HEARING BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

"Refund-Related Identity Theft"

Testimony of
Michael E. McKenney
Acting Deputy Inspector General for Audit
Treasury Inspector General for Tax Administration

August 2, 2013

Washington, D.C.

TESTIMONY OF
MICHAEL E. MCKENNEY
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

"Refund-Related Identity Theft"

August 2, 2013

Chairman Mica, Ranking Member Connolly, and Members of the Subcommittee, thank you for the invitation to provide testimony on the important subject of identity theft and its impact on the Internal Revenue Service (IRS) and taxpayers. 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. The IRS has made this issue one of its top priorities and has made some progress; however, significant improvements are needed. In addition, there is a portion of the problem that cannot be fully addressed until the IRS receives income and withholding information before tax returns are processed, which may require legislative action.

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 June 29, 2013, the IRS had identified almost 1.9 million incidents of identity theft thus far in CY 2013. This figure includes approximately 212,000 incidents in which taxpayers contacted the IRS alleging that they were victims of identity theft, and almost 1.7 million incidents in which the IRS detected potential identity theft.[1]

[1] Taxpayers can be affected by more than one incident of identity theft. The 212,000 incidents affected over 180,000 taxpayers, and the 1.7 million incidents affected over 1.4 million taxpayers.

Since May 2012, my office has issued three reports on the subject of identity theft.[2] Our first report addressed the IRS's efforts to assist victims of identity theft, while the second dealt with the IRS's efforts to detect and prevent the filing of fraudulent tax returns by identity thieves. The third report, issued in June 2013, evaluated whether the Taxpayer Protection Program was effectively assisting taxpayers that the IRS proactively identifies as potential identity theft victims.[3] My comments today will focus on the results of those reports and on our ongoing work to assess the IRS's progress in detecting and resolving identity theft issues related to tax administration.

The IRS has described identity theft as the number one tax scam for 2013.[4] 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.

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 in 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. Under a pilot program, which started in April 2012 in the State of Florida, State and local law enforcement officials who had 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[5] and became permanent on March 29, 2013 as a nationwide program. In April 2013, the IRS announced that this partnership was expanded to

---

[2] 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); TIGTA, Ref. No. 2013-40-062, *The Taxpayer Protection Program Improves Identity Theft Detection; However, Case Processing Controls Need to Be Improved* (June 2013).

[3] This program reviews tax returns that are proactively identified by the IRS as potential identity theft and stops fraudulent refunds before they are issued.

[4] 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.

[5] Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania, and Texas.

include all 50 states, the District of Columbia, Guam, the Northern Marianas Islands, Puerto Rico, and the U.S. Virgin Islands. As of May 30, 2013, the IRS has processed 2,731 waivers from 244 different law enforcement agencies.

Detection and Prevention of Identity Theft

As of June 30, 2013, the IRS reports that during the 2013 Filing Season it stopped the issuance of $4.2 billion in potentially fraudulent tax refunds associated with almost 860,000 tax returns classified as involving identity theft. 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.

Although the IRS identified significantly more identity theft incidents in 2013, this is still a growing problem area for the IRS. In July 2013, TIGTA issued a draft report showing that the impact of identity theft on tax administration continues to be significantly greater than the amount the IRS detects and prevents.[6] Using the characteristics of tax returns that the IRS confirmed as involving identity theft and income and withholding information the IRS received in 2012 and early 2013, we analyzed Tax Year (TY) 2011 tax returns processed during the 2012 Filing Season and identified approximately 1.1 million undetected tax returns where the primary Taxpayer Identification Number on the tax return was an SSN. These tax returns have potentially fraudulent tax refunds totaling approximately $3.6 billion, a decrease of $1.6 billion compared to the $5.2 billion we reported for Tax Year 2010.[7] Although these tax returns met the characteristics of IRS confirmed identity theft cases involving the use of an SSN, some potentially fraudulent tax returns we identified could also be the result of non-reporting of income and withholding by the employer or an individual using his or her own SSN to file a fraudulent tax return.

In addition, we expanded our TY 2011 analysis to include tax returns where the primary Taxpayer Identification Number on the tax return is an Individual Taxpayer Identification Number (ITIN). We identified more than 141,000 TY 2011 tax returns filed with an ITIN that have the same characteristics as IRS confirmed identity theft tax returns. Potentially fraudulent tax refunds issued for these undetected tax returns totaled approximately $385 million, which is in addition to the approximately $3.6 billion referred to earlier. Although these tax returns met the characteristics of IRS confirmed

---

[6] TIGTA, Audit No. 201240044, *Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds*, report planned for September 2013.
[7] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

identity theft cases involving the use of an ITIN, some of the potentially fraudulent tax returns we identified could also be the result of misreporting of income and withholding by the employer or an individual obtaining an ITIN for the sole purpose of using the ITIN to file a fraudulent tax return.

