, and this is really, in some ways, the centerpoint for a tremendous amount of the work that we are doing in identity theft, where we have a team of folks working very closely with the Wage and Investment folks and with our Office of Privacy and Disclosure to take a look at patterns, trends, data analytics, bringing in third-party data, doing forecasting.

I can tell you, as a proud 28-year employee of Internal Revenue Service, this is data analytics like I have never seen before. And not only are we using that data analytic to try to get in front of the problem of identity theft, I think this kind of data analytics is going to help us with overall voluntary compliance and dealing with emerging non-compliance, because I think we all know, as Mr. George alluded to, these criminals go wherever they can find the money, and we know that they are not only coming against the tax system, they are going against other federal agencies.

So even having that kind of collaboration to say what are some of the common characteristics, because this is, I shared with you, it is like a balloon; we are pushing on one part of the balloon and it is popping up somewhere else. So data analytics is going to be key to helping devise unique strategies to try to stem this issue.

Mr. PLATTS. I am going to ask, Ms. Tucker, just one final comment and then yield to Mr. Towns or Connolly for their final round. But if you could respond to Ms. Olson and the issue of when there is a victim and the concern about decentralizing, because I use as

a casework, an office, we open about 4,000 cases every year, constituent casework in the district office, and one of the keys to success is we have had our staff kind of specialize, so if you have a Medicare case, you are going to get with one of my staff and they are going to be with you from day one until we address the issue. Now, we will have a backup so if they are out, somebody is also trained as the backup if they are out on vacation.

But that came through in her testimony here today and in her written testimony, and it is what we saw with our constituents, where they kept getting bounced around. And I know, in setting up the Taxpayer Protection Unit, where do we stand in that, that issue, specifically that that victim doesn't keep getting bounced around, that they get assistance, that they know, hey, I can call this person and get an update and I am really in good hands?

Ms. TUCKER. So we do have specialized units, and I think as my colleague, Ms. Olson, alluded to, it is our belief at the IRS that we have set up a structure that is going to provide the best resolution for the victims of identity theft. The bulk of the specialized units are sitting in our Wage and Investment Operating Division, where the bulk of the individual identity theft occurs, but we also know that there are some specialized identity theft issues that may fall out in our Small Business Self-Employed function or in other unique areas at IRS.

The Taxpayer Advocate and I have lots of, I think, very candid and robust discussions about this, and I think my belief is that the process that we have implemented this year, which is different than what we had, actually, last time that we talked with you, that we are going to be able to get this right and provide good level of service to the victims of identity theft.

But that said, it is incumbent on all of us to continue to analyze what is working and what is not, and I have no doubt that my friend and colleague, Ms. Olson, will be over in my office at any moment that we see that it is not working and that we need to do something differently.

Ms. OLSON. If I just might comment here. Taxpayer Advocate Service, in 2012, closed 46,000 identity theft cases. Those are what came to our office. And of those, 33,000 had more than one issue. The IRS doesn't track how many issues or how many multiple years a particular taxpayer has. So when Ms. Tucker says the bulk of the cases are in their Wage and Investment Unit, in Wage and Investment the employees work one issue or one year at a time; they don't have a sense of what the complexities of these cases or the pictures; whereas, my evidence demonstrates that the vast majority of the identity theft cases in fact have more than one issue and are going to bounce around between units.

So I am very concerned. If you asked me what was the most significant issue that victims are going to be facing next year, it is that very issue, this decentralization without a traffic cop. We have a traffic cop right now that needs to be beefed up, the IPSU unit, and what I am afraid is that they are going to reduce the focus on that traffic cop that makes sure the case gets from the right specialized unit to the other.

And I do think that having specialized units is a positive, because getting a group of people who see everything, see the identity

theft cases in a concentration is much better than having one of 2,000 employees see a case once every three months.

Mr. PLATTS. I guess the point that I was trying to emphasize is using my office, again, I will use INS. A lot of complexity with immigration; it is our largest area of casework and one of my senior LAs who just left took a new position with my departure became our expert. Now, she would deal with a lot of different entities within ICE and the various entities that deal with immigration, but she, for the constituent, they dealt with one person, her, and then she dealt with, and I think that is the point, Ms. Olson, that you make, that there may be 21 different units, special units that have to be involved, but you can't expect the taxpayer to be trying to work through those 21.

Ms. TUCKER. No, absolutely. That is not how this system is designed; it's not intended that the taxpayer has to figure out, to navigate through. And just to comment on something Nina just mentioned. She and I have had ongoing discussion about how do we measure success, how do we continue to have dialogue about is the new structure working.

Actually, sitting right behind me today are two executives that are really the cornerstone of the oversight and making sure that we have clean pass-offs. So I think this is one that the comment about the concern that we are going to reduce the strength of the IPSU, that is not in the plans. We know, to use a cliché, it takes a village to get this right, and IRS, with roughly 90,000 employees, we know we are going to have to continue to monitor, to train, and to ensure seamless resolution of these issues.

Mr. PLATTS. And my colleagues have been very patient with me as I used more than my share of time, and I appreciate that because while I am very concerned about the loss of revenue, taxpayer protection, I don't want us to ever lose sight that, when we get to this point where we have identity theft occur, that there is a victim of a crime.

And that is really why I kind of wrapped it up there, is that when that victim comes to us, the Federal Government, and they have been victimized, that we do right by them and that they don't feel, as in our testimony a year ago, that they were victimized a second time. And I know that is a priority, and I leave knowing that it is a priority of yours and a priority of Ms. Olson's and that we are in good hands, that you guys will make sure that we keep improving and working together to get to where we do right by every victim.

With that, I am going to yield to Mr. Towns. I don't know if you have other questions.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Let me say that I think that we all have to do more, Congress as well, and you. I think we have to sort of make the case, because as I am listening I am beginning to become more concerned about what is happening because I am not sure that even when we prosecute that we are getting convictions. And there are a lot of reasons as to why I feel that way, because I think that the evidence that has been put in place, based on the fact that it is coming from folks that in many instances might not be trained fully to be able to put the information where it needs to go.

So I am concerned about your relationship with local law enforcement. I am concerned about that, because when you cut staff, you eliminate folks that would go and be working with the local to be able to, because if a person feels that they can get away with this, they will encourage others to do the same and the situation will continue to exacerbate, and I think that is a real concern.

And I am not just saying for you. I just think that those of us in the Congress that fully understand need to help you make the case. And I understand that some people don't catch on as fast as others around here. Some people get it right away. My son, who is the commissioner of housing in the State of New York, says, Dad, you have to understand, there is a thing all about individual differences. He says some people just get it right away. He said it takes two and a half hours to watch 60 Minutes.

