HEARING BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT ORGANIZATION, EFFICIENCY, AND
FINANCIAL MANAGEMENT
U.S. HOUSE OF REPRESENTATIVES

"Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service, Part IV"

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

November 29, 2012

Washington, D.C.

TESTIMONY OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT ORGANIZATION, EFFICIENCY, AND FINANCIAL MANAGEMENT
U.S. HOUSE OF REPRESENTATIVES

"Identity Theft and Tax Fraud: Growing Problems for the
Internal Revenue Service, Part IV"

November 29, 2012

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, thank you for the invitation to provide testimony on the subject of identity theft and its impact on the Internal Revenue Service (IRS) in its function of administering the Nation's tax laws. Since I last testified before this Subcommittee on identity theft and tax fraud in April 2012,[1] my office, the Treasury Inspector General for Tax Administration (TIGTA), has issued two reports[2] on this subject. The 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 find and prevent identity theft. My comments today will focus on those results 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.

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 much work that still needs to be done.

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 that impacted our Nation's tax system. As of October 27, 2012, the IRS

---

[1] *Problems at the Internal Revenue Service: Closing the Tax Gap and Preventing Identity Theft*, *Hearing Before the H. Comm. on Oversight and Government Reform, Subcomm. on Government Organization, Efficiency and Financial Management*,112th Cong. (Apr. 19, 2012) (statement of J. Russell George).
[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).

identified almost 1.2 million incidents during CY 2012. This figure includes approximately 186,000 incidents in which taxpayers contacted the IRS alleging that they were victims of identity theft,[3] as well as more than one million incidents where the IRS detected the occurrence of potential identity theft.[4]

Detection and Prevention of Identity Theft

Despite the increased number of identity-theft incidents the IRS has found, 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 IRS detects and prevents.[5] Using the characteristics of confirmed identity theft, we analyzed Tax Year (TY) 2010 tax returns processed during the 2011 Filing Season and identified 1.5 million undetected tax returns with potentially fraudulent tax refunds totaling in excess of $5 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 shared by tax-related identity-theft cases is that the identity thief reports 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. In addition, many individuals who are victims of identity theft may be unaware that their identity has been stolen 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 individual files a tax return resulting in a duplicate filing under the same name and Social Security Number (SSN) that many individuals realize that they have become victims of identity theft.

When the identity thief files the fraudulent tax return, the IRS does not yet know that an individual'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 the SSN.[6] We estimate that more

---

[3] Taxpayers can be affected by more than one incident of identity theft. These incidents affected 154,139 taxpayers.
[4] These incidents affected 804,527 taxpayers.
[5] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).
[6] This estimate includes only those tax returns filed on tax accounts that contain an Identity Theft Indicator added on or before December 31, 2011.

than $70 million in potentially fraudulent tax refunds were paid to identity thieves who filed tax returns before the legitimate taxpayers filed theirs.[7] 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 tax returns we 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 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 plans to require additional personally identifiable information to be provided by the taxpayer. Nonetheless, authenticating taxpayers is a challenge whenever they call or write to the IRS requesting help with their tax account. The IRS has not adopted industry practices of shared secrets to authenticate taxpayers, such as security challenge questions (*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 identity-theft tax fraud 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 tax return filing begins.

In addition, another important tool that could immediately help the IRS prevent identity theft-related tax fraud is the National Directory of New Hires.[8] 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

---

[7] This estimate is based only on the duplicate use of the primary SSN.
[8] A Department of Health and Human Services national database of wage and employment information submitted by Federal agencies and State workforce agencies.

information is limited by law to just those tax returns with a claim for the Earned Income Tax Credit. The IRS included a request for expanded access in its annual budget submissions for Fiscal Years (FY) 2010, 2011, 2012, and has once again included a request in its FY 2013 budget submission.

Even with improved identification of tax returns with false wage and withholding being reported, verifying whether the returns are fraudulent will require 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, which indicates that the return information could be false. 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 refunds it identifies. The IRS will only select those tax returns that it can verify the identity of the taxpayer and/or the income based on resources while allowing other fraudulent refunds to 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 identity-theft-refund fraud cases is billions of dollars annually.

As we reported in July 2008[9] and July 2012, the IRS is not in compliance with direct deposit regulations that require tax refunds to be deposited to 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 quickly receive fraudulent tax refunds 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) used 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, we 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 in the name of the filer, it does help limit the potential or extent of fraud.

---

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

We also recommended and the IRS agreed to coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that tax refunds issued via direct deposit to either a bank account or 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 Financial Management Service to revisit this issue and reevaluate the feasibility of imposing such restrictions. Based on the discussions with the Financial Management Service, the IRS will determine whether such restrictions can be effectively implemented.

