AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IRS E-FILE AND IDENTITY THEFT

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

FIRST SESSION

JUNE 2, 2011

Serial No. 112–58

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

70–679 PDF WASHINGTON : 2011

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
EDOLPHUS TOWNS, New York
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

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, *Vice Chairman*
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas

EDOLPHUS TOWNS, New York, *Ranking Minority Member*
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
ELEANOR HOLMES NORTON, District of Columbia

CONTENTS

	Page
Hearing held on June 2, 2011	1
Statement of:	
Shulman, Douglas H., Commissioner, Internal Revenue Service	13
White, Jim, Director of Strategic Issues, Government Accountability Office; Sharon Hawa, identity theft victim; Lori Petraco, identity theft victim; and Lavonda Thompson, identity theft victim	41
Hawa, Sharon	60
Petraco, Lori	67
Thompson, Lavonda	73
White, Jim	41
Letters, statements, etc., submitted for the record by:	
Diaz-Balart, Hon. Mario, a Representative in Congress from the State of Florida, prepared statement of Ms. Vas Dagins	10
Hawa, Sharon, identity theft victim, prepared statement of	62
Petraco, Lori, identity theft victim, prepared statement of	70
Platts, Hon. Todd Russell, a Representative in Congress from the State of Pennsylvania:	
Prepared statement of	3
Prepared statement of Ms. Lee	30
Shulman, Douglas H., Commissioner, Internal Revenue Service, prepared statement of	15
Thompson, Lavonda, identity theft victim, prepared statement of	75
Towns, Hon. Edolphus, a Representative in Congress from the State of New York, prepared statement of	5
White, Jim, Director of Strategic Issues, Government Accountability Office, prepared statement of	43

IRS E–FILE AND IDENTITY THEFT

THURSDAY, JUNE 2, 2011

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

The subcommittee met, pursuant to notice, at 1:01 p.m., in room 2247, Rayburn House Office Building, Hon. Todd Russell Platts (chairman of the subcommittee) presiding.

Present: Representatives Platts, Lankford, Amash, Gosar, Guinta, and Towns.

Also present: Representative Diaz-Balart.

Staff present: Ali Ahmad, deputy press secretary; Michael R. Bebeau, assistant clerk; Molly Boyl, parliamentarian; Mark D. Marin, senior professional staff member; Tegan Millspaw, research analyst; Beverly Britton Fraser, minority counsel; and Cecelia Thomas, minority counsel/deputy clerk.

Mr. PLATTS. This hearing of the Subcommittee on Government Organization, Efficiency and Financial Management will come to order. Again, appreciate everyone's patience and flexibility here as we are juggling both the floor schedule and waiting for the full committee's hearing to conclude.

The purpose of today's hearing is to shed light on the growing problem of identity theft-related tax return fraud. Each year, thousands of American taxpayers fall victim to criminals who steal their identities and then use their personal information to claim fraudulent tax refunds.

I am going to submit my full statement for the record, but I would summarize that the three kinds of primary areas of focus that we are going to have today in this hearing is, first, the issue of internal controls at the Internal Revenue Service and the need for those controls to be dramatically improved to prevent fraudulent conduct from taking place, to prevent American taxpayers from being defrauded of millions and millions of dollars each and every year; to focus on the prosecution of these criminals who engage in this fraudulent conduct to make sure that the message is sent that if you defraud the American taxpayer, the American people, you are going to be held accountable; and, third and very importantly, that we do a better job of assisting the hardworking law-abiding American citizens who are victimized by these criminals and then not afforded the level of care and assistance that needs to be provided them by the Federal Government, especially in the case of the Internal Revenue Service, to ensure that these law-abid-

ing citizens are not victimized a second time by the poor assistance or treatment by the Internal Revenue Service.

I will submit my full statement for the record and, with that, I will yield to the ranking member, the gentleman from New York, Mr. Towns.

[The prepared statement of Hon. Todd Russell Platts follows:]

Rep. Todd Platts, Chairman
Subcommittee on Government Organization, Efficiency and Financial Management

Opening Statement - "IRS E-File and Identity Theft."
June 2, 2011

The purpose of today's hearing is to shed light on the growing problem of identity theft-related tax return fraud. Each year, thousands of American taxpayers fall victim to criminals who steal their identities and then use their personal information to claim fraudulent tax refunds.

It can be shockingly simple to steal someone else's tax return. All an identity thief needs is a victim's name and Social Security number. W-2s are not required, so a criminal can make up salary, withholding, and other figures. The IRS is unable to verify these figures until much later in the year, when it receives W-2s from employers. By that time, it is too late and the identity thief has already received a fraudulent tax refund.

Both the General Accountability Office and the Treasury Inspector General for Tax Administration have raised awareness of the growing problem of tax related identity theft in annual reports. In response, the IRS has begun to take steps to address tax fraud. It has implemented more intensive screening procedures for e-File returns, with filters designed to flag fraudulent returns. It has also put in place numerous provisions to help taxpayers after fraud has occurred. The IRS created a new unit to help identity theft victims, and is starting to issue personal identification numbers to legitimate taxpayers who have been victims of identity theft in order to increase security on their returns.

While the IRS deserves credit for its efforts to recognize and address the issue of identity theft as it relates to taxes, this is a huge and growing crime victimizing more and more law-abiding citizens every year. More must be done not only to stop tax fraud, but to help the innocent victims once the fraud has occurred.

Victims usually do not know there is a problem until they file their own tax return and receive a response from the IRS that their return has already been filed. The IRS has established the Identity Protection Specialized Unit to help victims, but according to numerous accounts, some of which we'll hear today, the customer service many people receive from the IRS is far from helpful, courteous, or professional.

It's bad enough that people are having their identities and tax refunds stolen, but victims must often spend hours on the phone, day after day, with IRS representatives who by too many accounts are unsympathetic and rude, trying to convince the IRS that they are who they say they are and have been defrauded. It can often take up to six or more months for victims to satisfactorily prove who they are and finally get their tax return from the IRS. The stories I have heard personally and have read about in the press concern me greatly – legitimate taxpayers who have been victimized deserve courtesy, understanding, and a quick resolution of their case.

I appreciate the willingness of today's witnesses to appear before the Subcommittee to discuss the problems leading to identity theft-related tax fraud as well as what can be done to halt its spread and provide a better response to its victims. I look forward to your testimony.

Mr. TOWNS. Thank you very much, and let me say that I will follow that, I will make certain that I do likewise by submitting my full statement to the record and just indicate that I am really, really proud that the witnesses are coming forth. I think that through this kind of dialog maybe we can get to the bottom of this.

But at the same time, Mr. Chairman, I think it is going to require additional resources to be able to fix this and to make certain that people are not inconvenienced in this fashion. We can do better, and I know we can do better. But the point is that in order to get to where we need to go, we might have to spend some resources to get there to be able to protect people, because I think that we have an obligation and responsibility to do that.

I know that a solution is on the way, but it is going to really require some resources, and I think that members of the committee here might have to recognize that. But at the same time these kind of discussions are very, very important, and on that note I yield back.

[The prepared statement of Hon. Edolphus Towns follows:]

Opening Statement

Rep. Edolphus Towns, Ranking Member Subcommittee on Government Organization, Efficiency and Financial Management

Hearing on "IRS E-File and Identity Theft"

June 2, 2011

Today's hearing on "IRS E-File and Identity Theft" is an important and timely examination of a problem that grows worse for Americans each day. In the last few years, we have seen identity theft evolve not only to victimize the public, but now it is victimizing the United States Treasury.

With this hearing, the committee begins what will be a series of inquiries as to how we can solve the problem of identity theft and the tax fraud which is plundering the Treasury. I want to thank the victims of identity theft who are our witness today. Your stories and experiences will help to shed light on this issue and will help millions of Americans as we work toward a

solution. I also want to thank our witnesses, IRS Commissioner, Mr. Shulman who has responsibility over the entire Internal Revenue Service, and Mr. White from GAO who is also working with the IRS to stay on top of this problem.

In fiscal year 2010, the IRS processed hundreds of millions of tax returns. It collected $2.3 trillion in federal tax payments, and paid about $467 billion in refunds to taxpayers. Due to this significant volume, the IRS has placed extensive reliance on the *E-File* system to efficiently fulfill its tax processing responsibilities. Overall, the number of individuals filing returns electronically has increased from 35 million in 2000 to more than 100 million in 2010.

While the IRS reports that it has stopped over a billion dollars in fraudulent refund claims, the IRS has also identified 470,000 incidents of identity theft affecting 390,000 innocent tax paying citizens. This number is outrageous and unacceptable. It shows that the scam artists and criminals are becoming more bold and

sophisticated as they target Americans and the American government.

Identity theft victims who are also tax fraud victims have to spend countless hours obtaining the necessary documents to prove who they are, while dealing with inconsistent messages and conflicting instructions from customer service agents at the IRS and the taxpayer advocate. Victims are forced to wait months before their cases are resolved and they received tax refunds. Some are even victimized again by the same scam even though the IRS is watching.

Sophisticated criminals keep pushing to government to become more and more creative in our solutions. I know that a solution is on the way but it requires work.

I am looking forward to the testimony of all of our witnesses. With the information we gather at this and other hearings, this Committee will continue to work to put an end to tax refund fraud using stolen identities.

Mr. PLATTS. I thank the gentleman and certainly look forward to working with him and his staff as we have always done so in a bipartisan way, not just today in this hearing, but as we go forward to continue the dialog with the IRS and all interested parties to make sure we do much better in protecting the American taxpayers, protecting our citizens against this type of fraudulent conduct.

I ask unanimous consent to recognize a member of our Appropriations Committee, including one who serves on the committee with oversight over funding regarding the Internal Revenue Service, a gentleman who has had a good number of constituents also defrauded by criminals in this regard, the gentleman from Florida, Mr. Diaz-Balart, for an opening statement and submission for the record.

Mr. DIAZ-BALART. Mr. Chairman, thank you so very much. I want to thank you for, first, your leadership and for indulging me for some minutes this morning. I want to thank you and I want to thank the ranking member and the committee again for your leadership.

Some of you are probably wondering why I am here. Well, some of you may know that South Florida has been one of the most affected areas really in the country when it comes to IRS identity theft issue. What you don't know, I am sure, is that I, years ago, was also a victim of identity theft. Now, I was one of the lucky ones and it wasn't the IRS issue that we are dealing with, but I can tell you what a nightmare it is to deal with if it does happen to you.

It is bad enough going through this traumatic event of having your identity stolen, but then to find out that even a Federal agency cannot protect you against identity theft, frankly, is just beyond disheartening. The fact that so many people who this happens to is, frankly, intolerable and unacceptable, and I think we can all agree that the IRS has been slow, frankly, very slow to respond not only to the individual identity theft issue, but also just overall.

Mr. Chairman, you mentioned that I am on the subcommittee that deals with the funding issue. It is obviously something that we are going to be also looking at there, but before the committee started, Mr. Chairman, if I may kind of say what you and I were talking about. The chairman and I were talking about how, if you use your credit card and you go to a gas station that you don't go to a lot, or you travel or you use it twice in a gas station, like I have done when I will fill up my tank and then I will fill up my wife's tank on one credit card, you will get a call from the credit card company. A red flag goes up.

And this happens kind of regularly. And obviously we don't expect the IRS to be perfect, but clearly there must be a better detailed plan to prevent further fraud issues from taking place and also a plan, as the chairman said, to make sure that taxpayers who have fallen victim to this issue are dealt with in a quicker and more fair fashion.

I will point to you, Mr. Chairman and members of this committee, that a journalist from South Florida, the Sun Sentinel in South Florida, her name is Sally Kestin, has written several really, really good articles on the issue, and I am going to have my staff,

if that is all right with you, give it to the members of the committee. I think they would show you just how bad it is.

I would also like to recognize, as the chairman said, a constituent from south Florida. Her name is Sheila Vas Dagins. She had fallen victim to this crime with the IRS not once, but twice. So imagine that. It is hard enough to go through it once, but imagine having to go through it again. So the IRS was aware of it and somehow, the next year, it happened to her again. So, again, it tells you that the protocols that are there are not effective; a lot needs to be done.

And I again, once again, thank you, Mr. Chairman, for your leadership and this committee. She was not able to be here today to testify, but she has supplied us with her story in a very compelling written testimony, and I would very respectfully, Mr. Chairman, ask to allow me to submit her testimony for the record, if that is possible.

Mr. PLATTS. Without objection, so ordered.

[The information referred to follows:]

Written Statement of Sheila Vosdoganes
Pompano Beach, Florida

To Whom It May Concern:
05/26/2011

We are idenity theft victims. So far it has only effected IRS that we know of, but daily we pray not to hear of our credit also. Working a lifetime to build good credit and have it effected overnight is sad.This has not been just once but for two years in a row. Someone has filed with Internal Revenue Service using my name & social security number. Each time they filed a couple weeks prior to my joint filing on line with my husband. The first year Jan 2010 this person even received a refund. This year they filed again but we do not know if they received payment or not.

Feb 2010 (for year of 2009) our CPA whom has handled our account for over 11 years and is also a friend filed on line for us. It was rejected,saying my number had already been used. We have filed joinly for many years, I have been employed at the same job 23 years, lived at the same address for 11 years, prior address for 14 years. Why are none of these noted on IRS files, so when totaly different information popped up somone noticed ?

In the next 24-36 hours we contacted all agencies that we were told to. Internal Revenue Service, IRS Tax Advocate Service, IRS Protection Unit, Federal Trade Commission, Social Security, local police department and the three major credit agencies. All forms were filed to each as requested. Our personal idenitfication was sent to a Tax Adocate assigned to our case (I had to really force the issue in order to have an advocate assigned both years).

During this time I received the name,address & phone number of where the other refund was mailed. I do not know this person. I do not know how for sure this person got my personal information, as a bookkeeping I am extremely cautious with all paperwork. There as one instant I noted to all as I will list later. We have never contacted this other "Sheila" in any way. At this point I have knowledge that law inforcement or IRS has been in touch with her either. Will this person ever be held accountable at all? A sad justice system it is for us. A of a call yesterday to our local police department, they had visited the woman where my refudn was mailed, and made no progress. They made their report to IRS and were informed IRS would follow up.nothing here has been done that they know of, they were told IRS was handling it.

My first IRS advocate was taken off case & a new one in local area assigned. Very nice lady but the process did not move any faster. It was many months of calls, faxes & letters before we received our due refund in late July. I feel the IRS office's did very little to move anything along faster than normal. We had to be the ones to keep calling IRS and asking what was happening. All this during a time when as an only child my husabnd & I were handling my Mother in Hospice. A time when I personally lost 40 pounds from stress. IRS certainly played a major part of that stress.

I was infromed at that time (2010) a "flag" would be put on our account for the following year so we would not have to experience this again. False. Feb 2011 (for year 2010) once again our on line filing was kicked out. I began the process all over again. Thsi year they did not want to assign an advocate, as I was not a "needy case". After many calls and much pushing they gave in, but also advise me next year that would not be able to help again should this happen. So what good is a "flag" ? What help are these advocates ? Come next year I'm on my own to solve it and try and receive our refund ?

This year we had to once again prove by numerous copies sent to IRS advocate we are the true Nicholas & Sheila Vosdoganes. The first certified package sent to the Pittsburg office was lost. Lost by the US Postal Service for weeks. Sitting in a bin where IRS had not picked it up from what I was told. It was also faxed to the advocate to speed up the process. Ha. No speed from that office. I was informed last week (when I called the advocate again) that the fraud dept was taking a hold off it and it was forthcomming. In the meantime that advocate is now on vacation and we are still waiting for our money. This has been no faster than last year, and honestly there should of been no delay at all. Internal Revenue has all our correct information on file, why should be be penalized for them accecpting a false filing ?

My mother was with Hospice for 17 months prior to her death in Sept 2010. That on top having lost my health insurance at work (paying $400 a month on my own), my husbands health issues, paying three mortgages & two set of condo maintence fees and a job position that after 23 years is shaky. We have our own mortage and a home equity line due to huge assesment and damages in the 2005 hurricane. Then my Mother's condo was up for sale and nothing has happened as of yet, due to this economy. Condo rules do not allow rentals there, nor would they make an exception during her decline. There was no estate left by my Mother, no extra monies to help us thru the rough patches.

Should not some of all these allow the IRS tax advocate office to help me? What are we paying for? We have kept detailed records of dates calls,letters & follow-ups Feb 2010 to the present. Feel badly for anyone that has no direction on how to begin the process, unsure of where to turn.

There is only one place I feel it was even possible our information was at risk. Apx June 2009 we bought a computer thru the Apple store in Fort Lauderdale. At the tiem they had a credit card offering no finance charges fro one year. The credit app. had to be doen in store only. Management assured us this information was cleared out the minsute application was submitted then. We applied & were approved. The bank was Barclay Card.

Then a few months after we received card ,credit etc... Barclay's bank called to ask if I was opening a 2nd credit card. They verified some information with me and I clearing stated no. But was glad they had contacted me. My huband and I went to the manager of the Apple store (also wrote a letter to main office). Explained it all and manager more or less brushed us off. That store, an employee of Apple or Barclay's may have been where this began. We are not on line shoppers and keep our cards & information close at hand.

I personally handle payroll at work. Files are kept tightly guarded.

Apx six weeks ago a newspaper writer in our area began a fantastic series of articles on this subject. Ms. Sally Kestin at The Sun-Sentinel. She has brought this epedimic to light in this area. I am sure until now even our friends found it hard to beleive the red tape we have been experiencing. Her insight & investigation is greatly appreciated.

We would like to see Internal Revenue put into place a stopgap, especially for people that have already been victims once. We heard they may give out pin numbers for filing, but that is only a rumor. No one has suggested of anyway we can avoid this huge issue again next year. Feel like we are hanging by a thread with no lifeline from IRS.

I wish I could be there personally to speak, my writing is far from short or complete.
Any help I could be in this huge fraud system, my husband & myself, please contact us.

Very truly yours,
Sheila Kuhn Vosdoganes

Mr. DIAZ-BALART. Thank you, Mr. Chairman. With that, I just want to thank the committee for your leadership. Thank you, Mr. Chairman, for making this a priority issue. It is a big problem in South Florida, it is a big problem nationally, and as bad as identity theft is, when it happens with the IRS and when people who work hard, pay their taxes, play by the rules, and all of a sudden their refund checks go to some crook, it makes a horrible crime even worse. I cannot thank you enough for your leadership and I thank you for the opportunity to be here this morning. Thank you, Mr. Chairman. I yield back.

Mr. PLATTS. The gentleman yields back.

Just housekeeping for everyone. We are going to recess now because we have about 40 seconds left on the floor vote, the first of seven, so the rest of the Members and I will head to the floor, returning with an estimated start time again at 1:45. And with the agreement of our first panel of witnesses, we are actually going to flip-flop the panels and we will have the IRS Commissioner, Mr. Shulman, when we come back testifying first, then followed by our witness panel with GAO and our citizens.

So we appreciate everyone's flexibility in willing to work with us, your patience, and, thankfully, when we come back we should have a long break before the next series of floor votes, which will allow us then to get into this issue in substance and, as the gentleman from Florida said, really make sure that we do better by all of our constituents and all of our citizens to protect them.

So, with that, the hearing stands recessed until approximately 1:45.

[Recess.]

Mr. PLATTS. This hearing of the Subcommittee on Government Organization, Efficiency and Financial Management will be reconvened.

I know our ranking member, Mr. Towns, does plan on rejoining us coming back from the floor fairly quickly as well. I do want to express regrets for a number of my Democratic colleagues who were planning on being here, but are now on their way to the White House for a Democratic Caucus meeting with President Obama, and they asked me to extend their regrets in not being able to hear the verbal testimony here today, but are glad to receive the written testimony from all of our witnesses.

Again, we appreciate everyone's patience and flexibility as we juggle the schedule.

We are delighted to have with us the 47th Commissioner of Internal Revenue, the Honorable Douglas H. Shulman. Commissioner Shulman, we appreciate your work and the work of your department, and your working with this committee, members and staff, as we try to address this very important issue of how better to protect American taxpayers from being defrauded collectively by tax identity theft or identify theft as tax related, and also to protect each and every citizen who is victimized by these criminals when such fraudulent conduct occurs.

I am not going to go through your whole bio, in the interest of time. You have been very patient as we juggle schedules, as the other witnesses have been, so we will go right to your testimony.

It is the practice of the Oversight Committee to swear all their witnesses in, so if I could ask you to stand and raise your right hand.

[Witness sworn.]

Mr. PLATTS. Thank you, Commissioner. The record will reflect that the witness affirmed that oath and, with that, I will turn it over to you for your statement.

STATEMENT OF DOUGLAS H. SHULMAN, COMMISSIONER, INTERNAL REVENUE SERVICE

Mr. SHULMAN. Chairman Platts, thank you for the opportunity to testify before the committee on the important issue of identity theft.