In total, the IRS could issue potentially fraudulent refunds of approximately $4 billion annually as a result of identity theft tax refund fraud. A common 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. Another aspect to this problem is that 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 IRS receives income and withholding information later in the year that the IRS may determine the tax return was false and possibly the result of identity theft. If the taxpayer is required to file a tax return, often the IRS discovers the identity theft when two or more tax returns are filed under the same name and SSN.

When the identity thief files the fraudulent tax return before the legitimate taxpayer, 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, this tax return is identified as being a duplicate tax return and the refund is held until the IRS can confirm the taxpayer's identity. For TY 2011, we identified more than 174,000 SSNs that were used multiple times, *i.e.*, one or more potentially fraudulent tax returns were associated with the multiple use of an SSN.[8] We estimate that more than $183 million in potentially fraudulent tax refunds were paid to identity thieves who filed tax returns before the legitimate taxpayers filed theirs.[9] This is in addition to the $4 billion noted previously, which was related to taxpayers who do not appear to have a filing requirement.

Although the IRS is continuing to work towards finding ways to determine which tax returns are legitimate, it could do more to prevent identity thieves from electronically filing (e-filing) fraudulent tax returns by strengthening controls. The majority (93 percent) of the undetected tax returns TIGTA identified were e-filed. Before a tax return can be submitted electronically, the taxpayer must verify his or her identity with

[8] 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.
[9] This estimate is based only on the duplicate use of the primary SSN.

either the prior year's tax return Self-Select Personal Identification Number or Adjusted Gross Income. However, we determined that this control can be circumvented.

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. Having third-party reporting information at the time tax returns are processed 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.[10] However, legislation would be 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 legislative proposal for expanded access to this information in its annual budget submissions for Fiscal Years (FY) 2010 through 2013 and has once again included this proposal in its FY 2014 budget submission.

Identifying potential identity theft tax fraud is the first step. Verifying whether the returns are fraudulent will require additional resources. Using IRS estimates, it would cost approximately $22 million to screen and verify all of the over 1.2 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.

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 selects only those tax returns for which it can verify the identity of the taxpayer and/or the

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

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, July 2012, and again in our current Draft Report, 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.[11] 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. The majority of the TY 2011 tax returns we identified with indicators of identity theft (84 percent) involved the use of direct deposit to obtain tax refunds totaling approximately $3.5 billion. There are indications that abusive practices are still ongoing. For example, one bank account received 446 direct deposits totaling over $591,000.

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 for the legitimate taxpayer, it does have the potential to limit the extent of fraud. As of June 2013, the IRS is still considering this recommendation, but the IRS did develop new filters for the 2013 Filing Season designed to identify and stop tax returns with similar direct deposit characteristics. As of May 30, 2013, the IRS indicated it had identified 154,302 tax returns from these filters and prevented approximately $470 million tax refunds from being issued.

We also recommended, and the IRS agreed, that it 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. In January 2013, the IRS implemented a pilot program with the Department of the Treasury Fiscal Service[12] designed to allow financial institutions to reject direct deposit tax refunds based on mismatches between the account name and the name on the tax return. Once the refund is identified by the institution, it is sent back to the Fiscal Service to be routed

---

[11] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (Sept. 2008).
[12] Formerly, the Department of the Treasury Financial Management Service.

back to the IRS. As of June 29, 2013, there have been 18,247 refunds returned from financial institutions totaling more than $60 million. This is a promising first step in recovering fraudulent tax refunds issued via direct deposit.

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. In Processing Year 2012, there were 11 filters that identified approximately 325,000 tax returns and prevented approximately $2.2 billion in fraudulent refunds from being issued. In Processing Year 2013, the number of filters increased to more than 80, which has enhanced the IRS's ability to identify identity theft tax refund fraud. As of May 30, 2013, the IRS identified 151,010 tax returns and prevented approximately $840 million in fraudulent tax refunds from being issued. This represents a 90 percent increase over the number that the IRS identified for the same period in Processing Year 2012.