[Laughter.]

Mr. TOWNS. It doesn't mean they can't watch it, it just takes them longer.

So I am feeling that somewhere or another we have to sort of make this case to other members of Congress what is going on here. And I understand you trying to put together units, but the point is that we are not really addressing the issue in the way that we need to address it; and in order to do that we need resources. But we also have to make the case that when we get the resources, that the Federal Government is benefitting from the resources. And at the same, people who are involved in criminal activities will eventually get the message. We need to buy a new tire and stop patching.

Yes, Mr. George?

Mr. GEORGE. It seems counterintuitive, Mr. Towns, but Title XXVI, Section 6103, in the wake of Watergate and the abuses that occurred during that period, provided a lot of protection for taxpayers, and rightfully so.

Mr. TOWNS. Right.

Mr. GEORGE. However, the unintended consequence of Title XXVI, it limits tremendously, both in terms of civil and criminal penalties, the way we, the IRS, the Federal Government, Congress overall handles taxpayer information. And the most surreal aspect of this is that there are times when we have, or the IRS has someone as the subject of an investigation, the alleged criminal, and you need to get their permission, in many instances, to gain access or to share the information that is contained in the allegation; and obviously if that person has an attorney or anyone who would say, no, I am not going to give you permission to share that information. And that is just one example of how Congress could readily change that, but who knows what the consequences are.

Ms. OLSON. I would have to differ a little bit with my esteemed colleague here. I have done extensive analysis of 6103 and consulting with IRS chief counsel, and I think that there is ample ability within the constraints of 6103 today to be able to release information to the places where it is needed. I think there was a rightful culture of being conservative in doing that, and some of the identity theft stories have made us all sit and really look at the statute. And I think the example of what Ms. Tucker talked about, the sharing, and Congressman Diaz-Balart talking about the shar-

ing of the information, we have come up with a procedure that both places in the victim's hands the decision to release their information from one government agency to another that does not have the protections of protecting that information as we do. And I think that is the right balance, to say there is an agency that wants the information; taxpayer, you are the victim, are you willing to give that? And that is all possible within 6103.

Ms. TUCKER. If I might, I would be remiss if I didn't talk about the positive outcomes that we have seen in the past 12 months, just as an example in proactively working with our colleagues in law enforcement, in particular, to try to get our hands around some of the more egregious criminal activity. So specifically the investigations the IRS has initiated, we have tripled that in the last 12 months. We closed the fiscal year with almost 900 CI investigations.

Mr. TOWNS. How is the conviction rate?

Ms. TUCKER. So for the sentencing, I am the eternal optimist, we do have 223 sentenced, as compared to 80 last year. So still probably not large numbers as it compares to the overall size of the problem, but we are seeing increased numbers from a year ago. The other thing that, to follow up on Ms. Olson's point, the new process that we implemented in Florida earlier in the year and that we expanded last month, we do have great hope that that is going to lead us to additional cases, investigations, and prosecution indictments.

Mr. TOWNS. Let me just ask one last question, Mr. Chairman.

Let me ask are you satisfied with the agencies in terms of that report to give you the information that you need? Are you satisfied with Social Security giving it to you in a timely fashion? Because I am thinking in terms of other ways that we might be able to help you here in the Congress. What prevents a funeral parlor from reporting a form, the fact that this person has expired, which would be information that would go directly to you?

Ms. TUCKER. Well, I am thinking about from a logistics standpoint. It is much easier for IRS to take information in from centralized points, so we do receive the death master file information from the Social Security Administration. Several of my colleagues have talked about receipt of wage information either from Social Security or from the new hire database.

So obviously the initiative that we are looking at right now, as it relates to Real Time tax administration, would be successful. The more quickly IRS is able to take in good validated data in large quantities and be able to then program our systems to basically ping against that information more quickly.

Mr. TOWNS. I guess the reason I raise this is that Social Security has its problems too. That is the reason why I raised that. I am trying to figure out a way that you might be able to get additional information. Maybe the State could provide it. I don't know. But I think that we need to look at various ways that we could sort of cut down on that, I mean, this is just unacceptable.

Ms. TUCKER. If I might, and this is a kudo, actually, to the State of New York. We are engaged in discussions with our counterparts in State tax administration because I think, as Ms. Olson alluded to, we know that there are States, as well as other governments,

that do make decisions on refund issuances and say we are not going to issue a refund until we have made ourselves comfortable that we have the right taxpayer or this is the right income amount.

So part of what we are doing with Real Time tax administration in our testing is actually working with a handful of State tax agencies who will be giving IRS some data from State wage information that we will then use to say, gee, is this information valid earlier that we could maybe even use as an additional filtering. So kudos to the folks up in the State of New York Department of Finance; they have been terrific partners for us.

Mr. TOWNS. Thank you. And I am happy to hear that positive statement about my State. Thank you.

Mr. PLATTS. Mr. Connolly?

Mr. CONNOLLY. Thank you, Mr. Chairman. I just have, well, maybe two follow-ups.

One is, Ms. Tucker, is I heard your statistics on convictions.

Ms. TUCKER. Yes, sir.

Mr. CONNOLLY. We had at least 1.2 million identity theft fraud incidents, and Mr. George thinks that is an understatement, and we had 280-something, did you say, convictions?

Ms. TUCKER. So we had—

Mr. CONNOLLY. No, no, just give me the number.

Ms. TUCKER. Eighty sentenced in 2011 and 223 this year.

Mr. CONNOLLY. That is pretty pitiful. I mean, if I am a criminal and I am looking at that probability, boy, I am going to expand my identity theft fraud activities, especially at IRS. Why wouldn't I?

Mr. GEORGE. Mr. Connolly, in their defense, too, at the federal level they have thresholds in which they will accept or will not accept a case, and in the event that they decline to prosecute, they can attempt to seek justice at the State and local level.

Mr. CONNOLLY. Well, okay.

Mr. PLATTS. Mr. Connolly, would you yield?

Mr. CONNOLLY. Yes, of course, Mr. Chairman.

Mr. PLATTS. One clarifying point is, using the case like with Puerto Rico, where it could be one individual or six individuals, but with 100,000 cases.

Ms. TUCKER. With multiples, right. Correct.

Mr. PLATTS. That is the one issue.

Ms. TUCKER. The other thing that I would be remiss if I didn't point out, and I appreciate Mr. George's backup on the fact that IRS develops cases and then we work with our counterparts to hopefully provide enough information to move those forward.

Mr. CONNOLLY. Wait a minute, counterpart? What do you mean counterpart? Who is your counterpart?

Ms. TUCKER. So the folks that we would work with with Department of Justice and the locals.

Mr. CONNOLLY. Okay. Thank you. This is where I was headed, if you will let me ask the question.