Before I discuss the efforts the IRS has taken to combat identity theft and to assist its victims, I just want to personally apologize to the taxpayers sitting behind me. I had a chance to talk with them and apologize to them personally. I know that they had a frustrating experience with the IRS. As the head of the IRS, which serves 140 million individual taxpayers, I always stress to our employees that we need to walk in each taxpayer's shoes and understand their specific situation and needs.

And while most taxpayers have a smooth, seamless experience with the IRS, we obviously need to do better with the taxpayers who are here today. On behalf of the agency, I apologize, and I have asked my staff to followup immediately with each one of them to make sure all their issues have been resolved.

Let me talk about identity theft for a minute. First, I want you to know that we take the identity theft issue around the tax system very seriously. Regrettably, by the time that we detect and stop a perpetrator from using someone else's personal information, that victim's data has already been compromised outside of the tax filing process. I think it is very important to state for the record that all of the examples here today, the IRS is not the cause of the identity theft. Rather, the taxpayer's sensitive information was stolen outside the tax system and the perpetrator then uses that stolen identity to try to get a tax refund.

This is a growing problem nationwide, identity theft, and we have seen a fivefold increase of tax-related issues around identity theft in the last 5 years. In 2007, because we saw this as an issue, we created the Office of Information Protection and Data Security. Let me briefly highlight some of the actions we take to try to get ahead of this.

First of all, we set up filters and we stopped about $1 billion since 2008 of potentially fraudulent returns coming in due to identity theft. We have also tried to set up ways to assist victims of identity theft. We put markers on accounts, which puts heightened scrutiny on those accounts when they came through. The key to those markers is setting up the right filters that block the criminals and don't put too much burden on the victims.

While not perfect, we have gotten a lot better. Two years ago 80 percent of the returns that were tripped by our filters ended up being legitimate taxpayers. This year that is almost reversed; 75 percent of the tripped returns ended up being the fraudulent taxpayers. So we are going to keep getting better every year.

We have also, this year, launched a very promising program, which is we have given 56,000 taxpayers a PIN. When they file the return, it will go through if you have the PIN. If a PIN comes in with that Social Security Number with no PIN, it will be blocked. I really think this is the future and I commend my staff for being in front of this and working on it, although it didn't help the folks who did not have a PIN.

I could go on and on. We do a number of other things. We have criminal investigations; we coordinate with the Justice Department, the FBI, the Federal Trade Commission, and I am happy to talk about it in questions.

Before I conclude, let me just turn to the written testimony of the witnesses who experienced unprofessional behavior on the part of some of the phone assisters that they encountered at the IRS. I must tell you, in all candor, that all of my personal experience and the data that I review on a regular basis suggests that our telephone representatives, on a whole, are extremely professional and courteous. All of our customer satisfaction measures, those measured both by the IRS and by external third parties, show that while we run one of the largest phone centers in the world, the IRS manages to provide high quality service with a high degree of accuracy.

With that said, I take these taxpayers at face value that they had a bad experience with the IRS, and I take this very seriously. I believe the conversations we have with victims of identity theft present unique challenges to our assisters. Often it is during the initial conversation with the IRS that the taxpayer is told that they have been victimized.

As we have heard, these can be very emotional conversations and they are very unlike the majority of calls that we receive on a daily basis with specific questions about your account or the tax law. So for many of our assisters, especially the ones on our general toll free line, this may be the first time that they have received a call from a victim of identity theft.

So based on this testimony and what I have heard, I am initiating a thorough review of the training provided to all of our phone assisters to ensure that they have the tools and the sensitivity they need to respond in an appropriate manner to victims of this heinous crime.

Let me conclude by telling you that I realize that in the process of increasing our efforts to block attempts by identity thieves to exploit the tax system, there have been inconveniences and frustrations created for honest, hardworking American taxpayers. For that, I am deeply sympathetic. As identity theft continues to grow as a problem for our country, we need to do our part in the tax system to assist innocent victims.

We have dedicated significant resources over the last few years, streamlining the processes for innocent taxpayers caught up in identity theft. These efforts are starting to pay off, but we are going to need to keep working on it, and you have my commitment that we are going to be focused from this day forward on continuing to improve our operations in this area.

[The prepared statement of Mr. Shulman follows:]

PREPARED STATEMENT
DOUGLAS H. SHULMAN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE
SUBCOMMITTEE ON GOVERNMENT ORGANIZATION, EFFICIENCY AND FINANCIAL MANAGEMENT
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
ON
IDENTITY THEFT
JUNE 2, 2011

Introduction

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, thank you for the opportunity to appear today to discuss identity theft and how it can affect taxpayers when they interact with the Internal Revenue Service (IRS). I will describe the actions the IRS is taking to detect and prevent taxpayer identity theft, and just as importantly, our efforts to work with and help the victims as best we can.

Since 2009, the IRS has protected $929.3 million in refunds from fraudulent returns from being erroneously sent to identity thieves. At the IRS, we understand the victims' frustrations and are committed to working with them to mitigate the consequences of identity theft. This means identifying identity theft issues affecting the tax filing process and getting the victims the tax refunds to which they are entitled as soon as possible.

We have developed a comprehensive identity theft strategy that is focused on preventing, detecting, and resolving instances of tax-related identity theft crimes. In doing so, we are working to ensure that tax filing issues are resolved, and future instances of such crimes are minimized. To carry out this strategy, we put in place prevention measures to stop identity thieves from taking advantage of unsuspecting taxpayers and established new programs and initiatives to educate and support legitimate taxpayers interacting with the IRS. We have made great progress on both fronts.

I want to emphasize that, by the time we detect and stop a perpetrator from using someone else's personal information for his own benefit, the taxpayer-victim's personal data had already been compromised outside the tax filing process. Thus, the IRS was not the cause of the identity theft. The fraud perpetuated by individuals using a taxpayer's stolen identity should be seen within the context of a much larger problem in the United States and across the globe. The public and private sectors are targets of identity theft, including small businesses, large corporations, banks, and other government agencies.

Identity theft is one of the fastest growing crimes in the United States. In fact, for the 11th year in a row, it was the number one consumer complaint received by the Federal Trade Commission (FTC), the Federal agency that is responsible for protecting consumers against identity theft. The FTC reported that, of the almost 1.4 million complaints received in 2010, 19 percent were related to identity theft. Fraud perpetrated against the government in 2010 was the most common form of reported identity theft crime, followed by credit card fraud. For tax years, 2009 through 2011, the IRS has experienced significant increases in tax issues resulting from taxpayers having their personal identification stolen.

Identity Theft and Tax Administration

There are a number of situations in which tax filings are affected by identity theft. For example, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity theft perpetrator will use a stolen

Social Security Number (SSN) to file a forged tax return and attempt to obtain a fraudulent refund early in the filing season. The legitimate owner of the SSN may be unaware that this has happened until he files the return later in the filing season and it is discovered that two returns have been filed using the same SSN. We call this type of identity theft a refund-related crime.

Employment-related identity theft is another way in which an identity thief can take advantage of tax information for personal benefit. This occurs when an identity thief uses someone else's name and SSN in the process of obtaining a job. In this situation, the identity thief's employer will report the employee's wage information to the IRS, just as the legitimate taxpayer's employer reports his legitimate wages. However, if the legitimate taxpayer is unaware that an identity thief is using his SSN for employment, the IRS may conclude that he has not properly reported all earned income and a notice of unreported/underreporting income would be generated and sent to the taxpayer. As a result, the legitimate taxpayer must work with the IRS to resolve his account issues and obtain an identity theft marker on his account.

IRS Actions to Combat and Prevent Tax-Related Identity Theft Crimes

As Commissioner, one of my highest priorities is to ensure that taxpayer information is secure and protected. In doing so, we use various techniques to detect and stop refunds on questionable claims. In addition to using internal screening and data mining processes to evaluate returns submitted to the IRS, we also receive referrals from within the IRS and from external sources that are critical to verifying the validity of a return.

In July 2007, the IRS created the Office of Privacy, Information Protection and Data Security (PIPDS) to provide a centralized privacy program. In creating a centralized office, we recognized the need to develop and implement standardized identity theft processes across all IRS organizations.

Our Criminal Investigation (CI) Division also plays a vital role in the IRS' effort to combat identity theft. CI investigates and detects tax fraud and other financial-related fraud, including identity theft, and coordinates with PIPDS and other IRS offices to ensure that false refunds involving identity theft are identified and addressed as quickly as possible, and that the appropriate steps are taken to mark victims' IRS accounts to help prevent future victimization. CI recommends prosecution of refund fraud, including identity theft, to United States Attorney's Office nationwide.

Prevention and Prosecution

The IRS is working to prevent a taxpayer's personal information from being used by someone else before the tax return is processed. Our internal processes check selected information contained in the return against information in our internal databases. If the return is rejected, the legitimate taxpayer has the option of correcting the return and resubmitting it or filing the return by paper. As we move forward, we continue to refine our systems to ensure that the taxpayer's information is protected.

CI investigates cases involving questionable refund schemes, including refund-related identity fraud, and recommends them for prosecution to the Department of Justice (DOJ). For example, in 2010, 41 schemes of national scope were investigated by CI, demonstrating our commitment to pursue prosecutions having a large impact on U.S. taxpayers. Last year, 95 percent of individuals who DOJ prosecuted for refund-related identity theft went to prison.

As a result of our work in combating abuses in this area, there have been a number of convictions involving identity thieves filing false claims for refunds. For example, in 2011, a California woman was sentenced to 30 months in prison, three years of supervised release, and was ordered to pay more than $800,000 in restitution for participating in such a scheme to defraud the IRS. She pleaded guilty to two counts of mail fraud and one count of aggravated identity theft. In 2010, her husband was also

charged in the indictment and was sentenced to 70 months in prison, three years of supervised release, and ordered to pay restitution for his involvement in the scheme.

In 2009, a Florida man and his wife were sentenced to 22 months and 14 months in prison, respectively. Both defendants were ordered to serve three years of supervised release and to pay almost $400,000 in restitution. A year earlier, they were arrested and charged in a 45 count indictment with conspiracy to defraud the United States, filing false claims, misusing SSNs, and aggravated identity theft. The indictment stated that the defendants obtained the personal identifying information of numerous individuals, and used this information to prepare and file fraudulent Federal income tax returns in those individuals' names.

Taxpayer Outreach

The IRS has undertaken several outreach initiatives to provide taxpayers, employees, and other stakeholders with the information they need to prevent and resolve tax-related identity theft issues proactively. We created IRS Form 14039, *IRS Identity Theft Affidavit*, which is used when a taxpayer is an actual or potential victim of identity theft related to a tax filing and would like the IRS to mark his account to identify any questionable activity. The form makes the process easier and less burdensome for taxpayers, particularly because some police departments will not take identity theft reports.

The IRS has partnered with the DOJ and numerous other Federal agencies in the Financial Fraud Enforcement Task Force to address identity theft. The Task Force's website, STOPFRAUD.gov, has information from each agency about what to do if you suspect you are a victim of identity fraud. This partnership also includes pooling investigative resources to investigate identity theft schemes.

The IRS has also featured information on identity theft in our yearly summer tax forums for the practitioner community. Practitioners are typically the first contact, as

more than 8 out of 10 taxpayers use a return preparer or tax software to prepare their returns. At the forums, our management leaders present information to practitioners on identity theft and online fraud detection and prevention. Approximately 14,000 practitioners participate nationwide in these forums.

Lastly, we continually update the IRS.gov website with the latest identity theft information, including emerging trends, phishing sites, fraud schemes, and prevention strategies. The site also provides key information from other Federal agencies, including the FTC. In March 2011, we issued tax tips with the *"Ten Things the IRS Wants You to Know About Identity Theft"* as part of our external communications during the filing season.

Victim Assistance

The IRS recognizes that outreach alone is not enough, and therefore, we also provide significant assistance to taxpayers whose personal information has been stolen and used by a perpetrator in the tax filing process. Beginning in 2008, the IRS implemented new Service-wide identity theft markers that are placed on a taxpayer's account after a taxpayer provides us with certain substantiation documentation. We developed and implemented a total of eight identity theft markers to address unique types of identity theft issues across the IRS. These markers are used to reduce taxpayer burden by (1) distinguishing legitimate returns from fraudulent returns, (2) tracking taxpayers with identity theft-related tax problems and issues encountered by identity theft victims, and (3) preventing victims from facing the same problems every year. To date, we have identified more than 470,000 incidents of identity theft, of varying degrees of severity, affecting more than 390,000 taxpayers.

If the IRS receives multiple tax returns for the same individual(s), the taxpayer will be asked to substantiate his identity to the IRS by providing a copy of a valid Federal or State issued identification, such as a driver's license, or passport, together with a copy of a police report or a completed *IRS Identity Theft Affidavit*. Once we review and verify

the documentation to determine the rightful taxpayer, the return will be processed, and if a refund is due, the taxpayer will receive it. The taxpayer's account will be marked with an identity theft marker to provide additional protection in the future from identity thieves, beginning with the next filing season. We only require this additional documentation where it is not immediately apparent from the face of the tax return which is legitimate. While there is some utility in comparing returns to prior years, the American taxpaying public is extraordinarily mobile and dynamic. Addresses, employers, and family sizes routinely change every year.

Once the initial identity theft case is resolved, IRS computer systems will systematically evaluate future returns submitted on accounts marked with the identity theft marker. If a return has questionable information on it, the return will be manually reviewed to ensure the return was submitted by the legitimate taxpayer and prevent processing of the return if it is believed to have been submitted by an identity thief.

In addition to programming our systems to detect repeat instances of identity theft, we also developed a new program that will help ensure that taxpayers who were subject to identity theft in the past do not encounter delays in processing their tax returns. In January 2011, we began issuing an Identity Protection Personal Identification Number (IP PIN) that these taxpayers will use when filing their future year's return. IP PIN notices were sent to approximately 56,000 taxpayers allowing them to file a return with the IP PIN. We also revised the 1040 series tax forms for the 2010 tax year to allow for the entry of the IP PIN. Taxpayers will receive a letter with a new unique IP PIN each year that the identity theft marker is active on their account.

The purpose of the PIN is to avoid delays in filing and processing Federal tax returns for taxpayers who have been verified by the IRS to be victims of identity theft. This filing season was a pilot year for the program, and it will be expanded to include more taxpayers beginning next filing season.

In 2008, we also established a special unit to serve as a central contact point for taxpayers who had their identities stolen and wanted to notify the IRS. This unit provides a dedicated toll-free number, staffed by English and Spanish-speaking IRS employees, trained to review taxpayers information and account histories, answer questions, and explain the actions necessary to resolve their identity theft issues. Since its inception, the unit successfully provided service to almost 500,000 taxpayers, while maintaining an 83.4 percent level of service.

We also established an online fraud program to address the increasing and evolving threat of online fraud affecting taxpayers. To combat the highly sophisticated attack methods employed by the fraudsters from all around the world, we are proactively looking for web sites and phishing sites posing as the IRS or legitimate e-file providers and shutting them down as soon as possible. Since the beginning of FY 2009, we shut down 8,296 sites, 610 of which have been shut down in FY 2011.

In addition, we established a relationship with the Internet Crime Complaint Center (IC3), a federal working group responsible for investigating Internet crimes, including identity theft. The IC3 receives Internet-related criminal complaints and researches, develops, and refers the criminal complaints to law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. For law enforcement and regulatory agencies, IC3 provides a central referral mechanism for complaints involving Internet-related crimes, like identity theft.

Internal Checks and Balances

Through process modifications, we have implemented operational changes that have streamlined case resolution and reduced taxpayer burden. One example of this is in the circumstance of two returns filed with a single SSN. This situation can occur from honest mistakes, such as keystroke error. However, it could also be the result of identity theft. In the past, when this occurred and the IRS could not make a determination of the true owner of the SSN, we would take a number of steps, including contacting the SSA,

to resolve the issue. These extra steps could often take a significant amount of time. In the interim, refunds associated with the impacted returns could be frozen while a determination of ownership was made. When there was an identity theft, we found that the frozen return would often end up being that of the legitimate owner of the SSN. This was frustrating for both the taxpayer and the IRS as it would make a bad situation worse for the victim. Upon conducting an internal review, we modified our procedures and empowered our employees to exercise judgment based on certain analytical criteria to streamline and improve the process. I believe that these modifications will allow us to improve our turnaround time for taxpayers impacted by identity theft.

In addition, we have developed and implemented a suite of key performance measures to assist in determining the effectiveness and efficiency of our identity theft program. These performance measures are critical to guide the future direction of the identity theft program, and to continuously improve it.

Conclusion

Thank you again, Mr. Chairman, for the opportunity to appear this morning and update the Subcommittee on how tax filing is affected by identity theft. This is an issue that affects millions of Americans each year. It is not only a matter the IRS is confronting, but this is a concern for many other segments of the economy as well.

It is our goal to provide taxpayers with the best possible service to ensure their interactions with the IRS are efficient and that we meet their needs. In all tax-related identity theft crimes, IRS employees work with each taxpayer victim to resolve his unique situation. Identity theft cases are becoming increasingly complex, involving a dedicated review process to ensure we resolve the case satisfactorily for the victim.

As indicated earlier in my testimony, we have taken steps to establish a more consistent, more proficient, and less burdensome manner for handling these cases. We continue to make great progress in preventing tax-related identity theft before it happens,

and stop it when it does happen as quickly and efficiently as possible. We are also constantly looking for new and innovative ways to improve our processes and techniques and recognize that we must work diligently every day to protect taxpayers and ensure that their personal information is safe and secure.

Mr. PLATTS. I thank the Commissioner for your statement and the commitment you have made as far as going forward. I am certainly grateful for your apology for those witnesses here today and all those who have been victimized and perhaps believe they have not received a level of assistance that they should have received, whether they are here today or around the country.

I think what you have said here, as far as going forward, you all captured in your April 6th address at the National Press Club, and it was about continuous improvement; that since you joined the IRS in 2008 and, in your own words, have made it one of my top priorities to put the IRS on a path of continuous improvement to evolve, to get better. We should perform the best we can today while embracing change so we can perform even better in the future.

I think that is what this is about, especially when we look at the numbers in this area, where we see identity theft-related tax issues jumping about 500 percent in roughly 2½, 3 years, 50,000 or so that we are aware of to over 250,000 in the most recent year.

And I think that goes to your other statement about retraining of the staff who are on the 1–800 number that is, for most constituents, going to be their first point of contact, that commitment you have made to go back and evaluate and strengthen that training, because as we get more and more of these cases, as we are seeing, that is who is going to get that initial call.

And as you reference the written statements of the citizen witnesses who will be testifying a little later today, their description of the treatment they received is pretty outrageous. And not putting words in their mouth, but quoting them, as we will hear from LaVonda Thompson, "I spoke with the most rude and discourteous person I have ever spoken with in my life." Another witness, after dealing with an IRS agent in person in a local IRS office, and feeling so frustrated in how the engagement occurred, I went out to my car and cried; I was very overwhelmed.

This is a case where we have individuals who were victimized and then, in essence, feeling victimized a second time, and your acknowledgment of that and your commitment to go forward to improve the training of your staff is much appreciated. And I am one, as we have talked before, yesterday, who believes in the ideals of public service and am grateful for the work of all public servants, and that includes all of the personnel at the IRS who are out there each day trying to do a good job, and that we not paint with a broad brush in the misconduct of certain individuals to paint a bad picture of any and all IRS agents, personnel. We know that is not the case.

So as a committee we certainly will be grateful to be kept in the loop as you move forward with those training changes or upgrades so that we can make sure that we are doing better with the assistance provided to the victims of identity theft.

A number of issues I would like to address with you. You mentioned about $1 billion in savings that you have prevented from being fraudulently paid out and that the filter system is now identifying, of those that are kicked out, about 75 percent were fraudulent, that would have otherwise been paid out but for being caught. Do you have a number, roughly, what you think in, say, the last

3 years, best estimate of what you have identified what was paid fraudulently and then what, if any, of those dollars have been recouped since being identified?

Mr. SHULMAN. Let me just address that. We have the specific identity theft filters, which are pretty new and evolving. We also have very sophisticated algorithms and filters that kick out a whole bunch of fraud. We block over 2 million returns every year that never go out, and a bunch of those are probably identity theft, because they can be duplicate PINS but they just haven't gotten an identity theft marker, so we don't know what that is. So we don't have a good number as of today around how much potentially went out that we know was identity theft, but it is something that we are going to work on going forward.

The other thing I just would mention, there were a bunch of statements in the testimony that assumed, just because the innocent taxpayer's refund was blocked, that the perpetrator's refund went out, and that is not necessarily the case. There is a bunch of these cases, it happens all the time, where we get a flag on the first one and we are working that; a second one comes in and then it gets a flag because it is a duplicate; and then you have to sort out who is who.

And as I mentioned to you yesterday, we get some where someone has a purse stolen, someone gets their identity, they sell it to 20 people, so we could get multiple filings with the same—it doesn't mean that any of those necessarily go out; a lot of times we are holding them all, trying to sort out exactly who is who and who deserves the refund.

