

S. HRG. 112-491

**THE SPREAD OF TAX FRAUD BY IDENTITY THEFT:  
A THREAT TO TAXPAYERS, A DRAIN ON  
THE PUBLIC TREASURY**

---

---

**HEARING**

BEFORE THE

SUBCOMMITTEE ON FISCAL RESPONSIBILITY  
AND ECONOMIC GROWTH

OF THE

**COMMITTEE ON FINANCE  
UNITED STATES SENATE**

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

—————  
MAY 25, 2011  
—————



Printed for the use of the Committee on Finance

—————  
U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 2011

75-283—PDF

---

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

COMMITTEE ON FINANCE

MAX BAUCUS, Montana, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	ORRIN G. HATCH, Utah
KENT CONRAD, North Dakota	CHUCK GRASSLEY, Iowa
JEFF BINGAMAN, New Mexico	OLYMPIA J. SNOWE, Maine
JOHN F. KERRY, Massachusetts	JON KYL, Arizona
RON WYDEN, Oregon	MIKE CRAPO, Idaho
CHARLES E. SCHUMER, New York	PAT ROBERTS, Kansas
DEBBIE STABENOW, Michigan	MICHAEL B. ENZI, Wyoming
MARIA CANTWELL, Washington	JOHN CORNYN, Texas
BILL NELSON, Florida	TOM COBURN, Oklahoma
ROBERT MENENDEZ, New Jersey	JOHN THUNE, South Dakota
THOMAS R. CARPER, Delaware	RICHARD BURR, North Carolina
BENJAMIN L. CARDIN, Maryland	

RUSSELL SULLIVAN, *Staff Director*

CHRIS CAMPBELL, *Republican Staff Director*

---

SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

BILL NELSON, Florida, *Chairman*

MAX BAUCUS, Montana	MIKE CRAPO, Idaho
KENT CONRAD, North Dakota	TOM COBURN, Oklahoma
JEFF BINGAMAN, New Mexico	RICHARD BURR, North Carolina

# CONTENTS

## OPENING STATEMENTS

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

## WITNESSES

Hawa, Sharon, Bronx, NY .....	3
McClung, Terry, Jr., Finksburg, MD .....	5
Victim of identity theft, Miami, FL .....	6
Olson, Nina E., National Taxpayer Advocate, Internal Revenue Service, Washington, DC .....	12
White, James R., Director, Tax Issues, Government Accountability Office, Washington, DC .....	14
Tucker, Beth, Deputy Commissioner, Operations Support, Internal Revenue Service, Washington, DC .....	16

## ALPHABETICAL LISTING AND APPENDIX MATERIAL

Hawa, Sharon:	
Testimony .....	3
Prepared statement .....	29
McClung, Terry, Jr.:	
Testimony .....	5
Prepared statement .....	34
Nelson, Hon. Bill:	
Opening statement .....	1
Prepared statement .....	37
Olson, Nina E.:	
Testimony .....	12
Prepared statement .....	40
Tucker, Beth:	
Testimony .....	16
Prepared statement .....	53
Victim of identity theft:	
Testimony .....	6
Prepared statement .....	62
White, James R.:	
Testimony .....	14
Prepared statement .....	65

## COMMUNICATION

Ellingson, Robert E. ....	81
---------------------------	----



**THE SPREAD OF TAX FRAUD BY IDENTITY  
THEFT: A THREAT TO TAXPAYERS,  
A DRAIN ON THE PUBLIC TREASURY**

---

**WEDNESDAY, MAY 25, 2011**

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

The hearing was convened, pursuant to notice, at 2:07 p.m., in room SD-215, Dirksen Senate Office Building, Hon. Bill Nelson, (chairman of the subcommittee) presiding.

Also present: Ryan McCormick, Legislative Assistant; Mike Quickel, Senior Policy Advisor.

**OPENING STATEMENT OF HON. BILL NELSON, A U.S. SENATOR  
FROM FLORIDA, CHAIRMAN, SUBCOMMITTEE ON FISCAL RE-  
SPONSIBILITY AND ECONOMIC GROWTH, COMMITTEE ON FI-  
NANCE**

Senator NELSON. Welcome. This is the first of several hearings on the newly created Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth. The subcommittee is charged with examining how major revenue and expenditure policies affect our economic outlook and the prospects for long-term growth. The subcommittee's jurisdiction also extends to management of the public debt and Treasury Department operations. Broadly speaking, the subcommittee is concerned with the efficient allocation and management of taxpayer dollars.

Our ranking member is Senator Crapo. He is tied up in another meeting. He will be here before the end of the hearing and has asked me to go ahead and proceed.

The Fiscal Responsibility and Economic Growth Subcommittee will look at the big-picture trends related to spending revenue, deficits, as well as the narrower issues that involve government waste and inefficiency in programs or agencies that fall under the jurisdiction of this overall Finance Committee; thus, the topic of today's hearing.

Even in the best of years, the income tax filing process is sometimes an unwelcome event for millions of taxpayers required to navigate the ins and outs of a complex tax code. But, for an increasing number of taxpayers, the initial preparation of an income tax return may be just the beginning of an extended nightmare that can continue for months, or even years, because victims of tax-

related identity theft are the casualties of a system ill-equipped to deal with the growing proficiency and sophistication of today's tax scam artists.

Just since 2008, the IRS has identified 470,000 incidents of identity theft affecting more than 390,000 taxpayers. That is a high number. And, while the IRS reports that it has stopped over \$1 billion in fraudulent refund claims, there is no reliable estimate of how much it has disbursed to criminals, to scam artists, and to other fraudsters.

For individual taxpayers, a Social Security number is the key to unlocking and accessing the Federal tax system. At one time, Social Security numbers had a sole purpose: facilitating participation in the Old Age, Survivor's, and Disability Insurance program. But in today's modern wired world, Social Security numbers are shared with little thought almost anytime a private or public entity requests a unique, exclusive number to identify and track a customer or a client.

In short, the keys to the tax system have been copied many times over. It should come as no surprise then that, when our tax system is bombarded with sham returns that use stolen names and stolen Social Security numbers, they are going to be claiming fraudulent tax refunds.

With the ease with which the scam artists can readily file electronic tax returns, the availability of prepaid debit cards and other hard-to-trace options for the delivery of tax refunds, and the low risk that criminal sanctions or penalties will be imposed, it has created in many respects the perfect crime, but for the victims caught in the middle of these schemes. Tax-related identity theft imposes extraordinary burdens and economic hardship, as we will hear from our first panel of witnesses.

Taxpayer victims spend countless hours obtaining the necessary documents to prove who they are. Inconsistent messages and conflicting instructions from customer service agents at the IRS can worsen the situation. Innocent taxpayers whose identities have been stolen frequently find themselves in a confusing and frustrating forum of bureaucratic ping pong and bureaucratic run-around.

Last month, following several recent reports of tax-related identity theft schemes in Florida, I asked the Treasury Inspector General for Tax Administration to launch a new investigation into this issue. That work is under way, and this committee looks forward to those findings.

We have also been working with several of our colleagues to strengthen the information-sharing program to crack down on the tax scams by prison inmates, which often involve stolen identities. Legislation to extend that program will be needed, and we are going to be working in this subcommittee to get it done.

The purpose of our hearing today is to investigate the growing problem of tax fraud through identity theft. First, we will hear from taxpayers who have fallen victim to complex identity-related tax scams. Their stories are naturally heart-tugging.

The second panel, which includes the Taxpayer Advocate, the Director of Tax Issues at the Government Accountability Office, and the Deputy IRS Commissioner, will explore the scope and mag-

nitude of identity theft in the tax system and examine the laws, regulations, and administrative practices that are in place to prevent the processing of fraudulent tax returns and trying to protect these victims.

The hearing testimony will help guide the development of new legislation to crack down on tax fraud and to shield victims from further hardship. I fully expect this first hearing on this issue to lay the groundwork for congressional action and to generate novel ideas for a legislative initiative to aggressively combat the growing problem of tax-related identity theft.

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

Senator NELSON. So I want to welcome our first panel. Ms. Sharon Hawa is from Bronx, NY; Mr. Terry McClung is from Maryland; and we have a victim of identity theft from my home State of Florida, from Miami. These witnesses are our first panel, and then we will go to the second panel, which will be our National Taxpayer Advocate, a representative Director on Tax Issues from the GAO, and then the Deputy Commissioner in the IRS.

When Senator Crapo arrives, I will of course recognize him for his comments. But he is in another very important meeting at the time, and I expect him to get here not until the tail end of our meeting.

So let us just start in the order in which I introduced you all. Do you want me to call you Ms. X, or Madam X, or Miss X? Otherwise, one of our victims. So, Ms. Hawa, would you please start?

#### **STATEMENT OF SHARON HAWA, BRONX, NY**

Ms. HAWA. Good afternoon, Mr. Chairman. Thank you for allowing me this 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 organized 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 both infuriates and 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 from the IRS that they rejected my return because my Social Security number was used more than once. Scared and in shock, I immediately took measures to try to secure all of my personal assets, my credit reports, and my accounts. I obtained a police report. I filed with the Federal Trade Commission. I 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, the IRS's Identity Protection Specialized Unit assigned me to an incredibly rude and hard-to-

reach taxpayer advocate. I had to explain my situation, resubmit my 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 spent a lot of time, money, and energy drafting letters and sending 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 how antiquated the taxpayer system is. I realize that the IRS has been dealing with this crime nearly since the start of the millennium, so why do they seem so inexperienced and incompetent in handling the matter, and why has nothing been done to combat it?

The very process designed to accommodate taxpayers has been a windfall for thieves. There has been an increase 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 previous year's return, information that is easily obtainable.

Furthermore, direct deposit only requires a bank's routing number in order to release the funds, so no further vetting of personal information or identity is required. So, on two separate occasions, identity thieves e-filed early in the tax system before I even physically received my W-2 forms, and they used direct deposit accounts to steal my refunds. To make matters worse, in 2009 they received about \$1,895 more than I was due, and I received a notice from the IRS stating that I owed that money back in over-payment!

Electronic filing was created to save the IRS millions of dollars, since e-filed returns cost the IRS 19 cents, versus a paper return which costs \$3.29. But I urge you to look at the many millions of dollars fraudulently paid out to these criminals. Cases jumped 644 percent from 2004 to 2007, an additional 300 percent since last year. And many millions of taxpayer dollars are 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 to me 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.

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 year after year, and for the rest of their lives.



I, second, demand that the Federal Government work more closely with State and local law enforcement agencies to target and catch these criminals, 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.

Thank you for your time and effort in making these critical changes happen now. I appreciate your ear.

Senator NELSON. Thank you, Ms. Hawa.

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

Senator NELSON. Mr. McClung?

**STATEMENT OF TERRY McCLUNG, JR., FINKSBURG, MD**

Mr. McCLUNG. Thank you, Senator.

On December 3, 2008, my family experienced the highest of highs: my wife Stephanie, seated behind me, gave birth to our beautiful daughter Kaitlyn. On May 6, 2009, we felt the lowest of lows: our happy, healthy 5-month-old daughter died due to Sudden Infant Death Syndrome, SIDS. Losing a child, especially so unexpectedly, is every parent's worst nightmare. Thankfully, we found some support from other SIDS families that we have met in an on-line support group.

It was through that group that we first learned of a pretty despicable act. In 2010, several people posted that their 2009 tax returns were rejected because someone had already claimed their babies. Some of these people were already struggling financially and were counting on that refund. Some still had funeral expenses to pay. One family paid their tax preparer a total of \$450 because of all this. In total, just through that online support group, we know of eight families throughout the country who had their taxes rejected for the same reason.

Stephanie and I e-filed on the evening of February 16. I woke up the next day to two new e-mails stating that both our Federal and State tax returns were rejected because "the dependent's Social Security number cannot appear in more than one tax return." I made countless phone calls that day without much progress. When I called the IRS, I was told I had to talk to the Social Security Administration.

When I called the Social Security Administration, I was told I would have to deal with the IRS. I called every phone number I was given and that I could find, retold my story more times than I care to remember, and filled out an identity theft report. After a whole day of spinning wheels, I finally found out how the process would work. We had to submit paper returns instead of e-filing, and we would still get our refund.

By sometime within the next year, both we and whomever else claimed Kaitlyn would receive a letter stating that whichever one of us had mistakenly claimed her would have to file an amended return. We received that letter on November 3rd. If neither one of us amended our return, we would both get another letter requesting proof that Kaitlyn was our dependent. As long as the other person amended their return, this would all go away and that person would not have to pay any penalty or face any consequences. Learning that made all this more sickening.

That same day we learned about the Social Security Death Index on *Ancestry.com*, the first result if you Google that phrase. In mere seconds, anybody in the world can access Social Security numbers and other personal information for anyone in their database, which today includes almost 90 million records. Of course, Kaitlyn is in that database. Every other family who had their taxes rejected found their deceased babies on there as well.

I e-mailed a complaint that Kaitlyn's information was posted without our consent. Two days later, I received a generic response stating that the list is "published by the Social Security Administration, and we post records of this kind on our website as we receive them."

We contacted the I-Team at WBAL-TV in Baltimore to see if they could help us get to the bottom of this. Lisa Robinson suggested we contact Dick Myers in Senator Mikulski's office. He quickly put me in touch with the Baltimore Taxpayer Advocacy office. I gave them the link to the *Ancestry.com* database and the list of the victimized families we knew. I had at least a dozen phone calls back and forth with the advocacy office, but the little bit of information they could give us came in slowly.

In July, our contact told us that they had discovered that three of the eight cases were all filed by the same tax preparer, and that the others were all prepared in the same State. The IRS had opened a Federal investigation, and that is the last information we were allowed to be told. This past October I was contacted by Patricia Farrie in the IRS Office of Privacy, Information Protection, and Data Security. They are investigating our cases as well.

Our story aired on WBAL-TV on March 31. I have spoken with journalists in Cincinnati, Atlanta, and Charlotte who have produced similar stories. A national reporter from NBC News contacted me as well. They have all received little or no response from the IRS. To this day, we do not know what if anything has come out of this. We hope the person who stole our innocent daughter's Social Security number will pay the consequences, but, from what we have been told, that is doubtful.

If anything does ever come out of these investigations or my testimony for this hearing, it will not change anything we have gone through. But Stephanie and I, and all the other victims, can only hope that the IRS will get tougher on these criminals and prevent future families from having to go through all this on top of the anguish of losing a child.

Thank you for your time and attention.

Senator NELSON. Thank you, Mr. McClung.

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

Senator NELSON. Ms. X?

**STATEMENT OF A VICTIM OF IDENTITY THEFT, MIAMI, FL**

Ms. X. Thank you. Thank you, Senator. Thank you for the opportunity.