Ms. TUCKER. Absolutely.

Mr. CONNOLLY. How would you evaluate the level of cooperation and the seriousness with which the U.S. attorney's offices are taking this problem? Because, for example, it took a long time for us to get U.S. attorney's offices to take Medicare fraud seriously. It is now a huge part of their portfolio. We have 99 U.S. attorney's of-

fices around the United States. Some of them are now engaged in multi-billion dollar recoveries and convictions of Medicare fraud. That is a good thing to try to stamp out Medicare fraud and to recover assets for taxpayers.

So I am asking the same question of you, not to ding on IRS or anybody else for that matter, but how would you assess at this point that relationship with what you call your counterparts, but I would call, I hope, DOJ and U.S. attorney's offices, and how seriously are they taking that problem? Or do you think we still have some education to do there, like we had to do once on Medicare fraud?

Ms. TUCKER. I think we have had excellent cooperation, and let me give you a specific example. Florida, where the Congressman talked about so much of the identity theft is taking place, we have had multiple meetings locally with Department of Justice, with the U.S. attorney's office, with local law enforcement. We have that going across the Country. I think one of the things that we are seeing is that a lot of these departments, they are dealing with the same things we are, multiple competing challenges. But I have nothing but positive things to say about the level of support, as well as the recognition of how heinous a crime this is.

Mr. CONNOLLY. So you are not finding any reluctance, when you deal with them, to pursue it?

Ms. TUCKER. No. I think within the bounds of the resource limitations they face, as well as their tolerances.

Mr. CONNOLLY. Good. Good. I mean, that is heartening to hear. That is really heartening to hear.

You would concur, Mr. George?

Mr. GEORGE. I would, but, in all candor, it depends on the jurisdiction.

Mr. CONNOLLY. Yes.

Mr. GEORGE. And in all honesty, too, the squeaky wheel gets the grease.

Mr. CONNOLLY. Yes.

Mr. GEORGE. So a case in Florida, very egregious, it got a lot of attention and so, yes, the U.S. attorney's office is being very aggressive. We have also, my organization, too, when we prosecute IRS employees, we find that certain jurisdictions, for example, Fresno, California, the U.S. attorney extraordinarily cooperative. And when you get into larger jurisdictions, New York, Chicago, it varies because they have other issues they are contending with.

Mr. CONNOLLY. Sure. It is a really good point you are making.

Mr. Chairman, it might be something we do as a swan song for the Subcommittee, in terms of formally thinking about imploring Attorney General Holder and his colleagues to ramp this up and to maybe issue explicit instructions to all 99 U.S. attorney's offices to redouble our efforts; not to single anyone out for praise or criticism, but we need their help and they have to take this seriously. And I think if they hear from Congress that we take it seriously, it might be a thought.

And my final question goes to you, Mr. White. You have been remarkably laconic, if not silent, and I want to give you an opportunity to comment on some of the topics we have been covering here, because I would like to know what GAO's views are about the

need for more resources; the efficacy of more resources; the deployment of such resources; how much maybe, as Ms. Olson has pointed out, without intending, we have collectively put some burdens on IRS and others that actually contribute, making it easier for this identity theft; and, I don't know, anything else you want to share with us before the holiday.

Mr. WHITE. Thank you. First of all, IRS has done a lot in this area. They have been innovative; they have put in place a number of new initiatives; in terms of tracking the performance of those initiatives, they implemented our recommendation from 2009. One example of what you learn from doing that is on the PIN program, for example, they have been tracking pretty carefully the way that program has worked.

One of the things they have learned from that is that they handed out hundreds of thousands of PINs; tens of thousands of people lost them or misplaced them and had to be reissued. So by tracking performance that way, you learn something about how well these efforts are working, and then you can tweak the design to make them even more effective. So they are doing that.

In the short term, again, I come back to the point I made earlier, and IRS is doing some of this, but more systematic efforts to learn from cases that get through the filters, to then use that knowledge to, in turn, redesign the filters and try to make progress. It is incremental, it is hard work to do this, but it is one way to make progress in terms of preventing these cases up front. At the back end it gets very expensive and very difficult to resolve the cases for the taxpayers and to try to track the crooks down after the fact.

Mr. CONNOLLY. Any views about the wisdom of Congress actually increasing, instead of cutting, the IRS budget in terms of efficacy of return?

Mr. WHITE. I think that budgets matter, obviously. You all have to make decisions about how to trade off across agencies. I would emphasize the importance of not just giving IRS additional resources, but making sure that they are working smarter with whatever level of resources they have got. And, again, they are doing, I don't want to imply that they haven't been working in that direction.

Mr. CONNOLLY. But, Mr. White, that is easy to say; they should be smarter, it is not always just a matter of resources. But as Ms. Tucker pointed out, we have cut their budget \$350 million. You can be smart all you want; that is a real cut. That means they are handicapped in terms of the resources probably they need to have a critical threshold to be dealing with this subject in an efficacious way, or not.

What do you think, GAO? Because otherwise you are inviting us, you don't mean to, but the inference could be drawn from what you just said, well, good, let's merrily keep on cutting, because they just need to be smarter. And at some point they can't meet their core mission. I mean, at some point we do less with less, do we not?

I mean, I agree with you that up to a certain point the denial of resources can make people more efficient and smarter, and actually have to figure out new ways of doing business, and that could be inefficiency. But at some point that is not what we are talking about. And I am deeply worried that in the case of the IRS, out

of ideological opposition, it has nothing to do with somebody, a priori, saying I want to make them more efficient, that is why I am doing this painful surgery.

No, I don't like the IRS. I don't like their mission; I don't like what they do. I think they are emblematic of the kind of intrusive role of government that I, ideologically, don't like, and if they go away tomorrow it would be a good thing. I don't like paying taxes, while I am at it.

And we are dealing with that up here and I just caution that it is good to urge that we be more efficient and that sometimes big flat blow to budgets, of course, aren't the answer, that is true. But, on the other hand, if we treat where we are headed right now in this Congress, in terms of the denial of resources, I am deeply worried that we can have all the hearings we want about problems like this that need to be managed, and managed by the IRS, and we are blowing smoke, because we are engaged in a fiction because the thing not said is I am not willing to give you the resources to do what I am baiting you up about. And I am very concerned about that, and I would hope GAO would be too, because the Congress relies on you for objective analysis, and sometimes even unwelcomed recommendations, but recommendations nonetheless.

Mr. WHITE. Well, let me say this. IRS, across the board, over the last 15 years, has made substantial efficiency gains based on a lot of innovations. In spite of those efficiency gains across the board, it is the case that in a number of areas, when you look at IRS, not just in identity theft and IRS's ability to keep up with the identity theft workload, but across the board at IRS, you do see IRS falling behind; that in terms of telephone service to taxpayers, for example, they are falling behind.