Mr. PLATTS. I understand you don't have an exact amount perhaps that is identity theft related in the rent year or years. Is there a number that you have at this point of how many returns were filed that are identity theft related, whether you know the exact amount or not, that——

Mr. SHULMAN. Our cumulative number is a little over 400,000 since we started tracking those, but those are the ones we have put the marker on. So, for instance, the ones that are coming in this year until the case is resolved the marker is not on it, because sometimes—the most common mistake in tax filing is someone not transcribing their Social Security Number right, so sometimes it is literally somebody misses a number, it goes in. That is not necessarily identity theft, it is what we call a dupe Social Security filing.

But the cumulative number over 3 years has been 400,000 that we have marked as having some identity theft related. Some there has never been a return, but we have found through other criminal investigation a cache of information that has a bunch of Social Security Numbers, so we will mark that. Some the taxpayer identifies; some we find the way that most of the people who testified found out, which is when they file they realize somebody else had filed.

Mr. PLATTS. I know one of the issues you kind of touched on that comes through in the testimony of where a fraudulent return was paid out and then the law-abiding citizen submits and then is told it is going to be 4, 6 months or longer. Can you address that? We have cases that have been brought to our attention where a fraudu-

lent return was paid out within 2 weeks of an E-file being submitted in, say, January or February; then the law-abiding citizen—and that was based on just a name and Social Security Number, and no supporting documentation done in the E-file, and they created an employer ID and income.

But then the law-abiding citizen comes forward with all the documentation, W–2s, all the proper ID to show that they are the legitimate taxpayer. Why is it four, six, or I think in the one witness it was about a year and a half until they got their legitimate refund? I know there is a manpower issue here, but that seems pretty extreme that the victim has to go that long, given how quickly we paid out the fraudulent payment.

Mr. SHULMAN. So one thing I just really want to clarify, because I think there was confusion in much of the press reports and other things. The first return that came in was received and put into our system. That doesn't mean the refunds were paid out. So the refunds weren't necessarily paid out in all those.

But then to address the question of when the real person comes in, what can take so long, one is there were some staffing issues and, as I told you recently, we more than doubled the staff that is working those cases now so that we can get this addressed. Frankly, we just didn't know there was going to be this explosive growth and we were trying to balance budget cuts and potential government shutdowns, and we were managing lots of things during filing season. So once we found out there was growth, we threw more resources at it.

Mr. PLATTS. It that in just this current calendar year?

Mr. SHULMAN. Yes, this current calendar year.

Mr. PLATTS. OK.

Mr. SHULMAN. We are trying to balance resources as we go. Second is there are cases, and one of I think the witnesses described the case where the person had their W–2, had their employer, had their dependent, all those things. When you get all of that, identity theft has become a very serious organized crime, and it is one thing you get a Social Security Number, you file; you probably will trip a filter and get blocked. And if you don't, when the real person comes in, they are obvious.

But sometimes we write to both people and both people come back with a driver's license, with a Social Security Number on it, maybe they have gotten a passport, they know the names of all the dependents, they know what the AGI last year was. That usually means it is some sort of a work-related crime or someone has gotten into some sort of payroll processing system where they get information. And when that happens it can take a while to sort through.

Some of the delay was we had some things sitting on the shelf, waiting for our people to get to it. We think we have addressed a lot of that by putting more people, but sometimes when our analysts get there they have to start making calls to employers, they have to ask for more information. And, again, this can be 30 people that they are trying to unsort those cases. So those will always take really long.

Mr. PLATTS. Understandably.

Mr. SHULMAN. And I guess the other thing I would say is I looked into—there were a lot of public accounts about people, and without getting into any taxpayer, there were lots of public accounts that I saw where someone said someone told me it would take 6 months, but we know for a fact they got their refund within a couple of months and a lot earlier than that. So I think it depends on circumstances.

With that said, it shouldn't take 9 months, it shouldn't take a year and a half, and we should get better at sorting this through. I think the PIN I mentioned is going to be one of the real solutions. Everyone who testified here today we would like to make sure they get a PIN next year, assuming the pilot works as it goes. Their refund will fly through. Anyone else who tries to use their Social Security will just be blocked. It is much better than the flag and the filter, which is a step in the right direction, but the PIN could be the real solution here.

Mr. PLATTS. And I certainly understand where you have a fraudulent claim where they didn't just get a name and Social Security Number, but they got access to all that information, so they are filing correct status, everything is good other than where the money is going, I understand those are going to take a lot longer. Those where it is just a name and Social Security Number—and this kind of comes back to the issue of the training of your staff and how they handle it.

I think maybe as you look at how you improve your training program, is that initial saying we are going to do this as quickly as possible; hopefully, it will be a month or whatever you are going to think is the best case scenario, but it could be 6 months, but please know that we are going to be giving you regular updates. That is part of what I would call an internal control on the training side and the follow-through.

My wife, Leslie, served on the Victims Assistance Board in your county in our home community a number of years back and when you are dealing with victims of crime, it should be one of our highest priorities in how we handle them because it is not just what they lost. Here it is the taxpayer loses the money ultimately, collectively the American taxpayers, but it is a financial impact on the law-abiding citizen who has been victimized, and for those especially who are really looking to that refund to pay whatever pressing bill they have, whatever it may be, there is going to be a financial impact.

But there is really a mental health aspect to it as well, and I think that is what came through to me, not just, again, the witnesses we are going to have here today, but the other cases. I think we have 12 cases that we are currently working in my office, and having talked to my colleagues, Mario Diaz-Balart in Florida and around the country, is that we really look at these individuals appropriately. They have been victimized by criminals, so we really have to prioritize how we go about.

And I think one of those is that regular contact between your agency and those individuals once they have been identified, so they are not sitting out there waiting for knowledge, but kind of get those regular updates.

I am going to touch on one other area that you just mentioned before I turn to the ranking member, and that is in trying to prevent it. And I appreciate that preventive approach.

In fact, in your April 6th statement at the National Press Club, I appreciate that you were looking at how to be proactive and not just catch them after the fact and do something, but to prevent fraud and other misconduct, and I think one of the things you mentioned is about trying to have the employer identification number and information up-front, those W–2 data up-front, rather than getting it, in a sense, after the fact and then trying to play catch-up.

And I realize that is a substantial engagement to pursue, and I think maybe it was good that Congressman Diaz-Balart being here as an appropriator on the subcommittee that directly oversees IRS, as you are looking to make those type of improvements that will prevent fraud up front, that we engage him in what those financial aspects may be as far as making those improvements.

But you mentioned the PIN, the thorough system and putting flags on, and I think one of our witnesses in the next panel will testify that they were supposed to have been flagged and apparently were not properly flagged, so they were a victim of identity theft a second time regarding their refund; whereas the PIN approach seems like it would more likely prevent that.

Where do we stand in that pilot program? I think it was 50-some thousand individuals in the current year. And how quickly do you envision anybody identified as even a possible victim of identity theft being able to get that PIN to try to make certain that only they will be receiving their refund?

Mr. SHULMAN. We have all the data now, although people still file after April 15th, they have gotten themselves an extension. But we have most of the data in. We are looking at it and are parsing it. Like I said, I think it is very positive. My desire would be to expand it dramatically and potentially give it to anyone who has been a victim. For next year we have to balance that against all of the demands, but I think unless we see something that we are not expecting to see by next year, we are going to try to dramatically increase that.

Mr. PLATTS. My hope is that we can move in that direction. In fact, not a witness here today, but one of the victims that has submitted a written statement, Pamela S. Lee, from York, and, without objection, I am going to submit her statement for the record. And in the name of full disclosure, as I have shared with you before, this is a family member, my, I will say, big sister. Although she is in the audience, she stands about 4 feet 10 inches, maybe if that.

[The information referred to follows:]

Pamela S. Lee

York, PA 17402

I filed my income tax return by mail on Feb. 19, 2011. I was due a refund of $4142.28. I filed married filing jointly with one more dependant for a total of 3 dependants. My husband's name is Rick I. Lee and my son is Joseph A. Lee.

I checked on April 1 at "Where's My Refund" on the IRS site and was told electronically that there was some kind of problem (one of many on a list) and my return should be issued by April 19. The site also said that I should not inquire again until after April 19.

I called on April 21 and was told that I had filed duplicate returns. After many questions and on my third IRS representative, I finally learned that an electronic return was filed on January 26, 2011 for $4526 and the money was sent to that person who filed single from a New York address. I was told that I must file IRS form 14039, Identity Theft Affidavit, which I sent by fax on 4/21/11.

My experience on the phone was frustrating and disturbing. Three IRS representatives were rude, impatient and completely lacking in compassion.

1. 8:15 Ms. Wright #1001181346. She told me I had filed a duplicate return but refused to give me any details or any information as to what this meant or what I should do. She put me on hold without telling me she was doing so; she never returned to the phone and after waiting about 15 minutes, I hung up.

2. After waiting on hold again for 15 minutes, the phone was answered by a man who gave his name and number so quickly that I could not understand it. I asked him to repeat is and he again said it so fast that I could not get it. I asked a third time for him to repeat it so I could write it down. He hung up on me. His name sounded like Mr. Lizzy. I could not understand the number.

3. 9:15 or so, Ms. Logan #1000246795. This representative was at first rude and impatient. When I explained things to her, she said at one point, "I got that. You already said it five times." When I said that my frustration was so bad that I might have to call my Congressman, she said, "Why don't you hang up right now and do that." After I asked her to stop yelling at me, she became more cooperative and finally told me that an electronic filing took place on 1/26/11 by someone filing single in my name from a New York address. That person received a return of $4526.00. When I told her that I did not file that return she put me on hold to do some research. She came back and told me I would have to go to www.irs.gov and get form 14039, the Identity Theft Affidavit which I should then fax to the IRS. She told me I should then call back in two weeks to get an update on my case.

I contacted my County Controller who suggested I talk to the DA Detective who told me to file a police report.

I filed a police report with Springettsbury Township, filed a report with Social Security and with the Federal Trade Commission, and checked my credit reports.

I contacted the IRS Identity Theft Hotline at 1-800-908-4490 and was told that I would receive my own return in 4 or more months. She told me that people file fraudulent information with fake W-2's and have the money directly deposited on a money card from places like Walmart so they are impossible to track. She said the law would not permit me to have any information about the fraud committed in my name.

I spoke with LaVonda Thompson who works for the County of York as I do. She had a similar experience. Her phone number is 1-717-683-2236

Two more York County employees have had this happen – Lori Petraco in Juvenile Probation and Renee Lavetan in MHMR

We are working with Donna Austin in Congressman Platts' office to get our returns and with the Congressional Oversight Committee in D.C. to investigate the issue.

Major Concerns

I have learned that the only information needed to file electronically is a matching name and Social Security number. There is no matching of actual W-2 information, so whoever files first with a matching name and SS number gets the refund.

Returns are sent to untraceable cards.

No flags went up when the identity thief used a different address, filing status, employer, and income amount from my own.

I was never contacted when I filed my paper return with actual W-2 forms.

IRS representatives on the phone were impatient, rude, and unhelpful.

Possible Solutions
All filings should be matched to employer filed information.
Large returns filed early should be automatically flagged for follow-up.
Returns with new addresses, employers or filing status should be flagged for follow-up.
Refunds should be sent by check or by direct deposit to a bank account, but not to cards.

Mr. PLATTS. But she is one of these victims, and because of it being a family member, I am most familiar with how her case played out, and the filter system is what really worries me, that if we rely on that, while I am glad it is getting 75 percent of those that are kicked out are ones you want to catch, is how many we are not catching with the filter system, because as in this case, my understanding is it was a different filing status, different employer, different address, different dependents.

I mean, there was one, what I would call that Mario referenced earlier, one red flag after another that I would have thought that filter system would have caught and kicked it out to say, hey, something is askew here. Unfortunately, it didn't. And then when the written returns were received by the IRS, about a month after the fraudulent returns, nothing happened for another 2 months, until the taxpayer, Ms. Lee, then contacted the IRS saying where is my refund.

So now it is 3 months after the fraudulent return was submitted and paid out in January, 2 months after the IRS has received paper documentation that there is something wrong here, yet even then nothing had been done. So that is why I do worry about the filter approach versus getting to the PIN as a way to better protect.

And this may be too broad a sentiment or thought, is there the possibility of getting beyond just the Social Security Number for each and eery taxpayer? What would be the cost of the PIN being sent annually, here is your PIN, not just the half million or so that have been possible identity theft? Is that something you are even considering or is that, because of the additional cost, whether it would be effective or not?

Mr. SHULMAN. If you don't mind, if I could just address the two things that you had mentioned. One is that series of filters, you said why didn't it stop someone?

Mr. PLATTS. Right.

Mr. SHULMAN. I just learned of the taxpayers'—and obviously I can't discuss individual taxpayers publicly——

Mr. PLATTS. Understood.

Mr. SHULMAN [continuing]. But there is nothing to say that it didn't trip a filter or that refund didn't get stopped. So we are going to look into all of these. But I will tell you, like I said, there are 2 million refunds that get stopped, and it is just those kinds of things, if there is enough indicia there. We change these every year; we are very sophisticated. The crooks keep testing all our tolerance levels, but we are very serious about stopping refund fraud.

Mr. PLATTS. And I don't want to imply otherwise. As I have said to you, I know you want to prevent every fraudulent filing and payment as much as I do, and I know that your department, across the board, shares that, and that why the purpose of this hearing is how do we partner with you to help you do just that.

Mr. SHULMAN. On the PIN, it is an interesting idea. As you know, everybody is in very tough fiscal times. My guess is it would be very expensive. We are looking first to expand the PIN. First make sure it works; second, expand it to the group of people most likely to have one of these problems. Right now the Social Security Number is what is used. I think it has been an overstatement in some of the testimony submitted today that all you know is a name

and a Social Security Number, and you automatically get that refund. There are a lot of things that go into looking at that.

With that said, I am very open. As you quoted from a speech earlier this year, we should always be looking at how we do it better, and it is certainly something, as identity fraud goes, we are going to have to figure out how to stay on top of it.

Mr. PLATTS. I do appreciate that it is not necessarily that simple. That is a statement from a conference call with an IRS employee stating that to committee staff, that Social Security Number and name is all you need to E-file and that it is that simple. So that is not just citizens, witnesses making that statement, that is one of your employees saying that to my committee staff.

Mr. SHULMAN. Well, I will look into both the employees who were rude to people on the phone and that employee, then, because there is a lot more that goes into issuing a refund than just a name and Social Security Number.

Mr. PLATTS. I won't identify the individual here.

Mr. SHULMAN. No, I take it at face value what you said.

Mr. PLATTS. But I would be glad to share that information with you. I am not finding the exact one, but we will get it to you, because that seemed to be what was being conveyed to us.

A final question, then I am going to yield to Mr. Towns. Is there any consideration, again, we are looking at ways of how to prevent this wrongdoing, to stop the criminals, protect the innocent. I know in some of these cases, and I don't know if it is consistent or something that you have identified as a consistency in the fraudulent claims. They were filed in January electronically, before most Americans, I know I never get a W–2 until the end of January, the last minute, from the current Federal Government as my employer or from previous employers.

Is there any consideration that is a specific red flag, that anybody who is filing electronically in January, that we look at with extra scrutiny because of the propensity that they are trying to beat the law-abiding citizen who hasn't yet got their W–2s? I am generalizing here, and I may be wrong, but most Americans are not able to file until at least the end of January or into February, until they get their employer information, and then go forward and submit everything. that would be a specific red flag, that anybody filing electronically that early would get extra scrutiny? Is that something that you would consider?

Mr. SHULMAN. I guess there are two things about that. One is a lot of the common perception is that April is when everyone files. The reality is our peak starts January, February, and there are a lot of people who file, as you discussed earlier, people who are really counting on that money, and they will go get from their employer, because most employers, especially large employers who employ large chunks of lower income workers, can make the W–2 available earlier. So there are a lot of people who file who are some of the neediest taxpayers, who really need that money.

Second of all, as we talked about yesterday, I just want to be clear, we have seen no nexus between electronic filing and this identity theft tax-related fraud, because you can get your return in just as quickly by sending overnight mail to us. And the speed

issue, a lot of times it is about whether you get a check or direct deposit and we have to send something to FMS.

So, again, everything is on the table, and I certainly would look at anything, but usually the time is not the issue, because the thing that nobody wrote about, and obviously there wouldn't be a hearing and a lot of interest in it, but we stop lots of people who the legitimate taxpayer filed, got their refund, never knew anything happened, and then the crook comes in later; and we block those too. Obviously, those ones aren't devastating to the victim; the victim—

Mr. PLATTS. Good news doesn't sell, right?

Mr. SHULMAN. But it is certainly something we look at. What I will tell you is we have technologists, statisticians, economists who continually are looking at our screens, refining them year after year, looking at patterns, working with our criminal investigators and other people, and I get briefed on them all through December to make sure we test them; we test them against last year's data, we test them throughout the year.

So we are looking at these filters very carefully and we are trying to get, as Jim White from GAO testifies, the key to these things is stop the bad returns and don't burden the honest taxpayers.

Mr. PLATTS. Am I mistaken though, if you file a paper return, then you do have to have your W–2s? I thought when you file an electronic return, you don't send any W–2s in with that because you are doing it electronically. But if you file by paper, I thought you then did have to file your W–2s with the return.

Mr. SHULMAN. The electronic return usually has, you can do it electronically. We have been working on our E-file. Next year we will be able to actually PDF any attachment to an electronic return.

Mr. PLATTS. But I meant as far as that identity theft is paper or electronic, isn't it harder to do it with paper because you have to have those W–2s attached?

Mr. SHULMAN. A lot of people get them late. What I can tell you is we look, we screen with the same material on paper and electronic.

Mr. PLATTS. Because I am looking for that nexus that you referenced. And I would encourage you, if you see anything with that 75 percent of those that you did kick out and were fraudulent, you know, that analysis, was a large percentage of them in January and what percentage of them was electronic? If your staff could followup with the committee on those two specific issues, that would be great.

Mr. SHULMAN. Sure.

Mr. PLATTS. And my ranking member has been very tolerant of me going very long here. I yield to the former chairman of the full committee and the ranking member of the subcommittee, the gentleman from New York, Mr. Towns.

Mr. TOWNS. Thank you very much. No, I think that your questioning I think is just so important to try to get to the bottom of it and not get involved in terms of a blame game, because we are all in this together. So your questioning I thought was really right on point and to the point.

I am always concerned about if people do things and get away with it, then they will almost encourage them to do it again, because if nothing really happens—and then, of course, others hear that they did it and nothing really happened. So I guess the point that I want to ask you, since 2008 how many prosecutions have there been?

Mr. SHULMAN. So I actually don't have—I will have to come back to you. I don't have a cumulative number, but I put in my testimony and mentioned earlier—

Mr. TOWNS. Mr. Chairman, can we keep the record open so we can receive that?

Mr. PLATTS. Yes.

Mr. SHULMAN [continuing]. Just last year we took to full investigation and recommended to prosecution—and we don't do that if we haven't coordinated with the Justice Department—prosecutions of people who had stolen 50,000 identities that had been used in tax crimes.

So when we prosecute we obviously, like every other agency, we have a very small part of our operation as a criminal investigation division, we have to spread it across terrorist financing, offshore tax evasion, any number of things. As this problem has grown, we have put more resources and plan to continue to put my resources into it, and we try to find prosecutions, A, where we can get the proof but, importantly, ones that impact large numbers of taxpayers is, frankly, the ones that U.S. attorneys will take and work with us on, etc.

So if you look at 50,000, I think the number was actually 56,000 taxpayers who were affected with the prosecutions that we took all the way through our criminal investigation chain, that represented more than a quarter of all the identity theft that was identified, which is a pretty high number for any Federal or, frankly, State or local investigator to be able to followup on that percent.

Mr. TOWNS. Would you know the rate of conviction?

Mr. SHULMAN. What is that?

Mr. TOWNS. Would you know the rate of conviction, have any idea?

Mr. SHULMAN. Very high rate of conviction. I believe it is 95 percent, but let me get back to you for sure on the record.

Mr. TOWNS. How much of the fraudulent paid money has been recovered from thieves?

Mr. SHULMAN. So every year we block billions of dollars of fraudulent refunds. We blocked about $1 billion over 3 years with identity theft. I mentioned to the chairman we haven't tracked specifically identity theft numbers related that has gone out and what we have gotten back, we haven't started tracking that; we plan to as this problem grows. So I don't have a number for you, Mr. Towns.

Mr. TOWNS. You know, my concern is that sometimes we don't have the resources. We know there are things that should be done, but we don't do them because we don't have the resources to do it. And, of course, sometimes in that process the wrong kind of message gets out. So I know that as the Commissioner, that you just can't come up here and bang, bang, bang, saying that you want money, money, money, but the point is that I think that when you see a problem that I think it becomes our responsibility here to

give you additional resources to be able to go out and fix the problem, because if a person is expecting his or her return, and then they don't get it, and then all of a sudden they can't get an answer because, really, somebody else has gotten it, and the frustration around that and the problem, to me, is something that we need to really take very seriously; and I am talking about Members of the Congress as well.