On December 1, 2010, around 2:30 p.m., I stopped at a gas station in Miami. As I was pumping gas, my handbag was stolen from my car with both mine and my daughter's Social Security numbers, as well as my driver's license, home address, credit cards, et cetera.

Very concerned about my daughter's safety and my own, even after taking all possible precautions from that day on, I started calling the police to give them updates on numerous fraud attempts to my accounts. Through the end of December, there was no detective assigned to my case. The day I went to the police station to meet Detective Alce, I was informed by another police agent that I should be prepared to face fraud on my upcoming taxes. The agent who was alerting me had also been robbed and experienced tax fraud for many years.

Entering January 2011, my concern was to avoid a more serious crime. I contacted the IRS to alert them that my daughter and I were victims of identity theft and to place an alert regarding my 2010 tax return. The IRS has a web page on identity theft explaining how to prevent fraud. They request proof of identity and an affidavit.

By January 11—and not March as my statement shows—that was a mistake—I sent out all the required documents and also called the IRS to follow up. On February 9, upon the arrival of my W-2, my accountant filed my taxes electronically, only to receive a message stating that my taxes had already been filed. I immediately called the IRS to report what I understood was a fraud and to ask for help in correcting it. The response I got was that it was going to be a long wait, and that I had to send my taxes via mail, along with a new affidavit and proof of identity.

This case was a clear fraud. Someone in Miami had filed taxes under my Social Security number and had already received a check. Nobody could explain why my previous alert and affidavit did nothing to prevent the fraud. Along with my personal efforts, Senator Nelson's office was open to listen to my case and help with directing it to the right hands.

By the end of February, I received a call from the IRS Advocate's representative who was going to direct my case to another representative. She was sympathetic to my case due to the fact she had also been a single mother, and that, added to identity theft, was too much to take. She then changed the code on my case in order to expedite it.

On March 22, the assigned advocate called me requesting new copies of my tax file and telling me to wait for updates. On April 7, I received my tax return check for \$4,299, and my case was closed.

On April 15, I received a letter from the IRS documenting the fraud and alerting me on identity theft. I was also informed that the 3-year identity theft indicator would be attached to my account. I hope the indicator will help protect my account, but I am also aware of the delay it will cause on my tax return. I heard about the PIN number that will be issued by the IRS to identity theft victims, but so far I do not have a clear answer on how it works or how to get one.

From police leads that were never followed, a criminal who was never caught, a Social Security number that has become a major concern, banks that still cannot guarantee the account's safety, financial institutions that still rely on Social Security numbers as a master proof of identity, taxpayers that pay for criminals' fraudulent tax returns, nothing is really in place to protect the honest cit-

izen from a fast-growing crime such as identity theft, which is good for the criminals who are taking full advantage of this scenario to take money from hardworking people. Thank you.

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

Senator NELSON. Let me ask you, Ms. X, did you expect the IRS would take the extra precautions with your taxpayer account?

Ms. X. Yes, I did.

Senator NELSON. And because of this special person whom you got who had been through a similar situation, they responded to you fairly quickly.

Ms. X. Exactly.

Senator NELSON. In your case, the identity thief actually opened a residential electricity account with the electric company and a landline phone using your Social Security number. Is that correct?

Ms. X. They actually added an address to my electric bill, yes. I reported this address to the police, and so far nothing has happened to it. I had the landline also that was recorded by Bloomingdale's, as they tried to defraud my account with Bloomingdale's.

Senator NELSON. But, in this particular case, the thief actually opened a residential electricity account and a landline phone using your Social Security number.

Ms. X. It was linked to my account. They did not open a new account, they added an address to my existing account.

Senator NELSON. Was it an accurate address of the thief?

Ms. X. I do not know. I reported it to the police, hoping for an investigation. The answer I got from the detective was that they had been there once. There was furniture in there. They did not have time to go back and check and really talk to whoever lived there because they had so many cases in their hands.

Senator NELSON. Were you ever referred to the IRS Identity Protection Specialized Unit by anyone in the IRS?

Ms. X. I have the letter that was sent to me acknowledging the fact that I had been a victim of fraud that comes from, exactly, the Identity Theft team. But the contact with them is also difficult, because, for instance, I asked them to check on my daughter's situation and if there was any fraud related to her Social Security number, and they could not inform me of that. They could not inform me about a safe PIN number that could be issued. But apparently they are handling the case, yes.

Senator NELSON. Apparently you also contacted the Secret Service because they investigate financial and electronic-related crimes. What did they tell you?

Ms. X. They told me they could not touch the case, even with all the leads I had, until the IRS itself would send them a file, would send them the case. So, until then, they could not really do anything, follow any lead, including the address I had in my hands where the check, the IRS check, went to.

Senator NELSON. And, to this point, you do not know if any of the local officials or the IRS has gone and pursued this case against the thief?

Ms. X. No. I know the police have closed the investigation on my case, and nothing else has been done as far as I know.

Senator NELSON. So somebody has taken your identity and filed a false IRS claim, as well as they have opened an electricity ac-

count and a phone account, and all of that is being done in your name. At this point you are not sure if the authorities have gone after this person?

Ms. X. No. Actually, my impression is that nothing has been done to prevent further action. I have been fighting against this. I have been working on the subject nonstop. I have phone calls that last forever, very frustrating attempts to even change my Social Security number, which they tell me I cannot do because there is so much history attached to it, unless something really terrible happens, which makes me question—so do I have to wait till I am financially broke to finally get a new Social Security number? My daughter's number also cannot be changed for a new one. I do not get any solution from anybody in the meantime.

Senator NELSON. Do you think, aside from your daughter's identity, that your identity, now that you have been helped by this helpful IRS agent who took some concern directly, do you think that your identity is now secure at the IRS?

Ms. X. No, not at all. I have been trying to find out about this PIN number that would make my next tax return safe. That is what I understand, that the number would have to be matched to the number they have once they receive the return, otherwise it would not be valid. Nobody can give me an exact answer on this. So, no. I know there is an alert on my account now, but I do not feel that is going to do it, no.

Senator NELSON. Well, I wanted to start my questioning with your case first because you found a helpful IRS agent who jumped on it and helped you immediately, and yet you are still in limbo.

Ms. X. Yes.

Senator NELSON. You do not know what is going to happen. You do not have any idea if the person has been caught, prosecuted, jailed, whatever. You do not have any idea.

Ms. X. Yes, I imagine.

Senator NELSON. And somebody is running around masquerading with your identity.

Ms. Hawa, let me ask you, would you describe to the committee the economic hardship that you have experienced as a victim of this tax identity theft?

Ms. HAWA. Sure. Well, in 2009 was when my organization—I work for a nonprofit organization—starting doing a lot of cuts with regard to salary and all that, so I was really relying on my tax refund to try to pay off some bills so I would not accrue more interest on my credit card statements, and really try to get ahead of the game.

But unfortunately, with this tax identity theft issue, it really just put a damper on things. I was really concerned about what my long-term credit report would be because I knew that I would default on some credit card payments.

This year it has been magnified twice over. I am still waiting for my IRS refund. My State refund just came last week, but I am still waiting for my IRS refund. I am in a similar situation, if not worse. I am about to potentially be laid off from my place of employment, and it really just scares me because I think that it is going to continue to happen. I mean, I have no faith right now that the IRS

is doing anything to combat this issue. This is the second time in 3 years.

Senator NELSON. In the first case, it was, you were looking for a 2008 calendar-year income tax refund, and you waited 16 months before you finally got it. What was the message that you were getting from the IRS while you were waiting?

Ms. HAWA. Well, I called the IRS probably about 60 times throughout that entire 14- to 16-month time frame, and it was the same story: we are looking into it. We are looking into it. We are looking into it. I was never assigned anybody until the 12th month.

Senator NELSON. So you had multiple people whom you had to deal with?

Ms. HAWA. Every single time I called, I would get a different agent and would have to start the entire process of explaining who I was and what happened all over again.

Senator NELSON. Do you have any evidence of action that the IRS took to go after the thief who filed your fraudulent return using your name?

Ms. HAWA. None. Zero. In fact, I was given the routing number from the 2008 tax season. I was given the routing number, the date, and the amount of the refund that was fraudulently filed. I found the routing number belonged to a bank in New York City, called the bank, found out that they had video surveillance of that amount being withdrawn, gave it to the New York City Police Department. They subpoenaed the bank, had video of the person, and nothing was done to capture this individual. According to the New York City Police Department, because the case became a Federal case rather quickly, they were pulled from it, and they were no longer allowed to pursue the individual.

Senator NELSON. Over this long nightmare that you have endured, have you seen any improvements in the IRS processing of your return?

Ms. HAWA. Ironically, I think this year it seemed more disorganized than the first year it happened. The first year it happened I was automatically given to the IRS Identity Protection Specialized Unit. This year, I called the IRS, and they did not even know what that unit was. They could not even refer me to them. Agents never heard of it. It took me a while until I found that number again, and when I called I just got the same run-around: we are looking into it, we are looking into it, we are looking into it.

Senator NELSON. Do you have a single point of contact now that is working on your case?

Ms. HAWA. No. I asked to be referred to the Taxpayer Advocate. They told me that I needed to call the Taxpayer Advocate Service. I called them. The Taxpayer Advocate Service said that IRS needed to refer me to them. I called the IRS again, and they said, we cannot refer you until we figure out what is going on with your account. So it is just the same run-around, and I have absolutely no one to call. But the conversations are lengthy. I have never been off the phone in under 30 minutes, and it is the same conversation over and over and over again with no answers.

Senator NELSON. All right. Ms. Tucker, when you come up in the next panel as the Deputy Commissioner, I want to know for the

record here for this committee what we are going to do to straighten out these kind of administrative problems.

Mr. McClung, obviously your loss is extraordinary and you are very kind to be here with us today. Why do you think your daughter's identity was targeted as a potential victim by this scam artist?

Mr. McCLUNG. I do not know that it was necessarily her that they were targeting. I think they are just going after any numbers that they can get and claiming any babies that they can. Like I said, we know of eight. So I do not think it was necessarily a personal thing on us. I think they got a hold of her name and were quickly able to find her Social Security number and use it to make a buck.

Senator NELSON. And how do you think the thief found your daughter's Social Security number?

Mr. McCLUNG. While I do not know it for a fact, just by simply Googling "Social Security Number Death Index" you can access anyone's Social Security number who has passed away. Our daughter was on there. That is a very easy way that anybody in the world could find her Social Security number. She was only 5 months old, so her Social Security number was not bouncing around many places. So our only guess is, it was through that index.

To this day we do not understand why that information, all that private information, has to be out there so quickly. If Social Security numbers are used for ancestry research, that is fine. But give it a year and let us get through the tax season before that stuff goes public. Let us close things out on that tax season.

Senator NELSON. Do you have any knowledge that the IRS has made any effort to catch the thief?

Mr. McCLUNG. None. We have gotten very little information from the Taxpayer Advocacy office. They did tell us that they linked ours and two other cases that I told them about with the same tax preparer, and that an investigation was under way. Where that investigation has gone, is going, went, we have no idea, and we were told we are not allowed to know because of privacy reasons.

Senator NELSON. If your daughter's Social Security number was not so easily available as you just indicated, do you think this would have occurred?

Mr. McCLUNG. I do not think so. I do not understand how else anyone could have gotten her Social Security number. We filled out the paperwork at the hospital when she was born, but we did not get a number then. We only got a number after we filled out the paperwork in the hospital and the card was mailed to us. It never left our house.

The only place her number ever went was perhaps medical insurance and life insurance. It is not like her number was out in paperwork at a taxpayer office, a tax filing center where somebody could have gotten into those papers and found that number. Her number did not go many places. So, no. If it was not for that index, I really doubt we would have gone through all that.

Senator NELSON. Well, thanks to you. You have communicated with parents of other SIDS victims who have had their children's identity stolen and used to commit tax fraud. Do you want to share some of those hardships with our committee?

Mr. McCLUNG. Sure. In our situation, Kaitlyn passed away in May, so we have a total of, I guess, almost 9 months by the time we filed our taxes for at least a small portion of that pain to go away. I mean, not that it ever completely goes away. But some of these families, their children had just passed away at the end of that year, and then they had that on top of it, the heartache there, just from a personal level.

Then, as I mentioned in my testimony, some people really counted on that money. The funeral expenses—nobody plans for funeral expenses for a baby. So, some of those families were counting on that money from their tax refund to pay those bills. With the economy today, everybody is really counting on their refunds. Whenever they get delayed, whether it is because of my situation or the other situations you have heard here, it can be a hardship on anybody.

Senator NELSON. I want to thank you all personally for coming up and sharing what is a bureaucratic nightmare and has become a personal nightmare. This is what we wanted to get out on the record here, what is happening to a lot of people across the country. We are going to try to do something about it. Identity theft is a major problem today, but this is where it is important, in this particular area where it is so lethal, for people just to be able to cope. You all are certainly good examples of what being a victim of this kind of identity theft will do. The committee wants to thank you very much.

I am sorry that Senator Crapo has not gotten here in time. If you would, as I dismiss you, if it is possible that, if you do not have a flight to catch, you could stay. When Senator Crapo gets here, I would like for him to have the opportunity to meet you and ask you any questions.

So with that, let me ask the second panel if you all will come up, please.

Well, thank you all for being here. The first witness on our second panel is Ms. Nina Olson, National Taxpayer Advocate. She has been sounding the alarm on this issue since 2005. Identity theft has been on the Taxpayer Advocate's list of the most serious tax problems for several years, and we appreciate your participation.

Our next witness is James White, the Director of Tax Issues at the Government Accountability Office. Mr. White is going to discuss GAO's audit and investigative work on the issue of tax fraud through identity theft.

Our third witness is Beth Tucker, the Deputy Commissioner, Operations Support, at the IRS. Ms. Tucker reports directly to the IRS Commissioner. She oversees IRS support functions and business practices. Ms. Tucker, we appreciate very much you being here as well.

So let us just start in the order in which I introduced you. Ms. Olson, if you will proceed.

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

Ms. OLSON. Chairman Nelson, thank you for inviting me to testify today about the subject of identity theft. I first want to apologize to Ms. Hawa for what she found an unsatisfactory experience with the Taxpayer Advocate Service. I can assure you that my of-



office gives the highest priority to these cases, and we have successfully resolved tens of thousands of these cases each year. Moreover, as you noted, I have covered this issue with specific recommendations, both to Congress and the IRS, since 2005.

Ms. Hawa, I will be glad to speak with you after this hearing so we can make sure your case is resolved.

Senator NELSON. Thank you very much for that. I would encourage anybody who is listening to this hearing to take advantage of Ms. Olson's office.