In terms of their ability to keep up with correspondence they are falling behind. Identity theft, we have said today, is another case where IRS has done a lot, they have devoted more resources to the issue, they have made a lot of innovations, but the problem is still growing. They seem to be falling behind.

Ms. OLSON. If I may add. You all charged me with submitting a report to Congress every year, every December, to identify the top 20 problems of taxpayers, or at least 20 of them, and in my 2011 report last year I identified as the number one most serious problem of taxpayers the fact that the IRS had too much work and too little funding with which to do that work.

And Mr. White has identified a number of areas, and I think Ms. Tucker and Mr. George have both talked about the fact that although the IRS has built up the number of employees that are dealing with identity theft, it is a finite universe, so those employees are removed from doing other work that taxpayers desperately need done.

And the diminution of taxpayer service in our budgets has been, I am able to speak without the constraints that maybe Ms. Tucker has or Mr. White, partly because of the authority you all have vested in me, that from my perspective the taxpayer is really being harmed by the diminution of taxpayer service funding to the IRS; and that will come back in reduced compliance, reduced collections, and general frustration not just at the IRS, but at Federal Govern-

ment as a whole, and that is not a very good recipe for good administration, much less good tax administration.

Mr. PLATTS. Ms. Olson, we appreciate the frank assessment, and it is an important part of your duty and the charge you have had.

We have been joined by the full Committee chairman, Mr. Issa from California.

Mr. ISSA. Well, I will be brief.

First of all, I haven't come to a lot of your hearings because there has been no need to. I have a colleague that I came into Congress with 12 years ago, and you will be departing. I understand this will be potentially your last hearing. I may schedule another one, though, Todd.

And speaking of Mr. Towns, the former Chairman of the full Committee and my friend, and I do have a couple of quick questions, but I really came to thank both of you for your friendship and your leadership. In fact, back when Mr. Towns was Chairman of the full Committee and for all the years that you and I have worked together, since we came in together, you are not people that need to be watched. Your efforts to go after waste, fraud, and abuse in government will stand the test of time around here. As a matter of fact, Mr. Connolly is trying to figure out how to catch up to the good work that you guys have done when you are gone.

So I wanted to thank you and take this opportunity to say that you should have a portrait here sitting next to Mr. Towns'. It is not in the rulebook, but in my heart you will.

Mr. PLATTS. Well, Mr. Chairman, I appreciate the kind words. One, if I was going to have a portrait here, I would want it to be a duet that Mr. Towns and I would be together in the portrait, because we have been linked for so many years.

Mr. ISSA. Well, you know, there is a holiday party coming up. We can take that picture.

[Laughter.]

Mr. PLATTS. And I did nominate Mr. Connolly as the new ranking member of these issues in this Committee and whatever the new structure is, so he will be a great one to follow on on our efforts.

Mr. ISSA. Thank you. And I will be brief. I realize I haven't been here for most of the hearing; I have been tied up with a couple other things in another hearing. It turns out that the 6 million people and their families afflicted with autism are very concerned about our hearing today, rightfully so.

Ms. Olson, if you were asked, just tell me if it is already in the record, but as we are balancing the new demands under the Affordable Health Care Act with these shortages, how do you view our role in essentially urging you to prioritize? Because I think what you said, very rightfully so, is if we are taking from these roles of identity theft and so on, which is more important to the American people, being basically done under Obama Care or having their money not essentially stolen from them?

Ms. OLSON. Well, I actually have to say I would not be able to choose between those two.

Mr. ISSA. Well, you wouldn't without congressional action.

Ms. OLSON. If you forced me to choose, I wouldn't know how to make that choice. I think that the single greatest risk in the ad-

ministration of the Affordable Care Act is that IRS not be funded adequately to administer it. That is where the risk is. I am in agreement with Mr. White on the way that we can use data to improve our protection, our identity of our protections, but there is just the simple fact that we need more bodies in the IRS as a whole on the taxpayer service side to deal with the victims.

Mr. ISSA. Well, oddly enough, Mr. White, you were my next question. All of us on the dais here voted for the Data Act, which would include the ability for the IRS to have, if appropriate, unfettered access to government-wide data in a format that would allow them to search without, if you will, significant overhead of new people writing programs, because the metadata would be there so that, in fact, particularly for identity theft and things of that sort, you would be able to see the link behind, if you will, the operation of the thieves, where they go from what they have done, where else they have hit.

How would you view, from an accountability and cost standpoint, the access? In other words, how much of what we don't succeed in doing is because we don't have the tools to quickly identify these repeat offenders? Identity theft is not a one-time event of one identity; it is very often a gang activity that hits thousands, or even millions, of individuals.

Mr. WHITE. I think it is clear to all of us, I think, that part of the long-term solution to the problem, a big part of the solution in the long term is better access to information. If IRS can match, before issuing refunds, if IRS can match taxpayers' tax returns to information returns that come in about their income and expenses, and have access to other information like the Social Security death file, that would prevent—

Mr. ISSA. Or even expanded census information and all the other things that might give you a heads-up that this individual is not that individual.

Mr. WHITE. Yes. Yes. How useful each piece of information is, each type, remains to be seen, but there is no doubt that being able to match to useful information before issuing refunds would prevent a lot of the problem. That is long-term, but that is clearly the direction to move.

Mr. ISSA. And, Mr. George, as we know, regrettably, sometimes these activities are in the system, not outside the system. What would, in fact, be the tool that Congress could mandate, essentially that OMB and others execute on, that would help you more quickly have the tools at your disposal to, I want to be accurate in saying that, do the work you already do, but do it with a fraction of the time that it often takes your men and women?

Mr. GEORGE. Chairman Issa, relaxation, to some extent, of the restrictions imposed by Title XXVI, Section 6103, which is, again, within the mandate or jurisdiction of the Ways and Means Committee in the House, Finance Committee in the Senate.

Mr. ISSA. Well, we are all good friends here, so we can work that part out.

Mr. GEORGE. Thank you, please. But it really does, in many ways, tie one hand behind our back in terms of getting permission, sometimes from the accused or the perpetrator, to share informa-

tion with local and other law enforcement types. That is the immediate answer that comes to mind.

Mr. ISSA. So very targeted legislation related to identity theft that would expand that sharing, if and for that purpose only, would be sufficient to crack open some of your needs?

Mr. GEORGE. It would give us more leeway, sir.

Mr. ISSA. Okay. We look forward to working with you on that.