And I agree with the chairman. I was so happy that we had one of the appropriators here today, and I think that if you feel that you need additional resources, don't hesitate to make that case because I think at the end we are going to save money by you doing that, at the end of the day, based on what I am hearing and what has been said here, that if we spend it to fix it, then, in the long run, we will be much better off.

And I know how difficult it is to make the case for resources, especially in this atmosphere and climate, but sometimes we have to do that in order to be able to correct the situation that we now find ourselves in and to make certain that people have the confidence and not to be worried about whether somebody is going to get my return because of my identity.

Let me ask you what department really covers this in your shop? What department, the name of the department that handles this?

Mr. SHULMAN. Handles? I am sorry.

Mr. TOWNS. Handles the claims in terms of the identity. You must have a department that takes a look and handles the identity theft. What is that called?

Mr. SHULMAN. Oh. Well, we have this centralized office of Information Protection, Privacy and Security that sets all policies and coordinates the fraudulent—most of it is in our Waging Investment Division, which deals with individual taxpayers. That is where all the service issues are that we have talked about with the victims' testimony. And then our criminal investigation is the arm, obviously, that follows up on fraudulent schemes that we see.

Mr. TOWNS. Right. Now, was that the department—I know there were some cutbacks. Was that the department that was cut back?

Mr. SHULMAN. Well, we had some cutbacks in every part of the IRS this year.

Mr. TOWNS. Because I am really concerned about making certain that you have the resources to do the job that needs to be done, and that is really where—I think sometimes, you know, we are involved in situations where we have a problem and we know that resources are actually needed to correct the problem, but we do not deal with it.

And we are guilty of that here in the Congress, so I want to let you know that I stand ready to push, to be able to assist you to get what you need to be able to correct this situation, because it is going to grow if you don't, and that is the problem. You see, when people do something and get away with it, they tell others, and then it gets bigger and it gets bigger and bigger, and then the problem becomes one that becomes a lot more costly to be able to handle.

So I think that if we can sort of move forward now and correct some of the things that are going on and send a message forward that this is not something you do. If you do this, you are going to

spend time in jail. I think that point has to be made, because if people do it and they get away with it, they are being encouraged.

Mr. SHULMAN. I couldn't agree with you more. What I will say, and I am obviously biased because I am the Commissioner of the Internal Revenue Service and responsible for this agency, but this problem is a good illustration of why I advocate for the right resources for the IRS, because on one side we need to have the service resources to quickly process the returns and the refunds for the victims, and on the other side we need to get the enforcement resources to pursue this kind of crime.

The service resources I think are fundamental because every American is expected to pay taxes; this isn't a choice, this isn't an optional department. And we owe it to the American citizens to treat them right. The enforcement resources are just obvious from an economic standpoint, where there is a huge return on investment. We return, for our enforcement programs, anywhere from 8 to 1 to 23 to 1, $23 for every $1 we spend, and that doesn't even count, that is conservative accounting that OMB and CBO have come up with; that doesn't count the deterrent effect of people seeing and just never doing it to begin with.

So this is a kind of microcosm of why we always argue this agency is a little different collecting the money for the government because it has a huge return on investment and a real obligation to serve every taxpayer in a way that is dignified and respects their own individual situation.

Mr. TOWNS. But the problem, Mr. Shulman, is that people compare you with other agencies. For instances, talk about in terms of American Express, and they say, well, this person went to purchase something with their American Express card and they called me. But the point is that they can do that because they have the staff and they have the system in place that they paid for to be able to raise these kinds of flags. So that is the point I want to make, because you are going to be compared with them.

In fact, some of my colleagues have already done that today. I was on the floor of the House and a guy came over to me and said he doesn't understand the problem because of the fact that and he went on to talk about in terms of how the credit card company woke him up. He was asleep at 2 a.m., and they called him and said are you making this purchase.

But the point is that in order to do that you have to have staff, you have to have resources, and that is the difference. I also told him there is a big interest on that card, whatever he has, there is a big interest on it, so, therefore, they can hire staff, they can do things and say things. And we just want you to know that we sit here. We are not just going to blame; we want to work with you, and we think that together we can do better.

That is what I am saying. And I know that in order to do that we would have to do some things on this side of the aisle, other than just saying you have to stop it. We have to help you stop it, and I am prepared to do that.

Mr. SHULMAN. Appreciate that.

Mr. TOWNS. On that note, I yield back.

Mr. PLATTS. I thank the gentleman.

Commissioner, we will wrap up quick for you. Just a couple quick followups. One is on the issue that the ranking member raised on the prosecutions. There was a press story in the Sun Sentinel in Florida, end of April, that identified—I will read it verbatim: "Prosecutions for identity theft-related tax fraud are rare. Agents for the Internal Revenue Service who are responsible for criminal investigations have pursued just 412 such cases nationwide since 2007."

Now, they are specifically referencing identity theft-related tax fraud. I take it that you agree that is an inaccurate number?

Mr. SHULMAN. As I told Mr. Towns, I don't have the cumulative number with me, but I will get back for the record.

Mr. PLATTS. If you could.

Mr. SHULMAN. But I think the important thing is a lot of these people are committing, there is one criminal with thousands of taxpayers, so that could represent a lot.

Mr. PLATTS. That may not mean one victim, it might have been 100 victims.

Mr. SHULMAN. Yes. That may very well be the number, but what I am telling you is, as this problem grows, we are going to devote more resources and our investigations will continue to grow and our recommendations to Justice for prosecutions will continue to grow.

Mr. PLATTS. And that kind of follows up with what Ed just said. As a committee, we are an authorizing committee, an oversight committee, we are not appropriators, but we are glad to work with our friends on appropriations in kind of two areas that I think you are looking are doing. One is your manpower commitment to the victims so that, after being victimized by the criminal, that the government does right by them so it is not 6 months or 9 months until they get their legitimate, and that is a manpower issue.

But also a manpower issue of going after the criminals, because if that number is accurate, 412, when we talk about the number of identity theft cases, tax-related going from 50-some thousand to 250-some thousand, obviously that is a very small percentage of prosecutions, if we are accurate in those numbers.

A question on the prosecutions. I know that in IRS statute you are understandably restricted pretty significantly in what information you can share with anybody because you are protecting very personal data. Are there statutory restrictions on you that in some way are preventing your criminal investigation division in working not just with Justice, but with local law enforcement? Because I understand that, as with some of the cases I have heard about or we are going to hear about here today, where it 3,000 or 4,000, and it is not multiple, but one person defrauding using one name and Social Security and information.

When that goes into the Department of Justice and they prioritize all these criminals they are going after, that is probably going to go pretty low in that totem pole because of the amount. But for local law enforcement, they prosecute shoplifters who maybe stole $100 worth of goods. It is something that they know how to do. Is there anything that prohibits the agency from working with local law enforcement so that we can, when we know who the person is, they don't get the message, as Mr. Towns expressed

concerns that, hey, as long as I don't ask for too much, each year I can pocket $3,000 or $4,000 because they are never going to come after me.

And we are sending that message that I am good to go and just don't get too greedy; as long as you don't get too greedy, you are safe. I think to combat that we have to engage, I would contend, local law enforcement. I don't know if, here, today, you know if there is anything that prohibits or restricts it or hinders that.

Mr. SHULMAN. What I will say is I think some of the articles might have overstated the restrictions, but there are some restrictions around specific information. We need to give information that is pertinent to the investigation to know where the investigation is going, etc. I always tell people I got sworn in as IRS Commissioner; when I came back to the office, the people who talk about the laws around taxpayer privacy were in my office, just as an example of how seriously this agency takes data protection. And there are very restrictive laws because we are holding very sensitive information about taxpayers.

We can, though, do coordination with other law enforcement agencies; it is not always just come troll our data bases, look at everything or share everything that comes in, but there are specific things we can do. I would be happy to have further conversations about exactly where there could be some restrictions.

If you don't mind, I also just want to be clear, because I might not have been clear earlier. When you said 250 cases of identity theft with only 400 prosecutions—

Mr. PLATTS. Two hundred fifty thousand.

Mr. SHULMAN. And that those numbers seem skewed. One is 250,000 was the flags that were put on. We put some of those on because we haven't defined a data base or someone called and said my wallet was stolen. So those aren't necessarily anything; there hasn't been a crime committed, it is just a flag so that we can put it through more screening.

Mr. PLATTS. OK.

Mr. SHULMAN. And, second of all, even though last year it was 116 investigations, 41 of them ended up with recommendations for prosecutions, that was still 50,000 taxpayers. So the number was more like 50,000 for 200,000. And I don't know that I was clear earlier.

Mr. PLATTS. Right. Again, because of the likely prosecutions at this point are those more large schemes involving multiple or significant numbers of taxpayer IDs being taken. So the number of cases might be small that you are prosecuting, but the impact is that 50,000 number.

Mr. SHULMAN. Yes. I just wanted to make sure I was clear in my explanation earlier.

Mr. PLATTS. One other item just if you can followup for the record, my earlier questions about of those identified and kicked out as being fraudulent, how many were E-file, how many were in January. Also the issue of how many were asked to be refunded in the form of a debit card versus a check or a direct deposit.

Again, I am looking, trying to help personally so I can better work with you and your agency of what is common issues here that we need to try to look at, and it comes back ultimately to the broad

issue of internal controls and how do we ratchet up our controls to address whatever is most common. Knowing, as you well stated, that the criminals are always going to try stay—whatever we do, they are going to try to get a step ahead of whatever we did, but if we could have that information about the debit card refunds that are identified, that they were asking for refunds and you caught them, but they were looking to get it on a debit card and, again, the belief that maybe is easier and get away with it, versus if they know they have to go to a bank, have some kind of contact with a bank to get that fraudulent refund from that bank.

With that, Mr. Towns, did you have any other questions?

Mr. TOWNS. No.

Mr. PLATTS. I am going to thank you for our testimony, conclude by saying, while I think, as you have referenced in written testimony and we are about to hear from our other witnesses, we do have a lot of progress to make, work to do. Also want to recognize the progress you have made and the commitment that you are making that your understanding of this is a growing problem, it isn't because we asked for this hearing; it is because you are seeing the data as we are looking at it and are out there trying to lead the effort forward in a positive way.

And for those hardworking public employees in the department who are providing great service to hand out, we are grateful for them, and hopefully those who haven't provided that level of service that you clearly want to be provided, that they will learn from their mistakes and do a lot better in the future with the American public that they interact with.

But thank you again for your testimony. Look forward to continue working with you and your staff, and our thanks for being flexible here today with the schedule.

Mr. SHULMAN. Thank you. And if you wouldn't mind, since I was up here at 12 and I had hoped to be here when the other witnesses spoke, I am going to have to step out, but my team is going to stay to followup. But you all do have my apologies again for having a frustrating experience with the IRS.

Mr. PLATTS. And we appreciate your understanding of their testimony from the written and as we discussed yesterday in pretty good detail the subject or the message of their testimony, and your staff's willingness to stay with us is also appreciated. Thank you, Commissioner.

We will take about a 2-minute recess while we get the next panel situated and then begin.

[Recess.]

Mr. PLATTS. We will continue with our second panel. We are honored to have four individuals with us, first, Mr. Jim White, Director of Strategic Issues at the Government Accountability Office. Mr. White, we appreciate not just your presence here today, but day in and day out, you and your colleagues at GAO and the important work you do for all of our Nation, but especially for Congress and the resources that you bring to our work here on the Hill.

As well as three citizen witnesses, unfortunately who have been victims of identity theft as it relates to their tax filings. We have, first, Sharon Hawa from the Bronx; we have Lori Petraco from York, Pennsylvania; and Ms. LaVonda Thompson also of York.

We are grateful for all four of you being here and, as I have said a number of times now, you have been very flexible with us and very patient as we have tried to figure out the hearing schedule around the floor schedule and the full committee, so we are grateful for that.

If I could ask for all four of you to stand so I can swear you in. If you would raise your right hands.

[Witnesses sworn.]

Mr. PLATTS. And the record will reflect that all four witnesses affirmed the oath.

We are going to set the clock at 5 minutes, but if you need a little more time than that, we want you to be able to give your testimony as you see fit, and we are glad to hear it.

Mr. White, we will start with you.

STATEMENTS OF JIM WHITE, DIRECTOR OF STRATEGIC ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; SHARON HAWA, IDENTITY THEFT VICTIM; LORI PETRACO, IDENTITY THEFT VICTIM; AND LAVONDA THOMPSON, IDENTITY THEFT VICTIM

STATEMENT OF JIM WHITE

Mr. WHITE. Chairman Platts, Ranking Member Towns, thank you for inviting me. As you will hear from the victims, ID theft-related tax fraud is an insidious crime. To begin, I want to describe a hypothetical and simplified example of refund fraud, which is illustrated on page 3 of my statement and I think up on the screen.

First, a thief steals a taxpayer's identity. This happens outside of IRS. Second, the thief files a tax return claiming a refund using the name and Social Security Number of the innocent taxpayer. After verifying that the name and Social Security Number match—and this, again, may be simplified—then the IRS issues a refund to the thief. Later, the legitimate taxpayer files a return. At that time IRS discovers two returns have been filed using the same name and Social Security Number. IRS holds up any refund while it notifies the taxpayer of a problem and investigates. The notification from IRS may be when the taxpayer first learns his or her identity has been stolen.

Employment fraud is different, also illustrated on the screen. With employment fraud, a thief uses a stolen name and Social Security Number to get a job. The following year, when taxes are due, the employer reports the income to IRS on a wage statement and the innocent taxpayer files a tax return. IRS matches the two and discovers income reported in the name of the innocent taxpayer that was not included on the taxpayer's return. IRS sends a notice of underreported income to the taxpayer, and that is when the taxpayer and IRS may first learn about the ID theft.

So, to summarize so far, IRS learns about an identity theft affecting taxpayers long after the theft occurs, and available evidence suggests the problem is growing.

Now I want to outline what IRS is doing to resolve taxpayers' ID theft problems, detect fraud, and prevent future problems. Starting in 2004—and the Commissioner summarized some of this—IRS created an ID theft strategy, set up an office to oversee it, put theft

indicators on victims' accounts, screened some returns for fraud, and sets up the Identity Protection Specialized Unit and an ID theft hotline.

In 2009, we recommended that IRS develop measures and data for assessing the effectiveness of IRS's efforts. IRS agreed and has since taken new actions. To help resolve innocent taxpayers' problems, since identity theft makes it appear they either claimed two refunds or underreported their wage income, IRS is placing a temporary ID theft indicator on accounts, while still investigating. The purpose is to alert all IRS offices that ID theft may be the explanation for what appears to be tax evasion.

To detect ID theft-related tax fraud, IRS screens returns filed in the names of past victims. The screens are not perfect. If, for example, IRS screens out returns with a change of address, it will slow refunds to some legitimate taxpayers who moved. If it screens too loosely, more fraudulent returns get through. This year, about 200,000 returns failed the screens; 146,000 were fraudulent; and 50,000 were innocent. Also, IRS is experimenting with screens for the Social Security Numbers of deceased taxpayers to try to prevent thieves from filing using those identities.

Another new step gives past fraud victims special PIN numbers. IRS screens out returns filed in the names of those taxpayers unless the PIN is attached.

IRS's ability to address identity theft is constrained by law, timing, and resources. The laws governing the privacy of taxpayer data limit to some extent, as the Commissioner also described, IRS's ability to disclose information about suspected ID thieves to Federal, State, or local law enforcement agencies unless certain conditions are met. Complicating any investigation is the fact that IRS typically discovers the ID theft long after it occurred.

Finally, criminal investigations require resources. Last year, IRS initiated about 4,700 criminal investigations of all types, including ID theft, tax evasion, money laundering, and other financial crimes, far fewer than the number of ID theft cases.

Given all of this, can IRS do more? Options exist, but they come with tradeoffs. IRS could screen tax returns filed in the names of known identity theft victims more tightly, but that will increase the number of false positives and delay refunds to those taxpayers. It could also burden employers who could be contacted about reported wages.

Looking forward, IRS needs to continue assessing its efforts, such as PINs and screens, for deceased taxpayers to learn what is effective. We have not assessed the effectiveness of these steps. In the long term, IRS should be looking at how to take more advantage of the new processing systems it is building. With better processing, IRS might some day be able to match tax returns to wage statements before refunds are issued and thus prevent more refund fraud. However, such pre-refund matching would require employers to file wage statements earlier in the year.

Mr. Chairman, that completes my statement. I would be happy to take questions.

[The 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 12:30 p.m. EDT
Thursday, June 2, 2011

TAXES AND IDENTITY THEFT

Status of IRS Initiatives to Help Victimized Taxpayers

Statement of James R. White, Director
Strategic Issues

GAO-11-721T

June 2, 2011

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-11-721T, testimony before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, House of Representatives

TAXES AND IDENTITY THEFT

Status of IRS Initiatives to Help Victimized Taxpayers

Why GAO Did This Study

Identity theft is a serious and growing problem in the United States. Taxpayers are harmed when identity thieves file fraudulent tax documents using stolen names and Social Security numbers. In 2010 alone, the Internal Revenue Service (IRS) identified over 245,000 identity theft incidents that affected the tax system. The hundreds of thousands of taxpayers with tax problems caused by identity theft represent a small percentage of the expected 140 million individual returns filed, but for those affected, the problems can be quite serious.

GAO was asked to describe, among other things, (1) when IRS detects identity theft based refund and employment fraud, (2) the steps IRS has taken to resolve, detect, and prevent innocent taxpayers' identity theft related problems, and (3) constraints that hinder IRS's ability to address these issues.

GAO's testimony is based on its previous work on identity theft. GAO updated its analysis by examining data on identity theft cases and interviewing IRS officials.

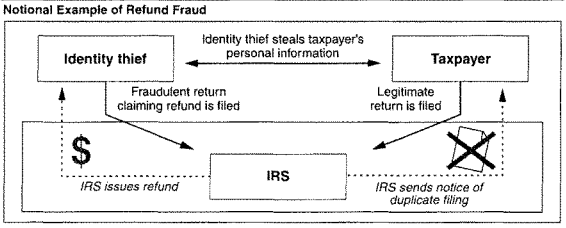
GAO makes no new recommendations but reports on IRS's efforts to address GAO's earlier recommendation that IRS develop performance measures and collect data suitable for assessing the effectiveness of its identity theft initiatives. IRS agreed with and implemented GAO's earlier recommendation.

View GAO-11-721T or key components.
For more information, contact James R. White at (202) 512-9110 or whitej@gao.gov.

What GAO Found

Identity theft harms innocent taxpayers through employment and refund fraud. In refund fraud, an identity thief uses a taxpayer's name and Social Security Number (SSN) to file for a tax refund, which IRS discovers after the legitimate taxpayer files.

Notional Example of Refund Fraud



Source: GAO.

In employment fraud, an identity thief uses a taxpayer's name and SSN to obtain a job. When the thief's employer reports income to IRS, the taxpayer appears to have unreported income on his or her return, leading to enforcement action.

IRS has taken multiple steps to resolve, detect, and prevent employment and refund fraud:

Resolve—IRS marks taxpayer accounts to alert its personnel of a taxpayer's identity theft. The purpose is to expedite resolution of existing problems and alert personnel to potential future account problems.

Detect—IRS screens tax returns filed in the names of known refund and employment fraud victims.

Prevent—IRS provides taxpayers with information to increase their awareness of identity theft, including tips for safeguarding personal information. IRS has also started providing identity theft victims with a personal identification number to help identify legitimate returns.

IRS's ability to address identity theft issues is constrained by

- privacy laws that limit IRS's ability to share identity theft information with other agencies;
- the timing of fraud detection—more than a year may have passed since the original fraud occurred;
- the resources necessary to pursue the large volume of potential criminal refund and employment fraud cases; and
- the burden that stricter screening would likely cause taxpayers and employers since more legitimate returns would fail such screening.

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

I am pleased to be here to discuss how identity theft harms taxpayers and how the Internal Revenue Service (IRS) works to resolve, detect, and prevent these problems. Identity theft is a serious and growing problem in the United States. According to the Federal Trade Commission (FTC), millions of people have been victims of the crime, some of whom may go years without knowing it. Within the tax system, a taxpayer may have his or her tax refund delayed if an identity thief files a fraudulent tax return seeking a refund using the legitimate taxpayer's identifying information. Taxpayers may also become subject to IRS enforcement actions after someone else uses the identity theft victim's identity to fraudulently obtain employment and the thief's income is reported to IRS by an employer in the victim's name. In 2010 alone, IRS identified over 245,000 identity theft incidents that affected the tax system. The hundreds of thousands of taxpayers with tax problems caused by identity theft represent a small percentage of the expected 140 million individual returns filed, but for those affected, the problems can be quite serious.