Ms. OLSON. Thank you.

I note that identity theft requires a careful balancing between protection of taxpayers from a devastating crime and imposing an unreasonable burden on all taxpayers. Some protections would increase return on refund processing time for all taxpayers, not just the victims. In our testimony today, we have sought to strike the right balance between protection and burden.

Over the last 3 years, the IRS has made significant progress in this area, including adopting many recommendations from my office. The IRS has provided greater discretion for its employees to determine the true owner of an SSN in question without referring the matter to the Social Security Administration, which would require years to resolve.

It has developed an electronic marker to mark accounts of verified identity theft victims. It has created an IRS identity theft affidavit form. It has adopted a standardized list of acceptable documents to substantiate identity theft. It has established a centralized unit to provide assistance to identity theft victims. It has provided a global account review prior to closing an identity theft victim's case to ensure that all related issues have been resolved. And it is issuing PINs to verify taxpayers that will enable them to file tax returns electronically.

Notwithstanding these efforts, the IRS is seeing unprecedented levels of identity theft casework, and the current approach is not working as intended. The population of taxpayer accounts with an identity theft indicator has grown significantly, subjecting almost a million accounts to business rules. If a return does not pass these business rules, it will be considered unpostable, meaning it will not be processed until it is manually reviewed, resulting in longer processing times and refund delays.

In 2009, the IRS established the Identity Protection Specialized Unit, or IPSU. IPSU, however, is struggling to effectively manage identity theft cases. Whether because of resource constraints or a policy decision, the IPSU is not staffed to handle cases itself. Rather, it attempts to coordinate with up to 16 different IRS functions. Without adequate staffing in the IPSU and the related functions that actually work identity theft cases, the benefits of any process improvements will be minimal for both taxpayers and the IRS.

IPSU procedures accept unreasonable IRS processing delays, allowing 60 days for the IPSU to follow up with a function to see if the requested action was taken and not considering a case aged until after 180 days or 6 months has passed. The IRS does not currently track any data about the cycle time for identity theft cases, but they can languish for months without resolution. The Taxpayer

Advocate Service has made numerous additional recommendations to address tax-related identity theft.

These include allowing taxpayers the option to turn off the ability to electronically file so that the thief cannot beat them to the punch filing electronically, systematically retiring expired Social Security numbers, utilizing information reporting earlier in the filing season, notifying taxpayers of potential identity theft, and working with the Social Security Administration to keep SSNs out of the public domain.

As noted earlier, the SSA now makes significant personal information public upon a person's death, including the decedent's full name, Social Security number, date of birth, date of death, and the county, State, and zip code of the last address on record. This information is now regularly obtained and used by government agencies, credit reporting agencies, financial firms, and genealogists. Unfortunately, it is also used by identity thieves to commit tax fraud.

While I understand the competing policy concerns, the government's provision of all this information in unredacted form aids and abets identity theft and tax fraud and is frankly appalling. It provides identity thieves with the opportunity to steal potentially billions of dollars of Federal funds through fraud. Not insignificantly, there is also a compelling personal and emotional cost to all of this.

I urge Congress and the SSA to address the problem immediately. Congress could pass legislation for the SSA similar to Internal Revenue Code 6103, which is our confidentiality provision. A least comprehensive solution would be to redact all but the last four digits of the number.

I appreciate the opportunity to appear before you today, and I will be glad to answer any questions you might have.

Senator NELSON. Thank you, Ms. Olson.

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

Senator NELSON. Mr. White?

**STATEMENT OF JAMES R. WHITE, DIRECTOR, TAX ISSUES,  
GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC**

Mr. WHITE. Thank you, Chairman Nelson. Thank you for inviting me to this hearing.

As the victims made clear, identity theft-related tax fraud is an insidious crime. To begin, I want to describe a typical case of refund fraud, illustrated on page 3 of my statement and on the easel.

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, IRS then issues the 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 it investigates. The notification from IRS may be when the taxpayer first learns his or her identity has been stolen.

Employment fraud is different, as illustrated on page 4 of my statement. 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 and tax statement, and the innocent taxpayer files a tax return.

IRS matches tax returns with the employer reports after April 15 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 under-reported income to the taxpayer, and that is when the taxpayer and IRS first learn about the identity theft.

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 will outline what IRS is doing to resolve IRS's ID theft problems, detect tax fraud, and prevent future problems. Starting in 2004, IRS took a number of steps which Ms. Olson summarized, so I will not repeat. In 2009, we recommended that IRS develop measures and data for assessing the effectiveness of these efforts. IRS agreed, has done some assessments, and has taken new actions based on those assessments.

To help resolve innocent taxpayers' problems, since identity theft makes it appear they either claimed two refunds or under-reported 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 identity 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 over 200,000 returns failed the screens and 146,000 were fraudulent. Also, IRS is experimenting with a new screen for the Social Security numbers of deceased taxpayers. The intent is to prevent thieves from filing using the identities of deceased taxpayers.

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. This is an experiment that has not been applied to all taxpayers yet, or all ID theft victims yet.

IRS's ability to address ID theft is constrained by law, timing, and resources. The laws governing the privacy of taxpayer data limit IRS's ability to disclose information about suspected ID thieves to Federal, State, or local law enforcement agencies. Complicating any investigations 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 identity theft, tax evasion, money laundering, and other financial crimes, far fewer than the number of ID theft cases.

All of this raises the question of whether IRS can and should be doing more. Options exist, but they come with trade-offs. 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 would also burden employers who could be contacted about reported wages.

Looking forward, IRS needs to continue assessing its efforts, such as PINs and the 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 someday be able to match tax returns to wage statements before refunds are issued, and thus prevent more refund fraud. To do such pre-refund matching, the due date on employers' wage statements would have to be moved earlier.

Mr. Chairman, this completes my statement. I would be happy to answer questions.

Senator NELSON. Thank you, Mr. White.

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

Senator NELSON. Ms. Tucker?

**STATEMENT OF BETH TUCKER, DEPUTY COMMISSIONER, OPERATIONS SUPPORT, INTERNAL REVENUE SERVICE, WASHINGTON, DC**

Ms. TUCKER. Chairman Nelson, I appreciate the opportunity to testify on the very important issue of identity theft. Let me start by saying, deep apologies to the taxpayers who shared their stories. I know this has been extremely frustrating, and it is a heart-breaking experience to have to go through.

One of our highest priorities at the IRS is to ensure that taxpayer information is secure and protected. We take identity theft very seriously. Regrettably, by the time we detect and stop a perpetrator from using someone else's personal information, the victim's data has already been compromised outside of the tax filing process.

The IRS is not the cause of the identity theft. The fraud perpetrated by individuals using a taxpayer's stolen identity should be seen within the context of a much larger problem in the United States and around the world. The public and private sectors are targets of identity theft, including small businesses, large corporations, banks, and other government agencies.

Although the initial theft takes place outside tax administration, interaction with the IRS is sometimes the first instance in which taxpayers become aware that they are victims, as we heard from the earlier panel members. I will provide context on how we see identity theft play out at the IRS and then outline our efforts to address this problem, assist taxpayers, and protect the integrity of tax administration.

Generally, victims of identity theft could experience two tax issues. First, someone could steal another person's identity and use the Social Security number to file a tax return and fraudulently obtain a refund. The rightful owner of the Social Security number will be unaware that this has happened until the person attempts to file his return. It is then discovered that two returns have been filed using this same number. We call this type of fraud a refund-related crime.

The second tax issue an identity theft victim could experience is when someone steals his Social Security number and uses it to ob-

tain employment. In this instance, the IRS receives a W-2 or a 1099 that reports income that the rightful owner of the Social Security number did not earn. We call this type of fraud an employment-related crime.

In 2007, we created the Office of Privacy, Information Protection, and Data Security to focus on identity theft prevention, assistance, and collaborative partnerships. I would like to briefly highlight our efforts to date on the respective prongs of this strategy. Through prevention we seek ways to protect innocent taxpayers and keep taxpayer dollars out of the hands of criminals.

In fact, since 2009 we have protected nearly a billion dollars in fraudulent refunds from going out the door of Treasury. We recognize the need to provide assistance to taxpayers who are identity theft victims. We have created a series of identity theft markers that are placed on taxpayers' accounts when they are verified as victims of either a refund-related or employment-related identity theft crime. Returns related to marked accounts pass through a series of filters, as Mr. White just testified to, that try to identify fraudulent returns before the refunds are processed. These markers help to prevent a victim from experiencing similar tax issues year after year.

Since 2008, the IRS has placed nearly 400,000 markers on taxpayers' accounts. In addition, we have established a customer service unit with specially trained assisters dedicated to answering the questions of the victims. As you have heard earlier, we have recently initiated a pilot where we have issued identity protection Personalized Information Numbers, or PINs, to 56,000 taxpayers who have been victimized by identity theft. The PIN provides the IRS and the taxpayer with greater assurance that the return filed is coming from the legitimate taxpayer rather than an identity thief.

The third prong of our strategy is collaboration and partnership. We collaborate with other Federal agencies, such as the Federal Trade Commission and the Department of Justice. We have recently entered into a new partnership with the Internet Crime Complaint Center, coordinated by the FBI and the National White Collar Crime Center. The IC-3 receives criminal complaints related to cyber security and identity theft and has agreed to accept victim referrals from the IRS to conduct additional investigation of identity theft issues that fall outside the scope of tax administration. This is very new, and we are very pleased and will keep you posted on how this new partnership goes.

Let me conclude by telling you very candidly that, in the process of increasing our efforts to block attempts by identity thieves to exploit the tax system, there have been many inconveniences and delays created for honest, hardworking taxpayers such as we saw earlier today. We need to do a better job at the IRS in this area. We have dedicated significant efforts over the last few years to streamline the process for taxpayers caught up in identity theft. These efforts are starting to pay off.

I know how frustrating it is for individuals to be stuck in sometimes long delays while they depend on their tax refund, and for that we are deeply sympathetic. This is a particularly challenging problem for all of us to deal with, and you have my commitment,

Senator, that we are focused on continuing to improve our operations in this area.

Thank you. I will be happy to answer any questions you might have.

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

Senator NELSON. You mentioned, Ms. Tucker, that you will provide a PIN number to someone who requests one. How do we get the taxpayer educated to know that they can request a PIN number so that they have that extra means of protection against continuing to be victimized?

Ms. TUCKER. Yes. Senator Nelson, the PIN number is actually a pilot that we launched the start of this filing season, so we have provided PIN numbers to 56,000 victims of known identity theft. So we randomly selected the 56,000 for part of this pilot for this filing season. We are currently in the process, now that the filing season is over, of going back and evaluating, first of all, how many of the taxpayers whom we gave that PIN to actually used it, for how many of the taxpayers who used the PIN did we effectively block another perpetrator coming in and trying to use it again, and then, based on the results of the study, we will be making determinations about expanding that pilot and providing that additional lock-down PIN to other victims of identity theft.

Senator NELSON. So a pilot study with 56,000; but we actually in the last 3 years had half a million incidents of identity theft, and only 40 to 50 are annually referred to the Justice Department for prosecution. So how do you see the issuing of this PIN number as a means of protection for the taxpayer?

Ms. TUCKER. This one is so difficult, as you have heard everyone talking about. Every time we identify a scheme, the perpetrators seem to be trying multiple other ways to get in and use that identity. We believe, however, through the use of this PIN, if in fact the PIN is protected and is not also somehow compromised—so, for example, we have reports of folks whose tax returns are taken in the course of a robbery. Of course, if your secret PIN number is actually written on your file, that could be a problem. But what our plan is, if this pilot goes as we expect, Senator Nelson, we would be reissuing the PIN every year to the taxpayers who have been known victims of identity theft.

Senator NELSON. In other words, you are going to change the PIN number each year?

Ms. TUCKER. Correct. Of course, as I said, this is all contingent on us looking at how successful the pilot has been. Of course, too, as Mr. White from GAO just testified to, we are in a fine balancing act at IRS. This past filing season, we processed 132 million tax returns, and they are still coming in. As you know, folks have extensions. Trying to balance keeping tax administration moving and getting refunds out quickly to the valid taxpayers is a priority, and I think something that the American public expects of us. At the same time, with budget constraints, as we try these different avenues to stop the perpetrators, it is a constant balancing act.

You mentioned the prosecution recommendations. Just to give you a little additional context on that, this past year we did recommend working—as you know, the process is, the IRS identifies cases, we refer them to the Department of Justice, and they make

decisions about which cases are moved forward. We did make 41 recommendations. There were 55,000 taxpayer accounts associated with those prosecution recommendations. As a result, 32 indictments were handed down, 20 individuals have been sentenced to prison time. Average sentencing is 4 years. Our criminal investigation folks who do those tougher investigations have spent roughly 400,000 hours on identity theft since 2008.

Senator NELSON. So the figures that I have—half a million incidents of identity theft in the last 3 years and only about 40 to 50 cases annually referred to the Justice Department for prosecution—those are not correct?

Ms. TUCKER. The prosecution recommendations for 2010 were 41. So those are the recommendations, but the context around it, that includes—those recommendations actually cover 55,875 taxpayers who have been caught up in the identity theft.

Senator NELSON. Well, 55,000 just in the year 2010?

Ms. TUCKER. Yes, sir. In the referral that we made.

Senator NELSON. Well, our information is that there were half a million incidents of identity theft in the last 3 years.

Ms. TUCKER. That is correct. The total number of identity theft cases that we actually have had since 2008 that we have coded is 401,209 cases, but the context I was giving you was around the prosecution cases.

Senator NELSON. All right. Well, with this small amount of prosecutions, does this look somewhat like almost a risk-free crime?

Ms. TUCKER. Here is the difficult thing with a lot of these cases. The schemesters are, as you know, very savvy. In a large number of instances, IRS has no idea who these people are because they are filing from hotspots, they are filing from places that are not traceable. They are having the refunds sent to a bank account that could be opened and closed fairly expeditiously.

In one of the areas that we are actually seeing grow, the fraudsters can actually go in through a return preparer and, based on some of the software agreements, they can actually have the refund deposited against a debit card, which is not traceable.

A lot of these are onesies and twosies, where maybe one person decides to steal someone's identity and then they move on. I think the other thing that is important to remember with the volume of cases that we are seeing at IRS—roughly 132 million cases coming in this filing season—our criminal investigation unit has to develop the cases, potential fraud cases, on a wide array of other tax crimes, whether it is under-reporting, other types of tax evasion schemes. So identity theft, as egregious and horrible as it is, is just a piece of the tax crimes that IRS and the Department of Justice are dealing with.

Senator NELSON. We talked about how providing a personal identification number is one way to at least stop the crime from being committed. I want to ask Ms. Olson and Mr. White, do you believe that the IRS should be making these personal identification numbers more readily available?

