JOINT HEARING BEFORE THE
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEES ON OVERSIGHT
AND SOCIAL SECURITY
U.S. HOUSE OF REPRESENTATIVES

"Identity Theft and Tax Fraud"

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

May 8, 2012

Washington, D.C.

TESTIMONY OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEES ON OVERSIGHT
AND SOCIAL SECURITY
U.S. HOUSE OF REPRESENTATIVES

"Identity Theft and Tax Fraud"

May 8, 2012

Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and Members of the Subcommittees, thank you for the invitation to speak before you today on the subject of identity theft and its impact on taxpayers and tax administration. Since I last testified on this subject in November 2011,[1] we have completed our assessment of the IRS's efforts to identify and prevent identity theft and plan to issue our final report in June of this year. We have also recently issued a report on the assistance that the IRS provides to victims of tax fraud-related identity theft. My comments today will focus on this recently completed work.

As we have reported previously, a substantial number of individuals continue to submit tax returns reporting false income and/or withholding for the sole purpose of receiving a fraudulent tax refund. Many of these claims involve identity theft. For Processing Year 2011,[2] the IRS reported that of the 2.2 million tax returns that it identified as fraudulent, approximately 940,000 tax returns with $6.5 billion in associated fraudulent tax refunds involved identity theft.

The IRS acknowledges that it does not have complete statistics on identity theft. In Calendar Year 2011, the IRS identified over 1.1 million incidents of identity theft that affected the Nation's tax system. This figure includes incidents in which taxpayers contacted the IRS alleging that they were victims of identity

[1] *Identity Theft and Tax Fraud*, *Hearing Before the H. Comm. on Oversight and Government Reform, Subctm. on Government Organization, Efficiency and Financial Management*,112th Cong. (Nov. 15, 2011) (statement of J. Russell George).
[2] A Processing Year is the year that the tax return is processed.

theft (110,750 incidents[3]) as well as instances where the IRS identified identity theft (1,014,884 incidents[4]). Many of the taxpayers that the IRS identified were not aware they were victims of identity theft because they either did not file tax returns or did not have filing requirements.

Detection and Prevention of Identity Theft

At the beginning of the 2012 Filing Season, the IRS announced the results of a nationwide sweep cracking down on suspected identity theft perpetrators as part of a stepped-up effort against refund fraud and identity theft. This effort is part of the IRS's identity theft strategy to prevent, detect, and resolve identity theft cases. In addition to this crackdown by its law-enforcement division, the IRS has stepped up its internal reviews to spot false tax returns before tax refunds are issued. These efforts include designing new identity theft screening filters that the IRS believes will improve its ability to identify false tax returns before they are processed and before any fraudulent tax refunds are issued.

Tax returns identified 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. Once a taxpayer's identity has been confirmed, the tax return is released for processing and the tax refund is issued. 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. As of April 19, 2012, the IRS reports that it has stopped the issuance of $1.3 billion in potentially fraudulent tax refunds as a result of the new identity theft filters.

The IRS also continues to expand its efforts to prevent the payment of fraudulent tax refunds claimed using deceased individuals' names and Social Security Numbers (SSNs). The IRS began a pilot program in Processing Year 2011 which locked taxpayers' accounts where the IRS Master File and Social Security Administration data showed a date of death. The IRS places a unique identity theft indicator on deceased individuals' tax accounts to lock their tax account. This will systemically void tax returns filed on a deceased taxpayer's account. As of March 1, 2012, it had locked 90,570 tax accounts and prevented approximately $1.8 million in fraudulent tax refunds claimed using deceased individuals' identities since the lock was established.

---

[3] Taxpayers can be affected by more than one incident of identity theft. These incidences affected 87,322 taxpayers.
[4] These incidences affected 553,730 taxpayers.

Recognizing that victims of identity theft can be affected in multiple tax years, the IRS also places an identity theft indicator on each tax account for which it has determined an identity theft has occurred. All tax returns filed using the identity of a confirmed victim are flagged during tax return processing and sent for additional screening before any tax refund is issued. This screening is designed to detect tax returns filed by identity thieves who attempt to re-use a victim's identity in subsequent years and to prevent the issuance of fraudulent tax refunds.

To further assist victims in the filing of their tax returns, the IRS, in Fiscal Year 2011, began issuing Identity Protection Personal Identification Numbers (IPPIN) to these individuals. The IPPIN will indicate that the taxpayer has previously provided the IRS with information that validates their 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 IPPIN correctly input at the time of filing will be processed as the valid tax return using standard processing procedures. A new IPPIN will be issued each subsequent year before the start of the new filing season for as long as the taxpayer remains at risk for identity theft. For the 2012 Filing Season, the IRS sent 252,000 individuals an IPPIN.