My testimony today will cover (1) when IRS detects identity theft-based refund and employment fraud, (2) the steps IRS has taken to resolve, detect, and prevent innocent taxpayers' identity theft-related problems, (3) constraints that hinder IRS's ability to address these issues, and (4) the potential for more rigorous screening to prevent refund or employment fraud now and in the future. My testimony is based on our previous 2009 and 2011 reports.[1] IRS agreed with and implemented our recommendation in our 2009 identity theft report to develop performance measures and collect data suitable for assessing the effectiveness of its identity theft initiatives. We updated our analysis with current data on identity theft cases and interviewed IRS officials in the Office of Privacy, Information Protection and Data Security (PIPDS). 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.

[1]GAO, *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) and *Taxpayer Account Strategy: IRS Should Finish Defining Benefits and Improve Cost Estimates*, GAO-11-168 (Washington, D.C.: Mar. 24, 2011).

Our prior reports and this May 2011 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 new information in this statement with IRS officials, and they concurred with our findings.

IRS and Taxpayers May Not Discover Refund or Employment Fraud until after Legitimate Tax Returns Are Filed

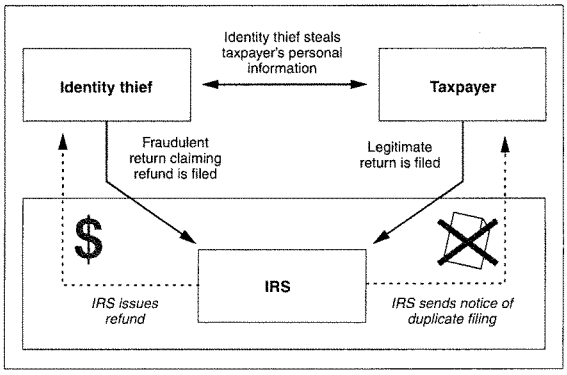
The number of tax-related identity theft incidents (primarily refund or employment fraud attempts) identified by IRS has grown:

- 51,702 incidents in 2008,
- 169,087 incidents in 2009, and
- 248,357 incidents in 2010.

Refund Fraud Delays Innocent Taxpayers' Refunds

Refund fraud can stem from identity theft when an identity thief uses a legitimate taxpayer's name and Social Security Number (SSN) to file a fraudulent tax return seeking a refund. In these cases, the identity thief typically files a return claiming a refund early in the filing season, before the legitimate taxpayer files. IRS will likely issue the refund to the identity thief after determining 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). IRS often first 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 Refund Fraud

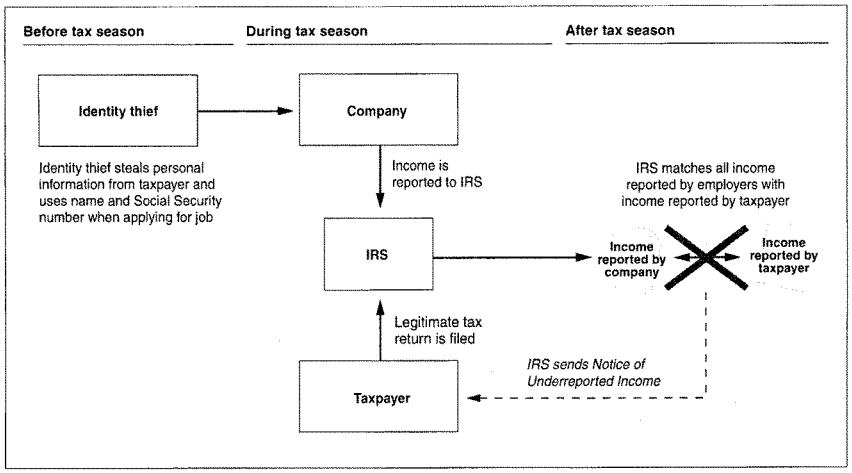


Source: GAO.

Employment Fraud Exposes Innocent Taxpayers to Enforcement Actions for Unreported Income

Employment fraud occurs when an identity thief uses a taxpayer's name and SSN to obtain a job. IRS subsequently receives income information from the identity thief's employer. After the victim files his or her tax return, IRS matches income reported by the victim's employer and the thief's employer to the tax return filed by the legitimate taxpayer, as shown in figure 2. IRS then notifies the taxpayer of unreported income because it appears the taxpayer earned more income than was reported on the tax return. Employment fraud causes tax administration problems because IRS has to sort out what income was earned by the legitimate taxpayer and what was earned by the identity thief.

Figure 2: Notional Example of Employment Fraud



Source: GAO.

To Date, Known Cases of Identity Theft Have Occurred outside IRS

The name and SSN information used by identity thieves to commit refund or employment fraud are typically stolen from sources beyond the control of IRS. IRS officials told us they are unaware of any incidents where information was stolen from IRS and used to commit employment or refund fraud. However, there are risks at IRS. In a recent audit, we found that although IRS has made progress in correcting previously reported information security weaknesses, it did not consistently implement controls intended to prevent, limit, and detect unauthorized access to its

systems and information, including sensitive taxpayer information.[2] In 2009, we also reported that third-party software used to prepare and file returns may pose risks to the security and privacy of taxpayer information.[3] IRS agreed with our recommendations to address these and other issues. We recently followed up with IRS on this issue and learned that IRS has begun monitoring adherence to security and privacy standards in the tax software industry.

IRS Has Taken Multiple Steps to Resolve, Detect, and Prevent Employment and Refund Fraud

In 2004, IRS developed a strategy to address the problem of identity theft–related tax administration issues. According to IRS, the strategy has evolved and continues to serve as the foundation for all of IRS's efforts to provide services to victims of identity theft and to reduce the effects of identity theft on tax administration.

Indicators—account flags that are visible to all IRS personnel with account access—are a key tool IRS uses to resolve and detect identity theft. IRS uses different indicators depending on the circumstances in which IRS receives indication of an identity theft–related problem. Once IRS substantiates any taxpayer-reported information, either through IRS processes or the taxpayer providing documentation of the identity theft, IRS will place the appropriate indicator on the taxpayer's account and will notify the taxpayer. IRS will remove an indicator after 3 consecutive years if there are no incidents on the account or will remove an indicator sooner if the taxpayer requests it.

The three elements of IRS's strategy are resolution, detection, and prevention.

Resolution. Identity theft indicators speed resolution by making a taxpayer's identity theft problems visible to all IRS personnel with account access. Taxpayers benefit because they do not have to repeatedly explain their identity theft issues or prove their identity to multiple IRS units. Indicators also alert IRS personnel that a future account problem may be

[2]GAO, *Information Security: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data*, GAO-11-308 (Washington, D.C.: Mar. 15, 2011). We made recommendations for corrective action, and IRS agreed to develop a detailed corrective action plan to address each recommendation.

[3]GAO, *Tax Administration: Many Taxpayers Rely on Tax Software and IRS Needs to Assess Associated Risks*, GAO-09-297, (Washington, D.C.: Feb. 25, 2009).

related to identity theft and help speed up the resolution of any such problems.

Since our 2009 report, IRS developed a new, temporary indicator to alert all IRS units that an identity theft incident has been reported but not yet resolved. IRS officials told us that they identified a need for the new indicator based on their ongoing evaluation of their identity theft initiatives. The temporary indicator's purpose is to expedite problem resolution and avoid taxpayers having to explain their identity theft issues to multiple IRS units.

As discussed in our 2009 report, taxpayers with known or suspected identity theft issues can receive assistance by contacting the Identity Protection Specialized Unit.[4] The unit operates a toll-free number taxpayers can call to receive assistance in resolving identity theft issues.

Detection. IRS also uses its identity theft indicators to screen tax returns filed in the names of known refund and employment fraud victims. During the 2009, 2010, and 2011 filing seasons, IRS screened returns filed in the names of taxpayers with identity theft indicators on their accounts. There are approximately 378,000 such taxpayers. In this screening, IRS looks for characteristics indicating that the return was filed by an identity thief instead of the legitimate taxpayer, such as large changes in income or a change of address. If a return fails the screening, it is subject to additional IRS manual review, including contacting employers to verify that the income reported on the tax return was legitimate. In addition to U.S. taxpayers with indicators on their accounts, IRS officials also told us that they screened returns filed in the name of a large number—about 350,000—of Puerto Rican citizens who have had their U.S. SSNs compromised in a major identity theft scheme.[5]

As of May 12, 2011, 216,000 returns filed in 2011 failed the screens and were assigned for manual processing. Of these, IRS has completed processing 195,815 and found that 145,537 (74.3 percent) were fraudulent.

[4]GAO-09-882.

[5]The number of accounts with indicators is not the same as the number of returns that are screened. A single taxpayer account, for example could be subject to many refund fraud attempts.

In January 2011, IRS launched a pilot program for tax year 2010 returns (due by April 15, 2011) using a new indicator to "lock" SSNs of deceased taxpayers.[6] If a locked SSN is included on a tax return, the new indicator will prompt IRS to automatically reject the return. PIPDS officials told us they intend to expand the pilot to include more SSNs of deceased taxpayers after analyzing the results of the initial pilot.

A program IRS uses to identify various forms of refund fraud—including refund fraud resulting from identity theft—is the Questionable Refund Program. IRS established this program to screen tax returns to identify fraudulent returns, stop the payment of fraudulently claimed refunds, and, in some cases, refer fraudulent refund schemes to IRS's Criminal Investigation offices.

Prevention. As described in our 2009 report, IRS has an office dedicated to finding and stopping online tax fraud schemes.[7] IRS also provides taxpayers with targeted information to increase their awareness of identity theft, tips and suggestions for safeguarding taxpayers' personal information, and information to help them better understand tax administration issues related to identity theft. Appendix I summarizes information IRS and FTC provide to taxpayers to protect themselves against identity theft.

Since our 2009 report,[8] IRS began a pilot program providing some identity theft victims with a 6-digit Identity Protection Personal Identification Number (PIN) to place on their tax return. IRS officials told us they created the PIN based on their ongoing evaluation of their identity theft initiatives. When screening future years' returns for possible identity theft, IRS will exclude returns with a PIN, which will help avoid the possibility of a "false positive" and a delayed tax refund. IRS sent letters containing an identity theft PIN to 56,000 taxpayers in the 2011 filing season. IRS will provide taxpayers a new PIN each year for a period of 3 years following an identity theft.

[6]The pilot consists of 6,000 deceased taxpayers who died before 2009, but filed returns in 2009. IRS selected these taxpayers for the pilot because of the high probability the taxpayers' returns were fraudulent.

[7]GAO-09-882.

[8]GAO-09-882.

IRS's Ability to Address Identity Theft Issues Is Constrained by Law, Timing, and Resources

Privacy and Other Laws Limit IRS's Coordination with Other Agencies and Taxpayers

IRS's initiatives to address identity theft are limited in part because 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.[9] As discussed in more detail in our 2009 report, IRS can disclose identity theft–related events that occur on a taxpayer's account to the taxpayer, such as the fact that an unauthorized return was filed using the taxpayer's information or that the taxpayer's SSN was used on another return. However, IRS cannot disclose to the taxpayer any other information pertaining to employment or refund fraud, such as the perpetrator's identity or any information about the perpetrator's employer. Additionally, IRS has limited authorities to share identity theft information with other federal agencies. When performing a criminal investigation, IRS can make only investigative disclosures, that is, the sharing of specific, limited information necessary for receiving information from other federal agencies that might support or further IRS's investigation. Disclosure of taxpayer information to state and local law enforcement agencies is even more limited.

IRS Is Often Unable to Detect Suspicious Cases until after the Fraud Has Occurred

Because of the timing of tax return filing, IRS is often unable to detect suspicious cases until well after the fraud occurred. Validating the identity theft and substantiating the victim's identity takes further time. For example, IRS may not be able to detect employment fraud until after the following year's tax filing deadline of April 15 when it matches income reported by employers against taxpayers' filed returns. It is only after IRS notifies a taxpayer of unreported income that IRS may learn from the taxpayer that the income was not the taxpayer's and that someone else must have been using his or her identity. By the time both the victim and IRS determine that an identity theft incident occurred, well over a year may have passed since the employment fraud.

[9]Section 6103 of Internal Revenue Code.

IRS Does Not Pursue Criminal Investigations in Every Case of Potential Refund and Employment Fraud because of Resource Priorities

IRS officials told us that IRS pursues criminal investigations of suspected identity thieves in only a small number of cases. IRS's Criminal Investigations (CI) Division's investigative priorities include tax crimes, such as underreporting income from legal sources; illegal source financial crimes; narcotics-related financial crimes; and counterterrorism financing. In fiscal year 2010, CI initiated 4,706 investigations of all types, a number far smaller than the total number of identity theft–related refund and employment fraud cases identified in that year.

Also, the decision to prosecute identity thieves does not rest with IRS. CI conducts investigations and refers cases to the Department of Justice (DOJ), which is responsible for prosecuting cases in the federal courts. IRS officials said that the small number of tax-related identity theft cases that they investigate recognizes that DOJ has to conclude that the case is of sufficient severity that it should be pursued in the federal courts before it will be prosecuted. According to data from CI included in our prior report, the median amount of suspected identity theft–related refunds identified in the 2009 filing season was around $3,400.

CI has investigated tax-related identity theft cases that DOJ has successfully prosecuted. In our prior report we cited the example of a former Girl Scout troop leader serving 10 years in federal prison for stealing the SSNs of girls in her troop and then claiming more than $87,000 in fraudulent tax refunds.

Improved Detection of Employment and Refund Fraud Must Be Balanced against Burdens on Innocent Taxpayers and Costs

Options exist, now and in the future, to improve detection of identity theft–related tax fraud, but they come with trade-offs.

Known identity theft victims. IRS could screen returns filed in the names of known identity theft victims more tightly than is currently done. More restrictive screening may detect more cases of refund fraud before IRS issues refunds. However, more restrictive screening will likely increase the number of legitimate returns that fail the screenings (false positives). Since returns that fail screening require a manual review, this change could harm innocent taxpayers by causing delays in their refunds. Using more restrictive rules would also place additional burden on employers because IRS contacts employers listed on all returns that fail screening.

All taxpayers. Beyond screening returns with known tax-related identity theft issues, screening all tax returns for possible refund fraud would pose similar trade-offs, but on a grander scale. For example, as noted above,

one way to check for identity theft is to look for significant differences between current year and prior year tax returns, but this could be confounded by a large number of false positives. IRS officials told us that in 2009 there were 10 million address changes, 46 million changes in employer, and millions of deaths and births. Checking all returns that reflect these changes for possible refund fraud could overwhelm IRS's capacity to issue refunds to legitimate taxpayers in a timely manner.

Looking Forward. IRS's identity protection strategy and the creation of PIPDS were part of an effort to more efficiently identify refund and employment fraud as well as to assist innocent taxpayers. Since adopting the recommendation in our 2009 report regarding using performance measures to assess effectiveness,[10] IRS has followed through, using its improved performance information to identify additional steps it could take. These include the new indicators for taxpayer accounts, improved routing of suspect returns, and PIN numbers. However, none of these steps will completely eliminate refund or employment fraud. By continuing to monitor the effectiveness of its identity theft initiatives, IRS may find additional steps to reduce the problems faced by both taxpayers and IRS.

Looking further forward, other long-term initiatives underway at IRS have at least some potential to help combat identity theft–related fraud. In April 2011, the Commissioner of Internal Revenue gave a speech about a long-term vision to increase up-front compliance activities during returns processing. One example is to match information returns with tax returns before refunds are issued. Before this could happen, IRS would have to make significant changes. Third-party information returns would have to be filed with IRS earlier in the filing season.[11] IRS would also have to improve its automated processing systems; IRS's current Customer Account Data Engine (CADE 2) effort is one key step.[12] While these efforts are part of a broad compliance improvement vision, they could also detect some identity theft–related fraud. If, for example, IRS could match employer information to tax returns before refunds are issued, identity thieves could not use phony W-2s to claim fraudulent refunds.

[10]GAO-09-882.

[11]Many information returns, such as forms W-2 filed by employers, are not due to the government until the end of February.

[12]GAO-11-168.

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 Acknowledgments

For further information on this testimony, please contact James R. White at (202) 512-9110 or whitej@gao.gov. In addition, 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; Donna Miller; Erika Navarro; Melanie Papasian; and Sabrina Streagle made key contributions to this report.

Appendix I: Things Taxpayers Can Do to Protect Themselves if They Suspect Identity Theft

Both the Internal Revenue Service (IRS) and the Federal Trade Commission (FTC) provide helpful information to taxpayers to deter, detect, and defend against identity theft. IRS provides taxpayers with targeted information to increase their awareness of identity theft, tips and suggestions for safeguarding taxpayers' personal information, and information to help them better understand tax administration issues related to identity theft. For example, IRS has published on its website the list in table 1 below.

Table 1: IRS's Top 10 Things Every Taxpayer Should Know about Identity Theft

1.	The IRS does not initiate contact with a taxpayer by e-mail.
2.	If you receive a scam e-mail claiming to be from the IRS, forward it to the IRS at phishing@irs.gov
3.	Identity thieves get your personal information by many different means, including: • Stealing your wallet or purse • Posing as someone who needs information about you through a phone call or e-mail • Looking through your trash for personal information • Accessing information you provide to an unsecured Internet site.
4.	If you discover a website that claims to be the IRS but does not begin with 'www.irs.gov', forward that link to the IRS at phishing@irs.gov
5.	To learn how to identify a secure website, visit the Federal Trade Commission at www.onguardonline.gov/tools/recognize-secure-site-using-ssl.aspx
6.	If your Social Security number is stolen, another individual may use it to get a job. That person's employer may report income earned by them to the IRS using your Social Security number, thus making it appear that you did not report all of your income on your tax return.
7.	Your identity may have been stolen if a letter from the IRS indicates more than one tax return was filed for you or the letter states you received wages from an employer you don't know. If you receive such a letter from the IRS, leading you to believe your identity has been stolen, respond immediately to the name, address or phone number on the IRS notice.
8.	If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost wallet, questionable credit card activity, or credit report, you need to provide the IRS with proof of your identity. You should submit a copy of your valid government-issued identification – such as a Social Security card, driver's license, or passport – along with a copy of a police report and/or a completed Form 14039, Identity Theft Affidavit. As an option, you can also contact the IRS Identity Protection Specialized Unit, toll-free at 800-908-4490. You should also follow FTC guidance for reporting identity theft at www.ftc.gov/idtheft
9.	Show your Social Security card to your employer when you start a job or to your financial institution for tax reporting purposes. Do not routinely carry your card or other documents that display your Social Security number.
10.	For more information about identity theft – including information about how to report identity theft, phishing and related fraudulent activity – visit the IRS Identity Theft and Your Tax Records Page, which you can find by searching "Identity Theft" on the IRS.gov home page.