Mr. WHITE. I think that the approach that needs to be taken with the pilot is to study the effectiveness of the first year's use of these numbers before putting them into widespread use. That was our recommendation in 2009. IRS has been doing these sorts of as-

sessments. They are surprised sometimes at what does not work or what does work here. They also need as part of that research to make sure they understand the impact on innocent taxpayers.

So the screening that was done this year—for example, they screened out over 200,000 returns that looked suspicious, and 145,000 of those were fraudulent but over 50,000 of them were not fraudulent. Those were innocent taxpayers who had their refunds held up. So I do think it is important to learn from the pilot before going ahead. It sounds like it has merit.

Senator NELSON. Ms. Olson?

Ms. OLSON. I agree with Mr. White. I think the pilot will show us a lot. It will help those 50,000 some-odd taxpayers who are part of that pilot, and we will learn how to refine it. A few years ago the IRS put out the screening rules, and last year was a good year. The year before, we stopped many, many more innocent taxpayers' returns, and so created a burden on them unnecessarily.

We have recommended that taxpayers be given the option to turn e-filing off under their Social Security number because, for some preparers, for some thieves, e-filing is the name of the game. You just basically go in and try to get what you can and then leave. If they have to do paper, they will not necessarily follow that route. But as Ms. Tucker has observed, these thieves, these criminals are incredibly creative, and they will adapt to whatever we do.

We have thought about—and this is a very extreme measure and it shows the hard choices that the IRS has to make—do you basically say, on April 15, that is the day we are going to issue everybody's refunds? We wait until April 15 to see whose come in? It is not the first to file anymore that goes through, it is whose do come in. But just think about the 140 million taxpayers and what we are doing to them by making them wait for April 15. There is no one silver bullet for this problem.

Senator NELSON. Ms. Tucker, is it IRS policy to notify victims when it determines that a fraudulent tax return has been filed?

Ms. TUCKER. The process—and I actually have to commend Mr. White for his charts; I think he had a good illustration—the process that we use at IRS is, unless there is some other indicator on the account, when the first return comes in, if it does not hit our screens and we go ahead and process it through, we would issue the refund. In many instances, as I said in my testimony, especially if it is a refund-related crime, the valid taxpayer would know that their identity has been compromised when we reject their return. In many instances, that is their first time to know. It is also the IRS's first time to know that we have a duplicate taxpayer.

So the other way that an individual could find out from the IRS that it appears there is a problem with their Social Security number is in the employment-related scheme that I mentioned earlier, where someone has used my Social Security number to gain employment and, if they do not come in and file a tax return then, once we do the matching of all the information documents, we could then go back to the valid taxpayer and give them a notice and say, you have failed to report this additional W-2 income. And then they would begin to engage in a process with us around validating that they in fact did not work for that other employer, and



that is usually another indication that they have had their identity compromised.

Ms. OLSON. Senator Nelson—

Senator NELSON. Hang on 1 second.

Ms. OLSON. I am sorry.

Senator NELSON. Let me just follow that up. I am trying to understand; is it the IRS policy to notify victims when you have determined that a fraudulent tax return has been filed? What you just described, you would indicate that a tax return has already been filed. So is that considered the notice?

Ms. TUCKER. The notice would be when we receive the second return, and the valid taxpayer, their return is rejected. Then I think we actually had that situation explained from two of the prior witnesses. That was how they became aware that someone had in fact compromised their identity.

Senator NELSON. So I am trying to relate it to something else, like a credit card company will notify a customer if they suspect fraudulent activity. I have been amazed. Some of the credit card companies have apparently some elaborate system set up by which they can detect something out of the ordinary, and they will call the customer and say, did you purchase such-and-such at such-and-such a place? But I take it the IRS would have no way of knowing that, because you get a return, and, even though it is fraudulent, you are leaving it up to the taxpayer, when they get that rejection of them filing their legitimate claim, then they have to take the next step.

Ms. TUCKER. Chairman Nelson, let me put some flavor on this just to show you how difficult it would be for IRS to even know when, in many instances, this first return comes in. Our records show that 10 million families move every year, so the address on their return could change, legitimate taxpayers; 46 million individuals change jobs; 2.1 million individuals marry, so the names on the joint return could legitimately change; 1.1 million individuals divorce; 4.1 million births; and 2.4 million deaths.

So, when you look at all of that change that legitimately rolls through the filing of the tax return, for someone to have stolen someone's Social Security number and come in and filed with potentially the only change being a different address, that would not prompt us to proactively reach out, to use Mr. White as an example, to pick up the phone and call Mr. White and say we are holding your tax return because we see that your address changed, especially when this happens so frequently.

Senator NELSON. Ms. Olson, you had a comment?

Ms. OLSON. Well, I agree with Ms. Tucker how difficult it would be for some of these screens, for all the reasons that she says. I do think we can do a better job, when we are rejecting a return where we have already received a prior return, to provide some information saying, we have already received a return and you might call us, and we will walk you through the identity theft protection and the issues.

There is a category of cases, however, that we have covered over the years that does not have to do with return filing, per se. It has to do with when we have a return where someone has used someone else's Social Security number to get work and they are filing

their actual returns under an Individual Taxpayer Identification Number—not the SSN—but the SSN shows up on a W-2. We will often see these issues where we know the SSN that has been compromised. We are not going to work that particular case because it may be a low-dollar case and it just does not justify being worked, so we do not pursue the wages that were reported under that Social Security number.

But there is a clear indication that that number has been compromised, and we know, usually, the owner of that number. We now have legal authority. We have an opinion from the Chief Counsel in the IRS that we can contact the owner of that Social Security number to say someone is out there using your number. It is associated with a return that is an ITIN rather than your return. We are not doing that. We have recommended for years that the IRS do that. We have now a clarification of our legal authority, and I really do not understand why—that could be a computer-generated notice.

Senator NELSON. And that would come from the IRS?

Ms. OLSON. Yes, because we are seeing a return being filed under an ITIN, but the W-2 attached to it has a Social Security number attached. So it is clear that someone is using that Social Security number illegally to get work in the United States. We have the authority to contact the true owner of that Social Security number to say, someone is using your Social Security number illicitly, and that would allow the owner of that Social Security number to then take protective steps, including calling us to put a marker on their account to protect them in the future, but also maybe ask for a PIN, if we go beyond the pilot, but also contact, take steps just on their credit bureau reports and things like that.

Senator NELSON. What do you think about that, Ms. Tucker?

Ms. TUCKER. The issue that Ms. Olson is bringing up involving the ITINs is one that is also extraordinarily complex, so I think what we would want to do based on the legal opinion that our Taxpayer Advocate just mentioned, is to go back and take a look at it. So, if you would allow, we will look at that and get back with you.

Senator NELSON. Is this pilot study that you have done, is it providing personal identification numbers to the taxpayers?

Ms. TUCKER. The pilot for the 56,000 taxpayers, we do give them a PIN number that we gave them the option to use when they filed the past tax return. That basically is the key to unlock the account and allow the return to come through, so it is a PIN directly associated with those 56,000 Social Security numbers.

Senator NELSON. How did you select the 56,000?

Ms. TUCKER. I will need to go back and verify this, but it is my understanding that it was a random selection.

Senator NELSON. What is your experience when a taxpayer will come to you substantiating with a police report or an official affidavit that they have been victimized by the theft of their Social Security number or their wallet that would have their Social Security number? Does that raise any threshold where you would consider issuing a PIN to them?

Ms. TUCKER. Just to go back again, the PIN pilot that we just initiated, we are really waiting now to see, was that effective. But I think the interesting thing, in trying to sort all the different num-

bers out—so let me give you an example. Lost wallets, where either—I think we had one of the panelists talk about the fact that her wallet was stolen.

We had roughly 23,000, I believe, taxpayers who have come to us saying they have lost their wallet. A lot of times they find their wallet. It is not as direct as actually seeing someone take your wallet. And I think this gets back to the balance in tax administration. If we put a PIN on every account, it will slow down the processing of returns, so that is the fine balancing act.

That said, I think at this point at IRS, just like the pilot I mentioned, we have another pilot that we have under way this year with 6,000 deceased taxpayer accounts, where there is still the ability to file that final return, but then we are locking that account after the final return is filed.

So candidly, I think the PIN may be a good solution, but, until we evaluate the test, I think it is hard to know. The other thing I would say, IRS is going to have to stay in front of this for years and years to come. I do not think there is one solution to solve this.

Senator NELSON. When are you going to have this data evaluated?

Ms. TUCKER. So what we will be doing, after all the returns are processed through, and we are still—a lot of people think filing season ends on April 15th. It actually goes on for quite a bit longer as we process the returns. Then we will go back in and actually investigate all 56,000 accounts to see how many of those taxpayers did use the PIN. Did a perpetrator try to ping that account, and was it blocked with the PIN? Then we will evaluate the effectiveness of the pilot. So I would say, by later this summer we should know.

Senator NELSON. All right. Well, then later this summer, are we talking about July?

Ms. TUCKER. I would probably say August/September time frame.

Senator NELSON. All right. I am going to invite you to come back.

Ms. TUCKER. I would welcome the opportunity.

Senator NELSON. I would like to have a report on what you have concluded because, if this thing is working, I think it is in the interest of the American taxpayer to get this thing off dead center and get it moving. Part and parcel of that, I want you to come back to us about, what should we be doing with the Social Security numbers of deceased Americans that could otherwise be utilized, as was painfully described by the dad, Mr. McClung. So we have a lot that we can do here, but, needless to say, you heard the testimony of the three victims. This is a nightmare.

Now, when you get to senior citizens, they do not necessarily want to file an electronic return. Some of them just feel more comfortable in filing on paper. Ms. Olson has recommended allowing taxpayers to turn off electronic filing on their tax account. Why does the IRS not allow taxpayers to turn off electronic filing?

Ms. TUCKER. One thing I failed to mention earlier—and I think this is probably a good time to talk about this—we have talked about enhancements that have been made over the years, and I truly do appreciate the role of the Taxpayer Advocate and GAO as well in partnering with IRS on recommendations to enhance this program.

I think Ms. Olson's recommendation about the ability to lock down the account is something where we actually will have a task group that kicks off in June that the Taxpayer Advocate Service is a member of. And we are actually going to be doing another end-to-end review of our identity theft program, as well as considering all of the additional enhancements that are coming in, not only from the Taxpayer Advocate, but actually recommendations that we have received from citizen advocacy groups as well. So that will be something else we will be able to report back to you later in the summer.

Senator NELSON. So you are saying that, when we meet again, then you are going to be able to tell us if the IRS is going to allow taxpayers to turn off electronic filing?

Ms. TUCKER. Correct.

Senator NELSON. All right.

Let me ask you, do you have any estimate of how much identity theft costs U.S. taxpayers in lost revenue?

Ms. TUCKER. Mr. Chairman, this is a tough area for us to totally estimate. We have really good figures on the fraud that we are keeping from going out the door—that is the billion-dollar figure. Our latest estimate is from 2009, and I believe GAO actually was involved as well in helping us put that estimate together. That was that, for filing season 2009, roughly \$15 million in fraudulent refunds were issued.

Senator NELSON. Fifteen million.

Is there any limit on the number of wrong attempts of someone filing before the IRS would freeze an account?

Ms. TUCKER. Yes. So I think you are referring to the phone and web authentication, when someone is filing an electronic return. So this is one where the identity thief obviously has a deeper amount of information potentially than just the Social Security number. So there are five data elements that the identity thief would need to know to be able to electronically file, and they are locked out after six attempts.

Senator NELSON. All right. Now, if I go down to an ATM, and I type in the wrong code three times, that is it. So, in this case, it is six times?

Ms. TUCKER. It is six times to actually e-file the return. But the perpetrator actually would have, to even be able to get that far, quite a bit of information already at their disposal.

Senator NELSON. Other than the Social Security number.

Ms. TUCKER. Right. They would need to know—I really hate to actually share that information—

Senator NELSON. Well, then we will—

Ms. TUCKER [continuing]. Because it is a bit of a road map.

Senator NELSON. Then we will share it offline.

Ms. TUCKER. All right.

Senator NELSON. Here is what I am trying to get at. If an ATM will shut me down after three times, and a thief has the Social Security number, shouldn't we have some program set up so that once we have identified that there is a thief using this Social Security number, that automatically there is a program that would reject that out the next time that the thief uses that Social Security number?

Ms. TUCKER. Yes. This is the additional complexity here, and I think this gets back to something we have all talked about: the burden on the legitimate taxpayer as well, and also the fact that the electronic filing is really a tool to enter the tax system to perpetrate fraud.

The same thing could happen with a paper return. There is actually then additional security on what a perpetrator would have to know to even be able to electronically file. On the paper return, quite candidly, the perpetrator could still get that return through with greater ease than through the electronic filing system just by the nature of what is requested on the paper return.

Senator NELSON. Does the staff have any additional questions? [No response.]

Senator NELSON. All right. I want to ask our first panel, do any of you have any question that you want me to ask our witnesses? All right. Come up and just use the microphone next to Ms. Olson.

Ms. X. I recently called the IRS after my case was solved, asking for information about next year, and they were checking my identity before talking to me. I was very surprised that the questions asked to check my identity could have been easily answered by the criminal. I know I was robbed. I have a police paper saying that I was robbed. The police know that, not only was I robbed, I am a victim of identity theft. I actually told the IRS before the fraud occurred that I was a victim of identity theft. I am still surprised that the fraud actually happened, being that I sent the affidavit. Now the questions I get as security questions are questions that do not really mean anything.

Senator NELSON. So you are getting security questions from the IRS, like what?

Ms. X. Like my Social Security number, my address.

Senator NELSON. You have already turned in, of course, that information.

Ms. X. Well, the criminal has this information. They have my wallet.

Senator NELSON. Yes.

Ms. X. They know the name of my daughter and her Social Security number as well.

Senator NELSON. But the IRS is asking you that?

Ms. X. Yes.

Senator NELSON. Well, would they not be asking you that for verification that you are who you are?

Ms. X. Yes. Exactly. What I am trying to say is, as security questions, these will fail. They absolutely will fail, because I can tell you that my daughter's name is so and so, that my Social Security is so and so, and my address is so and so. So can the criminal.

Senator NELSON. All right. Ms. Olson, will you pick up on that and elaborate, please?

Ms. OLSON. I think that is a very interesting and valid point, that when somebody's identity has already been compromised, the standard authorization or authentication questions actually are useless because the thief will have all the information that banks, credit cards, anybody asks. If we have an identity theft marker on the account, what I think our next step is—and I applaud you for

raising this because this is a great issue—is that it should trigger a different series of questions.