I guess, Ms. Tucker, lest you think that I am not going to ask one more question, Mr. Connolly, who I am afraid has departed, and I will be working Monday on legislation for the next Congress that would define the CIO once and for all as a single individual per entity. There are about 23 entities in the government, independent entities; there are over 100 CIOs. So how many chief information officers do 23 entities need?

From a standpoint of operational support, the whole question of the IRS, the use of its database, its centers, and getting meaningful information that everybody on the dais wants, would a single point of authority and accountability within your jurisdiction, would that help you and would it help you in a meaningful way, or today having multiple CIOs in multiple places where multiple assets are controlled, is that good enough?

Ms. TUCKER. I probably don't have enough insight into the issue to fairly consider and respond.

Mr. ISSA. And I could ask it in the reverse way. Do you know who you go to for single point accountability on information that the entire system needs today? And, if not, would it be better to have that?

Ms. TUCKER. So, at IRS, obviously, we do have multiple data exchange agreements with Social Security Administration, with basically any agency. We do have folks that are assigned to give the care and feeding to those particular exchange agreements. In my way of thinking, there are a lot of things that are made more cumbersome by multiple points of contact. Do we make it work? I think that is what all of us in government are about right now, trying to find ways to piece things together.

Mr. ISSA. Well, I might say that when I started flying commercial airlines, there were five people in the cockpit to get me from one end of the world to another. Today there are two. That is because, really, automation doesn't require you have a radio operator and you have a navigator and you have a flight engineer. So I might ask if you think of any examples where you think streamlining could occur, we would love to see it, because I know that Ms. Olson would love to see the freeing up of those dollars and slots, assuming that the benevolence of Congress and the President doesn't give you just a new pot of money. And it is a real shame because all the money flows through you; you just don't get to keep it, you have to ask for it back.

[Laughter.]

Mr. ISSA. Mr. Chairman, I want to thank you for your indulgence. I went quite a bit over time. And thank you for the hearing and, once again to both of you, you will be missed until, well, I don't know about you, Todd, for sure, because you are within driving distance, but I expect, Mr. Towns, when he is going between his Florida home and his New York home, to stop in and see us.

I yield back.

Mr. PLATTS. Thank you, Mr. Chairman. I certainly appreciate your participation and allowing me the privilege of chairing the Subcommittee for the past two years.

As this is our last one, I want to first thank our witnesses. You have each been with us previously and I know you will continue to work with whoever sits in these chairs in the coming term, as well as with staff.

A final comment, with this being our last one, is I know I speak for Mr. Towns and myself, that we couldn't do what we do without a tremendous staff, and as you and your staffs have worked very closely with the Committee staff on both sides of the aisle, that is really where, day in and day out, the work gets done. So I want to make sure I put on the record to Republican and Democratic staff, those who are here with us today and have worked with us over many years, we are personally indebted to them and wish them great success as we move on and they continue to hold down the fort here with the Subcommittee.

We will keep the record open for seven days for any other materials, and again thanks to the witnesses and, Mr. Towns, it has been quite a privilege. I look forward to continued friendship. And as I gavel this closed, I am going to do it on behalf of you and me, as Chairman, Ranking Member now, and throughout the years Chairman and Ranking Member.

Mr. TOWNS. Thank you very much, Mr. Chairman. I would like to associate myself with your remarks in reference to the staff. Thank you so much.

Mr. PLATTS. This hearing stands adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

Opening Statement of Todd Russell Platts
Subcommittee on Government Organization, Efficiency, and Financial Management
Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service, Part 4
November 29, 2012, 10:00 a.m., Rayburn 2247

The purpose of today's hearing is to address the serious and rapidly growing problem of identity theft related tax fraud. This is the fourth hearing the Subcommittee has had this Congress on this important issue, and it will continue our examination of how fraud is occurring and what can be done to stop it. We will review the Internal Revenue Service's (IRS) actions to prevent and detect identity theft tax fraud, and evaluate what more can be done to reduce the problem and assist victims.

Identity theft-related tax fraud occurs when a fraudster uses stolen information to file a fraudulent tax return in the victim's name. If the victim has not filed a tax return yet, the fraudster can file a return and end up receiving a tax refund from IRS. When the legitimate taxpayer goes to file a tax return, it may be flagged by IRS as a duplicate claim. Many victims are unaware that their identities – and in many cases, their tax refunds – have been stolen until they file their own return and are notified that someone else has already filed in their name. It can take months or even years for IRS to resolve cases of identity theft and issue a tax return to the legitimate taxpayer.

In the last few years, the number of incidents of identity theft-related tax fraud has drastically increased from about 51,700 cases in 2008 to over 1.1 million cases in 2011. This number represents only the known cases of identity theft. The total number of incidents that go undetected is unknown, but the Treasury Inspector General for Tax Administration, or TIGTA, says the number could be much higher. In TIGTA's review of tax returns filed in 2011, TIGTA identified an additional 1.5 million potentially fraudulent returns that were not detected by IRS.

TIGTA and the Taxpayer Advocate have also raised concerns that victims of identity theft do not receive adequate assistance from IRS. In June 2011, this subcommittee heard from three witnesses who had been victims of identity theft and learned that their interactions with IRS were often uninformative, frustrating, or discourteous. One witness stated that, "the way I feel I have been treated by the IRS system has made me a victim a second time." IRS has made efforts to improve its assistance to victims, including creating a Taxpayer Protection Unit and providing better training to their employees. However, there are still significant problems that must be addressed to ensure victims get the assistance they need.

In addition to its impact on victims, identity theft related tax fraud results in a significant loss to the U.S. Government and taxpayers. TIGTA estimates that IRS could issue \$21 billion in fraudulent tax refunds over the next five years resulting from identity theft. The average amount of a fraudulent tax refund is only about \$3,400, so it is often difficult or impossible for IRS to devote resources to investigate every case. Some fraudsters manage to collect millions of dollars

through multiple refunds, though. Given the severity of the problem, we must work to find better deterrents to fraud.

Another key problem is the lack of information IRS has about identity theft related tax fraud. The Government Accountability Office (GAO) has raised concern that IRS needs better performance measures and data collection to help assess the effectiveness of its initiatives to stop fraud. IRS agreed with GAO's recommendation, but there is still a shortage of information about this problem. IRS is also failing to take advantage of information it already possesses, including case files of victims of identity theft. Once a case has been resolved, files are deleted without IRS using this information to identify trends or study them for ways to detect and prevent future fraud.

IRS has launched several pilot programs to combat fraud, and we will hear about them today. One is a Personal Identification Number or PIN, which is given to victims of identity theft. This PIN is used by the victims to identify their returns and add an extra level of security to the legitimate return. IRS also just finished its first pilot of a program designed to share sensitive taxpayer information with local law enforcement officials in order to better investigate fraud. IRS tested this pilot in Florida, and in October IRS expanded the pilot program to eight additional states, including my state of Pennsylvania and Mr. Towns's state of New York.