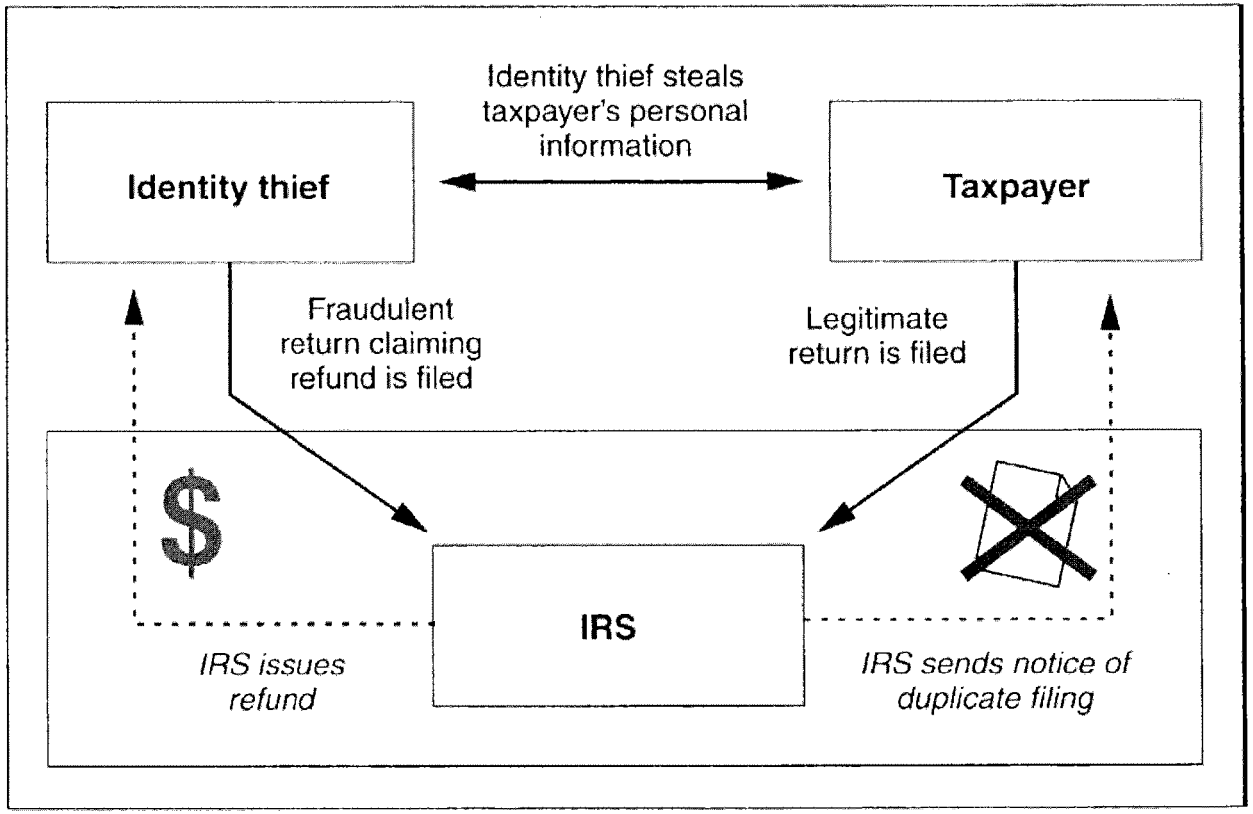
Source: IRS

The FTC operates a call center for identity theft victims where counselors tell consumers how to protect themselves from identity theft and what to do if their identity has been stolen (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or www.ftc.gov/idtheft). The FTC also produces publications on identity theft, including *Take Charge: Fighting Back*

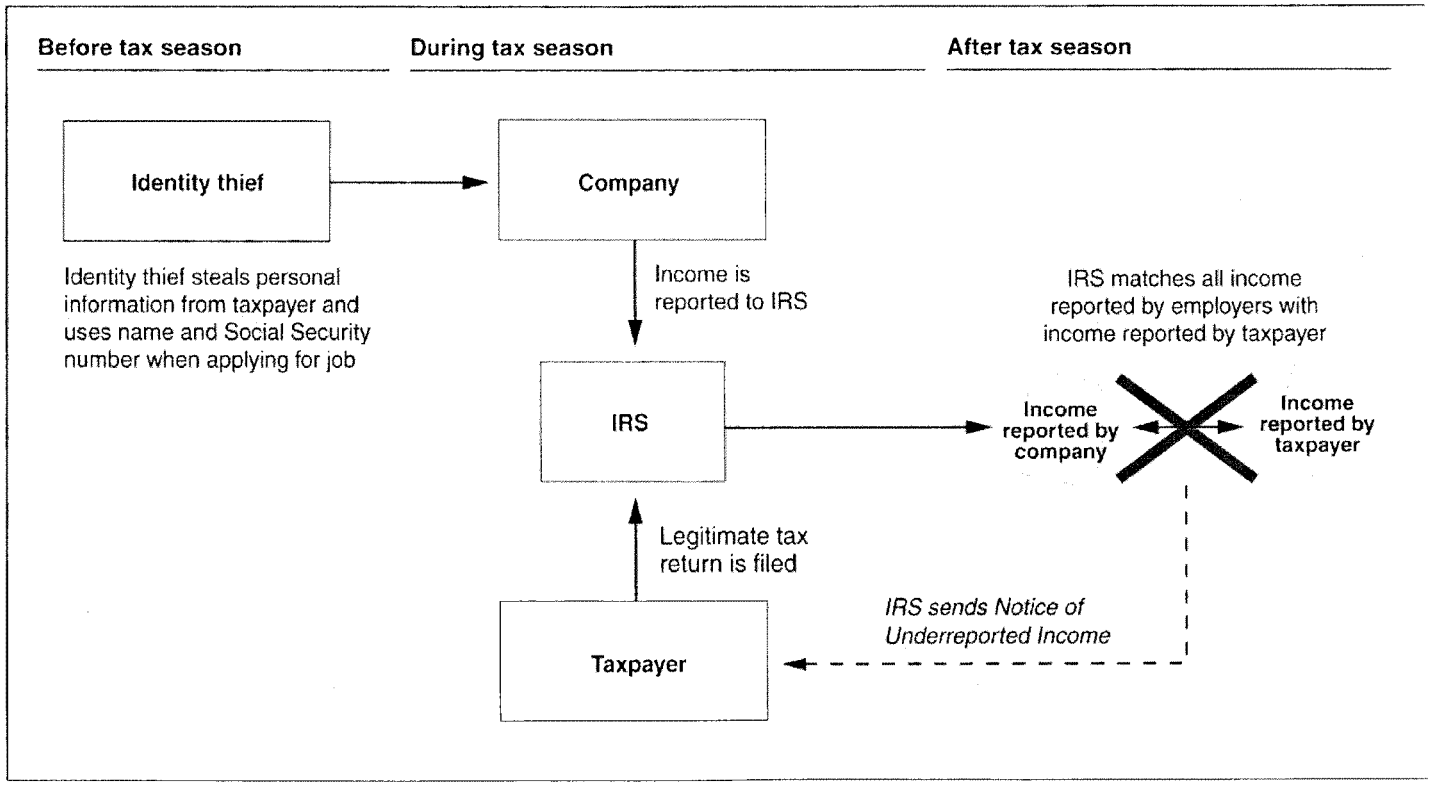
Against Identity Theft.[1] This brochure provides identity theft victims information on

1. immediate steps they can take, such as placing fraud alerts on their credit reports; closing accounts; filing a police report; and filing a complaint with the FTC;
2. their legal rights;
3. how to handle specific problems they may encounter when clearing their name, including disputing fraudulent charges on their credit card accounts; and
4. minimizing recurrences of identity theft.

[1]Federal Trade Commission, *Take Charge: Fighting Back Against Identity Theft* (Washington, D.C., February 2006). This brochure is available at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm (accessed May 11, 2011).


Identity thief steals taxpayer's personal information
Identity thief
Taxpayer
Fraudulent return claiming refund is filed
Legitimate return is filed
$
IRS
IRS issues refund
IRS sends notice of duplicate filing

Source: GAO.


Before tax season
During tax season
After tax season
Identity thief
Company
Identity thief steals personal information from taxpayer and uses name and Social Security number when applying for job
Income is reported to IRS
IRS matches all income reported by employers with income reported by taxpayer
IRS
Income reported by company
Income reported by taxpayer
Legitimate tax return is filed
IRS sends Notice of Underreported Income
Taxpayer

Source: GAO.

Mr. PLATTS. Thank you, Mr. White.
Ms. Hawa.

STATEMENT OF SHARON HAWA

Ms. HAWA. Good afternoon, Chairman Platts and Ranking Member Towns. Thank you for allowing me the opportunity to provide you with my testimony regarding this atrocious and rapidly increasing identity theft crime. It not only impacts individual livelihoods, but it also steals millions of dollars from the U.S. Treasury year after year, and will continue to do so until something is done to prevent it.

This unfortunate situation has taken a tremendous emotional toll on me. The stress, fear, and anxiety are all compounded by having to deal with terribly unorganized agencies such as the IRS and the Taxpayer Advocate Service, which only adds to feeling victimized by their inefficient systems and lack of communication. Knowing that I and other legitimate taxpayers like me remain vulnerable tax season after tax season leaves me both infuriated and it also frustrates me.

In 3 years, thieves managed to steal my tax refunds twice by filing fraudulent tax returns in my name. The first time was in 2009, after I filed through my local tax preparation office, as I had for the previous 5 years. Two days later I received word that the IRS rejected my return because my Social Security Number was used more than once.

Scared and in shock, I immediately took measures to secure all my personal assets, credit reports and accounts; I obtained a police report, filed with the Federal Trade Commission, and mailed in hard copies of my returns to various IRS addresses, as instructed by different units within the IRS. After 12 months of back and forth confusion, the IRS's Identity Protection Specialized Unit assigned me to an incredibly rude and hard to reach taxpayer advocate, where I had to explain my situation, resubmit the documents, and prove my identity all over again.

It took a painstaking 14 months until I finally received my $6,604 refund. Meanwhile, I had to take on a second job to support myself and spend a lot of time, money, and energy drafting letters and sending in the necessary information.

In 2010 I was unaffected, but I still remained extremely anxious. When I finally received both my 2009 and 2010 tax refunds a few weeks apart, I hoped the worst was over. But this year I learned that I had fallen victim to this crime yet again, and this time they also stole my State refund, together totaling $6,335.

Research has shown me just how antiquated the taxpayer system is. I realize that the IRS has been dealing with this crime since nearly the start of the millennium. So why do they seem so inexperienced and incompetent in handling the matter? And why hasn't anything been done yet to combat it?

The very process designed to accommodate taxpayers has also become a windfall for thieves. There has been an increased in tax theft as a result of E-filing and direct deposit, which do not necessitate validating personal identity when filing. A digital signature to E-file simply requires a self-select personal identification number, which is the taxpayer's adjusted gross income from their pre-

vious year's return, information that is easily obtainable. Furthermore, direct deposit only requires a bank's routing number in order to release the funds; no further vetting of personal information or identity is required.

So on two separate occasions identity thieves E-filed early in the tax season, before I physically received my W–2 forms, and used direct deposit accounts to steal my refunds. To make matters worse, in 2009, they received $1,895 more than I was due and I received a notice from the IRS stating that I owed that amount in overpayment.

Electronic filing was created to save the IRS millions of dollars, since every E-filed return costs the IRS $0.19 versus a paper return which costs $3.29.

But I urge you, instead, to look at the many millions of dollars fraudulently paid out to these criminals. Cases jumped 644 percent from 2004 to 2007 and an additional 300 percent since last year, and many millions of taxpayer dollars needlessly and disgustingly wasted due to this broken and exposed system. In an era where technology is so prevalent, one would hope that priority would be placed on this issue. It is absolutely absurd that the government pays out twice on a single stolen refund, multiplied by hundreds of thousands of stolen refunds each year. Since the country is facing one of the worst economic situations in its history, this appalling travesty needs immediate attention and repair.

This entire ordeal is in large part due to the unacceptable lack of security measures that the IRS and the U.S. Government have placed on the personal identities of taxpayers, and, as an upstanding citizen of this country, I demand change. I demand first that legislation be enacted to force Federal and State tax offices to put appropriate measures in place that prevent thieves from taking the people's hard-earned refunds away from them and forcing them to fight for their identity and their tax refunds for the rest of their lives.

I, second, demand that Federal Government work more closely with State and local law enforcement agencies to target and catch these criminals so that victims like me can rest better knowing that these criminals are serving time. And I, third, demand that each State develop and enact the necessary laws to protect consumers from corporate tax preparation offices that have few incentives to safeguard their customers' personal information.

I hope that, by hearing our testimony today, measures will be put in place that we will no longer have to deal with this nightmare any longer. I thank you for your time and your effort in making these critical changes happen now.

[The prepared statement of Ms. Hawa follows:]

Testimony of

Sharon Hawa

Bronx, NY

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

Hearing on IRS E-File and Identity Theft

Thursday, June 2, 2011, 12:30 pm

Dear Chairman and Members of the House:

I am extremely grateful for the opportunity to provide you with my testimony regarding this atrocious and rapidly increasing identity theft crime spree that not only impacts individual livelihoods but steals millions of dollars from the United States treasury, year after year, until something is done to prevent it.

I have, for the second time in the past three years become the victim of tax identity theft where thieves have twice filed fraudulent tax returns and received my tax refunds. The first time it happened was in 2009 after I went to my local tax preparation office as I had for the previous 5 years to file my 2008 taxes. However, two days after my return was electronically submitted, I received a phone call from the tax preparer's office stating that the Internal Revenue Service (IRS) rejected the refund citing "Code 0515: SSN was used more than once to file a return."

I felt extremely scared and anxious not knowing how else my identity may have been violated so I immediately took measures to secure all of my personal assets and accounts and followed the steps that the tax office suggested I take as they acknowledged this happened to some of their other clientele the same year. I obtained a police report, filed with the Federal Trade Commission (FTC) and mailed in a hard copy of my return to the IRS. I then called the IRS a week later to verify that they received my paperwork but they referred me to the Identity Protection Specialized Unit who told me a different set of instructions. I needed to draft a letter explaining what happened and re-submit all of the same paperwork I already did (police report, FTC affidavit and a hard copy of my return) to a different address than to the one I already sent. I followed up with numerous phone calls, having to explain my situation and verify my identity over and over again to each IRS agent and it took a painstaking 14 months until I finally received my $6,604.00 refund. As I relied on this refund to pay some extra bills I incurred, I had to take on a second job to support myself. In addition, all of the energy, time and money spent on combating this issue were increasing as well. I had to take several days off of work just to make appropriate phone calls, secure personal accounts and draft and mail letters certified, return-receipt to each respective address I was given.

By month 12, I was assigned a taxpayer advocate who was incredibly rude and difficult to reach which only added to the stress and frustration of the entire situation. I had to re-submit all of the paperwork I sent out to the IRS, to the taxpayer advocate as she stated that the IRS did not provide her with any information on my situation. Any questions I had I learned to refrain from asking as she clearly had no answers and did not seem willing to assist me any further than just getting me my refund.

The 2010 tax season brought with it a lot of anxiety when I filed. However, luckily I was spared, having experienced no new issues with tax identity theft, minus the continuous waiting for the previous year's refund. I thought that perhaps the worst was over, but I was mistaken.

In 2011, I quickly learned after filing through a family accountant (and not through the same tax preparation office since the first incident of identity theft) that I had fallen victim to this crime

once again and this time they managed to steal my State return as well, together totaling $6,335.00.

Unfortunately, the IRS seemed more disorganized this year than the first year it happened to me. Misplacing the phone number to the IRS Identity Protection Specialized Unit, I called the general IRS number and two different agents were unclear of what the Identity Protection Specialized Unit was, stating they had "never heard of it." When I finally got a hold of that unit, they told me I needed to call the Taxpayer Advocate office and provided me with the number. When I called the Taxpayer Advocate office, they told me they could not do anything for me without the IRS "referring me."

As I still await my second stolen refund, I have yet to be referred or assigned to any one individual who could provide me with status updates on my situation. Yet, another tax identity theft victim whom I met back in 2009, was immediately referred to a taxpayer advocate when he found out his refund was stolen this year and he is able to get clarity on his situation on a regular basis, while it took nearly two weeks before I could just get anyone at the IRS to even give me a straight answer about what to do.

Adding insult to injury, I also found out that the red flag the IRS told me they would put on my account back in 2009 was never placed, leaving my information vulnerable to thieves again.

Furthermore, I learned about a Personal Identification Number (PIN) pilot program that the IRS was "aggressively testing," and the IRS agent that told me about it stated "That's strange that you never received one since this already happened to you."

After doing some investigative research I noticed these tax theft incidents started happening since the start of the millennium, making me wonder why the IRS seems so new and disorganized in handling the matter. They continue to treat me as if I am the one to blame – adding even more stress to the situation. There is no clear process in place to prevent this from happening or to provide identity theft victims with the necessary steps they must take to receive their refunds and further protect their identity. Many agents are either very forthcoming with information about the fraudulent return or too secretive about it. The first year, I had to plead with them for simple information on what the thieves obtained, such as the amount of the refund received, the routing number of the direct deposit check and the date that it was issued, so I could thwart any additional potential damage they would do to my identity. And once I was armed with this information I was able to locate the bank, find the date that this amount of money was withdrawn and provide this information to the New York City Police Department (NYPD) who started an investigation, subpoenaed the bank for the video surveillance that showed the man stealing my money. Yet an arrest never happened because the IRS did not (and continues not to) share any information with local law enforcement to ever catch these criminals. How is it that I was able to find information about this criminal faster than the IRS?

My research has led me to conclude that the very process designed to accommodate taxpayers has also become a windfall for thieves. There has been an increase in tax theft as a result of e-

filing and direct deposit – each of which does not necessitate the need for validating personal identity when filing. A digital signature to e-file simply requires a "Self-Select Personal Identification Number (PIN)" which is the taxpayer's Adjusted Gross Income (AGI) from their previous year's filed taxes – information that is easily obtainable but must be entered in the exact dollar and cents amount. Furthermore, direct deposit options only require a bank's routing number in order to release the funds and no further vetting of personal information or identity is required to ensure that the legitimate taxpayers receive their refunds.

So on two separate occasions, identity thieves have found a way to e-file my returns early in the tax season, before I even physically received my W-2 forms in the mail from my employer, and they used direct deposit accounts to steal my refunds. In 2009, they received $1,895.00 more than I was due and in October of that year I received a notice from the IRS stating that I owed that amount in overpayment – which required me to explain the entire situation all over again.

This year, when the thieves first e-filed they received an IRS rejection message on their first attempt but boldly tried again the next day; got through and were quickly issued a direct deposit refund! What concerns me here is: 1) How did they find out my previous year's AGI when my refund was not stolen during the 2009 tax season and I was no longer getting my taxes done at a tax preparation office?; and 2) How is it possible that the IRS issues refunds before checking the accompanying W2 forms for accuracy? Any individual(s) with bad intentions either working for a tax preparation company or for the IRS can easily make millions of dollars through this ineffective and wasteful process.

These government systems are too antiquated and require a desperate overhaul, and there must be better communication between the various departments within the IRS, especially as this new form of tax fraud is increasing with every passing year. Electronic filing (e-filing) was a system created to save the IRS millions of dollars since every e-filed return costs the IRS $.19 versus the paper return which costs $3.29, but I urge you to look at the millions (or billions) of dollars fraudulently being paid out in return to these criminals. Cases have jumped 644% in 2007 from 2004 and an additional 300% since last year, and millions or billions of taxpayer dollars are needlessly and disgustingly being wasted due to this broken and exposed system.

The focus regarding identity theft from a consumer protection standpoint is mostly on credit card fraud. I am only one of now hundreds of clients who were victimized by this tax preparation office that has done little to protect our personal information housed in their office and database. The current state law for New York indemnifies and protects these companies from bearing the responsibility of consumer protection by way of a general arbitration clause which you, as a customer are forced to sign if you need your taxes prepared by one of their professionals. By signing, it states that if you have a dispute with the company you have no legal recourse to file a lawsuit unless you opt out which is a challenge in of itself. Identity theft is not a dispute – but rather violation of consumer protection. Laws need to be updated to reflect and protect its citizens from companies and criminals like these who look for irresponsible measures and general legal clauses to get away with their crimes.

In an era where technology is so prevalent, one would hope that priority would be placed on this issue since millions of taxpayer and government monies are being stolen. Realize the absurdity when the government must pay out twice on a single refund – once to the tax identity thief and then reparation to the legitimate tax payer – and now multiply that by the hundreds of thousands of refunds that are stolen each year!

Since the country has been facing one of the worst economic situations in its history, this appalling travesty needs immediate attention and repair!

I refuse to accept this as my fate as this ordeal is in large part due to the unacceptable lack of security measures that the IRS and the U.S. Government have placed on the personal identities of its taxpayers.

With all that I have mentioned and as an upstanding citizen of this country, I demand change.

I first, demand that legislation be developed and enacted that forces federal and state tax offices to put appropriate measures in place that prevent thieves from taking the People's hard earned refunds away from them and forcing them to fight for their identity and their tax refunds for the rest of their lives.

I second, demand that the U.S. Government spend more time working with federal, state and local law enforcement to target and catch these criminals.

I third, demand that each state develop and enact the necessary laws that protect consumers from corporate tax preparation offices who have little responsibility in safeguarding their customers' personal information.

Thank you in advance for your time and effort in making these critical changes happen now.

Mr. PLATTS. Thank you, Ms. Hawa.
Ms. Petraco.

STATEMENT OF LORI PETRACO

Ms. PETRACO. Good afternoon.

My story begins on March 15, 2011, when I retrieved my mail from my mailbox. I received an envelope from the Internal Revenue Service. Inside was a window envelope stamped by the Postal Service "Return to Sender, Attempted Not Known, Unable to Forward." Inside the window envelope was an IRS change of address form and, more importantly, a Notice CP–12 for tax year 2010 dated February 14, 2011. My Social Security Number and my first and last name, which were all accurate, but an address of 45 Ludlow Street, Apartment 3B, Yonkers, New York 10705. I had never lived at this address, let alone ever lived in Yonkers or the State of New York.

The form stated that I had a miscalculation on my 2010 form 1040-EZ in the area of tax credits and that my new refund amount would be $4,552. I read this form several times in disbelief and called my husband. I knew my joint tax return was prepared by an accountant, that we used the 1040 long form, since we have two children in college, and, finally, that we had just mailed our return within the last 2 weeks.

I wanted to believe an error was made that would explain this. I immediately called the IRS 1–800 number, but after 20 minutes on hold without being able to speak to anyone, I gave up. The local IRS office is about a mile from my home, but they were closed for the day, and so I spent a restless night wondering what this all means.

March 16th I arrived at our local IRS office early and was asked to step up to the counter. The clerk was courteous, but the counter is in no way private. Everyone sitting in the chairs directly behind me could hear our conversation and the lobby was full. When I showed the clerk what I had received, and that this wasn't my return, she blurted out, your identity has been stolen; I will need to fill out an identity theft affidavit. The entire waiting room heard this.

Until then I was still hoping this was just a mixup. She asked for me and for me to recite my Social Security Number. Just seconds ago this IRS employee proclaimed that I had been a victim of identity theft and was now asking me to recite, where others could hear, the same sensitive information she concluded had been stolen. I said no, that she could take the information from the form in front of her, and I would be happy to show her my driver's license. She asked, when did you lose your Social Security card? I replied, I didn't. She wanted to see it, but I don't carry it in my wallet because I don't want my identity stolen.