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. During CY 2012, as of September 30, 2012, the IRS reports that it has stopped the issuance of $9.3 billion in potentially fraudulent tax refunds associated with 1.4 million tax returns classified as involving identity theft. This represents a 49 percent increase in the number of fraudulent tax returns identified over the same period last year.

In addition, the IRS continued to expand its efforts to prevent the payment of fraudulent 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 false tax returns before they are processed and before any fraudulent tax refunds are issued. For example, the filters use Social Security benefit and withholding information from the Social Security Administration (SSA). This information is used to ensure that individuals reporting Social Security benefits and related withholding on tax returns received benefits from the SSA at the time the tax return is filed and before tax refunds are issued. Overall, this will help prevent the successful use of false Social Security benefits and withholding to obtain fraudulent refunds. We identified over 93,000 such tax returns in TY 2010 with fraudulent refunds issued totaling over $230 million. The IRS reports that it identified and confirmed identity theft on over 31,000 tax returns claiming fraudulent Social Securit benefits and withholding and stopped approximately $169 million in fraudulent tax refunds in Processing Year 2012.

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 halts processing of the tax return to prevent the issuance of a fraudulent tax refund. During CY 2012, as of September 30, 2012, the filters identified over 218,000 tax returns, stopping the issuance of approximately $1.5 billion in fraudulent tax refunds.

In January 2012, the IRS created the Identity Theft Clearinghouse in response to a TIGTA recommendation. The Clearinghouse was created to accept refund-related identity-theft leads from IRS Criminal Investigation field offices. The Clearinghouse performs research and develops each lead for the field offices and provides support for ongoing criminal investigations involving identity theft. As of October 25, 2012, the Clearinghouse had received over 2,000 identity-theft leads for development. These leads have resulted in the development of 264 identity-theft investigations.

In April 2012, the IRS launched a pilot program designed to help law enforcement obtain tax-return data vital to their efforts in investigating and prosecuting cases of identity theft. State and local law enforcement officials with evidence of identity theft involving fraudulently filed tax returns are now able, through a disclosure consent from the victim, to obtain tax returns filed using the identity-theft victim's SSN. This program was initially piloted in the State of Florida and has since been expanded to eight additional States.[10] As of September 30, 2012, the IRS has received 788 requests for information from State and local law enforcement.

The IRS is continuing to proactively lock[11] tax accounts to prevent the issuance of potentially fraudulent refunds. The IRS began a pilot program in Processing Year 2011, which locked taxpayers' accounts where the IRS Master File and SSA data showed a date of death. The IRS places a unique identity-theft indicator to lock the individual's tax account. This will systemically void tax returns filed on an individual's account if he or she is deceased. During CY 2012, as of September 30, 2012, the IRS had locked over 78,000 tax accounts and prevented approximately $548,000 in fraudulent tax refunds claimed using deceased individuals' identities. Since the program began, the IRS has locked over 97,000 tax accounts of deceased individuals and has prevented the issuance of approximately $2.3 million in fraudulent tax refunds.

The IRS has plans to expand its use of the tax account lock in CY 2013 to begin locking the accounts of minor children and taxpayers who do not have filing requirements. The IRS will place the same unique identity-theft indicator on these accounts, which will result in the systematic voiding of the tax return. This action should help to prevent additional identity-theft refund fraud. Our analysis of questionable TY 2010 tax returns that appeared to have been filed by an identity thief showed 2,274 children under the age of 14 had almost $4 million in refunds issued. In addition, almost

---

[10] Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania, and Texas.
[11] 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.

one million individuals whose income level does not require them to file a tax return[12] had over $3 billion in refunds issued.

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 tax returns.[13] Using the characteristics of confirmed 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.[14] 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.

The growth of identity theft presents considerable challenges to tax administration. In FY 2012, 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 staff years to resolve.[15] This inventory did not include 500,000 cases that were in the Duplicate Filing inventory,[16] many of which were identity-theft cases.

In FY 2012, the IRS dedicated 400 additional employees to the Accounts Management function[17] to work identity-theft cases. The Accounts Management function now has approximately 2,000 employees working these cases. However, the inventory of identity-theft cases has grown almost 50 percent from FY 2011 to 2012. In

---

[12] This category contains tax returns filed with income claimed for which there are no supporting income documents that would indicate the legitimate taxpayer was not required to file a tax return.
[13] 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.
[14] 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).
[15] One staff year is approximately 2,080 hours.
[16] 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.
[17] The function that works the majority of identity-theft cases involving individual duplicate tax returns.

FY 2011, the function received approximately 438,000 identity-theft cases and closed more than 300,000 cases. For FY 2012, the function received over 640,000 identity-theft cases and closed almost 440,000 cases. As of October 1, 2012, the Accounts Management function had over 370,000 identity-theft cases in its inventory.

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 been instances in which the SSA has issued to taxpayers the same SSN.