One of these filters uses benefit and withholding information from the Social Security Administration (SSA), which TIGTA had previously recommended. Beginning in Processing Year 2012, this information was used to verify that Social Security benefits and related withholding reported on tax returns matched the information reported by the SSA. Overall, this will help the IRS identify tax returns with false reporting of Social Security benefits and withholding in an attempt to obtain fraudulent refunds. As of May 30, 2013, the IRS indicated that it had identified 36,523 tax returns and prevented approximately $184 million in tax refunds from being issued based on the 2013 Filing Season Social Security filters.

Tax returns detected by the various expanded 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.

In January 2012, the IRS created the Identity Theft Clearinghouse within Criminal Investigation. 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 May 31, 2013, the Clearinghouse had received more than 3,400 identity theft leads that have resulted in the development of 478 investigations.

Finally, the IRS has significantly expanded the number of tax accounts that it locks by placing an identity theft indicator on the individuals' tax account.[13] Between January 2011 and May 2013, the IRS has locked approximately 10 million taxpayer accounts, which will assist the IRS in preventing future identity theft fraudulent tax refunds from being issued. Electronically filed tax returns using the SSN of a locked account will be rejected (the IRS will not accept the tax return for processing). Paper tax returns will be processed; however, the tax returns will not post to the taxpayer's account due to the account lock, and a refund will not be issued. As of May 31, 2013, the IRS had rejected 152,301 e-filed tax returns during the 2013 Filing Season. Additionally, the IRS has stopped 169,642 paper filed tax returns and prevented the issuance of approximately $5.6 million in fraudulent tax refunds since the inception of the lock.[14]

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.[15] 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 finishing our audit work on a follow-up review assessing IRS assistance to victims of identity theft and plan to issue a report in October 2013.[16] In this review, we selected a statistically valid sample of 100 identity theft cases closed between the period August 1, 2011 through July 31, 2012, and are reviewing the cases to determine whether the cases were timely and accurately resolved. Although the IRS was able to determine the rightful owner of the Social Security Number, cases continue to face delays, with some cases having significant inactivity in case processing. In addition, we are finding that tax accounts were not always correctly resolved before the

[13] When an account is locked, tax refunds are held.
[14] The IRS locked the majority of the 10 million accounts in December 2012; therefore, the increased benefit of refunds prevented should be realized during Processing Year 2013.
[15] 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).
[16] TIGTA, Audit No. 201240041, *Effectiveness of Assistance Provided to Victims of Identity Theft (Follow-Up)*, report planned for October 2013.

cases were closed. The incorrect resolutions resulted in delays in issuing refunds to taxpayers and in some cases resulted in the IRS issuing an incorrect refund.

In discussions with the IRS regarding our review of the 100 cases, management indicated that they have implemented a number of actions for the 2013 Filing Season which will further improve the processing of identity theft cases. For example, they implemented a process to expedite the processing of tax returns with an attached Identity Theft Affidavit. Paper filed tax returns with an attached Identity Theft Affidavit or police report are being marked with a special processing code and expedited directly to the IRS's Accounts Management function for case processing. The IRS indicated that the direct routing of these tax returns will shorten case processing by one to two months. We plan to review this new process in our next audit of identity theft.

Some corrective actions planned by the IRS in response to our May 2012 report were not scheduled to be completed until September 2013 or were not fully implemented, so they were not included in our review. We will evaluate the effectiveness of these corrective actions and any new processes in our next follow-up audit.

Despite these corrective actions, the IRS will continue to face significant challenges in assisting victims of tax fraud-related identity theft. In our FY 2012 report, we reported on several of these challenges.

Resources were not sufficient to work identity theft cases dealing with refund fraud. IRS employees who worked the majority of identity theft cases were telephone assistors who also respond to taxpayers' calls to the IRS's toll-free telephone lines. In addition, telephone assistors are not examiners and are not trained to conduct examinations. We recommended that the IRS provide additional training for assistors, to include training on the importance of documenting case actions and histories. We are currently evaluating the actions the IRS has taken on training for assistors.[17]

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. In our May 2012 audit, we found that victims were frustrated when they were asked numerous times to prove their identities.

---

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

The IRS sends the victims duplicate letters at different times, wasting agency resources and possibly confusing the victims. For example, the IRS sent taxpayers two different letters several weeks apart advising that the taxpayer's identity theft case has been resolved. Neither letter advised when the taxpayer should expect to receive his or her tax refund.

