HEARING BEFORE THE
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

"Tax-Related Identity Theft: An Epidemic Facing Seniors and Taxpayers"

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

April 10, 2013

Washington, D.C.

TESTIMONY OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

"Tax-Related Identity Theft: An Epidemic Facing Seniors and Taxpayers"

April 10, 2013

Chairman Nelson, Ranking Member Collins, and Members of the Committee, thank you for the invitation to provide testimony on the subject of identity theft and its impact on the Internal Revenue Service (IRS) and taxpayers, including the targeting of our Nation's senior citizens for identity theft. The Treasury Inspector General for Tax Administration (TIGTA) plays a critical role in providing taxpayers with assurance that the approximately 92,500 IRS employees who collect over $2.1 trillion in tax revenue each year, process over 147 million individual tax returns, and issue approximately $333 billion in tax refunds, do so in an effective and efficient manner while minimizing the risks of waste, fraud, and abuse.

TIGTA has provided ongoing oversight and testimony on the issue of tax fraud-related identity theft because of the rapidly growing nature of this tax crime and the need for further improvement in the IRS's handling of identity theft. Identity theft and other fraud schemes targeting senior citizens are on the rise. These financial scams have become so prevalent that they are being called the "crime of the 21st century."[1] Sweepstakes and lottery scams, e-mail and phishing scams, and investment scams are among the top ten fraud schemes used by criminals to target seniors.[2] Senior citizens are most likely to have a "nest egg," to own their home, and/or to have excellent credit – all of which make them attractive to con artists.[3] In addition, financial scams often go unreported by senior citizens or can be difficult to prosecute, so they are considered a "low-risk" crime.[4]

---

[1] *Top Ten Scams Targeting Seniors*, National Council on Aging, http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/savvy-saving-seniors/top-10-scams-targeting.html (last visited Apr. 4, 2013).
[2] *Id.*
[3] *Common Fraud Schemes*, *Fraud Target*: *Senior Citizens*, Federal Bureau of Investigation, http://www.fbi.gov/scams-safety/fraud/seniors (last visited Apr. 4, 2013).
[4] *Top Ten Scams Targeting Seniors*, National Council on Aging, http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/savvy-saving-seniors/top-10-scams-targeting.html (last visited Apr. 4, 2013).

Incidents of identity theft affecting tax administration have continued to rise since Calendar Year (CY) 2011, when the IRS identified more than one million incidents of identity theft. As of December 31, 2012, the IRS identified almost 1.8 million incidents during CY 2012. This figure includes approximately 280,000 incidents in which taxpayers contacted the IRS alleging that they were victims of identity theft,[5] and more than 1.5 million incidents in which the IRS detected potential identity theft.[6] As a result of the delay in the start of this year's filing season, we are unable to determine the extent of identity theft cases this year or compare trends with last year's filing season; however, it is highly likely that incidents of identity theft will show a continued increase when the current filing season is concluded.

Over the past year, my office has issued two reports[7] on the subject of identity theft. Identity theft affects the IRS and tax administration in two ways – with fraudulent tax returns and misreporting of income. Our first report, issued May 3, 2012, addressed the IRS's efforts to assist victims of identity theft, while the second, issued July 19, 2012, dealt with the IRS's efforts to detect and prevent the filing of fraudulent tax returns by identity thieves. My comments today will focus on the results of those reports and on the ongoing work we have underway to assess the IRS's progress on detecting and resolving identity theft issues related to tax administration.