As previously mentioned, 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. Nevertheless, because of limited resources and the high taxpayer demand for telephone assistance, assistors who work identity-theft cases also work the telephones on Mondays (and any Tuesday following a Monday holiday).

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 know the tax laws and related IRS operational procedures. Identity-theft cases can be complex and often present considerable challenges throughout the resolution process. We recommended that the IRS provide additional training for assistors, to include the importance of documenting case actions and histories.

The IRS responded that it has improved training and provided training to all IRS employees who work identity-theft cases. TIGTA is currently evaluating whether the IRS has provided additional training to the assistors.[18] The IRS is currently testing new

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

procedures for processing and working identity-theft cases. Interviews with more than 20 assistors showed that many believed the training was not adequate and that the new procedures are still constantly being revised and updated, which is creating confusion for the assistor and the taxpayer alike.

However, the IRS has implemented new tools and job aids for the assistors to use when attempting to resolve identity-theft cases, including an Identity Theft Case Building Guide and Identity Theft Tracking Indicator Assistant. Some assistors stated that they believe these tools have been helpful when working identity-theft cases.

The management information system that telephone assistors use to control and work cases can add to the taxpayer's burden. For instance, one victim may have multiple cases opened and multiple assistors working his or her identity-theft issue. A review of 17 taxpayers' identity-theft cases showed 58 different cases had been opened and multiple assistors worked their cases. 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 and copies of identification with their tax returns.

The IRS sends the victims duplicate letters at different times, wasting agency resources and possibly confusing the victims. For example, the IRS sends taxpayers two different letters advising them that their identity-theft case is resolved. Assistors working an identity-theft case send a letter to a 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 their case has been resolved. Neither letter advises when the taxpayer should expect to receive his or her tax refund.

Identity-theft case histories are so limited that it is extremely difficult to determine what action has been taken on a case; for example, 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 of the cases had been resolved or why those cases were still open. In most cases, auditors 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 changes 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 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.

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 now 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. We will be testing the effectiveness of the new identity-indicator codes during our current audits.

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 dedicated employees 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 has updated tax-return processing procedures 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 identified during the 2013 Filing Season 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.

To further assist victims in the filing of their tax returns, the IRS issues Identity Protection Personal Identification Numbers (IP PIN) 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. It plans to issue about 500,000 IP PINs for the 2013 Filing Season.

Finally, in January 2012, the IRS established a Taxpayer Protection Unit 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. During the 2012 Filing Season, taxpayers found it difficult to reach employees in this unit. The unit 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 will direct these telephone calls to its Accounts Management function where about 230 employees have been trained to respond to these calls.

We are currently evaluating whether the IRS is effectively implementing corrective actions to our prior report to improve assistance to victims of identity theft.[19] An initial review of 16 identity-theft cases[20] worked by the Accounts Management function shows that for eight of the 16 cases, IRS processes stopped refunds from being issued to the apparent identity thieves. The time it took to process the 16 cases to resolve the identity-theft cases ranged from 47 days to 735 days, or an average of 242 days.

Criminal Investigations of Identity Theft

When the crime of identity theft occurs within TIGTA's jurisdiction, TIGTA's Office of Investigations initiates an investigation. Identity theft not only has 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 refunds before the legitimate taxpayers file, the crime is simple tax fraud and falls within the programmatic responsibility of IRS Criminal Investigation. There are, however, other variations of tax-related identity theft that fall within TIGTA's jurisdiction and have a significant impact on taxpayers.

TIGTA focuses its limited investigative resources on investigating identity theft that involves any type of IRS employee involvement, the misuse of client information by tax preparers, or the impersonation of the IRS through phishing schemes[21] 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's Office of Investigations aggressively pursues IRS employees involved in identity-theft crimes.

For example, IRS employee George L. Albright was sentenced on August 15, 2012, to 24-months and one-day of imprisonment, followed by one-year of supervised release, for committing aggravated identity theft and making false claims. Albright was also ordered to pay restitution to his victims in the amount of $9,669 and a court

---

[19] TIGTA, Audit No. 201240041, *Effectiveness of Assistance Provided to Victims of Identity Theft* (Follow-Up), report planned for June 2013.
[20] Auditors plan to review a statistical sample of 138 identity-theft cases from a population of 78,477 identity-theft accounts with specific identity-theft indicators that were entered by the Accounts Management function accounts for the period of August 1, 2011 through July 31, 2012.
[21] Phishing is a fraudulent attempt, usually made through e-mail, to steal an individual's personal information.

assessment of $200. During the course of his employment with the IRS, Albright used his position to access Federal tax records to obtain the names, SSNs, and dates of birth of taxpayers to electronically file nine fraudulent Federal tax returns that were sent to the IRS. He requested refunds on these returns and then directed payments totaling $10,954 to be electronically deposited into bank accounts that he controlled. Albright ultimately received refunds from eight of the nine fraudulent returns totaling $9,669.[22]

Tax preparers who steal and disclose any taxpayer's Federal tax information as part of an identity-theft scheme cause serious harm to taxpayers. The following case highlights the work of our criminal investigators who investigated a tax preparer who stole the personal identifiers of several individuals and unlawfully disclosed the information to others to fraudulently obtain tax refunds.