However, the IRS does not know how many identity thieves are filing fraudulent tax returns or the amount of revenue being lost. TIGTA evaluated the IRS's efforts to identify and prevent fraudulent tax returns resulting from identity theft.[5] As part of our assessment, we identified and quantified potential refund losses resulting from identity theft.

Using characteristics of tax returns that the IRS has identified and confirmed as fraudulent filings involving identity theft, we analyzed Tax Year 2010 tax returns to identify additional tax returns that met the characteristics of these confirmed cases. Our analysis found that, although the IRS detects and prevents a large number of fraudulent refunds based on false income documents, there is much fraud that it does not detect. We identified approximately 1.5 million additional undetected tax returns with potentially fraudulent tax refunds totaling in excess of $5.2 billion. If not addressed, we estimate the IRS could issue approximately $26 billion in fraudulent tax refunds resulting from identity theft over the next five years.

---

[5] TIGTA, Audit No. 201140044, *Efforts to Identify and Prevent Fraudulent Tax Returns Resulting From Identity Theft* (planned report issuance in June 2012).

The primary characteristic of these 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. The individuals whose identities were stolen may not even be aware that their identities were used to file a fraudulent tax return. These individuals are typically those who are not required to file a tax return. Individuals are generally not aware that they are the victims of this type of identity theft unless they file a tax return, which causes the return to be rejected as a duplicate filing.

Access to third-party income and withholding information at the time tax returns are processed is the single most important tool the IRS could have to identify and prevent this type of identity theft tax fraud. In lieu of this, another important tool that could help the IRS prevent this type of fraud is the National Directory of New Hires.[6] 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 data 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 to the National Directory of New Hires in its annual budget submissions for Fiscal Years 2010, 2011, and 2012. The request was made as part of the IRS's efforts to strengthen tax administration. However, expanded access has not been provided for by law. The IRS has again requested expanded access to the National Directory of New Hires in its FY 2013 budget submission.

In a report that we recently issued to the IRS, we included a recommendation to develop a process that uses information from the National Directory of New Hires (if expanded access is provided in the law) along with third-party income and withholding information that the IRS maintains for the prior year's tax filings to better identify individuals who report false income. The IRS could use this information to confirm that the individual had no reported income or withholding in the prior tax year and did not obtain new employment in the current tax year. The IRS could then freeze the tax refund and attempt to verify the reported income and withholding.

---

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

Even with improved identification of these returns, the next step of verifying whether the returns are fraudulent will require resources. The IRS has faced budget cuts, a hiring freeze, and staffing reductions during the same time it has encountered a significant surge in identity theft 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 based on its resources.

Using IRS estimates, it would cost approximately $31.8 million to screen and verify approximately 1.5 million tax returns that we identified as not having third-party information to support the income and withholding reported on the tax return. 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 $5.2 billion annually.

The validation process that we have proposed has some limitations. It will not identify instances of identity theft in which the legitimate taxpayer is employed and has a filing requirement but has not yet filed an income tax return. The IRS needs further tools to identify those individuals who are improperly filing using the identity of a taxpayer with a tax return filing requirement.

In those cases involving identity theft, the fraudulent tax return is often filed before the legitimate taxpayer files his or her tax return. For Tax Year 2010, we identified 48,357 SSNs that were used multiple times as a primary Taxpayer Identification Number.[7] When the identity thief files the fraudulent tax return, the IRS does not yet know that the individual's identity will be used more than once. As a result, the tax return is processed and the fraudulent refund is issued. These instances result in 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. In Tax Year 2010, we estimate that $70.6 million in potentially fraudulent tax refunds were paid to identity thieves who filed tax returns before the legitimate taxpayers filed theirs.[8] This is in addition to the $5.2 billion in potentially fraudulent refunds noted previously related to taxpayers who do not appear to have a filing requirement.

---

[7] This estimate includes only those tax returns filed on tax accounts that contain an Identity Theft Indicator input on or before December 31, 2011. It does not include potentially fraudulent tax returns filed on tax accounts that do not contain an Identity Theft Indicator.
[8] This estimate is based only on the duplicate use of the primary SSN.

Although the IRS is working toward finding ways to determine which tax return is legitimate, it could do more to prevent identity thieves from electronically filing (e-file) tax returns. 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, 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, and obtain an Electronic Filing PIN by providing his or her name, SSN, date of birth, and the address and filing status on the prior year's tax return. The IRS then matches this information with the data on the prior year's tax return filed by the taxpayer.