The IRS has described identity theft as the number one tax scam for 2013.[8] Identity theft occurs when someone uses another taxpayer's personal information, such as name, Social Security number (SSN), or other identifying information, without permission, to commit fraud or other crimes. In many cases, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Unfortunately, senior citizens are not immune from this crime. During our audit,[9] we identified over 76,000 tax returns for Tax Year (TY) 2010 filed using the identities of senior citizens that had characteristics of an IRS-confirmed identity theft case. These tax returns resulted in potentially fraudulent tax refunds totaling over $374 million. Our

---

[5] Taxpayers can be affected by more than one incident of identity theft. The 280,000 incidents affected 233,365 taxpayers.
[6] These 1.5 million incidents affected 985,843 taxpayers.
[7] TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 2012); TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).
[8] IRS Press Release, IR-2013-33 (March 26, 2013), available at http://www.irs.gov/uac/Newsroom/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2013.
[9] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

analysis of TY 2010 returns that we identified as involving identity theft showed that the top five cities for these returns were located in Florida, Georgia, Michigan, and Texas.[10]

In addition, the identities of senior citizens are targets for identity thieves because many are not required to file a tax return. These individuals are often unaware that their identities have been stolen to file fraudulent tax returns. Similarly, the IRS is often unaware that the tax return is fraudulent unless the legitimate taxpayer files a tax return, resulting in a duplicate filing. If these fraudulent refunds are not recovered, taxpayer dollars will be lost.

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

One promising development occurred at the end of March 2013, when the IRS announced it was expanding a program designed to help law enforcement obtain tax return data for their investigations and prosecutions of specific cases of identity theft. The IRS initiated this program to assist local law enforcement with arrests and prosecutions related to identity theft. Under a pilot program, which was started in April 2012 in the State of Florida, State and local law enforcement officials who have evidence of identity theft involving fraudulently filed tax returns were able, through a written disclosure consent waiver from the victim, to obtain tax returns filed using the victim's SSN. The pilot was expanded in October 2012 to eight additional States.[11] There was widespread use of this program. Under the pilot, more than 1,560 waiver requests were received by the IRS from over 100 State and local law enforcement agencies in the nine States participating in the pilot. On March 29, 2013, the pilot was expanded to a permanent program that was effective for all 50 States and the District of Columbia.

Detection and Prevention of Identity Theft

Although it has found an increased number of identity theft incidents, the IRS is still challenged in detecting and preventing them. In July 2012, TIGTA reported that the impact of identity theft on tax administration is significantly greater than the amount the

[10] Tampa, FL; Miami, FL; Atlanta, GA; Detroit, MI; and Houston, TX.
[11] Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania, and Texas.

IRS detects and prevents.[12] Using the characteristics of tax returns that the IRS confirmed as involving identity theft, we analyzed TY 2010 tax returns processed during the 2011 Filing Season and identified 1.5 million undetected tax returns with potentially fraudulent tax refunds totaling approximately $5.2 billion. If not addressed, we estimate that the IRS could issue approximately $21 billion in fraudulent tax refunds resulting from identity theft over the next five years.

The primary characteristic of tax returns filed by identity thieves is the reporting of false income and withholding to generate a fraudulent tax refund. Without the falsely reported income, many of the deductions and/or credits used to inflate the fraudulent tax refund could not be claimed on the tax return. As I previously testified, many individuals who are victims of identity theft may be unaware that their identity has been stolen and used to file fraudulent tax returns. These individuals are typically those who are not required to file a tax return. It is not until the legitimate taxpayer files a tax return resulting in a duplicate filing under the same name and SSN that the taxpayer realizes that he or she has become a victim of identity theft.

When the identity thief files the fraudulent tax return, the IRS does not yet know whether the victim's identity will be used more than once. Instances of duplicate tax returns cause the greatest burden to the legitimate taxpayer. Once the legitimate taxpayer files his or her tax return, the duplicate tax return is identified and the refund is held until the IRS can confirm the taxpayer's identity. For TY 2010, we identified more than 48,000 SSNs that were used multiple times, *i.e.*, one or more potentially fraudulent tax returns were associated with the multiple use of an SSN.[13] We estimate that more than $70 million in potentially fraudulent tax refunds were paid to identity thieves who filed tax returns before the legitimate taxpayers filed theirs.[14] This is in addition to the $5.2 billion noted previously, which was related to taxpayers who do not appear to have a filing requirement.