She completed the affidavit and told me to come back with my Social Security card so that she could send the license and Social Security Number with the affidavit. She also told me because this person filed the return as a single person and got $4,552 already, my legitimate return would be held up and that I would not see my refund until perhaps October or November, roughly 8 or 9 months later.

I asked her, how can a person file a return and, without validation or proof of anything, receive a refund. She replied, do you know how many people file electronically? We expedite the return and match up the information later. Finally, she said, don't forget to file a report with the Federal Trade Commission, the Social Security Administration, and the three credit bureaus.

Again, the clerk was courteous, but her matter-of-fact manner and abruptness that this happens all the time, in front of a room full of strangers, was upsetting.

I went out to my car and cried. I was very overwhelmed. I was so upset that I began to wonder how far the thief would go. I went home, signed on to all three credit bureaus on the Internet and reported the identity theft and printed my current reports. Everything was OK.

I pulled up my bank accounts to see if my balances were OK. They were. I was late for work that day in order to protect all that I have worked hard for. I felt the need to report this to my supervisor, as well as to the chief, as I work in law enforcement and did not want someone to jeopardize my job or my good name.

That evening I filed a report with the Federal Trade Commission, and they requested that I file a police report with my local municipality. I am not sure why because this is a cyber crime involving someone in Yonkers, New York, and not York, Pennsylvania.

March 17th I contacted Springettsbury Township Police Department and spoke to Detective Raymond E. Craul and explained what had happened and what the Federal Trade Commission requested. He was familiar with the Federal Trade Commission's request and gave me an incident report number, but stated he had no jurisdiction to investigate. I added the police department's incident report number to the Federal Trade Commission's Web site on my incident page.

I again had to leave work early to go out to the Social Security office in York, Pennsylvania to inform them of the identity theft. Unfortunately, at that time they still didn't have my 2010 earnings to verify for accuracy. I was resigned to the fact that this nightmare would continue indefinitely, that the IRS would hang on to my tax refund, and that I would have to be vigilant with the credit bureaus for the rest of my life.

On April 27th I discovered I was not the only local government employee in York County affected by the identity theft via the IRS. One of these victims suggested that our local Congressman, Tom Platts, and his office could help. I followed through with contacting the York office and filling out the Constituent Service Form with all related documentation. On April 28th I told my story to two special agents from the Department of the Treasury out of Philadelphia, who were also launching an investigation.

I am here today to tell you that I am a victim of identity theft. I am forever changed. I will always need to check on my credit and be vigilant in what information is shared with others. I am a victim, being victimized by the IRS who is holding up my refund because they don't have checks and balances in place to prevent crimes like this from happening, to timely verify personal and fi-

nancial information, or to timely and adequately assist people like me who have fallen victim to identity theft.

If they did, they would have seen the following things: that I had filed my taxes with the same man as married, filing jointly for the last 28 years; that I have lived at the same location for the last 12 years and never filed any change of address with any other governmental agency, meaning Social Security or the Postal Service; and, finally, that we always complete the 1040 long form and that we always file by mail and not by using the Internet.

I thank you for the opportunity to tell my story in the hope that changes occur within the IRS that will prevent this from happening to others. Hopefully, my tax refund will not be delayed until October-November, so that this law-abiding citizen can get back to living her life. Thank you.

[The prepared statement of Ms. Petraco follows:]

LORI PETRACO

Identity Theft

My story begins on March 15, 2011 when I retrieved my mail from my mailbox. I received an envelope from the Internal Revenue Service. Inside was a window envelope stamped by the postal service "return to sender attempted-not known unable to forward". Inside the window envelope was an IRS change of address form and more importantly, a notice CP12 for tax year 2010, dated Feb. 14, 2011, my social security number and my first and last name, which were all accurate, but an address of 45 Ludlow St. Apt. 3B Yonkers, NY 10705. I had never lived at this address, let alone ever lived in Yonkers or the State of New York. The form stated that I made a miscalculation on my 2010 Form 1040EZ in the area of tax credits and that my new refund amount would be $4552.00. I read this form several times in disbelief..... and called my husband. I knew my joint tax return was prepared by an accountant; that we use the 1040 long form since we have 2 children in college and finally, that we had just mailed our return within the last 2 weeks. I wanted to believe an error was made that would explain this. I immediately called an IRS 1-800 number but after 20 minutes on hold without being able to speak to a person I gave up. The local IRS office is about 1 mile from my home but they were closed for the day and so I spent a restless night wondering what this all means.

March 16, 2011 I arrived at our local IRS office early and was asked to step up to the counter. The clerk was courteous but the counter is in no way private. Everyone sitting in the chairs directly behind me could hear our conversation and the lobby was full. When I showed the clerk what I had received and that this wasn't my return she blurted out "Your identity has been stolen, I will need to fill out an Identity Theft Affidavit". The entire waiting room heard this. Until then I was hoping that this was just a mix up. She asked for my name and for me to recite my social security number. Just seconds ago, this IRS employee proclaimed that I had been a victim of identity theft, and was now asking me to recite, where others could hear, the same sensitive information she concluded had been stolen. I said, no, that she could take the information from the form in front of her and I would be happy to show her my driver's license. She asked, "When did you lose your social security card?" I replied, "I didn't". She wanted to see it but I don't carry it in my wallet because I don't want my identity stolen. She completed the Affidavit and told me to come back with my social security card so that she could send the license and SS # with the affidavit. She also told me because this person filed the return as a single person and got $4,552.00 already, my legitimate return would be held up and that I would not see my refund until perhaps October or November, roughly 8 or 9 months later. I asked her "How can a person file a return and without validation or proof of anything receive a refund?" She replied, "do you know how many people file electronically? We expedite the return and match up information later." Finally she said don't forget to file a report with the Federal Trade Commission, the Social Security Administration and the 3 credit bureaus. Again the clerk was courteous but her matter of fact manner and abruptness....that this happens all the time.... in front of a room full of strangers, was upsetting. I went out to my car and cried. I was very overwhelmed.

LORI PETRACO

I was so upset that I began to wonder how far the thief would go. I went home, signed onto all three credit bureaus on the internet and reported the identity theft and printed my current reports. Everything was ok. I pulled up my bank accounts to see if my balances were ok. They were. I was late for work that day in order to protect all that I have worked for. I felt the need to report this to my supervisor as well as the chief, as I work in law enforcement, and did not want someone to jeopardize my job or my good name.

That evening I filed a report with the Federal Trade Commission and they requested that I file a police report with my local municipality. I am not sure why because this is cyber crime involving someone in Yonkers, NY, and not York, PA.

March 17, 2011 I contacted Springettsbury Twp. Police Department and spoke to Detective Raymond E. Craul and explained what had happened and what the Federal Trade Commission requested. He was familiar with the Federal Trade Commission's request and gave me an incident report number, but stated he had no jurisdiction to investigate.

I added the police department's incident report number to the Federal Trade Commission's website on my incident page. I again had to leave work early to go out to the Social Security office in York, PA to inform them of the identity theft. Unfortunately at that time they still didn't have my 2010 earnings to verify for accuracy.

I was resigned to the fact that this nightmare would continue indefinitely. That the IRS would hang on to my tax refund, and that I would have to be vigilant with the credit bureaus for the rest of my life.

On April 27, 2011, I discovered I was not the only local government employee in York County, PA affected by identity theft via the IRS. One of these victims suggested that our local US Congressman, Todd Platts, and his office could help. I followed through with contacting the York Office and filling out the Constituent Service Form with all related documentation.

On April 28, 2011, I told my story to two Special Agents from the Dept. of the Treasury out of Philadelphia who are also launching an investigation.

I am here today to tell you that I am a victim of identity theft. I am forever changed. I will always need to check on my credit and be vigilant in what information is shared with others. I am a victim, being victimized by the IRS who is holding up my refund because they don't have checks and balances in place to prevent crimes like this from happening, to timely verify personal and financial information, or to timely and adequately assist people like me who have fallen victim to identity theft. If they did they would have seen the following things: that I have filed my taxes with the same man as married filing jointly for the last 28 years, that I have lived at the same location for the last 12 years and never filed any change of address with any other governmental agency (meaning social security or the postal service) and finally that we always complete the 1040 long form and that we always file by mail and not by using the internet.

LORI PETRACO

I thank you for the opportunity to tell my story in the hope that changes occur within the IRS that will prevent this from happening to others. Hopefully, my tax refund will not be delayed until October or November so that this law abiding citizen can get back to living her life.

Thank you.

Mr. PLATTS. Thank you, Ms. Petraco.

Ms. Thompson.

STATEMENT OF LAVONDA THOMPSON

Ms. THOMPSON. Good afternoon.

My nightmare began on Monday, February 28, 2011. That day, my accountant was in the process of E-filing my Federal tax return. He received a message from a software provider alerting him that a tax return had already been filed for me. He responded by advising that it could not be filed already because he was trying to file it now.

He then called the IRS and they in fact confirmed that a return had been filed in my name. My accountant called me and told me what happened. He gave me the number to the IRS to call and find out what the person used to file their return, because they could not release that information to him. I called and was told they could not tell me anything.

Once I got home from work, I called the IRS again and spoke with Mr. Baird. He told me what I had to do as far as filing an Identity Theft Affidavit with copies of my driver's license and Social Security card; calling the Federal Trade Commission; filing a police report; contacting the credit bureau and Social Security Office.

Once I finished speaking with him, I called the Federal Trade Commission and spoke with an employee whose name was Mark. He took a complaint and gave me a confirmation number. I called Social Security and was informed that I had to call the Federal Trade Commission, and I informed the representative that I had just talked to someone. She said, OK, and wished me good luck. That day she said I was the fifth person that she had spoken with who had their identity stolen.

On February 28, 2011, I filed an incident report with the York County, Pennsylvania District Attorney's Office. On March 1, 2011 I filed a police report with the York City Police Department. A detective found out who did it, but he could not charge the person because that person is reportedly located in the State of New Jersey. He was told the IRS would bring charges against them.

On March 15, 2011 I forwarded a letter to the IRS with the following documents: Identity Theft Affidavit Form 14039, Preparer Explanation for Not Filing Electronically Form 8948, Incident Investigation Information, copies of my Social Security card and Pennsylvania driver's license.

On March 16, 2011, at approximately 10:25 a.m., I called to get some information on my case because they would not release it to the detective, and he wanted me to call and get it. I spoke with the most rude and discourteous I had ever spoken with in my life. When I asked her about my case, she proceeded to yell and scream at me. When I asked for her name and ID number again because she said it so fast when she answered the telephone, the phone went silent; she had hung up the telephone.

I then called the detective and told him what happened. He told me to calm down and call back, and hopefully I would get another person. At 10:30 a.m. I called back and Mrs. Bennett answered. I could not stop crying and told her what had just happened to me

when I had called a few moments earlier. Mrs. Bennett kept apologizing for the previous person, when she is not required to do so. She informed me that the person used my Social Security Number, first and last name, no middle initial to file that return. Once my return was received, the IRS considered it to be a duplicate return.

On March 18, 2011 I wrote a letter to the IRS about the situation on March 16, 2011 and I did not get a response. Aren't telephone calls monitored by the IRS for the purpose of hearing what is being said? Is this unhelpful attitude toward the public a single incident or is it a general attitude?

On March 30, 2011, at 11:10 a.m., I called again to get an update and spoke with Mrs. Dandridge. She informed me that it would take 16 weeks to 6 months for me to receive my return because of the identity theft. I thanked her for her help.

I had to close my checking and savings account and get a new one and order new checks because of this, an added expense, albeit a minor one, but one which I did not need. I had to pull my credit reports and, luckily, so far, there has not been any activity on the part of the thief. I had to put a 90-day alert on my Social Security Number.

On May 10, 2011, I wrote a letter to Experion to put a permanent alert on my Social Security Number. On May 17, 2011 I wrote letters to TransUnion and Equifax, requesting the same.

You may not be able to know how stressful this has been. I can't sleep; I wonder what the person will do next as far as trying to get credit cards or anything in my name. Now, since this has happened, I am told the IRS will monitor my Social Security Number for the next 3 years. When I file my return, it will take them longer to process it because of this.

What, if anything, is the IRS doing to rectify that this does not happen again to me or another person? In my work history I have had the occasion to see and work with victims of crime. I have seen the calming and encouraging effect of policemen, a prosecutor, or others involved in the criminal justice system have had on victims of crime. The system I worked with made every effort to avoid victimizing a victim a second time. The way I feel, I have been treated by the IRS system, I have been made a victim a second time. I ask and wonder how many people have had the same unpleasant experience.

Last, on Tuesday, May 31, 2011, I received correspondence from the IRS dated May 13, 2011 regarding another individual filing a tax return using my Social Security Number. This incident started February 28, 2011 and I am just now receiving correspondence. Why would it take 3 months for me to receive this information?

Thank you for your attention.

[The prepared statement of Ms. Thompson follows:]

Good afternoon, my name is LaVonda Rae Thompson and I am a victim of identity theft.

My nightmare began on Monday, February 28, 2011. That day my accountant was in the process of e-filing my federal tax return. He received a message from his software provider alerting him that a tax return had already been filed for me. He responded by advising that it could not be filed already because he is trying to file it now. He then called the IRS and they in fact confirmed that a return had been filed in my name. My accountant called me and told me what had happened. He gave me the number to the IRS to call and find out what the person used to file their return because they could not release that information to him. I called and was told they could not tell me anything.

Once I got home from work, I called the IRS again and spoke with Mr. Baird, IRS number 1000348798. He told me what I had to do as far as filing an Identity Theft Affidavit with copies of my driver's license and social security card, calling the Federal Trade Commission, filing a police report, contacting the credit bureau and social security office. Once I finished speaking with him, I called the Federal Trade Commission and spoke with an employee whose name is Mark. He took a complaint and gave me a confirmation number, 29452323. I called social security and was informed that I had to call the Federal Trade Commission and I informed the representative that I had just talked to someone. She said ok and wished me good luck. That day she said that I was the fifth person that she had spoken with who had their identity stolen.

On February 28, 2011, I filed an incident report with the York County Pennsylvania District Attorney's Office.

On March 1, 2011, I filed a police report with the York City Police Department. The Detective found out who did it but he could not charge the person because that person in reportedly located in the state of New Jersey. He was told the IRS would bring charges against them.

On March 15, 2011, I forwarded a letter to the IRS with the following documents: identity theft affidavit form 14039, preparer explanation for not filing electronically form 8948, incident investigation information, copies of my social security card and Pennsylvania driver's license.

On March 16, 2011, at approximately 10:25 a.m., I called to get some information on my case because they would not release it to the Detective and he wanted me to call and get it. **I spoke with the most rude and discourteous person I have ever spoken with in my life.** When I asked her about my case, she proceeded to yell and scream at me. When I asked for her name and ID number again because she said it so fast when she answered the telephone, the phone went silent. She had hung up the telephone. I then called the Detective and told him what happened. He told me to calm down and call back and hopefully I would get another person. At 10:30 a.m. I called back and Mrs. Bennett, IRS number 1000226568 answered. I could not stop crying and told her what had just happened to me when I had called a few moments earlier. Mrs. Bennett kept apologizing for the previous person, which she is not required to do so. She informed me that the person used my social security number and first

and last name, no middle initial, to file that return. Once my return was received, the IRS considered it to be a duplicate return.

On March 18, 2011, I wrote a letter to the IRS about the situation on March 16, 2011 and I did not get a response.

Aren't telephone calls monitored by the IRS for the purpose of hearing what is being said? Is this unhelpful attitude toward the public a single incident or is it a general attitude? Isn't monitoring of calls a standard practice to allow employee oversight?

On March 30, 2011 at 11:10 a.m., I called again to get an update and spoke with Mrs. Dandridge, IRS number 1000341362. She informed me that it would take 16 weeks to 6 months for me to receive my refund because of the identity theft. I thanked her for her help.

I had to close my checking and savings accounts and get a new one and order new checks because of this. An added expense albeit a minor one but one which I did not need.

I had to pull my credit reports and luckily, so far, there has not been activity on the part of the thief. I had to put a 90-day alert on my social security number. The confirmation number for that is 1059025974. On May 10, 2011, I wrote a letter to Experian, a credit reporting entity, to put a permanent alert on my social security number. On May 17, 2011, I wrote letters to TransUnion and Equifax, also credit reporting entities, requesting the same.

I cannot apply for any credit because if I do, my social security number is flagged for identity theft. I would have to show my identity theft affidavit to wherever I would go.

You may not be able to know how stressful this has been. I can't sleep. I wonder what the person will do next as far as trying to get credit cards or anything in my name.

Now since this has happened, I am told the IRS will monitor my social security number for the next 3 years. When I file my tax return, it will take longer for them to process because of this.

What, if anything, is the IRS doing to rectify that this does not happen again to me or another person?

In my work history, I have had occasion to see and work with victims of crime. I have seen the calming and encouraging effect, a policeman, a prosecutor and others involved in the criminal justice system have had on victims of crime. The system I worked with made every effort to avoid victimizing a victim a second time. The way I feel I have been treated by the IRS system has made me a victim a second time.

I ask and wonder now how many people have had the same unpleasant experience.

Thank you for your attention.

Mr. PLATTS. Thank you, Ms. Thompson.

Again, my thanks to all four of our witnesses. And to our three citizen witnesses, the victims of identity theft, I want to add my words of apology to the Commissioner's on behalf of not specifically the IRS, but on behalf of our Federal Government for how each of you have been treated as law-abiding citizens seeking to comply with your obligations as taxpayers and, instead, becoming victims not just of criminal conduct of those who sought to defraud you, but also victims of poor service from us, the Federal Government.

All of us bear responsibility for that, ultimately, especially as the elected representative of two of you, and I know for our third witness, on behalf of all my colleagues, we want to do better on your behalf.

I want to kind of focus a couple questions with you three and then Mr. White separately. And maybe, Mr. White, actually, ask you first. In the Commissioner's testimony and also in your written testimony and your testimony here today, Mr. White, you talked about the filter, the screening process, and I am not sure what, if any, detail GAO's reviewed that as far as how that filter process works and whether you are able to make any assessment of, it kind of relates to my questions earlier, where we have these three witnesses or others where it would seem that while it has worked certainly in the 140,000 or so, clearly it has let others slip through that seem to have a fair number of red flags that didn't get caught up. I am not sure if you can give an opinion on how to assess that process.

Mr. WHITE. We haven't assessed it ourselves. I can say several things, though. One, the filter process does not work perfectly, as we have heard. It does stop some fraudulent returns and some fraudulent refunds from going out the door at IRS; however, they are both false positives and false negatives.

So this past year, so far in 2011, there have been about 50,000 false positives. Those are returns of honest taxpayers that got stopped by the filters by mistake. So that creates a burden on those taxpayers. Then, on the other side, you have false negatives where fraudulent returns slip through the filters, perhaps because the ID theft stole so much of the honest taxpayer's identity that they could get through the filters; they had enough information to get through. So you have both kinds of problems there. The filters don't work perfectly.

We have recommended that what IRS needs to be doing, and they have agreed with our recommendation and started doing this, they need to be assessing every year the effectiveness of the actions they are taking. They have taken a number of steps. They are taking a number of new steps this year. Each year they need to be assessing those steps and then feeding back.

There needs to be a feedback loop where they learn from what they have done and then correct and adjust appropriately. Part of the problem here is the thieves are adjusting as well. So it needs to be a continuous process by IRS. They have started that.

Mr. PLATTS. In essence what I would call annually auditing their internal control system to prevent this type of fraud from occurring.

Mr. WHITE. Yes, to learn what is working, what is not working; do more of what is working. If the PIN numbers, for example, turn out to work well in their experiment, then that would be something to think about expanding, obviously.

Mr. PLATTS. On that specific, I know they are looking at the results of that pilot. Is that anything at GAO that you are engaged with IRS in assessing that pilot program?

Mr. WHITE. No, we are not. Our sense, though, based on the work we did in 2009, is that the PIN seems to be a promising approach. Now, it depends on taxpayers using it for it to work, but it ought to be an addition. It seems like it has the potential to be an addition to the filter system that would make that system work more effectively than it does right now.

Mr. PLATTS. OK.

Mr. WHITE. The problem is if an ID theft is stolen, a lot of a taxpayer's identify, more than just a name and Social Security Number, they can make up a return that will look realistic; they may have a copy of last year's tax return. So they can get through the filters. The PIN is a number that only the honest taxpayer would have, unless the thief is hacking into their home computer, for example. There is no perfect solution here, but that is a solution that seems to have a lot of potential.

Mr. PLATTS. And that, from what I have come to learn, seems to be the more we can expand that effort, if the data plays out as it seems like it may, that would be one way to really try to crack down and prevent this fraud from occurring.

