**WRITTEN TESTIMONY OF**
**STEVEN T. MILLER**
**ACTING COMMISSIONER**
**INTERNAL REVENUE SERVICE**
**BEFORE THE**
**SENATE FINANCE COMMITTEE**
**ON TAX FRAUD AND TAX IDENTITY THEFT: MOVING FORWARD WITH SOLUTIONS**
**APRIL 16, 2013**

## INTRODUCTION AND SUMMARY

Chairman Baucus, Ranking Member Hatch and members of the Committee, thank you for the opportunity to update you on the actions we are taking at the IRS to combat refund fraud and help victims of identity theft.

Refund fraud caused by identity theft is one of the biggest challenges facing the IRS today, and the harm it inflicts on innocent taxpayers is a problem we take very seriously. The IRS has a comprehensive identity theft strategy focusing on preventing refund fraud, investigating these crimes and assisting taxpayers victimized by identity theft.

The agency's work on identity theft and refund fraud continues to grow, touching nearly every part of the organization. For the 2013 filing season, the IRS has expanded these efforts to better protect taxpayers and help victims. More than 3,000 IRS employees are currently working on identity theft – more than double the number at the start of the previous filing season. We have also trained 35,000 employees who work with taxpayers to recognize identity theft and help victims. Since the beginning of 2013, the IRS has worked with victims to resolve more than 200,000 cases.

Our fraud detection efforts have increased as well. We expanded the number and quality of our identity theft screening filters, and we have suspended or rejected more than 2 million suspicious returns so far this filing season. The number of identity theft investigations by our Criminal Investigation (CI) division continues to rise, with more than 800 investigations opened so far this fiscal year. A more detailed description of all of our initiatives can be found later in the testimony.

Barriers to further progress do exist, however. One is the sheer volume and complexity of these crimes, as identity thieves continue creating new ways of stealing personal information and using it for their gain. Another is the need to further upgrade our technology in order to implement improvements such as more sophisticated filters and better taxpayer authentication procedures.

Yet another barrier to further progress is the difficult budget environment. The work we are already doing on refund fraud and identity theft involves a difficult balance of resources and staffing at a time when our budget has been reduced by $1 billion over the last two years. We will continue to dedicate staff to resolving identity theft cases,

even at the cost of having fewer people on our toll-free taxpayer service line or on our automated collection program that help us collect past due taxes.

As I describe for you in greater detail our efforts to combat fraud, I urge you to remember 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 IRS spent roughly $328 million on refund fraud and identity theft efforts in FY 2012.

The Administration's Fiscal Year (FY) 2014 Budget request provides $101 million to support IRS efforts to prevent identity theft-related refund fraud, protect taxpayers' identities, and assist victims of identity theft, and enhance the revenue protection strategy implemented in FY 2013. The funding level proposed will permit the hiring of more than 800 additional full-time employees dedicated to identity theft work. The administration's budget request also provides $18.3 million to support continued implementation of the Return Preparer Program, the goal of which is to increase competency levels of tax return preparers. This program complements the IRS' efforts on refund fraud and identity theft, given that these crimes often involve individuals who prepare tax returns on behalf of others to obtain fraudulent refunds.

The budget request also includes several important proposals needed to help us improve our efforts to stop refund fraud caused by identity theft. The Administration proposes to:

- Expand IRS access to information in the National Directory of New Hires for general tax administration purposes, including data matching and verification of taxpayer claims during processing;
- Restrict access to the Death Master File (DMF) to those users who legitimately need the information for fraud prevention purposes and to delay the release of the DMF for three years to all other users. This change would make it more difficult for identity thieves to obtain identifying information of deceased persons in order to file fraudulent returns;
- Grant the IRS the authority to require or permit truncated social security numbers on W-2 forms that employers send to employees, to reduce the risk that the information could be stolen from a paper payee statement by identity thieves;
- Add a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft; and
- Add the tax-related offenses in Title 18 and the criminal tax offenses in Title 26 to the list of predicate offenses contained in the Aggravated Identity Theft Statute under federal law.

**STOPPING THE REFUND AT THE DOOR – ENHANCED RETURN PROCESSING**

During FY 2012, the IRS protected $20 billion of fraudulent refunds, including those related to identity theft, compared with $14 billion in 2011. The IRS stopped 5 million suspicious returns in 2012 – up from 3 million suspicious returns stopped in 2011. Of the 2 million suspicious returns suspended or rejected so far this filing season, more than 400,000 were rejected at the point of filing, even before they entered IRS processing systems. The remaining returns generally require further review to determine whether the filer is legitimate. Because these returns require time to review, most are still in open inventory at this time. To date, we have stopped more than 350,000 refunds determined to be fraudulent, worth more than $2.5 billion. The IRS is committed to improving its multi-faceted approach to blocking these fraudulent refund claims, and we strive to operate in such a way that false returns are screened out at the earliest possible stage.