Authenticating taxpayers is a challenge, not only in processing tax returns, but also whenever taxpayers call or write to the IRS requesting help with their tax account. The IRS has not adopted common industry practices for authentication, such as security challenge questions (*e.g.*, mother's maiden name, name of first pet).

Direct Deposit and the Use of Debit Cards

Direct deposit, which now includes debit cards, is often used by identity thieves to obtain fraudulent tax refunds. Approximately $4.5 billion of the $5.2 billion in potentially fraudulent tax refunds we identified were issued by direct deposit.

In September 2008, we reported[9] that the IRS was 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.[10] We recommended that the IRS limit the number of tax refunds being sent to the same account. While such a limitation does not ensure that all direct deposits are in the name of the taxpayer, it does help limit the potential for fraud. The IRS was concerned about limiting the number of direct deposits to a single account because of situations in which an account is in the name of multiple individuals. In addition, the IRS places responsibility for compliance with Federal direct deposit regulations on the taxpayer. The IRS stated that it is the taxpayer's responsibility to ensure that their tax refunds are only directly deposited into their accounts. However, in our

[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).
[10] 31 C.F.R. Part 210 (2011).

opinion, the IRS is responsible for ensuring that direct deposits are made to an account in the name of the recipient. Representatives from the Financial Management Service also indicated that the IRS is responsible for enforcing the Code of Federal Regulations requirement.

To date, little has been done to ensure that tax refunds are directly deposited only into the taxpayer's account. Some bank accounts are obviously being used for the refunds of many different taxpayers. For example, we found that 4,157 of the potentially fraudulent tax refunds we identified totaling $6.7 million were deposited into one of 10 bank accounts. Each of these 10 bank accounts had direct deposits of more than 300 tax refunds.

The use of debit cards to receive tax refunds further increases the risk of tax fraud. Identity thieves are using debit cards to fraudulently obtain direct deposits of fraudulent tax refunds. For example, authorities confiscated over 5,000 debit cards during the investigation of a Tampa, Florida identity theft scheme. Individuals can obtain a debit card online or from a bank, a third-party provider, or a local retailer. This complicates the IRS's efforts to identify the holder of the debit card as well as the bank account and the tax account associated with the debit card. In addition, the debit card issuer is the only entity that can ensure the individual requesting the debit card and receiving the tax refund is the taxpayer.

The IRS has a process in place in which it works with banks to obtain information on questionable tax refunds. In December 2011, one bank associated with the confiscated debit cards from the Tampa scheme provided the IRS with a listing of 60,000 bank accounts, including debit card accounts, that it had identified nationwide with questionable tax refunds. The bank intercepted and prevented questionable tax refunds totaling $164 million from being deposited into these accounts.

IRS management has indicated that it is working to establish processes to recover potentially fraudulent tax refunds intercepted by banks. However, more action is needed to prevent tax refunds from being erroneously deposited into bank accounts. We are currently working with the IRS and the Department of the Treasury to determine ways in which the IRS could strengthen direct deposit controls. At a minimum, we believe the IRS should implement our previous recommendations to limit the number of direct deposits to a single bank or debit card account, and coordinate with financial institutions to develop a process to

ensure that tax refunds issued via direct deposit are issued only to accounts that are in the taxpayer's name.

We believe the Department of the Treasury will need improved policies and regulations to ensure that debit cards can be identified based on the direct deposit account information on tax returns and vice versa. Furthermore, because of the potential for fraud that can be perpetrated by an anonymous user of these debit cards, the Department of the Treasury should take steps to ensure that financial institutions and/or debit card administration companies authenticate the identity of individuals purchasing or obtaining debit cards before Government funds can be deposited on those cards. Direct deposits should not be made to debit cards issued by financial institutions and debit card administration companies that do not take sufficient steps to authenticate individuals' identities.

IRS Assistance to Victims of Identity Theft

We recently completed an audit that evaluated the assistance that the IRS provides to victims of identity theft.[11] We found that the IRS is not effectively providing assistance to these victims. Moreover, processes are not adequate to communicate identity theft procedures to taxpayers, resulting in increased burden for victims of identity theft. Of continuing concern is the length of time taxpayers must work with the IRS to resolve identity theft cases.

Identity theft cases can take more than one year to resolve. While we cannot provide specific case examples due to privacy and disclosure laws, the following timeline illustrates a typical path for an identity theft refund fraud case that is not complex:

February The identity thief files a fraudulent tax return and obtains a tax refund. Subsequently, the legitimate taxpayer (taxpayer) attempts to electronically file his tax return, for which he is due a tax refund. He receives an IRS rejection notice stating that his SSN cannot be used more than once on the tax return or on another tax return.