In addition, identity theft case histories were so limited that it was difficult to determine what action had been taken on a case. During our 2012 audit, we could not determine if some cases had been resolved or why those cases were still open. In most cases, the auditors had to reconstruct the cases to determine if all actions had been appropriately taken to resolve them.

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. The IRS 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) may 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 May 2012 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. We plan to evaluate whether the IRS is effectively implementing these corrective actions in a future follow-up audit.

The IRS took 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 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.

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 759,000 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.

In June 2013, we issued a report on our audit of the Taxpayer Protection Program, which evaluated whether the Program helps the IRS to effectively assist taxpayers and resolve identity theft cases. We found that the Program has improved identity theft detection. For example, the Program identified 324,670 tax returns in CY 2012 that involved identity theft and prevented the issuance of fraudulent refunds totaling $2.2 billion. These tax returns were identified before processing was completed to protect tax refunds from being issued. However, controls over identity theft tax returns worked in the Program need to be strengthened. We found that required identity theft indicators were not always input on taxpayer accounts. When these indicators are not input, there is the risk that the IRS will issue a fraudulent refund to an identity thief and the taxpayer continues to be at risk of an identify thief filing a fraudulent tax return using his or her identity.

In addition, we found that cases were not being clearly documented or closed accurately. For example, for the 12 cases we judgmentally selected and reviewed, we were not able to determine from the case notes whether the IRS took the appropriate actions when working the case.[18] We also determined that timeliness measures to track the time frame to resolve identity theft cases have not been established. Finally, we found that the IRS could not provide support confirming that employees working the cases received the required identity theft training to perform their assigned duties. The IRS agreed with all of our recommendations and plans to take actions to address our concerns.

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[19] and other means. Where there is overlapping jurisdiction, TIGTA and IRS-Criminal Investigation will work together to bring identity thieves to justice.

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

---

[18] There were 309,836 cases in the population that we selected the judgmental sample from. We selected a judgmental sample to determine if there were indications of problems and we did not plan to project the error rate to the population.

[19] 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.

disclosure of tax returns and return information. She subsequently pled guilty to those charges on August 14, 2012, and was sentenced on March 28, 2013, to 28 months of imprisonment with three years of supervised release.[20]

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.[21] The subject was sentenced to 15 years in prison and ordered to pay restitution in the amount of $515,257.75.[22]

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.[23]

Finally, TIGTA investigated a phishing scheme in which several individuals were deceived into divulging their personal identifiers and banking information to identity

---

[20] 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.
[21] S.D. Cal. Superseding Indict. filed June 19, 2012.
[22] S.D. Cal. Judgment dated May 30, 2013.
[23] 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.

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 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.[24]

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.[25]

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

---

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

[25] 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.

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. Because of the importance of this issue, we plan to provide continuing audit coverage of the IRS's efforts to prevent tax fraud-related identity theft and to provide 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 Mica, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to update you on our work on this critical tax administration issue and to share my views.

Michael E. McKenney
Acting Deputy Inspector General for Audit
Treasury Inspector General for Tax Administration

Mike McKenney serves as the Acting Deputy Inspector General for Audit for the Treasury Inspector General for Tax Administration (TIGTA). He leads a nationwide audit function consisting of 260 staff members who strive to promote the economy, efficiency, and effectiveness of tax administration.

The Audit program's reports and recommendations to the Internal Revenue Service (IRS) have focused on improving tax administration and addressing the IRS' management challenges in the areas of data and employee security, computer modernization, tax law compliance and complexity, human capital, and improper and erroneous payments.

Prior to this, Mike served as the Assistant Inspector General for Audit (Returns Processing and Account Services) for TIGTA, where he was responsible for providing audit oversight of IRS operations related to the preparation and processing of tax returns and the issuing of refunds to taxpayers. This includes customer service activities, outreach efforts, tax law implementation, taxpayer assistance, accounts management, notices, submission processing, and upfront compliance such as the Frivolous Returns Program and the Questionable Refund Program.

Mike served in various managerial positions with TIGTA, covering a broad range of IRS areas including the IRS Oversight Board, Agency-Wide Shared Services, Chief Human Capital Office, Office of Appeals, Taxpayer Advocate Service, Office of Research and Analysis, and the Office of Professional Responsibility. Mike also opened and managed TIGTA's Denver field office for the Office of Audit. He began his Federal auditing career in 1992 with the IRS Inspection Service in Los Angeles. Mike graduated from California State University, Fullerton with a B.A. in Business (Accounting).