IRS is working to stop the rise of identity theft related tax fraud and to better detect and prevent fraud. We appreciate their efforts and have followed their work closely throughout this Congress. However, this continues to be a serious problem and continued oversight is needed. Today we will hear from our panel of experts on how to combat identity theft related tax fraud, and how to better assist the victims of this fraud. I look forward to their testimony and want to thank all of our witnesses for their dedication and work in this area.

Subcommittee on Government Organization, Efficiency and Financial Management
Hearing on "Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue
Service, Part IV"

Identity theft and tax fraud are serious and growing problems. According to a July 2012 report from the Treasury Inspector General for Tax Administration (TIGTA), incidents of identity theft reported by the Internal Revenue Service (IRS) have skyrocketed from 51,702 in 2008 to over 1.1 million cases in 2011.

Even though ID theft and the related tax fraud continue to escalate, the IRS has been working diligently to get ahead of the identity thieves. More fraud cases are being detected by IRS filters. As a result, billions of dollars have been kept from the hands of criminals. But more effort is required for us to stay ahead of the criminals and to help the victims.

One of the most important priorities we must address is the quality of assistance given to taxpayers victimized by tax refund fraud. The Inspector General puts it bluntly: the IRS is NOT providing effective assistance to taxpayers who report being victims of identity theft. This must change. It also appears that a better job has to be done tracking ID theft tax fraud cases so that a clear solution can be developed. And most notably, we must increase the prosecution rates of fraudsters to serve as a deterrent to others.

Today's hearing is the fourth in a series held by this subcommittee examining how the IRS handles the problem of identity theft and tax fraud. Our witnesses are all well versed in the issues we will examine today. Each of them has had a hand in identifying problems and crafting solutions to the current crisis. I thank each of you for your appearance and I look forward to their testimony.

I have spent most of my 30 years in Congress pursuing initiatives that have resulted in a better, more efficient federal government. As you have heard, Mr. Platts and I have shared this commitment as we traded the Chairmanship of this subcommittee over the years. Unfortunately, this will be our last hearing. I look to you all and the returning members of this committee to

continue the hard work in the fight for a solution to this problem and all of the other issues that will make our great government a better one.

Mr. Chairman, it has been an honor and a great pleasure working with you. God bless you all!

Contact: Ashley Etienne, Communications Director, (202) 226-5181.

KENNETH H. RYESKY, ESQ., STATEMENT FOR THE RECORD, UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM, SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY, AND FINANCIAL MANAGEMENT, 29 NOVEMBER 2012 HEARING ON IDENTITY THEFT AND TAX FRAUD:

I. INTRODUCTION:

The House Oversight & Government Reform Committee, Subcommittee on Government Organization, Efficiency, And Financial Management, held a Hearing on 29 November 2012, regarding the use of identity theft by tax fraudsters. This Commentary is submitted for the record.

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, as detailed below, commentaries for Congressional hearings regarding identity theft and tax fraud.

As explained in greater detail in previous commentaries, the Commentator has a personal and sometime professional interest in genealogy.

Contact Information: Kenneth H. Ryesky, Esq., Department of Accounting & Information Systems, 215 Powdermaker Hall, Queens College CUNY, 65-30 Kissena Boulevard, Flushing, NY 11367. Telephone 718/997-5070; E-mail: kenneth.ryesky@qc.cuny.edu or khresq@sprintmail.com.

Disclaimer: Notwithstanding consultations between the Commentator and other interested individuals and organizations in the genealogy community, this Commentary reflects the Commentator's personal views, is not written or submitted on behalf of any other person or entity, and does not necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

III. COMMENTARY ON THE ISSUES:

A. *The Instant Hearing and Previous Hearings:*

The instant proceeding of 29 November 2012 is the fourth hearing held by the Subcommittee during the current 112th Congress. Though the relevant House bills are now under the cognizance of the Ways & Means Committee and the Judiciary Committee,¹ the confluence of identity theft and tax fraud commands and demands attention from diverse quarters and constituencies. Indeed, other Congressional hearings on related matters have similarly been conducted before other subcommittees/committees of the House or the Senate.

The Commentator has submitted commentaries for some of those previous hearings.² Those statements are incorporated into this current Commentary by reference.

The testimony at prior hearings has brought to light certain Internal Revenue Service (IRS) practices, policies and procedures which have condoned if not facilitated identity theft in the commission of tax fraud. This includes, but has not been limited to, a recklessness which effectively declined to allow the taxpayer-victim of identity theft to demonstrate that he or she was in fact a victim, while foolishly depending upon the criminal perpetrator of the identity theft to come forward and indicate that he or she has perpetuated the fraud upon the taxpayer-victim and upon the American public.³ In resolving disputes regarding the rightful recipient of mail, the United States Postal Service regularly employs a dispute resolution mechanism far simpler, far more expedient and far more evenhanded which avails each of the disputant parties meaningful opportunity to explain his or her entitlement to the mail delivery, instead of waiting for one of the parties to concede its nonentitlement to the mail.⁴

¹ H.R. 3215, H.R. 3482 and H.R. 6205. Additionally, S. 1534 and S. 3432 are now in the Senate Finance Committee.

² House Ways and Means Subcommittees on Social Security and on Health, 1 August 2012 <<https://docs.google.com/file/d/0B0erD-E9YY0rS3BFZEtpSXhoW1U/edit>>; House Ways and Means Subcommittees on Oversight and on Social Security, 8 May 2012 <<https://docs.google.com/file/d/0B0erD-E9YY0rOXAtamx1cmJYdjQ/edit?pli=1>>, also available at 2012 TNT 95-49; Senate Finance Subcommittee on Fiscal Responsibility & Economic Growth, 20 March 2012, <<http://www.fgs.org/rpac/wp-content/uploads/2012/04/senfincomm-taxfraud-20120320-corrected2.pdf>>, also available at 2012 TNT 56-30; House Ways and Means Subcommittee on Social Security, 2 February 2012, <<http://www.fgs.org/rpac/wp-content/uploads/2012/02/wm-ssdmf-comments-2012.pdf>>, also available at 2012 TNT 25-32.

³ 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>>.

⁴ 39 C.F.R. Part 965; see also *Matter of Blasingame and Blain*, P.S. Docket No. MD 12-58 (14 March 2012) <<http://about.usps.com/who-we-are/judicial/admin-decisions/2012/md-12-58-id.htm>>.