Although the IRS is working toward finding ways to determine which tax returns are legitimate, it could do more to prevent identity thieves from electronically filing (e-filing) tax returns. Of the 1.5 million undetected tax returns TIGTA identified, almost 1.4 million (91 percent) were e-filed. Before a tax return can be submitted electronically, the taxpayer must verify his or her identity with either the prior year's tax return Self-Select

---

[12] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).
[13] This estimate includes only those tax returns filed on tax accounts that contain an Identity Theft Indicator added on or before December 31, 2011. Identity theft indicator codes were developed to centrally track identity theft incidents and are input to the affected taxpayer's account.
[14] This estimate is based only on the duplicate use of the primary SSN.

Personal Identification Number (PIN) or Adjusted Gross Income. However, we determined that this control can be circumvented.

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

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

Another important tool that could immediately help the IRS prevent tax fraud-related identity theft is the National Directory of New Hires.[15] However, legislation is needed to expand the IRS's authority to access the National Directory of New Hires wage information for use in identifying tax fraud. Currently, the IRS's use of this information is limited by law to just those tax returns that include a claim for the Earned Income Tax Credit. The IRS included a request for expanded access to this information in its annual budget submissions for Fiscal Years (FY) 2010, 2011, 2012, and has once again included this request in its FY 2013 budget submission.

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

---

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

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

As we reported in July 2008[16] and July 2012, the IRS is not in compliance with direct-deposit regulations that require tax refunds to be deposited into an account only in the name of the individual listed on the tax return. Direct deposit, which now includes debit cards, provides the ability to receive fraudulent tax refunds quickly, without the difficulty of having to negotiate a tax refund paper check. Of the approximately 1.5 million TY 2010 tax returns we identified, 1.2 million (82 percent) involved the use of direct deposit to obtain tax refunds totaling approximately $4.5 billion. One bank account received 590 direct deposits totaling over $900,000.

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

We also recommended, and the IRS agreed, that the IRS should coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that tax refunds issued via direct deposit, either to a bank account or to a debit card account, are made only to an account in the taxpayer's name. The IRS indicated that it will initiate discussions with the Department of the Treasury Fiscal Service[17] to revisit this issue and reevaluate the feasibility of imposing such restrictions. Based on its discussions with the Fiscal Service, the IRS will determine whether such restrictions can be effectively implemented.

---

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

[17] Two offices of the Department of the Treasury were merged in FY 2013: The Bureau of the Public Debt and the Financial Management Service. The new office is Fiscal Service. The IRS discussed the direct deposit issue with the former Financial Management Service.

As I mentioned earlier, the IRS has continued to make changes to its processes to increase its ability to detect, prevent, and track fraudulent tax returns and improve assistance to victims of identity theft. As of December 31, 2012, the IRS reports that during CY 2012 it stopped the issuance of $12.1 billion in potentially fraudulent tax refunds associated with 1.8 million tax returns classified as involving identity theft. This represents a 96 percent increase in the number of fraudulent tax returns identified over the same period last year. While the amount of fraudulent tax refunds the IRS detects and prevents is substantial, it does not know how many identity thieves are filing fictitious tax returns and how much revenue is being lost due to the issuance of fraudulent tax refunds.

In addition, the IRS continues to expand its efforts to identify fraudulent tax returns and prevent the payment of tax refunds by processing all individual tax returns through identity theft screening filters. These filters look for known characteristics of identity theft cases to detect fraudulent tax returns before they are processed and before any tax refunds are issued. For example, beginning in Processing Year 2012 the filters use benefit and withholding information from the Social Security Administration (SSA). This information is used to verify that Social Security benefits and related withholding reported on tax returns match the information reported by the SSA. Overall, this will help prevent the false reporting of Social Security benefits and withholding in an attempt to obtain fraudulent refunds. We identified over 93,000 tax returns in TY 2010 which collectively resulted in the issuance of over $230 million in fraudulent refunds involving the false reporting of Social Security benefits and withholding. The IRS reports that it identified and confirmed identity theft on over 31,000 tax returns claiming fraudulent Social Security benefits and withholding, and stopped approximately $169 million in fraudulent tax refunds in Processing Year 2012 using the information provided by SSA. The IRS advised us that for the 2013 Filing Season, the filters have been refined and incorporate criteria based on the latest characteristics of confirmed identity theft tax returns.

