

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

**INTRODUCTION AND SUMMARY**

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

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

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

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

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

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

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

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

## **PREVENTING FRAUD**

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

### ***Stopping the Refund at the Door – Enhanced Return Processing***

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

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

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

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

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

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

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

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

## ***Criminal Investigation Work***

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

In response to the growing threat that identity theft poses to tax administration, IRS established the Identity Theft Clearinghouse (ITC), a specialized unit within CI that became operational in January 2012, to work on identity theft leads. The ITC receives all refund fraud-related identity theft leads from CI field offices. The ITC's primary responsibility is to develop and refer identity theft schemes to the field offices, facilitate discussions between field offices with multi-jurisdictional issues, and provide support to ongoing criminal investigations involving identity theft.

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

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

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

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

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

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

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

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

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

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

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

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

## **ASSISTING TAXPAYERS**

### ***Improving our Processes***

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

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

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

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

### ***Employee Training***



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

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

### ***Taxpayer Outreach and Education***

The IRS continues to undertake outreach initiatives to provide taxpayers, return preparers, and other stakeholders with the information they need to prevent tax-related identity theft and, when identity theft does occur, to resolve issues as quickly and efficiently as possible. As part of our outreach efforts, we overhauled and updated the identity protection training provided to tax practitioners at our annual Nationwide Tax Forums in 2011 and again in 2012. These annual events, held in several cities around the country, draw more than 16,000 practitioners, who attend to learn about key tax laws and issues. In addition, we met with practitioners to discuss the IP PIN program, the expansion of the program, and the modified procedures, forms, and notices associated with the program. We are also working closely with software developers to ensure that instructions regarding the use of an IP PIN are included in their products.

We have a far-reaching communications effort that uses both traditional and social media channels to relay information on identity protection issues. As part of this effort, we have produced new identity theft awareness videos for the IRS YouTube channel in English, Spanish, and American Sign Language, and we distributed identity protection information through IRS Twitter feeds and podcasts. We continue to update the identity theft information provided on the IRS.gov website. This includes emerging trends in identity theft along with fraud schemes, phishing sites, and prevention strategies. We also added a direct link to our Identity Theft page, to make it easier for taxpayers who visit IRS.gov to locate this information. We have issued a number of news releases and tax tips to help taxpayers and to highlight our continuing enforcement efforts. We plan to continue this sweeping communication effort in the upcoming filing season and beyond.

## **CONCLUSION**

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