Neil Thomsen worked as a tax preparer from January 2002 to June 2008. In 2010, Thomsen used the personal identifiers of other individuals to file false income tax returns and obtain refunds from the IRS. Thomsen had obtained most of the personal identifiers from 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. Thomsen and his co-conspirators ultimately defrauded or attempted to defraud the IRS out of at least $560,000 in tax refunds.[23]

Impersonation of the IRS as part of an identity-theft scheme takes many forms. Criminals involved in these schemes use creative ways to obtain victims' personally identifiable information to commit fraud. Phishing, which usually involves mass solicitation of potential victims through e-mail or other forms of electronic communication, is a widespread method used by criminals to steal another's identity. Often scammers send e-mails claiming to be from the IRS. These phishing e-mails contain a "hook" that induces the victim to take some overt action.

For example, victims may be told that they are due a refund, their tax payment was rejected, or that they owe taxes on lottery winnings and need to click on a link which opens an attachment or directs them to a website where they are prompted to enter their personal identifiers, Federal tax information, and credit card information. Victims also may be told that they are under investigation by the IRS and need to respond immediately by clicking on a link which, again, opens an attachment or directs

[22] M.D. Tenn. Judgment filed Aug. 15, 2012; M.D. Tenn. Plea Agr. filed May 18, 2012
[23] S.D. Cal. Superseding Ind. filed June 19, 2012.

them to a website where they are prompted to enter their personal information to verify the status of their tax matter.

The following case is an example of a phishing scheme where several individuals were deceived into divulging their personal identifiers and banking information to identity thieves who then defrauded them of over $1 million.

Christian Amaukwu 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 and a $200 assessment.

Amaukwu 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. Amaukwu and his co-conspirators obtained massive e-mail distribution lists containing thousands of e-mail addresses and sent unsolicited e-mails falsely informing victims that they had won a lottery or had inherited money from a distant relative. Follow-up e-mails instructed the victims to provide personal and bank account information to receive their lottery winnings or inheritance. Subsequent e-mails to victims falsely indicated that a Government or a quasi-governmental agency, such as the IRS or the United Nations, would not pay the money due to them because advance payment of taxes and other fees was required. The e-mails solicited the victims to wire money to pay the taxes and other fees to designated bank accounts controlled by Amaukwu and his co-conspirators.

If the victims were unable to pay the taxes and fees, Amaukwu and his co-conspirators offered to loan them the money. Victims were convinced to open online bank accounts and provide the necessary login information. Using this information, Amaukwu and his co-conspirators stole money from various bank accounts, transferred that stolen money to the victims' accounts, and instructed the victims to wire the money to foreign bank accounts controlled by Amaukwu and his co-conspirators as payment for taxes and other fees on their purported lottery winnings or inheritance. The victims never received any lottery winnings, inheritance, or other money in connection with the scheme.[24]

While phishing schemes may range in their technical complexity, most share a common trait: They involve computers located outside the United States. Despite the

[24] E.D.N.Y. Judgment, filed Aug. 9, 2012; E.D.N.Y. Response to Defendant's Sentencing Letter filed Dec. 19, 2011; E.D.N.Y. Superseding Info. filed May 10, 2011.

significant investigative challenges this poses, TIGTA's Office of Investigations has been successful in working with law enforcement personnel in foreign countries to identify the perpetrators and obtain prosecutions.

Identity thieves may also impersonate IRS employees or misuse the IRS seal to induce unsuspecting taxpayers to disclose their personal identifiers and financial information for the purpose of committing identity theft. The following case is an example of how an IRS employee was impersonated to facilitate a fraud scheme.

Jared Brewton, posing as an IRS "Audit Group Representative," 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 taxpayers without their knowledge or consent. The tax returns contained W-2 information such as income and withholding that was falsely and fraudulently inflated. As a result, Brewton received fraudulently-procured tax refunds in the names of those taxpayers and used the refunds to purchase personal items. Brewton 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.[25]

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 tax administration. We plan to provide continuing audit coverage of IRS 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 criminal investigations of identity-theft violations involving IRS employees, tax return preparers, and individuals impersonating the IRS.

Chairman Platts, Ranking Member Towns, 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.

[25] S.D.N.Y. Crim. Indict. filed Jan. 25, 2012.; S.D.N.Y. Minute Entry filed July 11, 2012.

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.