The taxpayer calls the IRS toll-free telephone line and explains the situation to the assistor. The assistor, after authenticating the taxpayer's identity, researches his tax account and determines that a tax return has already been filed using his name and SSN. The assistor advises the taxpayer to file a paper tax return, attaching an Identity Theft Affidavit (Form 14039) or a police report and a valid government-issued document such as a copy of a Social Security card, passport, or driver's license to the tax return and mailing it to the IRS.

[11] 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).

The IRS receives the paper tax return in one of its processing sites and a technician enters the data into the IRS computer system. The paper tax return with all attachments is sent to the Files Unit. It is rejected. A technician determines it is a duplicate tax return and inputs the appropriate transaction code. The duplicate return case is received in the Duplicate function, where an assistor identifies this as a possible identity theft case. The assistor requests the paper tax return. The case is set aside in a queue to be worked after April 15, when the filing season has ended.

April The taxpayer calls the IRS toll-free line again and asks when he will receive his tax refund. The assistor researches the taxpayer's account, determines a duplicate tax return has been filed, and advises the taxpayer that there will be processing delays and that he may receive correspondence requesting additional information. The assistor also advises the taxpayer to visit the IRS website at IRS.gov for additional information and links related to identity theft.

July The taxpayer's tax return is worked in the Duplicate function and determined to be an identity theft case. The duplicate tax return is transferred to another unit to an assistor whose responsibilities also include answering IRS toll-free telephone calls. The case is scanned into a management information system and queued.

September The assistor begins working the case, orders copies of original tax returns, and sends letters to the identity thief and the taxpayer to attempt to determine who the legitimate taxpayer is. The taxpayer responds, confirming that he did not file the first tax return the IRS received.

October The taxpayer calls the Identity Protection Specialized Unit and asks when he should expect his tax refund. The customer service representative researches the case and advises him his case is being worked. This representative sends a referral to the assistor working the case.

November The assistor determines who the legitimate taxpayer is, requests adjustments to the taxpayer's account, and sends a letter to the identity thief providing him or her with a temporary tax identity number and a letter to the taxpayer advising him he has been a victim of identity theft and his account has been flagged.

December The taxpayer receives the letter from the IRS and calls the Identity Protection Specialized Unit to inquire when he will receive his tax refund. The assistor advises him that it has been scheduled.

January The adjustments post to the taxpayer's account and the refund is released. The taxpayer receives another letter advising him he has been a victim of identity theft and his account has been flagged. A new tax account for the person who committed the identity theft is also established.[12]

The above illustration provides a "best case" resolution of an identity theft case given the IRS's current processes. However, most cases are more complex and can present considerable challenges throughout the resolution process. For instance, 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 the IRS when it requests information to resolve the case. As a result, the IRS may not be able to

[12] Even though a tax return is fraudulent, the IRS retains a record of the tax return by creating a tax account under a tax identification number that the IRS creates, and posting the tax return.

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. In certain instances, the Social Security Administration had issued two taxpayers the same SSN.

As a result of an assessment of its Identity Theft Program completed in October 2011, the IRS is currently planning improvements to its program. The IRS is reorganizing to have 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 will also begin collecting IRS-wide identity theft data to assist in tracking and reporting the effect identity theft has on tax administration. Nevertheless, these improvements may not be sufficient to significantly reduce the burden identity theft has placed on tax administration and on taxpayers whose identities have been stolen.

Identity theft cases have not been prioritized during the standard tax return filing process. The IRS plans to update 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 processing to be forwarded and assigned to an assistor, rather than continuing through the standard duplicate tax return procedures. This will reduce the time a taxpayer must wait to have his or her identity theft case resolved by three to five months. However, the IRS does not plan to put this change into place until June 2012.

Taxpayers could also be further burdened if the address on the tax return filed by the identity thief is used by the IRS instead of the address of the legitimate taxpayer. 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 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 the identity theft case, the identity thief's address is still 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. The legitimate taxpayer (the identity theft victim) will be unaware 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 at having his or her personal and tax information 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 when there is a claim of identity theft. The IRS developed tracking indicators to mark taxpayer accounts when the identity theft incident is initially alleged or suspected. It will explore leveraging this new indicator to suspend certain correspondence.

Resources have not been sufficient to work identity theft cases dealing with refund fraud and continue to be of a concern. IRS employees who work the majority of identity theft cases also respond to taxpayers' calls to the IRS's various toll-free telephone lines. Demanding telephone schedules and a large identity-theft inventory make it difficult for assistors to prioritize identity theft cases. The IRS has dedicated 400 additional employees to the Accounts Management function to work identity theft cases. However, because of limited resources and the high taxpayer demand for telephone assistance, the IRS plans to continue to have assistors who work identity theft cases also work the telephones on Mondays (and any Tuesday following a Monday holiday).