In yet another example, the IRS has incorporated an age analysis in its identity theft filters which should help to prevent additional tax fraud-related identity theft. Our analysis of questionable TY 2010 tax returns that appeared to have been filed by an identity thief showed that 2,274 tax returns filed by children under the age of 14 had received approximately $4 million in refunds. For one refundable tax credit for higher education expenses, we identified 109,618 taxpayers as of May 2, 2012, who received the refundable tax credit totaling more than $159 million for Tax Year 2011. The

individuals receiving the credit were of an age that is unlikely to be enrolled in a four-year college degree program.[18]

Tax returns detected by these new filters are held during processing until the IRS can verify the taxpayers' identity. IRS employees attempt to contact these individuals and request information to verify that the individual filing the tax return is the legitimate taxpayer. If the IRS cannot confirm the filer's identity, it suspends processing of the tax return to prevent the issuance of a fraudulent tax refund. During our current audit, the IRS advised us that the identity theft filters identified over 324,000 tax returns and enabled the IRS to stop the issuance of approximately $2.2 billion in fraudulent tax refunds in Calendar Year 2012.

In January 2012, the IRS created the Identity Theft Clearinghouse. The Clearinghouse was created to accept tax fraud-related identity theft leads from the IRS's Criminal Investigation field offices. The Clearinghouse performs research, develops each lead for the field offices, and provides support for ongoing criminal investigations involving identity theft. As of December 31, 2012, the Clearinghouse had received over 2,400 identity theft leads for development. These leads have resulted in the development of 329 identity theft investigations.

The IRS began a pilot program in Processing Year 2011 which makes use of a unique identity theft indicator to lock[19] taxpayers' accounts for which the IRS Master File and SSA data show a date of death. To date, the IRS has locked over 9.9 million tax accounts. These locks will systemically void tax returns filed on an individual's account after he or she is reported as deceased. For the 2013 Filing Season, the IRS indicates that for e-filed tax returns using the SSN of a deceased individual, the return will be rejected from processing. For paper tax returns, the IRS has prevented the issuance of over $487,000 in fraudulent tax refunds as a result of this program. The IRS does not yet have similar information for e-filed tax returns; however, we are reviewing this in our current audit.

To measure the success of the actions that the IRS took to combat identity theft in CY 2012, we are currently performing the same analysis we performed for TY 2010

---

[18] TIGTA, Ref. No. 2012-40-119, *The Majority of Individual Tax Returns Were Processed Timely, but Not All Tax Credits Were Processed Correctly During the 2012 Filing Season* (September 2012).
[19] A specific transaction code used to prevent a taxpayer's identification number (TIN), either a Social Security Number or Individual Taxpayer Identification Number, from being used as the primary or secondary TIN on a current or subsequent year Federal income tax return.

tax returns.[20] Using the characteristics of tax returns that the IRS confirmed as involving identity theft, we are analyzing TY 2011 tax returns processed during the 2012 Filing Season to determine whether we can identify any undetected tax returns with potentially fraudulent refunds resulting from identity theft.

IRS Assistance to Victims of Identity Theft

In May 2012, we reported that the IRS is not effectively providing assistance to taxpayers who report that they have been victims of identity theft, resulting in increased burden for those victims.[21] Moreover, identity theft cases can take more than one year to resolve, and communication between the IRS and victims is limited and confusing. Victims are also asked multiple times to substantiate their identities. Furthermore, during the 2012 Filing Season, identity theft tax returns were not prioritized during the standard tax return filing process. We are currently evaluating the IRS's corrective actions to our May 2012 audit report.[22]

The growth of identity theft poses a considerable challenge to tax administration. In CY 2011, the IRS reported that over 641,000 taxpayers were victims of identity theft. This figure includes taxpayers who contacted the IRS alleging that they were victims. In CY 2012, the IRS identified an additional 1.2 million of these taxpayers.