While the previous hearings served to inform the Congress of the nature and extent of the problem, the instant Hearing is effectively a progress report on the IRS's measures to take corrective action. It is important that Congress monitor the IRS's ongoing efforts in addressing the problem, and no less important that the American public see that the IRS has begun some forward motion to bring itself beyond the sorry cluelessness, insolence, indifference and incompetence which has not only facilitated the plunder of United States Treasury, but has also exacted a painful financial and emotional toll from thousands of individual American taxpayers, victims of identity theft, whose only crime was to try in good faith to comply with the tax laws.

As reflected in the testimonies of the witnesses at the instant Hearing, identity theft in tax fraud has many modes and manifestations. Despite having been aware of the problem for well over 10 years,⁵ the IRS still has a far, far path to travel before the problem is brought under any semblance of control.

B. Genealogical Research:

As detailed further in various submissions by the Commentator and by others for previous hearings, genealogical research plays a vital if not indispensable role in several legitimate areas of American life.

These include, but are not limited to, identifying the heirs to a decedent's estate,⁶ the holders of good title to real property,⁷ and qualification for housing loan guarantees.⁸ Genealogical research is often necessary to determine the status of Native American tribes and tribal members.⁹ Moreover, the effective repatriation of artwork looted during the Nazi era requires genealogical research data.¹⁰

⁵ For example, on 26 October 2001, Kipp Holley pleaded guilty to charges in connection with a scheme entailing the filing of multiple false tax returns using expropriated SSNs, claiming false refunds in excess of \$175,000. U.S. Attorney's Office, Southern Dist. of Indiana, Press Release, "New York City Man Sentenced in Tax Refund Conspiracy" (4 January 2002) <http://www.justice.gov/tax/usaopress/2002/txdv0201042002_1.htm>.

⁶ *In re Estate of Wright*, 1997 Del. Ch. LEXIS 26 (Del. Ch., 1997); *Matter of Swinearn*, 2011 N.Y. Misc. LEXIS 6019, 2011 NY Slip Op 33230(U) (Surr. Ct., Nassau Co., 2011); *In re Estate of Turkienicz*, 2008 N.Y. Misc. LEXIS 3117 (Surr. Ct. Bronx Co., 2008); *In re Estate of Rosen*, 819 A.2d 585 (Pa. Super 2003).

⁷ *Eaton v. Town of Wells*, 760 A.2d 232 (Me. 2000).

⁸ 12 U.S.C. § 1715z-13b(a)(6)(B)(i); 24 C.F.R. § 1007.5.

⁹ *James v. Dept. of Health and Human Services*, 824 F.2d 1132, 1138 (D.C.App. 1987); *Muwekma Ohlone Tribe v. Salazar*, 2011 U.S. Dist. LEXIS 110400 at *15 - *16 (Dist. D.C. 2011); *Timbisha Shoshone Tribe v. Dept. of Interior*, 2011 U.S. Dist. LEXIS 51892 at *2 - *3 (E.D. Calif. 2011); *Kirsty*

Genealogical research is often key to determining family medical histories and identifying those susceptible to various types of cancers and other diseases. And genealogical research is used to identify the remains of unclaimed decedents, many of whom are crime victims or military casualties.

If genealogical research is viewed as a hobby, it is a hobby that carries salient implications beyond the mere satisfaction of individual whims and curiosities.¹¹ The United States government has long taken proactive measures to encourage and support philatelic and numismatic hobbyists; genealogy is no less worthy or serious.

C. The Social Security Death Master File:

One major research tool for genealogists is the Social Security Death Master File (DMF).¹² The testimonies at the instant Hearing by Ms. Olson and Ms. Tucker each address the proposed imposition of restrictions upon the release of the DMF.¹³ It has been and continues to be the general contentions of the genealogy community that (A) the IRS can and should stanch the abuse of the DMF as an identity theft vehicle in tax fraud by properly cross-checking and verification of Social Security Numbers (SSNs) of taxpayers and their dependents¹⁴ and by

Gover, *Genealogy as Continuity: Explaining the Growing Tribal Preference for Descent Rules in Membership Governance in the United States*, 33 AM INDIAN L. REV. 243 (2008/2009).

¹⁰ Statement of Catherine A. Lillie, p. p. 26, Review of the Repatriation of Holocaust Art Assets in the United States, Hearing Before the Subcommittee on Domestic & International Monetary Policy, Trade, & Technology, Committee on Financial Services, U.S. House Of Representatives, 109th Cong., 2d Sess., Serial No. 109-113, at p. 26 (27 July 2006) <<http://archives.financialservices.house.gov/pdf/ArchiveHearing/109-113.PDF>>.

¹¹ There are thousands of individuals whose genealogical research activities are not undertaken as a business or occupation. While the genealogical activities of such individuals may be viewed as "hobby" activity for tax purposes, *see* I.R.C. § 183 and Treas. Reg. § 1.183-2, the research regularly accomplished by such individuals is frequently on par with that done by the professional genealogists.

¹² The Death Master File is commercially purveyed via the Internet, in searchable form, as the Social Security Death Index (SSDI).

¹³ Ms. Olson does specifically concede that genealogical research is a "reasonable" and "legitimate use" of the DMF. Olson Testimony at p. 16. <<http://oversight.house.gov/wp-content/uploads/2012/11/Olson-Testimony.pdf>>

¹⁴ The IRS has, in the past, lacked the organizational direction to properly track, process and coordinate Social Security Numbers of spouses, dependents, and related individuals and entities. *See, e.g.* United States v. Nielsen, 1 F.3d 855, 857 (9th Cir. 1993), *cert. denied*, 525 U.S. 827 (1998); Wallin v. Commissioner, 744 F.2d 674, 677 (9th Cir. 1984); United States v. Shafer, 1996 U.S. Dist. LEXIS 56165 (E.D. Pa. 1996); Grimland v. Commissioner, T.C. Memo 1993-367; *In re Washington*, 172 B.R. 415, 418

limiting the unquestioned issuance of multiple refunds to the same address; and (B) removing the DMF would still leave available numerous other sources for fraudsters to obtain SSNs of taxpayers and dependents, living and dead.¹⁵

Nevertheless, given the enormity of the problem, even the staunchest advocates of free and open access to the DMF concede that some restrictions might now be appropriate, and many could support the imposition of a two year embargo upon the release of DMF data such as the ones proposed in § 9 of H.R. 3215, § 11 of H.R. 3482 and § 9 of S. 1534 of the current Congress, provided that certain genealogists, including forensic genealogists, heir researchers, and those researching individual genetically inherited diseases, be eligible for certification for immediate access as provided in the aforementioned bills, and provided that the IRS steps forward to accept its considerable share of the responsibility to address the identity theft/tax fraud problem.