So, when you call to ask a question, the person answering the phone on the IRS side can look at your account and see, aha, you have the ID theft marker on, and then that triggers, we are going to go through a different series of questions because some aspect of your identity has been compromised. Now, what those questions are, I do not know because, in your case, what would he or she not know about you? That is really going to be hard.

If I can just follow up on one thing. Our victim here did raise the difficulty of getting a new Social Security number. In my private practice, when I was in private practice, I represented so many people who had been victims, and I know how difficult it is to get Social Security to issue a new number. Although it has been done, it really is very, very hard. I think that is worth looking into. Why, today, is it not possible, even though the number has a history, that you cannot retire that Social Security number and then get a new number so that the person can carry her history over, but start afresh?

Mr. WHITE. Mr. Chairman, the PIN might be one example of something. This would obviously be in the future, because so far PINs are only being used in the small pilot. But that would be a secret that presumably only the innocent taxpayer and IRS would know.

Senator NELSON. Any comment, Ms. Tucker?

Ms. TUCKER. I think that is absolutely right. You did point out the fact that, when someone calls our toll-free number—and I think the panelists have pointed out the frustration—that each time someone calls we do, regardless of who they are talking with, have to go back through the same basic set of questioning to ensure that we have the valid taxpayer on the line. I know that is frustrating, but I think to Mr. White's point, I mean, the PIN could potentially help cut through some of that red tape.

Senator NELSON. Any of the others? Yes, ma'am. Ms. Hawa?

Ms. HAWA. I just wanted to kind of get a sense from all of you about what the process is with the W-2 forms, and at what point does that get sent to the IRS so that, if the perpetrator files a higher adjusted gross income, the victim is not victimized once again by being asked to pay the difference.

Senator NELSON. All right. So the question is, once the identity is stolen and the thief is trying to make even more, what kind of safeguards are in place to try to prevent that?

Ms. OLSON. This situation was actually the initial reason for the identity theft marker, why we recommended it, because what was happening was that the victim would get a notice from us saying, yes, you filed your income tax return but you did not report all of your income under your Social Security number. The poor tax victim would have to come into the IRS and prove, in audit situation, that, one, their identity had been stolen, and two, there was no way that, living in Philadelphia, they could have worked in California at the same time as working in Philadelphia.

That put an additional burden on, so the idea was to have this marker where, if we knew that the person was a victim or that that Social Security number had been compromised in the work en-

vironment, that when this extra unreported income would show up, our systems would tell us this person has been a victim of identity theft, and then we would not bother that victim about it. We would know that those extra wages, reporting from some other State, were not that person's. Now, still you have to look, because maybe the victim did leave off some information, but it flags it so that we do not automatically issue that letter.

Senator NELSON. All right. Ms. Olson, I want you working with Ms. Tucker on that issue before we have Ms. Tucker come back in September to tell us about the pilot, if you will make that one of the matters that you discuss when you come back.

Mr. WHITE. Mr. Chairman, if I could add something here. I think it is an excellent question that was raised. Part of the problem here is that the W-2s are not required to be submitted by employers to IRS until well into the filing season. Many of them are not required to come in until the end of March. So IRS does not have anything to check in terms of a legitimate W-2 to verify what is on the tax return. This is still years in the future, but there is some potential that the Service can move to the point where, if they can match that information before issuing refunds, they could detect more fraud and prevent the refund from going to the thief.

Senator NELSON. I want to thank all of you. This has been a very—all right. We are not going to leave you out, Mr. McClung.

Mr. MCCLUNG. Sorry. I just had one more. A 2-part question, really quick.

Senator NELSON. Address it through me.

Mr. MCCLUNG. Through you. All right. What I would like to know is, how we get closure to our case. We were told that we would get the first letter saying that someone needed to amend their return sometime in a year, and then we would get another letter saying that, if neither of us amended our return, then we would have to provide proof. Well, we did not get that first letter until this past November. We are still in limbo, wondering whether that second letter is coming. So, would it not be nice to notify the victims that the case is closed and that it has gone away?

And really quickly, part two is, anytime we have tried to contact the IRS, or the reporters who have covered our case have talked to the IRS, all of a sudden, privacy and disclosure protects everybody, and they cannot talk to anybody. So, we do not need to know names, but it would be nice to know that something has been done and all of our complaints have not fallen on deaf ears.

Senator NELSON. I think that is a very legitimate request. Do you want to amplify on that, Ms. Olson?

Ms. OLSON. Well, the first thing is, I do think that your account has been taken care of, but I will go back and check, because the Taxpayer Advocate Service does do closing letters and things, and I was assured that your account had been taken care of, and the only reason why I can speak to you is because you have given me authorization to say this publicly, which goes to the next part about disclosure. Certainly, without the taxpayer's consent, we cannot disclose any information about cases.

For Mr. McClung, we have discovered information about the fraud that has occurred on his case. What I can say publicly is that we have made a criminal referral on that case, on the circum-

stances of what we have seen in that case and related cases. We cannot say anything more than that. There is an investigation that may or may not be going on, and no IRS employee or any Federal employee can compromise that investigation. That is very difficult for the taxpayer who, as you say, is wanting closure. But, you know.

Senator NELSON. Yes. When it gets into the hands of the Justice Department, it is a different matter, and they have their own set of laws that they go by, and they guard that pretty closely.

Well, this has been extremely illuminating. Ms. Tucker, I am going to look forward to visiting with you privately in September, and then we will determine if we want to have another hearing with regard to what you tell me as a result of this pilot study with 50,000-some taxpayers in the study. It seems to me that, if you have a good response, then we need to get this thing kicked off so that we are protecting these taxpayers.

Ms. TUCKER. I will look forward to speaking with you in September.

Senator NELSON. All right.

And I thank everybody here. It has been an illuminating discussion. Thank you. Have a good day.

The hearing is adjourned.

[Whereupon, at 3:53 p.m., the hearing was concluded.]



# **A P P E N D I X**

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

---

**Testimony of**

**Sharon Hawa**

**Bronx, NY**

**Before the United States Senate  
Committee on Finance, Subcommittee on  
Fiscal Responsibility and Economic Growth**

**Hearing on The Spread of Tax Fraud by  
Identity Theft: A Threat to Taxpayers, a  
Drain on the Public Treasury**

**Wednesday, May 25, 2011, 2:00 pm**

Dear Chairman and Senators of the Committee:

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.

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 16 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 14, 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, 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 \$2,049.00 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 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 demand that the U.S. Government spend more time working with federal, state and local law enforcement to target and catch these criminals. And I 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.

**Testimony of Terry D. McClung, Jr.**  
**to the United States Senate Committee on Finance**  
**Subcommittee on Fiscal Responsibility and Economic Growth Hearing:**

***The Spread of Tax Fraud by Identity Theft:  
A Threat to Taxpayers, A Drain on the Public Treasury***  
***May 25, 2011***

Dear Chairman Nelson and the Members of the Committee,

On December 3, 2008, my family experienced the highest of highs – my wife Stephanie gave birth to our daughter Kaitlyn. On May 6, 2009, we felt the lowest of lows. Our happy, healthy 5 month old daughter died due to Sudden Infant Death Syndrome (SIDS). Losing a child, especially so unexpectedly, is every parent's worst nightmare. Thankfully, we found some support from other SIDS families that we've met in an online support group.

It was through that group that we first learned of a pretty despicable act. In 2010 several people posted that their '09 tax returns were rejected because someone had already claimed their babies. Some of these people were already struggling financially, and were counting on that refund. Some still had funeral expenses to pay. One family paid their tax preparer a total of \$450 because of all this. In total, just through that online support group, we know of eight families throughout the country who had their taxes rejected for this same reason.

Stephanie and I e-filed on the evening of February 16. I woke up the next day to two new emails stating that both our Federal and Maryland State Returns were rejected because "the dependent's Social Security number cannot appear in more than one tax return." I made countless phone calls that day without much progress. When I called the IRS, I was told that I had to talk to the Social Security Administration. When I called the Social Security Administration, I was told that I'd have to deal with the IRS. I called every phone number I was given and that I could find, retold my story more times than I can remember, and filled out an identity theft report.

After a whole day of spinning wheels, I finally found out how the process would work. We had to submit paper returns instead of e-filing and we would still get our refund. But sometime within the next year, both we and whomever else claimed Kaitlyn would receive a letter stating that whichever one of us "mistakenly" claimed her would have to file an amended return. (We received this letter on November 3.) If neither one of us amended our return, we would both get another letter requesting proof that Kaitlyn was our dependent. As long as the other person amended their return, this would all go away and that person would not have to pay any penalty or face any consequences. Learning that made all this more sickening.

That same day we learned about the Social Security Death Index on Ancestry.com – the first result if you google that phrase. In mere seconds, anybody in the world can access social security numbers and other personal information for anyone in their database, which today includes almost 90 million records! Of course, Kaitlyn is in that database. Every other family

that had their taxes rejected found their deceased babies on there as well. I emailed a complaint that Kaitlyn's information was posted without our consent. Two days later, I received a generic response stating that the list "is published by the Social Security Administration and we post records of this kind on our website as we receive them."

We contacted the I-Team at WBAL-TV in Baltimore to see if they could help us get to the bottom of this. Lisa Robinson suggested we contact Dick Myers in Senator Mikulski's Office. He quickly put me in touch with the Baltimore Taxpayer Advocacy Office. I gave them the link to the ancestry.com database and a list of the victimized families we knew. I had at least a dozen phone calls back and forth with the Advocacy Office, but the little bit of information they could give us came in slowly. In July the Advocacy Office contact told us that they had discovered that three of the eight cases were all filed by the same tax preparer and that the others were all prepared in the same state. The IRS had opened a federal investigation, and that's the last information we were allowed to be told.

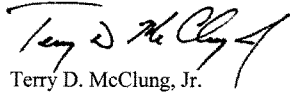
This past October, I was contacted by Patricia Farrie in the IRS Office of Privacy, Information Protection, and Data Security. They are investigating our cases as well.

Our story aired on WBAL-TV on March 31. I've spoken with journalists in Cincinnati, Atlanta, and Charlotte who have produced similar stories. A national reporter from NBC News contacted me as well. They've all received little or no response from the IRS.

To this day, we don't know what if anything has come out of this. We hope the person who stole our innocent daughter's social security number will pay the consequences. But from what we've been told, that's doubtful. If anything does ever come out of these investigations or my testimony for this hearing, it won't change anything we've gone through. But Stephanie and I, and all the other victims can only hope that the IRS will get tougher on these criminals and prevent future families from having to go through all this on top of the anguish of losing a child.

Thank you for your time and attention to this matter.

Respectfully submitted,

A handwritten signature in black ink that reads "Terry D. McClung, Jr." The signature is written in a cursive style with a horizontal line above the first name.

Terry D. McClung, Jr.

**Related Internet Links:**

***Ancestry.com Social Security Death Index:***

<http://ssdi.rootsweb.ancestry.com/>

***WBAL-TV (Baltimore, MD) - March 2010***

*I-Team Investigates 'Troubled Returns'*

<http://www.wbalv.com/video/23022637/detail.html>

***WCPO-TV (Cincinnati, OH) - April 2010***

*Can Someone Profit From A Child's Death?*

[http://www.wcpo.com/dpp/news/local\\_news/Can-Someone-Profit-From-A-Child%27s-Death](http://www.wcpo.com/dpp/news/local_news/Can-Someone-Profit-From-A-Child%27s-Death)

***WCPO-TV (Cincinnati, OH) - October 2010 Follow-Up***

*IRS: "We're outraged" someone stole IDs of dead babies*

[http://www.wcpo.com/dpp/news/local\\_news/investigations/irs%3A-%27we%E2%80%99re-outraged%27-someone-stole-ids-of-dead-babies](http://www.wcpo.com/dpp/news/local_news/investigations/irs%3A-%27we%E2%80%99re-outraged%27-someone-stole-ids-of-dead-babies)

***WSB-TV (Atlanta, GA) - November 2010***

*IRS Investigates Tax Fraud Using Dead Children*

<http://www.wsbtv.com/video/25802405/index.html>

***WSOC-TV (Charlotte, NC) - February 2011***

*9 Investigates: Tax Cheaters Use Deceased Children's Social Security Numbers*

<http://www.wsocv.com/video/26958099/index.html>



*The Spread of Tax Fraud by Identity Theft: A Threat to  
Taxpayers, a Drain on the Public Treasury*

Hearing before the Senate Committee on Finance  
Subcommittee on Fiscal Responsibility and Economic Growth

Chairman Bill Nelson

Opening Statement  
May 25, 2011

Welcome, today is the first of several hearings of the newly created Senate Finance Subcommittee on Fiscal Responsibility and Economic Growth.

The subcommittee is charged with examining how major revenue and expenditure policies affect our economy and the prospects for long-term growth. The subcommittee's jurisdiction also extends to management of the public debt and Treasury Department operations. Broadly speaking, the subcommittee is concerned with the efficient allocation and management of taxpayer dollars.

The Fiscal Responsibility and Economic Growth Subcommittee will look at big picture trends related to spending, revenue, and deficits, as well as narrower issues that involve government waste and inefficiency in programs or agencies that fall under the jurisdiction of the Finance Committee.

Which brings us to the topic of today's hearing.

Even in the best of years, the income tax filing process is an unpleasant and unwelcome event for the millions of taxpayers required to navigate the ins and outs of our terrifyingly complex tax code.

But for an increasing number of innocent taxpayers, the initial preparation of an income tax return may be just the beginning of an extended nightmare that can continue for months or even years.

Victims of tax-related identity theft are the casualties of a system ill-equipped to deal with the growing proficiency and sophistication of today's tax scam artists.

Just since 2008, the IRS has identified 470,000 incidents of identity theft affecting more than 390,000 taxpayers. That number is truly shocking. While the IRS reports it has stopped over a billion dollars in fraudulent refund claims, there is no reliable estimate of how much it has disbursed to criminals, scam artists, and other fraudsters.

For individual taxpayers, a Social Security number is the key to unlocking and accessing the federal tax system. At one time, Social Security numbers had a sole purpose, facilitating participation in the Old Age, Survivors, and Disability Insurance Program. But in today's modern, wired world, Social Security numbers are shared with little thought almost any time a private or public entity requests a unique, exclusive number to identify and track a customer or client. In short, the keys to the tax system have been copied many times over.

It should come as no surprise, then, when our tax system is bombarded with sham tax returns that use stolen names and Social Security numbers to claim fraudulent refunds.

The ease with which scam artists can readily file electronic tax returns, the availability of prepaid debit cards and other hard-to-trace options for the delivery of tax refunds, and the low risk that criminal sanctions or penalties will be imposed, have created, in many respects, the perfect crime.