In FY 2012, the IRS dedicated 400 additional employees to the Accounts Management function[23] to work identity theft cases. As a result, the function now has approximately 2,000 employees working these cases. However, its inventory of identity theft cases has grown almost 50 percent from FY 2011 to 2012. As of March 9, 2013, the Accounts Management function reported that it had over 249,000 identity theft cases in its inventory.

The IRS estimated that its inventory of more than 228,000 identity theft cases that had been carried over from FY 2010 to 2011 would require 287 full-time employees

---

[20] TIGTA, Audit No. 201140044, *Effectiveness of the Internal Revenue Service's Efforts to Identify and Prevent Fraudulent Tax Refunds Resulting from Identity Theft* (Follow-Up), report planned for April 2013.
[21] TIGTA, Ref. No. 2012-40-050*, Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 2012).
[22] TIGTA, Audit No. 201240041, *Effectiveness of Assistance Provided to Victims of Identity Theft* (Follow-Up), report planned for September 2013.
[23] The function that works the majority of identity theft cases involving individual duplicate tax returns.

to resolve.[24] This inventory did not include 500,000 cases that were in the Duplicate Filing inventory,[25] many of which were identity theft cases.

Most identity theft cases are complex and can present considerable challenges throughout the resolution process. For example, it can be difficult to determine who the legitimate taxpayer is or if the case is actually a case of identity theft. Taxpayers sometimes transpose digits in SSNs, but do not respond to IRS requests for information to resolve the case. As a result, the IRS may not be able to determine who the legitimate taxpayer is. With other cases we have reviewed, taxpayers claimed to be victims of identity theft after the IRS had questioned deductions or credits or proposed examination adjustments. There have also been instances in which the SSA has issued the same SSN to more than one taxpayer.[26]

Resources have not been sufficient to work identity theft cases dealing with refund fraud and continue to be a concern. IRS employees who work the majority of identity theft cases are telephone assistors who also respond to taxpayers' calls to the IRS's toll-free telephone lines. TIGTA is concerned that demanding telephone schedules and a large identity theft inventory make it difficult for assistors to prioritize identity theft cases.

Furthermore, telephone assistors are not examiners and are not trained to conduct examinations, which require skills and tools beyond those possessed by the assistors. Instead, assistors are trained to communicate with taxpayers and to know the tax laws and related IRS operational procedures. We recommended that the IRS provide additional training for assistors, to include training on the importance of documenting case actions and histories.

The IRS responded that it has provided improved training to all IRS employees who work identity theft cases. However, as of November 2012, interviews with more than 20 assistors showed that many believed the training was not adequate and that the constant revision of new procedures is creating confusion for the assistor and the taxpayer alike. The IRS has implemented new tools and job aids for the assistors to use when attempting to resolve identity theft cases, such as the Identity Theft Case

---

[24] A full-time employee working 40 hours per week for 52 weeks.
[25] A duplicate tax return condition occurs when a tax return posts to a taxpayer's account that already contains a tax return. The duplicate tax return becomes part of an inventory of duplicate tax return cases that require an IRS employee to work and resolve.
[26] Prior to 1961, only a fraction of SSNs were manually screened to determine if an SSN was previously assigned. Thus, issuing duplicate SSNs was possible. Today, automated systems with sophisticated matching routines screen for previously issued SSNs.

Building Guide and the Identity Theft Tracking Indicator Assistant tool. Some assistors stated that they believe these tools have been helpful when working identity theft cases. TIGTA is currently evaluating the actions the IRS has taken in response to our concerns with the training provided to assistors.[27]

The management information system that telephone assistors use to control and work cases can add to the taxpayer's burden. For instance, the IRS may open multiple cases for the same victim, and multiple assistors may work that same victim's identity theft issue. A review of 17 taxpayers' identity theft cases showed that 58 different cases involving those taxpayers had been opened, and multiple assistors had worked their cases. Our audit also found that victims become further frustrated when they are asked numerous times to prove their identities, even though they have previously followed IRS instructions and sent in Identity Theft Affidavits[28] and copies of their identification with their tax returns.