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.

In 2011, 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 enhanced our programming to increase efficiency, and expanded the IP PIN program to more than 770,000 taxpayers.

Over the last two fiscal years 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 built on our overall refund fraud detection program, which already identified a significant number of identity theft cases besides those identified by the new filters. We have added even more identity theft filters for the 2013 filing season, including 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 are accelerating 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. Once we confirm the fraud, we lock the accounts of these individuals so that no further misuse will occur. We also routinely lock accounts of deceased taxpayers once they no longer have a filing requirement. To date, we have locked more than 9 million accounts. As noted above, the Administration is proposing a 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 FY 2011. 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. Although the authority allowing us to share return information with prisons expired at the end of 2011, it was renewed and made permanent in the American Taxpayer Relief Act enacted earlier this year. In addition, the Social Security Administration is proposing reforms to use its prisoner data that will further help IRS reduce improper payments.

- 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.

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.

## ASSISTING TAXPAYERS

### *Improving our Processes*

The IRS understands that identity theft is a frustrating, complex process for victims. While identity thieves steal information from sources outside the tax system, the IRS is often the first to inform a victim that identity theft has occurred. 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.

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.

In the first three months of 2013, the IRS worked with victims to resolve and close more than 200,000 cases. This is in addition to the expansion of the IP PIN program mentioned above. The IRS has dedicated more employees to resolve victim cases. These are extremely complex cases to resolve, frequently touching on multiple issues and multiple tax years. Cases of resolving identity can be complicated by the thieves themselves calling in. The IRS is working hard to streamline its internal processes, but much more work remains. A typical case can take about 180 days to resolve; however, we are actively working to reduce this inventory to shorten that time period.

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.

### *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 have received this training.

### *Taxpayer Outreach and Education*

The IRS continues to undertake outreach initiatives to provide taxpayers, return preparers, and other stakeholders with the information they need to prevent tax-related identity theft and, when identity theft does occur, to resolve issues as quickly and efficiently as possible. 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.

## 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 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. In FY 2012, CI initiated 900 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 nearly 500 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.

This trend is continuing in FY 2013. Already through April 9, 2013, more than 800 criminal identity theft investigations have been opened. Indictments in identity theft-related cases total 607, with 197 individuals sentenced and an average time to be served of 44 months.

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 in January 2013. This nationwide effort against 389 identity theft suspects led to 734 enforcement actions, including 189 indictments, informations and complaints, and 109 arrests. Around the time of the sweep, IRS auditors and investigators conducted compliance visits to 197 money service businesses in a variety of locations across the country to help ensure that these businesses were not facilitating refund fraud and identity theft.

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

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.

The IRS also has been 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. To date the IRS has received more than 1,560 waiver requests from more than 100 state and local law enforcement agencies in the nine states that have been participating in the pilot. On March 28, 2013, the IRS announced that this program has been expanded to all 50 states.

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 April 3, 2013, a Florida man was sentenced to 70 months in prison and three years of supervised release for his participation in a $3.3 million identity theft scheme that resulted in charges of conspiracy to file fraudulent claims and aggravated identity theft. Some of the personal information used by this individual was stolen from a community college's financial aid office.

- On March 22, 2013, a New York man was sentenced to 41 months in prison on charges that included identity theft and impersonating an IRS employee and a New York State Department of Labor official. This individual fraudulently obtained tax refunds by stealing taxpayers' personal information or tricking them into disclosing the information to him.

- On March 18, 2013, a California man was sentenced to 54 months in prison and ordered to pay more than $1.3 million to the IRS in connection with a scheme involving the filing of false tax returns. The individual and his associates used the names and social security numbers of residents of Puerto Rico to file more than 1,000 false returns seeking refunds based on the earned income tax credit. This individual also used false out-of-state driver's licenses to set up private mailboxes to receive the refund checks.

- On March 7, 2013, a Florida man was sentenced to 192 months in prison, three year of supervised release, and ordered to pay more than $100,000 in restitution to the IRS on charges of access device fraud and aggravated identity theft. The individual was found to have in his possession 28 pre-paid debit cards loaded with $117,000 in tax refunds.

- On February 22, 2013, a Florida man was sentenced to 159 months in prison and three years of supervised release on charges of access device fraud and aggravated identity theft. By searching an online database, this individual obtained the social security numbers of more than 23,000 people whose birth dates he had already obtained. He provided this information to associates who filed fraudulent returns.

- On February 8, 2013, an Alabama woman was sentenced to 65 months in prison on charges including aggravated identity theft and fraud in connection with computers. While working at a medical center records office, this individual stole more than 800 names, social security numbers and other personal information from current and former patients, and then sold the information to another person who used the information to file false tax returns.

- 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.

**CONCLUSION**

Mr. Chairman, thank you again for the opportunity to 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 thus far have provided 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.