But for the victims caught in the middle of these schemes, tax-related identity theft imposes extraordinary burdens and economic hardship, as we will hear from our first panel of witnesses.

Taxpayer victims spend countless hours obtaining the necessary documents to prove who they are. Inconsistent messages and conflicting instructions from customer service agents at the IRS can worsen the situation. Innocent taxpayers whose identities have been stolen frequently find themselves in a confusing and frustrating form of bureaucratic ping pong.

Last month, following several recent reports of tax-related identity theft schemes in Florida, I asked the Treasury Inspector General for Tax Administration to launch a new investigation into this issue. That work is underway, and I look forward to his findings.

Also, I have been working with several of my colleagues to strengthen an information-sharing program to crack down on tax scams by prison inmates, which often involve stolen identities. Legislation to extend that program will be needed, and I will be working to get that done.

The purpose of our hearing is to investigate the growing problem of tax fraud through identity theft. First, we will hear from taxpayers who have fallen victim to complex, identity-related tax scams. Their stories are heart-wrenching.

The second panel, which includes the Taxpayer Advocate, the director of tax issues at the Government Accountability Office, and the Deputy IRS Commissioner, will explore the scope and magnitude of identity theft in the tax system and examine the laws, regulations, and administrative practices in place to prevent the processing of fraudulent tax returns and protect victims.

The hearing testimony will help guide the development of new legislation to crack down on tax fraud and shield victims from further hardship.

I fully expect our hearing today to lay the groundwork for Congressional action and generate novel ideas for a legislative initiative to aggressively combat the growing problem of tax-related identity theft.

**WRITTEN STATEMENT OF**

**NINA E. OLSON**

**NATIONAL TAXPAYER ADVOCATE**

**HEARING ON**

**THE SPREAD OF TAX FRAUD BY IDENTITY THEFT:**

**A THREAT TO TAXPAYERS, A DRAIN ON THE PUBLIC TREASURY**

**BEFORE THE**

**SUBCOMMITTEE ON FISCAL RESPONSIBILITY**

**AND ECONOMIC GROWTH**

**COMMITTEE ON FINANCE**

**UNITED STATES SENATE**

**MAY 25, 2011**

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

Thank you for inviting me to testify today about the subject of identity theft.<sup>1</sup> I have written extensively about the impact of identity theft on taxpayers and tax administration and have worked closely with the IRS to improve its efforts to assist taxpayers who are identity theft victims. Over the last three years, the IRS has made significant progress in this area, including adopting many of my recommendations, and it continues to engage my office as it works through new issues. Notwithstanding these efforts and the fact that the IRS has been put in the unenviable position of sorting through the aftermath of a devastating crime, it is clear that the current approach to identity theft is not working as intended.

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

1. The IRS has made a number of improvements to assist identity theft victims over the past several years.
2. Despite these changes, we are seeing unprecedented levels of identity theft casework.
3. There are several likely explanations for the increase in identity theft cases. Among them: there has been a continued increase in tax-related identity theft; there is increased public awareness of identity theft; identity thieves have become more proficient; and personal information has become more readily accessible.
4. The IRS Identity Theft Protection Specialized Unit (IPSU) is struggling to effectively manage identity theft cases.
5. The population of taxpayer accounts with an identity theft indicator has grown significantly, subjecting almost a million accounts to business rules.
6. The IRS does not track identity theft case cycle time.
7. TAS has made numerous recommendations to address tax-related identity theft. These include allowing taxpayers the option to turn off the ability to file electronically; systematically retiring expired Social Security numbers; utilizing

---

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

information reporting earlier in the filing season; notifying taxpayers of potential identity theft; and working with the Social Security Administration to keep Social Security numbers out of the public domain.

**I. The IRS Has Made a Number of Process Improvements to Assist Identity Theft Victims.**

In general, identity theft occurs in tax administration in one of two ways – when an individual intentionally uses the Social Security number (SSN) of another person to (1) file a false tax return with the intention of obtaining an unauthorized refund or (2) gain employment under false pretenses. When these types of identity theft occur, the victim often begins a journey through IRS processes and procedures that may take years to complete.

I have written about the growing problem of identity theft in tax administration for many years in my Annual Reports to Congress and in my testimony for various congressional hearings.<sup>2</sup> While it may not have happened as quickly as I would have liked, I am happy to report that the IRS has accepted many of my office's recommendations for improving identity theft procedures. At various times, I have advocated for the following improvements, each of which has been adopted in some capacity:

- Allowance of greater discretion for IRS employees to determine the true owner of an SSN in question without referring the matter to the Social Security Administration (SSA);
- Development of an electronic indicator to mark accounts of verified identity theft victims;
- Creation of an IRS identity theft affidavit form;
- Adoption of a standardized list of acceptable documents to substantiate identity theft;
- Establishment of a centralized unit to provide assistance to identity theft victims;

---

<sup>2</sup> See National Taxpayer Advocate 2009 Annual Report to Congress 307-317 (Status Update: *IRS's Identity Theft Procedures Require Fine-Tuning*); National Taxpayer Advocate 2008 Annual Report to Congress 79-94 (Most Serious Problem: *IRS Process Improvements to Assist Victims of Identity Theft*); National Taxpayer Advocate 2007 Annual Report to Congress 96-115 (Most Serious Problem: *Identity Theft Procedures*); National Taxpayer Advocate 2005 Annual Report to Congress 180-191 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-136 (Most Serious Problem: *Inconsistence Campus Procedures*); *Filing Season Update: Current IRS Issues, Hearing Before the S. Comm. on Finance*, 111th Cong. (Apr. 15, 2010) (statement of Nina E. Olson, National Taxpayer Advocate); *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance*, 110th Cong. (Apr. 10, 2008) (statement of Nina E. Olson, National Taxpayer Advocate).

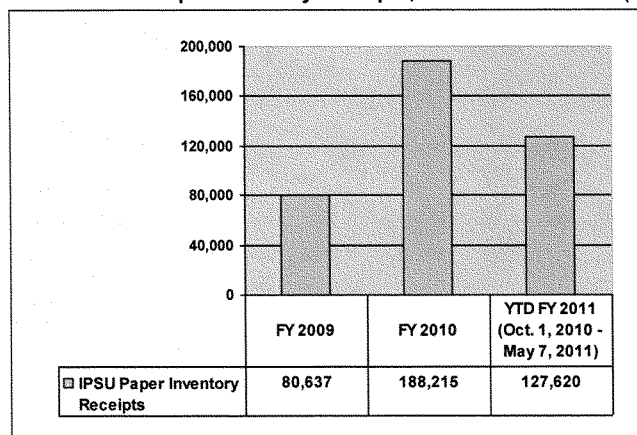
- Provision for a global account review prior to closing an identity theft victim's account to ensure that all related issues have been resolved; and
- Issuance of a PIN to verified taxpayers that would enable them to file tax returns electronically.

I can say that the IRS is in a much better position to help identity theft victims today than when I first included identity theft as a Most Serious Problem facing taxpayers in my 2005 Annual Report to Congress. However, there is still room for improvement.

## II. Despite Major Improvements, the IRS Is Seeing Unprecedented Levels of Identity Theft Casework.

Despite the sweeping changes made in the last few years, the IRS continues to struggle with identity theft. The Identity Protection Specialized Unit (IPSU), the centralized unit that helps identity theft victims, is experiencing unprecedented levels of case receipts.

**Chart 1: IPSU Paper Inventory Receipts, FY 2009 to FY 2011 (thru May 7)<sup>3</sup>**



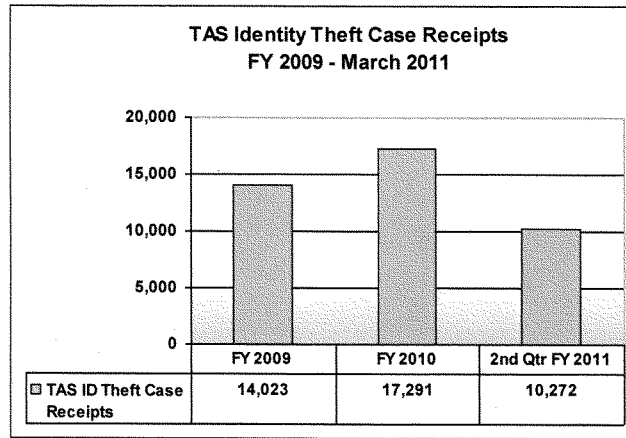
As this chart shows, identity theft cases will be substantially higher in fiscal year (FY) 2011 than they were last year if the trend through May 7 continues. Moreover, in FY 2010, the IPSU worked nearly 3,400 cases that would have otherwise been referred

<sup>3</sup> IRS, *IPSU Identity Theft Report* (May 7, 2011); IRS, *IPSU Identity Theft Report* (Oct. 2, 2010); IRS, *IPSU Identity Theft Report* (Oct. 3, 2009). This inventory includes all identity theft cases controlled by the IPSU paper unit, including self-reported non-tax-related identity theft cases, cases the IPSU monitors, and cases undergoing global account review.

to the Taxpayer Advocate Service (TAS). Through May 7, 2011, this number has already more than doubled, increasing to 7,742 cases so far this year.<sup>4</sup>

The Taxpayer Advocate Service has experienced similar increases in identity theft cases. Through the first two quarters of FY 2011, TAS has received 10,272 identity theft cases, compared to 6,427 cases during the same period in FY 2010 and 5,760 for that period in FY 2009.<sup>5</sup> This translates to a 60 percent increase in identity theft case receipts through the second quarter in FY 2011 over the same period in FY 2010, on top of an almost 12 percent increase in identity theft receipts for that period from FY 2009 to FY 2010. Accordingly, the Taxpayer Advocate Service is also feeling the impact of the IRS's inability to promptly address identity theft victims' tax issues.

**Chart 2: TAS Identity Theft Case Receipts, FY 2009 to FY 2011 (thru March 31)**



**III. There Are Multiple Likely Explanations for the Increase in Identity Theft Cases.**

While it is difficult to pinpoint exactly the reasons for the increase in IRS identity theft cases, I can share some possible explanations.

<sup>4</sup> IRS, *IPSU Identity Theft Report* (Oct. 2, 2010); IRS, *IPSU Identity Theft Report* (May 7, 2011). In addition to handling taxpayer cases that would have been designated TAS Criteria 5 – 7 (systemic burden) cases, the IPSU is responsible for identity theft monitoring, taxpayers who self-identify non-tax related identity theft, unpostable cases (*i.e.*, returns that will not be processed until it is manually reviewed), and global account reviews.

<sup>5</sup> TAS Business Performance Management System (Apr. 1, 2011).



a. *There Has Been a Continued Increase in Tax-Related Identity Theft.*

The increase of such cases in the IRS could simply reflect an overall increase in *tax-related* identity theft as opposed to other kinds of identity theft. Although the Federal Trade Commission (FTC) reports that overall identity theft complaints to its office have actually decreased for the first time since 2006,<sup>6</sup> tax return-related identity theft has increased nearly six percentage points since 2006.<sup>7</sup> The overall decline in incidents reported to the FTC may be attributable in part to the IRS's creation of its own identity theft affidavit in 2009.<sup>8</sup> Prior to 2009, the IRS required identity theft victims to obtain an identity theft affidavit from the FTC and submit it to the IRS to receive assistance.<sup>9</sup>

b. *There Is Increased Public Awareness of Identity Theft.*

The increase in identity cases may be due to increased public awareness of the issue as a result of more effective outreach. People may be checking their credit reports more frequently and may be more adept in detecting identity theft. If they see suspicious entries in their credit profile, they may contact the IRS to make sure no one has used their SSNs to file a return.

c. *Identity Thieves Have Become More Proficient.*

Criminals have become more proficient in devising schemes to steal identities. It is apparent that identity thieves are targeting populations that have no filing requirements, such as the elderly and children. Because these individuals often do not file tax returns, it can take years to discover that an identity thief has usurped their SSN. One of the more sinister schemes involves the misuse of a deceased taxpayer's SSN to obtain fraudulent refunds. Thus far in 2011, the IRS has received 660,000 decedent returns.<sup>10</sup> Effective April 17, 2011, the IRS instituted business rules to filter out some of these "decedent scheme" returns; within one month, it stopped 42,441 decedent-related returns claiming questionable refunds estimated at \$194 million.<sup>11</sup> The IRS estimates that an additional 221,000 returns claiming \$700 million in refunds would have been stopped had the business rules been in place at the beginning of the filing season.<sup>12</sup>

<sup>6</sup> See Federal Trade Commission, *Consumer Sentinel Data Book 5* (Feb. 2010), available at <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf>.

<sup>7</sup> See Federal Trade Commission, *Consumer Sentinel Data Book 3* (Feb. 2009), available at <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>.

<sup>8</sup> See Form 14039, *Identity Theft Affidavit* (rev. Mar. 2010), available at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>.

<sup>9</sup> See Internal Revenue Manual (IRM) 21.6.2.4.4.3(1) (Oct. 1, 2007) (superseded).

<sup>10</sup> TAS notes from IRS Decedent Schemes conference call (Apr. 25, 2011).

<sup>11</sup> TAS notes from IRS Decedent Schemes conference call (May 12, 2011, and Apr. 21, 2011).

<sup>12</sup> TAS notes from IRS Decedent Schemes conference call (May 12, 2011).

d. *Personal Information Has Become Readily-Accessible.*

There has been a proliferation of readily-accessible SSNs and other personal information. As I discuss later in the testimony, the Social Security Administration is required to make available certain information about deceased individuals, including their name and SSN. Anyone who conducts a quick web search can find a number of sites that provide this information, often free of charge.

**IV. The IPSU Is Struggling to Effectively Manage Identity Theft Cases.**

I believe the establishment of the IPSU may have created a false sense of well-being in the IRS with respect to identity theft issues. Commissioner Shulman, in his written response to Senator Baucus's follow-up questions stemming from an April 2008 hearing, described the unit as providing "a central point of contact for the resolution of tax issues caused by identity theft." His response further stated: "This unit will provide end-to-end case resolution. Victims will be able to communicate with one customer service representative to have their questions answered and issues resolved quickly and efficiently."<sup>13</sup> While this description fits the model for which my office advocated, it does not accurately reflect how the IPSU works in practice.

The reality is that the IPSU does not "work" an identity theft case from beginning to end; it simply "monitors" a victim's account every 60 days.<sup>14</sup> Whether because of resource constraints or a policy decision, the IPSU is not staffed to handle cases itself. Rather, it attempts to coordinate with up to 16 different functions within the IRS to obtain the necessary relief for the identity theft victim. The IPSU utilizes Identity Theft Assistance Requests (ITARs) to coordinate with other IRS functions.<sup>15</sup>

While the procedures call for the receiving functions to treat ITARs as a priority, there are no "teeth" to ensure this priority designation is followed. Unlike TAS, which can issue a Taxpayer Assistance Order<sup>16</sup> if another IRS organization does not respond to an Operations Assistance Request,<sup>17</sup> the IPSU procedures do not specify any consequences for functions that are unresponsive to an ITAR.