We also found in May 2012[29] that the IRS sends the victims duplicate letters at different times, wasting agency resources and possibly confusing the victims. For example, the IRS sends each taxpayer two different letters advising that the taxpayer's identity theft case has been resolved. Assistors working an identity theft case send one letter to the taxpayer when they have completed actions taken on the case. A second letter is systemically generated two to 12 weeks later advising the taxpayer again that his or her case has been resolved. Neither letter advises when the taxpayer should expect to receive his or her tax refund.

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

When our auditors reviewed a sample of cases, they could not determine if some cases had been resolved or why those cases were still open. In most cases, auditors

---

[27] TIGTA, Audit No. 201240041, *Effectiveness of Assistance Provided to Victims of Identity Theft* (Follow-Up), report planned for August 2013.
[28] IRS Form 14039, *Identity Theft Affidavit*.
[29] TIGTA, Ref. No. 2012-40-050*, Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 2012).

had to reconstruct the cases to determine if all actions had been appropriately taken to resolve them.

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

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

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

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

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

of identity theft and will explore leveraging these new indicators to suspend certain correspondence. The IRS's corrective actions are not expected to be fully implemented until September 2013.

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

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

To further assist victims in the filing of their tax returns, the IRS began issuing Identity Protection Personal Identification Numbers (IP PIN) in Fiscal Year 2011 to these individuals. The IP PIN will indicate that the taxpayer has previously provided the IRS with information that validates his or her identity and that the IRS is satisfied that the taxpayer is the valid holder of the SSN. Tax returns that are filed on accounts with an IP PIN that has been correctly entered at the time of filing will be processed as the valid tax return using standard processing procedures, including issuing any refunds, if applicable. A new IP PIN will be issued each year before the start of the new filing season, for as long as the taxpayer remains at risk of identity theft. For the 2012 Filing Season, the IRS sent 252,000 individuals an IP PIN. For the 2013 Filing Season, the IRS reports that it issued 772,000 IP PINs.

Finally, in January 2012, the IRS established a Taxpayer Protection Program to manage work arising from the identity theft indicators and filters used to detect tax returns affected by identity theft – both to stop the identity thief's tax return from being processed and to ensure that the legitimate taxpayer's tax return is processed. However, during the 2012 Filing Season, taxpayers found it difficult to reach employees in this program. The program received approximately 200,000 calls during FY 2012, but was only able to answer about 73,000. The average wait time for taxpayers was 33

minutes. For the 2013 Filing Season, the IRS increased the number of employees answering this program's telephone line from 10 to more than 200 employees.

We are currently evaluating whether the IRS is effectively implementing the corrective actions in response to recommendations made in our prior report to improve assistance to victims of identity theft.[30] As of November 2012, our preliminary review of 16 identity theft cases worked by the Accounts Management function shows that for eight of the 16 cases, the IRS's processes prevented refunds from being issued to the apparent identity thieves.

Criminal Investigations of Identity Theft

Not only does identity theft have a negative impact on the economy, but the damage it causes to its victims can be personally, professionally, and financially devastating. When individuals steal identities and file fraudulent tax returns to obtain fraudulent refunds before the legitimate taxpayers file, the crime is simple tax fraud, which falls within the programmatic responsibility of IRS Criminal Investigation. TIGTA's Office of Investigations focuses its limited resources on investigating identity theft that has any type of IRS employee involvement, the misuse of client information by tax preparers, or the impersonation of the IRS through phishing schemes[31] and other means.

IRS employees are entrusted with the sensitive personal and financial information of taxpayers. Using this information to perpetrate a criminal scheme for personal gain negatively impacts our Nation's voluntary tax system and generates widespread distrust of the IRS. TIGTA aggressively investigates IRS employees involved in identity theft crimes. When the Office of Investigations completes an identity theft investigation, it is referred to the Department of Justice for prosecution.