D. Imposing Embargoes:

As this Commentary is being written and submitted, there persists in the Congress a high-profile controversy on the Federal budget; most notably, debate over the appropriate balance between tax increases and spending cuts. A somewhat analogous balancing issue anent to the identity theft/tax fraud problem is the balance between an embargo on the release of the DMF data and an embargo on the remittance of refunds by the IRS.

There obviously are limitations to the amount of time the issuance of an IRS tax refund check ought to be delayed. Many Americans would suffer hardship if the refund check is delayed for too long (particularly in this year of extensive need for rebuilding and recovery from the devastations of Hurricane Sandy). This obviously includes those affected by tax refund anticipation loans.¹⁶

There are several approaches to the embargo of refund remittances. These include, but are not necessarily limited to, the following:

- 419 (Bankr. S.D. Ga. 1994), *see also* Ralph Vartabedian, "IRS Mistakenly Sends Warnings to 90,000 Taxpayers," *The Record* (Bergen Co., NJ), 7 August 1997, p. A22 (IRS fails to recognize its own transition from the TIN-based Form 940 to SSN-based Form 1040 Schedule H for employment taxes with respect to nannies and other household help).

¹⁵ Including the IRS itself. Mr. George's testimony, at 12 - 13, gives just one example of an IRS employee who has been known to expropriate the taxpayers' SSNs and other personal data from the IRS's database. <<http://oversight.house.gov/wp-content/uploads/2012/11/George-Testimony.pdf>>.

¹⁶ See, e.g., GAO Letter to Chairman John Lewis, Ways & Means Committee, GAO-08-800R "Refund Anticipation Loans" (5 June 2008) <<http://www.gao.gov/assets/100/95532.pdf>>.

Refund anticipation loans often figure into identity theft/ tax fraud schemes. See, e.g. United States v. Hill, 683 F.3d 867 (7th Cir. 2012); United States v. Nyamaharo, 364 Fed. Appx. 899 (5th Cir. 2010, *cert. denied* ___ U.S. ___, 130 S. Ct. 2394, 176 L. Ed. 2d 783 (2010); Gatamba v. United States, 2012 U.S. Dist. LEXIS 50804 (N.D. Tex., 2012), *magistrate's findings accepted* 2012 U.S. Dist. LEXIS 50806 (N.D. Tex. 2012).

1. Embargo the refunds claimed on tax returns which claim as a dependent an individual who was claimed as a dependent by another taxpayer for the previous year or two.

2. Embargo the refunds where the multiple tax returns beyond a given number claim remittances to be sent to the same address (allowing for multiple family dwellings) and/or the same bank account.

3. Embargo the refunds claimed on tax returns where the dependent claimed is under 10 years of age (or such other age deemed appropriate) and the SSN of neither the taxpayer claiming the dependent nor such taxpayer's spouse matches the SSN of the parent of such juvenile dependent as claimed on the Form SS-5 Application for a Social Security Card.

4. Embargo according to dollar value tiers if no "red flags" are otherwise present. Example: Refunds less than \$100.00 are sent out immediately, refunds \$100.00 to \$999.99 are embargoed until 1 May, refunds \$1,000 and above are embargoed until 15 May.

[One advantage of Approach 4 above is that it would provide an incentive for taxpayers to timely file their tax returns or timely request an extension to file by the familiar 15 April due date in order to reduce their vulnerability to identity theft by tax fraudsters.¹⁷ In order for such an incentive to be fully effective, the Form 4868 Application for Automatic Extension of Time to File U.S. Individual Income Tax Return would need to be modified to make provision for the taxpayer to enter the SSNs of those to be claimed as dependents (as would the Form 2350 for certain taxpayers living abroad).].

The Next Battlefield in the Tax Fraud Identity Theft War:

Notwithstanding the insistence by some, including witnesses at previous hearings, that the DMF is to blame for the identity theft/tax fraud problem, current events and incidents show that the identity thieves have not been totally dependent upon the SSNs of deceased persons, but are also extensively filing false returns using the identities and SSNs of living persons as well.¹⁸ Clearly, shutting down access to the DMF would only induce the identity thieves to seek out other sources for SSNs, whether of living or deceased individuals.

The Commentator expects to see the identity thieves continue to become increasingly sophisticated, and move onward to the use of business taxpayer identification numbers (TINs) in their tax fraud schemes. TINs are on the W-2 forms issued annually by businesses to their employees to report

¹⁷ The number of taxpayers filing delinquent individual income tax returns, as reflected in the net number of delinquency penalties assessed, has approached 3 million during FY 2011. See IRS Data Book 2011, Table 17 at 42 <<http://www.irs.gov/pub/irs-soi/11databk.pdf>>.

¹⁸ See, e.g. IRS, Examples of Identity Theft Schemes — Fiscal Year 2013 <<http://www.irs.gov/uac/Examples-of-Identity-Theft-Schemes-Fiscal-Year-2013>>; IRS, Examples of Identity Theft Schemes — Fiscal Year 2012 <<http://www.irs.gov/uac/Examples-of-Identity-Theft-Schemes-Fiscal-Year-2012>>.

compensation paid, and are on the various 1099 forms issued to various recipients of money who not employees. Former employees whose separation from their ex-employer was on less than amicable terms may well find enticing the prospect of exacting vengeance against their former employers in addition to the prospects of monetary gain from raiding the public fisc.

F. Conclusion:

The genealogical community appreciates the need to combat identity theft of all types, including identity theft in the context of tax fraud. Notwithstanding the roadblocks that a delay of the release of additions to the DMF would impose upon genealogical research, the genealogy community is could support measures which include a brief embargo for two or three years in order to lessen the burden upon the IRS and avail the IRS better opportunities to address identity theft in tax fraud.

Nevertheless, the DMF is a resource that is rightly in the public domain, and can in fact be put to good use to actually prevent identity theft. Any restrictions upon the DMF's accessibility must be done only to the extent reasonably necessary to secure the integrity of the taxation system, with the IRS and other governmental agencies doing their part to combat the problems of identity theft in the context of tax fraud.

Legislation "simply delaying release of the [DMF] information for several years" has been advocated at this instant Hearing —by Ms. Olson.¹⁹ A scheme along such lines can be crafted to fairly and reasonably balance the public's right to the information in the DMF against the need to ensure the integrity of the taxation system, but such a scheme can work only if the IRS seriously, intelligently and calculatedly applies and deploys its resources and know-how to address the problems of identity theft and tax fraud.

5 December 2012
Respectfully Submitted,



Kenneth H. Ryesky, Esq.

¹⁹ Olson Testimony at p. 13. <<http://oversight.house.gov/wp-content/uploads/2012/11/Olson-Testimony.pdf>>