---

<sup>13</sup> *Identity Theft: Who's Got Your Number, Hearing Before the S. Comm. on Finance, 110th Cong. (Apr. 10, 2008)* (response of IRS Commissioner Douglas H. Shulman to questions from Chairman Max Baucus), available at <http://finance.senate.gov/hearings/hearing/download/?id=f989b16e-5da3-452d-9675-b75d796fe2b4>.

<sup>14</sup> IRM 21.9.2.4.2(4) (Oct. 1, 2010).

<sup>15</sup> IRM 21.9.2.10.1 (Oct. 1, 2010).

<sup>16</sup> See IRC § 7811.

<sup>17</sup> An Operations Assistance Request (Form 12412) is the form that TAS employees use when requesting that the IRS complete an action on a TAS case when TAS lacks the authority to take that action.

To illustrate the IPSU's role in the identity theft resolution process, the following example describes the multiple steps necessary to assist a hypothetical identity theft victim who calls the IRS:

1. Taxpayer receives a notice that he has underreported his income for tax year 2008. He calls the number on the notice and learns that the income in question is from a Florida-based company.
2. Because the taxpayer lives in California and has never worked for this company, he suspects he might be a victim of identity theft. He locates the toll-free number for the IPSU telephone unit and explains the situation to the Customer Service Representative (CSR).
3. The IPSU representative verifies that the taxpayer has an open case in the IRS Automated Underreporter (AUR) function.<sup>18</sup> The CSR asks the taxpayer to send documentation substantiating the identity theft to the address on the notice, along with an explanation of why the tax is not owed.<sup>19</sup>
4. The CSR advises the taxpayer that there will be processing delays while the situation is resolved and that he may receive correspondence requesting additional information.<sup>20</sup>
5. The CSR advises the taxpayer that the IPSU will monitor the case and sends a letter to the taxpayer providing him with the name of the person who will be monitoring the account.
6. The IPSU CSR completes the form for monitoring, faxes the monitoring sheet for scanning, makes an account entry documenting the conversation, and refers the case to the IPSU paper unit.<sup>21</sup>
7. The CSR in the IPSU paper unit sends an Identity Theft Assistance Request to the IRS's AUR function to resolve the taxpayer's problem and make the appropriate account adjustments.
8. The IPSU CSR then waits for the account to be resolved and contacts the ID Theft Functional Liaison by e-mail if the function does not contact the taxpayer every 60 days.<sup>22</sup>

---

<sup>18</sup> The AUR Program is a compliance initiative that uses third-party information returns (such as Forms W-2 and Forms 1099) to identify income that was not reported on tax returns.

<sup>19</sup> IRM 21.9.2.3.2(1) (June 11, 2010).

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> IRM 21.9.2.4.2(4) (Oct. 1, 2010).

9. The AUR function eventually agrees that the wages should be removed from the California taxpayer's account, and an identity theft indicator will be applied to his account. For the next three years, any tax return filed with his SSN will have to pass through "business rules," a series of filters designed to kick out questionable returns, before being processed.<sup>23</sup>
10. The following year, the taxpayer is mailed a six-digit Identity Theft PIN.<sup>24</sup> He can use this one-time PIN in conjunction with his paper or electronic return to bypass the business rules. If anyone files a tax return using his SSN without this PIN, that return will be subject to the business rules.

These procedures are a vast improvement over IRS processes in effect as recently as three years ago. However, without adequate staffing in the IPSU and the related functions that make the adjustments on identity theft victims' accounts or that deal with the returns filed by the identity thieves, the benefits of these process improvements will be minimal for both taxpayers and the IRS.

**V. The Population of Taxpayer Accounts with an Identity Theft Indicator Has Grown Significantly, Subjecting Almost One Million Accounts to Business Rules.**

The IRS may have become a victim of its own success. Since the IRS started using an electronic indicator in 2009 to flag an account as being potentially compromised, it has marked over 980,000 accounts impacting over 600,000 taxpayers.<sup>25</sup> Each tax return associated with an account marked with an indicator must go through business rules. If a return does not pass these business rules, it will be considered "unpostable" – meaning that it will not be processed until it is manually reviewed, which means longer processing time and refund delays.<sup>26</sup>

Sometimes, it is easy to tell if the wages do not belong to the taxpayer. For example, if the taxpayer is a five-year-old, it is fairly obvious that the income is probably not his. However, if the Unpostable unit cannot quickly determine whether the SSN owner or an unauthorized user filed the return, it will refer the case to the IPSU to conduct research on various databases.<sup>27</sup>

<sup>23</sup> See IRM 10.5.3.2.2.1.1 (Dec. 10, 2010); IRS Notice CP 01.

<sup>24</sup> IRS Notice CP 01A.

<sup>25</sup> See IRS Office of Privacy, Information Protection, and Data Security (PIPDS) Incident Tracking Statistics Reports for calendar years ending 2009 and 2010 and for the period of January 1, 2011, through March 31, 2011.

<sup>26</sup> IRM 21.9.2.5 (Mar. 30, 2010).

<sup>27</sup> IRM 21.9.2.5(2) (Mar. 30, 2010).

If the IPSU determines that the return belongs to the true taxpayer, it instructs the Unpostable unit to process the return. If the IPSU is unable to make a determination, it sends a letter to the "good" taxpayer's address of record seeking additional information and then suspends the case for 45 days.<sup>28</sup>

#### **VI. The IRS Does Not Track Identity Theft Case Cycle Time.**

Although the IRS purports to treat ITARs as a "priority," it allows 60 days for the IPSU to follow up with a function to see if the requested action was taken. It is telling that the IPSU does not consider a case "aged" until after 180 days have passed. Unsurprisingly, identity theft cases controlled by the IPSU routinely languish for months without resolution. However, the IRS does not currently track any data about the cycle time for identity theft cases.

The IRS Office of Privacy, Information Protection, and Data Security (PIPDS) recognizes the need for a measure that tracks the length of time it takes the IRS to resolve a taxpayer's identity theft issue. PIPDS has engaged in dialogue with the various functions and with TAS to develop such a measure, but it has yet to implement any meaningful cycle time tracking and analysis. Without the ability to capture this data, it is difficult, if not impossible, for the IRS to determine whether identity theft cases are being treated with the urgency it intends.

#### **VII. Recommendations**

Employees from the Wage and Investment division and TAS have formed a team to review a sample of identity theft cases closed between January 1, 2011, and March 31, 2011. It will take a while to review the cases, but the goal is to identify both the underlying source of casework (e.g., Automated Underreporter, Examination, Collection, etc.) and any procedural gaps that contribute to increased receipts. This team expects to report its findings in July of this year.

In advance of these findings, we offer several recommendations that will improve the IRS's approach to identity theft, better protect victims, and prevent revenue loss.

- a. *Allow taxpayers the option to turn off the ability to file electronically.*

The IRS should allow taxpayers to turn off the ability to file electronically. While there are undoubtedly many benefits to e-filing, we must recognize that it also provides more opportunity for identity thieves to "ping" the system with multiple attempts to file fraudulent returns at little cost. For taxpayers (including parents of minor children) who are victims of identity theft and thus do not wish to e-file, the IRS should allow them to disable e-filing with their SSNs.

---

<sup>28</sup> IRM 21.9.2.5(11) (Mar. 30, 2010).

*b. Utilize information reporting earlier in the filing season.*

The IRS should explore ways to utilize information reporting earlier in the filing season. One of the tools it uses to verify wage withholding on questionable returns is the Information Returns Processing Transcript Requests (IRPTR) command code.<sup>29</sup> However, the IRPTR is not available until mid-May. If this resource were available even a month earlier, it would alleviate a great deal of burden for the thousands of taxpayers whose refunds are held up while the IRS undergoes its wage withholding verification process. I have previously recommended that the IRS study how to receive and utilize real-time information reporting data,<sup>30</sup> and I plan to include a more comprehensive analysis of this issue in my 2011 Annual Report to Congress.

*c. Work with the Social Security Administration to keep Social Security numbers out of the public domain.*

In 1980, the Social Security Administration created a Death Master File (DMF) as a result of a consent judgment reached in a Freedom of Information Act lawsuit brought by a private citizen. In essence, the individual had argued that SSN files are government records and that a deceased individual does not retain a privacy interest in his SSN and related information.

The SSA now makes public significant personal information upon a person's death, including the decedent's full name; SSN; date of birth; date of death; and the county, state, and zip code of the last address on record. This information is now regularly obtained and used by government agencies, credit reporting agencies, financial firms, and genealogists. Unfortunately, it is also used by identity thieves to commit tax fraud.

For tax filing purposes, the SSN of an individual may be used even after his or her death. For example, the surviving spouse of an individual who died in January of 2011 generally may file a joint return for 2011, which would require the decedent's SSN. The due date for the 2011 return, with an extension, would be October 15, 2012 – 20 months after the death occurred. For that reason, the IRS cannot immediately block the use of the decedent's SSN. In the interim, however, identity thieves may troll the DMF to obtain the decedent's SSN and then use it to file a fraudulent return claiming a refund.

A similar type of tax fraud arises with respect to dependency claims for minor children. In one recent TAS case that the taxpayers authorized me to discuss publicly, the taxpayers (husband and wife) had a child who died of sudden infant death syndrome

<sup>29</sup> The IRPTR command code allows IRS employees to request either online or hardcopy Information Returns Processing transcripts from the Information Returns Master File. IRM 2.3.35.1 (Aug. 1, 2003).

<sup>30</sup> National Taxpayer Advocate 2009 Annual Report to Congress 338-345 (Legislative Recommendation: *Direct the Treasury Department to Develop a Plan to Reverse the "Pay Refunds First, Verify Eligibility Later" Approach to Tax Return Processing*).

(SIDS) in 2009.<sup>31</sup> By law, the couple was entitled to claim the child as a dependent on their 2009 tax return. But by the time they filed their 2009 tax return in 2010, an identity thief had already filed a return claiming their child, so their claim was initially denied.

While I understand the competing policy concerns, the government's provision of all of this information in unredacted form aids and abets identity theft and tax fraud, and it is frankly appalling. It provides identity thieves with the opportunity to steal potentially billions of dollars of federal funds through fraud. It also has the effect of imposing untold burden on the innocent victims of identity theft, who often must spend hundreds of hours to prove who they are and straighten out their finances. Not insignificantly, there is also a compelling personal and emotional consequence to all this. One can only imagine how a taxpayer must feel first to lose a spouse or a child and then find out that his sense of privacy was violated by routine government release of information that allowed someone else to profit from the death and requires him to prove to an initially skeptical government agency that his spouse or child was indeed his relative and not the identity thief's.

I urge Congress and the SSA to address this problem immediately. The most comprehensive solution would be for Congress to pass legislation for the SSA similar to Internal Revenue Code (IRC) § 6103, which prohibits the IRS from releasing taxpayer return information (including SSNs and addresses), absent explicit statutory exceptions or taxpayer consent. (If Congress proceeds along these lines, I recommend that it create a statutory exception for sharing the DMF with the IRS, so the IRS may screen for and ultimately "retire" SSNs of deceased taxpayers from its own databases.) A less comprehensive but quicker solution is for the SSA simply to truncate SSNs in the DMF and make public only the last four digits of the number.<sup>32</sup> If that requires the SSA to ask the court to modify its 1980 consent judgment, it should do so.

*d. Systematically retire expired SSNs.*

The IRS should systematically retire expired SSNs. The IRS should use the DMF database provided by the SSA to retire the SSNs of decedents, perhaps three years after their death (which should allow sufficient time for the administrator of the decedent's estate to wind down his or her affairs). It is absolutely vital that the SSA continue to provide the IRS with access to the DMF database. Without this resource, the IRS will be unable to systemically and proactively identify questionable returns. Early access to this database will enable the IRS to better proactively and systemically screen out improper returns as they are filed.

---

<sup>31</sup> Consent to Disclosure of Tax Return Information (signed May 20, 2011).

<sup>32</sup> In response to an audit conducted by the Office of the Inspector General, the SSA replied "We are considering limiting the information included in the DMF version sold to the public to the absolute minimum required. We will also explore alternatives to the use of the full SSN." Social Security Administration Office of Inspector General, Audit Report A-06-08-18042, *Personally Identifiable Information Made Available to the General Public via the Death Master File D-4* (June 2008).

e. *Notify taxpayers of potential identity theft.*

In my 2007 Annual Report to Congress, I recommended that the IRS notify victims if their personal information has been misused.<sup>33</sup> In its response, the IRS committed to work with TAS to develop “a notification process for taxpayers who have been identified by the IRS as identity theft victims related to a refund scheme.” While it would do little to stop identity theft, such a letter would alert innocent taxpayers that their personal information may have been compromised. It is my understanding that the IRS received clearance from the IRS Office of Chief Counsel that such a letter, notifying a taxpayer that his or her SSN may have been used by an identity thief, does not violate IRC § 6103 and that draft language has been developed. Yet for reasons unknown to me, the IRS still has not begun to issue such a letter. I urge the IRS to implement its commitment to sending out this notification expeditiously.

### VIII. Conclusion

Next month, the IRS Office of Privacy, Information Protection, and Data Security will host a cross-functional Identity Theft Assessment and Action Group kickoff meeting to engage in a servicewide assessment of the identity theft program. The Taxpayer Advocate Service will participate in this working group and will continue to provide assistance and recommendations regarding IRS improvements to its processes to meet taxpayer expectations.

I urge the IRS to re-think its identity theft victim assistance strategy. In 2009, I expressed my desire that the IPSU be structured after the TAS model, where a case advocate works with a taxpayer from beginning to end, ensuring that all of the taxpayer’s issues are resolved in a timely manner.<sup>34</sup> As discussed above, the IRS has used a different approach with the IPSU. The IPSU refers identity theft cases to various functions, but it does not have the tools to ensure that these cases receive priority treatment.

I firmly believe that the IRS needs a specialized unit that works solely on identity theft cases from start to finish. Identity theft cases are too complex to be worked any other way. This centralized unit should be staffed appropriately, both in terms of numbers and experience, to deal with the increasingly complex identity theft cases we are seeing. Due to the large volume of identity theft cases, the IRS may need to centralize such a unit in two or more of its campuses. I realize that such an overhaul of the system will require a substantial investment of resources, and I ask Congress to address this need when it establishes the IRS’s budget.