For example, a former IRS employee was arrested after being charged by a Federal grand jury on June 26, 2012, for aggravated identity theft, mail fraud, unauthorized inspection of tax returns and return information, and unauthorized disclosure of tax returns and return information. She subsequently pled guilty to those

---

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

[31] Phishing is an attempt by an individual or group to solicit personal and financial information from unsuspecting users in an electronic communication by masquerading as trustworthy entities such as government agencies, popular social web sites, auction sites, online payment processors, or information technology administrators.

charges on August 14, 2012, and was sentenced on March 28, 2013, to 28 months of imprisonment with three years of supervised release.[32]

TIGTA also investigated a tax preparer who stole the personal identifiers of several individuals and unlawfully disclosed the information to others to fraudulently obtain tax refunds. According to the indictment, the subject of the investigation worked as a tax preparer from January 2002 to June 2008. In 2010, he used the personal identifiers of other individuals to file false income tax returns and obtain refunds from the IRS. The preparer obtained most of the personal identifiers in the course of his prior employment as a tax preparer and from other employment positions he held. He disclosed this information to co-conspirators so they could also file false income tax returns and obtain refunds from the IRS. The subject and his co-conspirators ultimately defrauded or attempted to defraud the IRS out of at least $560,000 in tax refunds.[33]

Identity thieves may also commit identity theft by impersonating IRS employees or misusing the IRS seal to induce unsuspecting taxpayers to disclose their personal identifiers and financial information. One such criminal posed as an IRS "Audit Group Representative" and, according to the indictment, sent letters to various employers demanding that they send him the names, contact information, dates of birth, and SSNs of their employees. He then prepared and filed false Federal tax returns with the IRS in the names of various such employees without their knowledge or consent. The tax returns contained W-2 information, such as income and withholding, that was falsely and fraudulently inflated. The subject of the investigation used the refunds to purchase personal items. The subject pled guilty to false impersonation of an officer and employee of the United States; identity theft; subscribing to false and fraudulent U.S. individual income tax returns; and false, fictitious, or fraudulent claims. He was sentenced to 41 months of imprisonment and three years of supervised release. He was also ordered to pay $8,716 in restitution.[34]

Finally, TIGTA investigated a phishing scheme in which several individuals were deceived into divulging their personal identifiers and banking information to identity thieves who then defrauded them of over $1 million. The subject and his co-conspirators operated a scheme to defraud numerous individuals through Internet solicitations, stealing more than $1 million and the identities of those individuals. The subject of the investigation was sentenced to a total of 30 months of imprisonment and

---

[32] E.D. Pa. Arrest Warrant executed July 5, 2012; E.D. Pa. Crim. Indict. filed June 26, 2012; E.D. Pa. Crim. Docket dated Jan. 22, 2013.
[33] S.D. Cal. Superseding Indict. filed June 19, 2012.
[34] S.D.N.Y. Crim. Indict. filed Jan. 25, 2012; S.D.N.Y. Minute Entry filed July 11, 2012; S.D.N.Y. Judgment filed March 25, 2013.

five years of supervised release for Aggravated Identity Theft and Conspiracy to Commit Wire Fraud. He was also ordered to pay $1,741,822 restitution to his victims.[35]

As I stated earlier, identity theft and other fraud schemes targeting senior citizens are on the rise. Sweepstakes and lottery scams, e-mail and phishing scams, and investment scams are among the top ten fraud schemes used by criminals to target seniors.[36]

While phishing schemes may vary in their technical complexity, many share a common trait: They involve computers located outside the United States. Despite the significant investigative challenge this poses, TIGTA has been successful in working with law enforcement personnel in foreign countries to identify the perpetrators and obtain prosecutions.