Mr. WHITE. Then I do think there are some long-term solutions here; these are years away. For example, right now IRS does not match tax returns to the wage statements, the W–2s that employers file, until months after the filing season ends. The first match is done in June. Part of the reason for that is employers don't have to send those information returns to IRS until either the end of February or the end of March; then the IRS matches later.

So the refunds go out the door first, then that kind of matching is done afterwards. If IRS can modernize their processing systems, and if the due date for those employer wage statements could be moved earlier in the year, IRS could do matching before refunds go out and catch more refund fraud. But this is something that is years away. They are working on their processing systems, but they are not where they need to be right now.

Mr. PLATTS. And that was part of my conversation and the Commissioner in his April speech referenced that in looking ahead and him trying to, again, be proactive in the long-term. And I didn't get the chance to ask him that question because the fact that we are providing W–2s to the employee by the end of January, once that employer makes that available to the employee, why wait another month or more before having it also shared? So that alone would hopefully allow us to move it up, just that one change. The earlier the better.

Mr. WHITE. Yes. And we have some work ongoing for the Ways and Means Committee, where we are looking at this, trying to see if there are some options to move that up.

Mr. PLATTS. Great.

Before I go to our other witnesses, I am going to yield to Mr. Towns for purpose of questions. Then I will come back with other questions.

Mr. TOWNS. Thank you, Mr. Chairman. Also, let me say to the witnesses I really apologize and regret that happened, but we are happy that you are able to take the time to come in and share with us in terms of what occurred. I really appreciate that.

Ms. Petraco, as I understand it, you discovered that your identity was compromised after receiving an address change request?

Ms. PETRACO. Yes.

Mr. TOWNS. Was the identity thief attempting to change your York, Pennsylvania address to a Yonkers, New York address? Could you explain that?

Ms. PETRACO. The letter I received had the change of address. The envelope that went to Yonkers and was rejected went back to the IRS. The IRS put it in another envelope and handwrote my name and address. I guess they got it from their files. Then that envelope came to me at my legitimate address in York, Pennsylvania. So, when I opened it up, I saw this Yonkers, New York address and I knew something was wrong.

Mr. TOWNS. Right. Have there been any other attempts to use your information?

Ms. PETRACO. No. To the best of my knowledge, this is the first.

Mr. TOWNS. No credit cards or anything like that have been used?

Ms. PETRACO. No.

Mr. TOWNS. So it appears that your ID was simply used to just commit tax fund fraud, that is what it was used for?

Ms. PETRACO. Correct.

Mr. TOWNS. Do you know anything about the status of the investigation being conducted by the Treasury Department?

Ms. PETRACO. No. Since I have been to the IRS office, I have heard nothing, except through Mr. Platts' office.

Mr. TOWNS. In other words, they have not been in touch with you?

Ms. PETRACO. No.

Mr. TOWNS. Ms. Hawa, has your ID or any of the other two victims been used for purpose other than tax refund fraud? Have they used anything else?

Ms. HAWA. Not to my knowledge.

Mr. TOWNS. How long did it take you to get assigned an agent while you were waiting for 16 months?

Ms. HAWA. The first year I was dealing with various agents within the IRS for about 12 months. Then after 12 months they assigned me to a National Taxpayer Advocate Service agent, who continued the quest to get my refund.

Mr. TOWNS. Have you received your refund?

Ms. HAWA. From 2008 it took 14 months, but this year, no, but I was just contacted saying I was going to get it within 10 days.

Mr. TOWNS. OK.

Ms. HAWA. And this year I did not get assigned an agent at all.

Mr. TOWNS. Do you have any indication that action is being taken by the IRS to find and prosecute the person that used your identity?

Ms. HAWA. It is very difficult to get information about the fraudulent claim. Just getting information about how much the refund was for, when it was issued is not something that they freely share, and that is after they use the verifiers to identify that you are the legitimate taxpayer. So, no, aside from just the basic information, which I had to plead for, I have no idea what the status is on the criminal investigation.

Mr. TOWNS. Let me ask you also do you have any idea as to where your identity was stolen, in terms of what happened, as to how they were able to ascertain it? And I will ask all three of you that.

Ms. HAWA. For me, in 2009, it started when I went to a local tax preparation office in my neighborhood. I had been going to this tax preparation office for 5 years, and I realized that it was the tax preparation office when 20 additional customers of this office came forward and said the same thing happened to them.

Ms. PETRACO. I have no idea. To the best of my knowledge, I thought everything was secure.

Mr. TOWNS. Ms. Thompson.

Ms. THOMPSON. No, I have no idea.

Mr. TOWNS. Let me just go with you too, Mr. White. You talked about the appropriate procedures that should be put in place and you also talked about modernizing the system. That costs money, doesn't it, to modernize the system?

Mr. WHITE. The IRS has spent a lot of money modernizing their systems to date. They have made progress. We have been reporting on this at GAO for a long time now, and after Congress passed the IRS Restructuring Act in 1998, IRS got much better at managing systems modernization. It is still not where it needs to be to do the sort of pre-refund matching we are talking about; they are probably several years away from that right now.

Mr. TOWNS. I am concerned about this money, everybody is concerned about, and I am just thinking that sometimes we sort of react to things, and when we should spend and we would save, we ended up not spending and ending up costing us more. It happens. I think that we do that a lot, especially in government. I am just concerned about that. I think we have to sort of make the point because I really view that this is very, very serious. If a person is waiting for his or her money and it is stolen, and they are sitting waiting, that is very frustrating.

Mr. WHITE. I agree. IRS, as you may know, has a separate appropriations account for systems modernization, and under the law at GAO looks at that account before they can spend money out of it, and the balancing act has always been making sure that IRS had the management capacity and the controls in place to be able to spend that money smartly so that they didn't get more money than they could spend effectively, but enough so that they continue to make progress modernizing.

Mr. TOWNS. Let me just say what my real concern here is, aside from the fact that a person has lost. I am thinking in reference to credit scores, employment, or other things, all the negative things that can happen, you can be impacted by this.

May I ask you how about your credit score? How have you dealt with this, all of you?

Ms. HAWA. Well, I am cautious to begin with, so even prior to this incident happening, the first year, I always kept up on my credit reporting agencies and I always had freezes on my accounts. So this just exacerbated my need to continue the freezes and always be on top of my accounts. I mean, this is going to be a lifelong issue to deal with. Even if my taxes aren't stolen next year, I am still going to be concerned that my identity is compromised and I will have to worry about accounts being opened in my name and whatnot. So this is not just a one-time thing that we have to deal with; this is a lifetime issue.

Mr. TOWNS. Ms. Petraco.

Ms. PETRACO. I agree. I don't see this ending for me any time soon. Currently it is just the IRS, but I will be vigilant about the credit scores, because I work in law enforcement, so the bigger impact for me is just the fact that I am the law-abiding citizen. I am supposed to protecting others in my role. So it does have an impact because I don't know what way this person is going to use my identity. And my name is unique, so that limits the amount of people that have that name out there, so it is me.

Mr. TOWNS. Ms. Thompson, it has been approximately, I think, 3 months since you discovered that your identity was used to commit tax fraud. You also reported the problem to the IRS and the FTC, is that correct?

Ms. THOMPSON. Yes.

Mr. TOWNS. Have you received any written communications from either of those agencies?

Ms. THOMPSON. The Federal Trade Commission wrote me a letter that had my confirmation number on it. IRS I never got anything from except the letter that I just got the other day.

Mr. TOWNS. What did that basically say?

Ms. THOMPSON. That an individual used my Social Security Number to file a return, but that was 3 months ago, and it is telling me what to do as far as the affidavit and contacting the Federal Trade Commission. But I already did all that, so it is 3 months late.

Mr. TOWNS. Right. Did you contact the York PD?

Ms. THOMPSON. Yes.

Mr. TOWNS. And what was their response?

Ms. THOMPSON. They have a police report; so does the District Attorney's Office.

Mr. TOWNS. Do they appear to be investigating? Would you know?

Ms. THOMPSON. The York City Police Department found an address and a name in New Jersey, but the IRS, when they came to talk to us the other month, said he can't arrest her; they are going to arrest her. He said he can't touch her.

Mr. TOWNS. When you say they are going to arrest her, you mean——

Ms. THOMPSON. The IRS.

Mr. TOWNS. Have you received either written or verbal communication from the IRS which gives you an update on the progress of tax fraud?

Ms. THOMPSON. No.

Mr. TOWNS. No progress report, just the one letter?

Ms. THOMPSON. No.

Mr. TOWNS. You know, Mr. Chairman, I think that is a real issue in terms of the amount that is involved, because if a person discovers that it is $3,000 or $5,000 and nothing is going to happen, the IRS is not going to pursue it and nobody, why not do it again next year? That might be the way you make your living from this point on, until something is done about it.

So I think that we need to look at the possible legislation that would encourage local law enforcement to also get involved, even if it is $1,000, 500. It doesn't matter; it is not theirs. And I think that until we come up with something of that nature, I think that this is going to continue. And I must say that we need to do everything we can to make certain that it does not continue, and I think that we might need to look at some legislation here.

I yield back.

Mr. PLATTS. I thank the gentleman and share the gentleman from New York's interest in pursuing this further, specifically on the prosecution standpoint, with our conversation with the Commissioner and with GAO of what, if any, current statutes prohibit the sharing of information from the IRS with local law enforcement. They partner with Justice, but as I kind of referenced earlier, when we are talking about a $3,000 case here, $4,000, Justice has limited resources as well, but our local law enforcement, they are pretty efficient in these type cases.

So I think, and this is something I have conveyed to our citizens who are with us, that when this hearing ends this effort doesn't end, and that we will continue to work in a nonpartisan way with the committee, with GAO, with the IRS officials to see how do we strengthen that ability, because I am one that believes exactly what you said, if we don't start sending a message that, whether it is $1,000 or $100,000, we are coming after you. If you steal money from American taxpayers and you victimize law-abiding citizens, we are not going to just ignore that; we are going to go after it and try to hold you accountable. So I look forward to doing that.

Yielding myself time now. I think, first of all, to our three victims here, one, a sincere thanks for your willing to tell your stories, because by being here you help raise public awareness of this issue; you have personalize it, you humanize it. But this isn't just about improper payments being made by the Federal Government to criminals; this is one piece of a huge, huge pie of improper payments.

The official number, most recent, is $125 billion a year of improper payments being made, and what is going on here one part of that, millions and millions of dollars going out in fraudulent tax refunds. So your helping to tell your stories is very important.

And in each of your statements you capture it in different ways, from the need for us to work with the Commissioner and his staff to strengthen the training of IRS agents in how we assist victims of crime, which is what each of you are. And you stated it in different ways but I think stated it very well. Ms. Petraco, "I am here today to tell you that I am a victim of identity theft. I am forever changed." Ms. Thompson, "The way I feel, I have been treated by the IRS system has made me a victim a second time." Ms. Hawa,

your statement, "They continue to treat me as if I am the one to blame, adding even more stress to the situation."

That is not acceptable, and the Commissioner acknowledged that and I appreciate the Commissioner's colleagues staying to hear your stories. If you haven't had the chance, Deputy Commissioner Beth Tucker, who is here with us, she was part of my meeting with Commissioner Shulman yesterday, understands the importance of us doing right by you and all victims of this type of criminal conduct, and I think captures the early reference that each of you unfortunately dealt with IRS agents who were not living up to the standard of assistance, as you well reflected in your statements, in your testimony. Deputy Commissioner Tucker is a 27-year employee of the IRS, dedicated to doing right by you, and her presence here today reflects that, along with her colleagues.

I guess a couple specific questions, and Mr. Towns touched on a number of them from a prosecution standpoint of what you have been told or what action you are aware of. On how the interactions with the IRS went, a couple additional questions. Ms. Hawa, I want to make sure I understand one part of your written testimony and what you shared here today. You were contacted in October 2009, I believe by writing, in writing, that you owed an amount of $1,895 back to the IRS.

Ms. HAWA. Correct.

Mr. PLATTS. And that amount was the difference between what you were lawfully supposed to get and the amount that the criminal had gotten fraudulently, correct?

Ms. HAWA. That is correct.

Mr. PLATTS. By this time, though, you were already dealing with representatives of the IRS, employees to kind of go after this, the identity theft that occurred, correct?

Ms. HAWA. Yes, but I didn't have one person I was dealing with; I would just talk to the Identity Protection Specialized Unit. Every time I called it was a different agent, so I didn't know how consistent my profile showed that I was a victim.

Mr. PLATTS. OK. That kind of captures what the Commissioner and I talked about the training aspect, that there is a breakdown in the training system, not just in the training, but the internal tracking system I guess is how I described it; that you were already in the system working on identity theft, and I assume probably maybe 7 or 8 months in to dealing with that, because this was the fall, yet the system kicked out, hey, we overpaid you. Well, they did overpay, but not you.

Ms. HAWA. Right.

Mr. PLATTS. They overpaid the other person the full amount. Also, when you were dealing with not those in the Identity Protection, the specialized unit, but also understand that two of the general agents that you dealt with were not aware that there was a specific unit to deal with victims of identity theft?

Ms. HAWA. That is correct. This year, when it happened to me, I had lost the number for the Identity Theft Unit, so I called the general 800 number, just thinking that they would transfer me over, and when I asked, they had no idea what unit I was even referring to, and they were giving me different instructions on how

to deal with filing my paper return, addresses to send to and what I really needed to file.

Mr. PLATTS. Right. Not understanding the scope of the issue you were trying to deal with?

Ms. HAWA. That is correct.

Mr. PLATTS. Because you had, unfortunately, been through it before. You knew what was going on and trying to get to the bottom of it.

Ms. HAWA. Right.

Mr. PLATTS. I am grateful for the Commissioner's statement that those agents that don't typically deal with identity theft, that is part of their review of how they can strengthen their training, so when someone such as yourself calls in.

One other specific question to you, Ms. Hawa, is that am I correct in understanding that after 2009 and you were supposed to be flagged, but were you also given a PIN number, or you were supposed to be given a PIN?

Ms. HAWA. I had requested a PIN because I had heard murmurings of people being issued out PINs when this first happened to me. Even a gentleman that had this happen to him earlier in 2000 and he said that he received a PIN, or some sort of verification method so it didn't happen to him again.

So I requested that immediately and they told me that they were going to look into it, and I never received it. But in 2010 I was not impacted at all, so I thought that the worst was over, so I wasn't going to bother the IRS for a PIN number. But then this year, when I found out it happened to me all over again, when I called the IRS to see why my profile wasn't flagged, as they had promised, they didn't know why and they had no explanation.

Mr. PLATTS. So it was actually back in 2009 where you were told it would be flagged, you asked for a PIN, that didn't happen, but you thought you were still flagged, but then in 2011 that didn't work.

Ms. HAWA. That is correct.

Mr. PLATTS. And that kind of comes to our discussions with the Commissioner, with Mr. White, that hopefully if we are able to expand that PIN process, that it will be more exact, and the three of you being examples. If next year you have to have that personal identification number, that it is not a question of it being flagged, but, hey, only you can file and be able to, with one caveat, and Mr. White hit it, is depending on how you receive that, if it was electronically, like personal email, versus mail or even mail, that PIN isn't stolen in some fashion. But that certainly would be another hurdle to guard against it.

I think I had one or two other ones. I appreciate everyone's patience here.

Ms. Thompson, Mr. Towns, I think, pretty well covered this. When you were dealing with the York City Police Department detective, understanding that because of the person identified as being the criminal here was in New Jersey, they weren't going to be pursuing it, IRS would. Were you told over the phone that they would be pursuing it or were you told by the detective that his understanding from the IRS?

Ms. THOMPSON. When the two IRS agents came a couple months ago to talk to us, they had told the detective that he could not arrest her, that the IRS would.

Mr. PLATTS. OK, and that was kind of when we engaged from a casework standpoint, they came out to look into your case from the Philadelphia office?

Ms. THOMPSON. Yes.

Mr. PLATTS. But you have not received any feedback about that since then from either of those agents?

Ms. THOMPSON. No, nothing at all.

Mr. PLATTS. OK.

A final question, Ms. Petraco. When you were in the York Office and understandably rattled, one, because you were just trying to figure out what is going on here, and then already being a little concerned and then being told that you were a victim of identity theft, and then the engagement that happened in a public setting, I guess just in general, did the agent that you were dealing with understand, get it when you didn't want to say the information publicly, with other people sitting there listening? Was there just an understanding, sorry about that, or was it just more they didn't realize what they were doing?

Ms. PETRACO. I think my tone of voice when I said no, no, get the information off the form, she goes, OK, OK. So I just don't think she really thought about what she was saying or, you know, just really didn't put it all together.

Mr. PLATTS. It was more just pro forma, name and Social Security Number.

Ms. PETRACO. Right. Right.

Mr. PLATTS. And not thinking that wait a minute, I have to be, I ask that because it is again on the issue of training of the sensitivity of this information that we are always on guard, because I am like each of you described your own approaches. My wife thinks I am the top shredder at home; anything that has any king of identifying goes into that shredder. For years I have been trying to be very protective because of this very concern, and it sounds like each of you have tried to do that and, unfortunately, it wasn't enough; not because of lack of effort on your part.

I don't have any further questions.

Mr. Towns, do you?

Mr. TOWNS. No, I don't. I really don't. As I indicated, though, I just think that a lot of things could sort of fall through the crack and not be dealt with. For instance, if the person is in another State and it is not a lot of money, that it could very easily almost be ignored because if you have to, if it is $750, so, therefore, why would you spend $15,000 to collect the $750? So you just sort of pass it along. And that is my concern.

So I am not sure that, we need to look at that because if they are saying that the person in York cannot make the arrest, and I am not sure that the arrest is going to be made, and I think the fact that there is no communication, to me, is very troubling, because the person that is the victim should be informed as to what is really going on, and I think that is something that really needs to look at, because also understand, in terms of the IRS, how much do you want to spend to collect $500? So I think that we have to

look at this and I think that we have a role to play here, and it is not just the blame game.

Mr. PLATTS. No, not at all.

Mr. TOWNS. I think you do some things legislatively to sort of make it possible for anybody that takes anybody else's money, that they should be charged.

Mr. White.

Mr. WHITE. Just following up on that point, I agree completely with the point, and I think the solution is to take the profit out of the crime, and you do that with better filters. So, in the short term, if these PIN numbers can be made to work, that would reduce the profit from the crooks; they lose the ability to make money off of IRS. Longer term, if there could be more pre-refund checking, again, that takes the profit out of the crime. Because you are absolutely right, IRS doesn't have the resources, and never will, and probably should not, to chase $500. It costs them much more than that to collect it. So it has to be prevented up front.

Mr. TOWNS. But the person that is the victim feels differently, and I think that is the way they should feel.

Mr. WHITE. Absolutely. That is why this is such an insidious crime. For the victims it is a big deal.

Mr. TOWNS. Right.

On that note, I yield back, Mr. Chairman.

Mr. PLATTS. Thank you, gentleman. And I would maybe wrap that discussion you just had where I started in the kind of three primary issues, is if we do better up front on internal controls and the PIN being one example of that, and even the filtering system, and that is why in my questions or comments earlier about the more flags that go off. I think, Ms. Petraco, you went through in your testimony all the things that have not changed in 28 years; your status, your address.

The filtering system itself, if it is a January return asking for a debit card refund and without any substantiating documents, that should be a big red flag. If we get into those who may be likely identity theft victims, we have the PIN. The more we do up front reduces the number of fraud cases, so that when they do occur there are fewer to pursue to throw the book at, to go after Mr. Towns' point that the message is $3,000 or not, we are coming after you, because otherwise if someone knows every year I can get an extra $3,000 to $5,000, do it once a year. So reduce the number so then there are fewer to go after to really hold accountable.

And then third is in doing that we do better with victims' assistance, because I am not a law enforcement professional, but my understanding is where there is criminal conduct and victims of crime, an important part of the healing process is the victim being kept fully informed all the way through that process of pursuing the criminal, the wrongdoing, to know that ultimately it is not just that they remain whole, as you are going to be made whole, you are going to get your refunds, but that justice was served.

And I think that is when we have, no matter what the dollar amount, that we are not pursuing them, justice isn't served. That prevents that ultimate healing process for the victims. So I think prevention, prosecution, victims' assistance, and I think by his statements the Commissioner understands that and is committed

to that not just today, but has been. But we need to partner with him and with the Deputy Commissioner and this committee and Appropriations and make sure that we are well devoting the necessary time, effort, and resources to this issue.

So my thanks again for our four witnesses here on this panel, to our IRS officials who are still here, and Commissioner Shulman on the first panel. You certainly have helped raise great awareness of this issue and allowed us as a committee to be more effective going forward to try to make sure that you three certainly are never again victimized in this way, as well as other Americans are not victimized as you have been, and we do right by you and do right by taxpayers in better protecting their hard-earned dollars that they send to the Federal Government.

We will keep the hearing open for 2 weeks for any additional information that either was requested or that you want to submit to the committee to supplement the record. With that, this hearing stands adjourned.

[Whereupon, at 4:05 p.m., the subcommittee was adjourned.]