---

<sup>33</sup> National Taxpayer Advocate 2007 Annual Report to Congress 112 (Most Serious Problem: *Identity Theft Procedures*).

<sup>34</sup> National Taxpayer Advocate 2009 Annual Report to Congress 316 (Status Update: *IRS’s Identity Theft Procedures Require Fine-Tuning*).



PREPARED STATEMENT OF  
BETH TUCKER  
IRS DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT  
BEFORE  
SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC  
GROWTH  
SENATE FINANCE COMMITTEE  
ON  
IDENTITY THEFT  
MAY 25, 2011

**Introduction**

Chairman Nelson, Ranking Member Crapo, and Members of the Subcommittee, thank you for the opportunity to appear this morning 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 11<sup>th</sup> 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 Deputy 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](http://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.

**Senate Committee on Finance**  
**Subcommittee on Fiscal Responsibility and Economic Growth**  
**May 25, 2011**

**Statement of a Victim of Identity Theft**

Dear Chairman and Senators of the Finance Committee, thank you for the opportunity to bring light to my recent experience with the Internal Revenue Service.

On December 1st, around 2:30 p.m., I stopped at a gas station in Miami, Florida, to get gas. As I am pumping gas, my handbag is stolen from my car, from the opposite side of where I was standing. I, immediately, report the case to the police and to the gas station owner. They looked through their video surveillance and found the video of my handbag being stolen and a good, but not perfect, image of the young afro-American man who stole my bag. The gas station owner told me, and the police, that the man in question lives in the neighborhood and shops there on a daily basis. Basically she tells us that she recognizes this man.

As I start calling credit card companies, banks, etc., to close and protect my accounts, I find out that the criminal had already used my ATM card for gas in another gas station, on Biscayne Blvd., where they could possibly have another video of him, given that I had the exact time of the transaction to provide them with.

In my handbag, there were my house keys, mail box keys, elevator card, wallet with driver's license and home address, mine and my daughter's social security numbers, my daughter's school security card and the information on her school, bank cards, credit cards, department store cards, health insurance cards, a video camera with videos of my family, my life, my home and my daughter, as well as a digital camera with very detailed pictures of my life, home, and daughter, apart from other personal and valuable items as well as the handbag itself and money.

Very concerned about my daughter's safety and my own, even after taking all possible precautions, from that day on, I started calling the police to give them updates on numerous fraud attempts to my accounts and to ask for updates on the investigation. Till almost the end of December, there was no detective assigned to my case due to the vague report written by the police agent at the crime scene (unless a certain amount is lost in property and money, the police don't even open a case). With the report now corrected, a detective was assigned to my case.

The day I went to the police station to meet with Detective Alce and review my report, I was informed by another agent in the station, that I should be prepared to face fraud on my upcoming taxes, and every year after that. The officer who was alerting me to the problem had also been robbed, a victim of Identity Theft, and her tax return fraud issues persisted for many years.

During my meeting with Detective Alce, I reported a couple of important leads as per an attempt of fraud on my FPL account, when an additional address was added to my existing electricity account—an address which, at that point, I had in my hands. Also, Bloomingdale's department store had informed me that someone tried to break into my account information, and a landline

number was recorded in its phone system and they would happily convey that number to the police. Moreover, I found out that when Detective Alce went to check on the video surveillance on both gas stations mentioned above, the videos were no longer available.

We were then entering January 2011. My concern was to avoid a more serious crime. I was, and still am, very concerned that the abundance of information in a criminal's hands could come back to hurt my home, my daughter, or myself; not to mention, my so far pristine credit, and a criminal with access to my financial information, continuously stealing money from me.

On my own, I then contacted Social Security in the hope of changing my own and my daughter's SSN. I contacted all credit agencies to freeze my SSN and open, at least a file, under my daughter's number, being that she is only 2½ years old. I hired Lifelock for both myself and my daughter, I closed accounts, blocked bank accounts and contacted the IRS to alert them of my situation as a victim of Identity Theft and to place an alert regarding my 2010 tax return.

IRS, on its website, has a page on Identity Theft problems and an explanation of what to do to prevent fraud. They request proof of identity and an affidavit stating the nature of the problem and the year in question. By March 11th, I sent out all the required documentation and also called the IRS pleading for them to put an alert on both my daughter's and my SSN.

By the beginning of February, I received my W-2 and hurried to get all my information to my accountant who has filed my taxes for many years.

On February 9th, my accountant filed my taxes electronically, only to receive a message back stating that there was already a tax return filed under my SSN, and therefore it was not possible to file any other return. I immediately called the IRS to report what I clearly understood as a fraud and to ask for help on correcting the situation. The response I got back was that it was going to be a long wait, and that I had to send my original tax file by mail, along with a new affidavit and proof of identity.

This case was a clear fraud. Someone in Miami had filed taxes under my SSN and had already received a check. I found out through the agent I was speaking to what address the IRS used to send this tax return check. Nobody could tell me why the IRS had filed a tax return under an SSN that had been flagged, without making at least one phone call to check the authenticity of it. Nobody could explain why the affidavit I previously sent didn't serve its purpose.

As a single mother, who is very organized, who has never delayed a bill payment, and has always followed all rules and regulations, I was in shock and extremely concerned about the tax return I was due to receive and I was very much counting on.

I immediately sent all necessary documents to the IRS. Along with my personal effort to deal with the IRS, I was hoping to find help from others to prevent my case from falling on a forgotten pile of cases to solve. Senator Nelson's office was open to listen to my case and to help me plead with the IRS for a prompt solution and correction of the fraud I had been a victim of unnecessarily.

By the end of February, beginning of March, I received a call from the IRS Advocates representative who was going to set my case with one of their representatives. She checked all the information necessary and heard my concern of such a long wait to receive my return and the fact that, as a single mother and a victim of Identity Theft, I had my hands full and needed help. She told me that she had also raised her kids alone and that she knew how difficult everything was. Then, she told me she was going to change the code on my case to expedite it. By March 22nd, the assigned advocate called me requesting new copies of my tax file documents and told me to wait for her updates.

On April 7th I received my tax return check for \$4,299.00, and my case was finally closed. I then thanked my tax advocate and asked her for information on a supposed PIN number that could be assigned by the IRS to ID Theft victims to avoid future frauds. She told me she did not know about it but offered to check into it. A couple of days later, she got back to me with information on a PIN that is actually designed for those who will submit their taxes electronically.

To my surprise, on April 15th, I received a letter from the IRS documenting that another individual had filed a tax return under my SSN. They also told me I could be a victim of Identity Theft and that they have placed an identity theft indicator on my tax account for 3 years. I can only hope the IRS will, in fact, mind their own alert and check any information received under my SSN. So far, nothing has been done to prevent fraud on my daughter's SSN, despite an affidavit sent to the IRS under her name and SSN as well.

I also looked for help with the Secret Service, as I was told that they are the organization responsible to investigate Federal Crimes such as Tax Fraud. The officer in charge told me that even if I had leads to offer, including the address used to receive the IRS check, they could not start a case until formally informed about the case by the IRS. Who knows how long this will take and if the leads would still serve any purpose by then.

I was born and raised in Brazil, visiting the U.S. often for vacations. It was clear to me that the U.S. was a country that functioned efficiently, a country where people had a stable system to count on. I have been here for 13 years and after studying and working here, also having my daughter here, this is home for me. It's really a pity to finally realize that after I was robbed, every step of the system has failed in solving my case or to protect myself and my family from ID Theft.

From police leads that were never followed, a criminal who lives around the corner from me and was never caught, an SSN that has become a nightmare in my life, banks that still cannot protect client's identity, credit cards that are still relying on SSN as master proof of identity, taxpayers that end up paying for a criminal to get someone else's tax return, and the Secret Service who cannot investigate a Federal Crime, as the fraud on my tax return, until the IRS is finally ready to send them an official file on the case, nothing was really in place to protect the honest taxpayer from a fast growing crime such as Identity Theft. Good for the criminals, who are taking full advantage of the failed system to steal money from hardworking people.

United States Government Accountability Office

---

**GAO**

Testimony  
Before the Subcommittee on Fiscal  
Responsibility and Economic Growth,  
Committee on Finance, U.S. Senate

---

For Release on Delivery  
Expected at 2:00 p.m. EDT  
Wednesday, May 25, 2011

## TAXES AND IDENTITY THEFT

### Status of IRS Initiatives to Help Victimized Taxpayers

Statement of James R. White, Director  
Strategic Issues



GAO  
Accountability • Integrity • Reliability

## Highlights

Highlights of GAO-11-674T, testimony before the Subcommittee on Fiscal Responsibility and Economic Growth, Committee on Finance, U.S. Senate

### 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-11-674T or key components. For more information, contact James R. White at (202) 512-9110 or whitej@gao.gov.

May 25, 2011

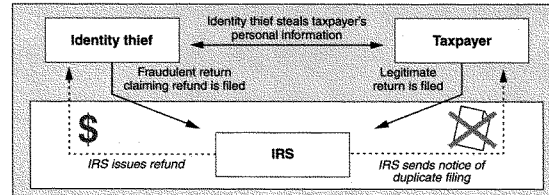
## TAXES AND IDENTITY THEFT

### Status of IRS Initiatives to Help Victimized Taxpayers

#### 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 Nelson, Ranking Member Crapo, 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.<sup>1</sup> 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 talked with agency officials about data quality-control procedures, reviewed relevant documentation, and tested data for obvious errors. We determined that the data were sufficiently reliable for the purposes of this report.

---

<sup>1</sup>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.

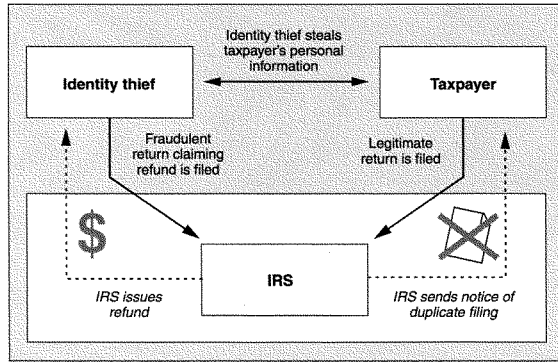
---

### **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

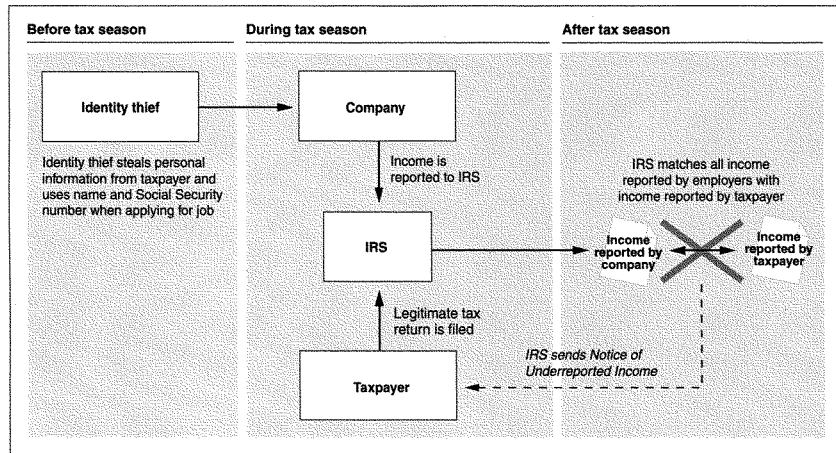


Source: GAO.

**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.<sup>2</sup> 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.<sup>3</sup> 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

---

<sup>2</sup>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.

<sup>3</sup>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.<sup>4</sup> 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.<sup>5</sup>

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.

---

<sup>4</sup>GAO-09-882.

<sup>5</sup>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.<sup>6</sup> 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.<sup>7</sup> 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, 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.<sup>8</sup> 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.

---

<sup>6</sup>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.

<sup>7</sup>GAO-09-882.

<sup>8</sup>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.<sup>8</sup> 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.

---

<sup>8</sup>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,<sup>10</sup> 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.<sup>11</sup> IRS would also have to improve its automated processing systems; IRS's current Customer Account Data Engine (CADE 2) effort is one key step.<sup>12</sup> 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.

---

<sup>10</sup>GAO-09-882.

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

<sup>12</sup>GAO-11-168.



---

---

Chairman Nelson, Ranking Member Crapo, 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](mailto: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](mailto: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](mailto: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](http://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](http://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](http://www.ftc.gov/idtheft)). The FTC also produces publications on identity theft, including *Take Charge: Fighting Back*

---

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

---

*Against Identity Theft.*<sup>1</sup> 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.

---

<sup>1</sup>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/idtheft04.htm> (accessed May 11, 2011).



## COMMUNICATION

---

**Statement by Robert E. Ellingson, Sisseton, SD**

**May 25, 2011**

### **The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, a Drain on the Public Treasury**

An ideal means for preventing the problem of tax fraud by identity theft is found in U.S. Patent No. 7,240,363 entitled *System and Method for Thwarting Identity Theft and Other Identity Misrepresentations*.

A possible implementation suggested by the patent would begin with the Internal Revenue Service (IRS) creating a new form. A taxpayer who chooses to prevent the nuisance of being a tax-fraud identity theft victim would obtain the form. The form is a request to the IRS to require identity verifiers (described below) before processing forms containing that individual's Social Security Number (SSN). The individual would send the IRS the form, photocopies of the individual's state-issued driver license or identification card, a utility bill, and a checking account or credit card statement. After the IRS receives the form and determines that the photocopied information is authentic, the IRS would mail the taxpayer the identity verifiers. The identity verifiers could be a set of 25 one-time-use passwords, each password consisting of a 14-digit apparently random number. Each of the 25 passwords sent to that taxpayer would be different.

Afterwards, when that taxpayer submits a form like a 1040 or a change of address to the IRS, the taxpayer must include one of the 14-digit passwords on the form and must cross that password off the taxpayer's list since the password can be used only once. Receiving the form, the IRS determines whether or not the SSN requires an identity verifier (one-time-use password). If the SSN does require an identity verifier, the IRS verifies that the form contains one of the taxpayer's identity verifiers that has not been used before. If a valid identity verifier has been presented, the IRS processes the form. Otherwise the IRS rejects the form as probably having been submitted by an identity thief.

In order to prevent hackers from electronically sending an avalanche of forms in hopes of eventually submitting a valid identity verifier, if a form is submitted electronically with a valid identity verifier, the taxpayer could be asked to wait a short time, perhaps 90 seconds, before submitting an additional identity verifier from the set of unused identity verifiers. Because each identity verifier can be used only once, the first one submitted would be marked as used and invalid for subsequent attempts if the second one submitted was found to be invalid by the IRS.

The patent referenced above contains implementation details.