TIGTA's Office of Investigations investigated an individual who, along with his co-conspirators, engaged in a fraud scheme that specifically targeted senior citizens. As part of the scheme, a co-conspirator would send e-mails to victims representing that he was an attorney or foreign government official who was responsible for distributing an inheritance. The e-mails sent to the unsuspecting victims falsely informed them that they owed additional taxes to the IRS, or had inherited millions of dollars but needed to pay processing fees to release the funds. When the victims responded to the e-mails, the subject of the investigation, or one of his co-conspirators, contacted them by telephone and e-mail pretending to be someone who could assist them in obtaining the promised inheritance. The victims were led to believe that these contacts were from legitimate business people, and were deceived into paying fees in advance of receiving the inheritance. However, the funds were never used to pay any fees, nor were any inheritance payments made to the victims. The subject of this investigation pled guilty to an indictment charging him with 15 counts of wire fraud and is awaiting sentencing.[37]

In addition, in February 2013, the IRS announced the results of a nationwide effort with the Department of Justice and local U.S. Attorneys offices targeting identity theft suspects in 32 States and Puerto Rico, which involved 215 cities and surrounding

---

[35] E.D.N.Y. Response to Defendant's Sentencing Letter filed Dec. 19, 2011; E.D.N.Y. Judgment filed Aug. 9, 2012.

[36] *Top Ten Scams Targeting Seniors*, National Council on Aging, http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/savvy-saving-seniors/top-10-scams-targeting.html (last visited Apr. 4, 2013).

[37] C.D. Cal. Opposition to Defendant's Ex Parte Application to Continuance of Trial Date filed June 6, 2012; C.D. Cal. Indict. filed Oct. 21, 2009; C.D. Cal. Crim. Complaint filed Aug. 3, 2009; C.D. Cal. Crim. Minutes Change of Plea filed July 31, 2012.

areas. This joint effort involved 734 enforcement actions related to identity theft and refund fraud, including indictments, informations, complaints, and arrests.

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

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

J. Russell George
Treasury Inspector General for Tax Administration

Following his nomination by President George W. Bush, the United States Senate confirmed J. Russell George in November 2004, as the Treasury Inspector General for Tax Administration. Prior to assuming this role, Mr. George served as the Inspector General of the Corporation for National and Community Service, having been nominated to that position by President Bush and confirmed by the Senate in 2002.

A native of New York City, where he attended public schools, including Brooklyn Technical High School, Mr. George received his Bachelor of Arts degree from Howard University in Washington, DC, and his Doctorate of Jurisprudence from Harvard University's School of Law in Cambridge, MA. After receiving his law degree, he returned to New York and served as a prosecutor in the Queens County District Attorney's Office.

Following his work as a prosecutor, Mr. George joined the Counsel's Office in the White House Office of Management and Budget where he was Assistant General Counsel. In that capacity, he provided legal guidance on issues concerning presidential and executive branch authority. He was next invited to join the White House Staff as the Associate Director for Policy in the Office of National Service. It was there that he implemented the legislation establishing the Commission for National and Community Service, the precursor to the Corporation for National and Community Service. He then returned to New York and practiced law at Kramer, Levin, Naftalis, Nessen, Kamin & Frankel.

In 1995, Mr. George returned to Washington and joined the staff of the Committee on Government Reform and Oversight and served as the Staff Director and Chief Counsel of the Government Management, Information and Technology subcommittee (later renamed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations), chaired by Representative Stephen Horn. There he directed a staff that conducted over 200 hearings on legislative and oversight issues pertaining to Federal Government management practices, including procurement policies, the disposition of government-controlled information, the performance of chief financial officers and inspectors general, and the Government's use of technology. He continued in that position until his appointment by President Bush in 2002.

In addition to his duties as the Inspector General for Tax Administration, Mr. George serves as a member of the Recovery Accountability and Transparency Board, a non-partisan, non-political agency created by the American Recovery and Reinvestment Act of 2009 to provide unprecedented transparency and to detect and prevent fraud, waste, and mismanagement of Recovery funds. There, he serves as chairman of the Recovery.gov committee, which oversees the dissemination of accurate and timely data about Recovery funds.

Mr. George also serves as a member of the Integrity Committee of the Council of Inspectors General for Integrity and Efficiency (CIGIE). CIGIE is an independent entity within the executive branch statutorily established by the Inspector General Act, as amended, to address integrity, economy, and effectiveness issues that transcend individual Government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General. The CIGIE Integrity committee serves as an independent review and investigative mechanism for allegations of wrongdoing brought against Inspectors General.