Assistors are trained to communicate with taxpayers and know the tax laws and related IRS operational procedures. However, identity theft cases can be complex and can present considerable challenges throughout the resolution process. Assistors are not examiners and are not trained to conduct examinations, which requires skills and tools beyond those of the assistors.

Additionally, the management information system that telephone assistors use to control and work cases can add to taxpayer burden. For instance, one victim may have multiple cases opened and multiple assistors working his or her identity theft issue. 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.

Victims also receive duplicate letters at different times, wasting IRS resources and possibly confusing the victims. None of the letters advise the victims when to expect their refunds, which could still be months away.

Identity theft case histories are so limited that it is extremely difficult to determine what action has been taken on a case; for example, if research was completed to determine which individual is the legitimate taxpayer. 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.

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.

The IRS acknowledges that it does not know the exact number of identity theft incidents or the number of taxpayers affected by identity theft. It also has not been able to quantify the amount of improper payments resulting from identity theft. The IRS reports cases only for accounts with identity theft indicators. It has procedures in place to input identity theft indicators on certain taxpayer accounts, depending on how the taxpayer's identity theft case was identified and if it affects Federal tax administration. However, these procedures are inconsistent and complex. Potential identity theft cases in process do not have indicators and are not counted.

Identity theft data are captured on 22 different systems throughout the IRS. These systems are not integrated and data must be manually compiled, hindering the IRS's capability of producing accurate and reliable identity theft reports. As a result, not all identity theft cases are counted. In addition, not all cases counted are actually identity theft cases. As of June 2011, the IRS estimated the number of unmarked accounts that should have identity theft indicators in the range of 240,000 to 280,000.

Finally, in November 2011, the IRS established a Taxpayer Protection Unit to manage work arising from the identity theft indicators and filters used to identify tax returns affected by identity theft—both to stop the identity thief's tax return from being processed and to ensure the legitimate taxpayer's tax return is processed. Currently, employees have only been detailed to the unit. The IRS will determine the needs of the unit after assessing the 2012 Filing Season.

During this filing season, taxpayers found it difficult to reach employees in this unit. The unit received more than 86,000 calls during the 2012 Filing

Season, but has only been able to answer about 21,000. The average wait time for taxpayers was almost one hour. The Taxpayer Protection Unit will be a significant component in the IRS's attempt to stop fraudulent refunds and provide assistance to victims of identity theft. TIGTA is currently conducting an audit of this unit and, during the 2013 Filing Season, we will be conducting a follow-up audit to assess the IRS's actions to improve the quality of assistance provided to identity theft victims.

Criminal Investigations of Identity Theft

When the crime of identity theft occurs within our jurisdiction, TIGTA's Office of Investigations (OI) investigates it as it impacts the economy, efficiency, and effectiveness in the administration of the Internal Revenue Code. Identity theft directly and destructively impacts law-abiding citizens. When individuals steal identities and file fraudulent tax returns to obtain fraudulent refunds before the legitimate taxpayers file, the crime is simple tax fraud and it falls within the jurisdiction and programmatic responsibility of the IRS. However, there are other variations of IRS-related identity theft that, although not widely covered by the media, falls within TIGTA's jurisdiction and has a significant impact on taxpayers.

TIGTA focuses its limited investigative resources on the following areas as they pertain to IRS-related identity theft:

- IRS employees who are involved in committing identity theft either as the source of the identity information or through active participation in a scheme;

- Tax preparers who improperly steal and disclose client information for the purpose of committing identity theft; and

- Individuals who impersonate the IRS in furtherance of committing identity theft.

TIGTA has conducted investigations of IRS employees who use their access to taxpayer information as a means for stealing identities for the purpose of committing identity theft. Noted below is an example of identity theft by an IRS employee:

On April 14, 2011, Monica Hernandez was indicted for making a false income tax return when she was a part-time data entry clerk for the IRS. During

the course of her employment with the IRS, Hernandez stole and/or misappropriated information of other taxpayers listed on various IRS forms. Hernandez used falsified and forged IRS forms with the victim's information to obtain large tax refunds from the IRS totaling $175,144.

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 OI pursues identity theft violations and conducts criminal investigations of IRS employees involved in these crimes.

Tax preparers who improperly 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 an instance when a tax preparer stole and improperly disclosed the identity of her clients in order to commit identity theft:

Kathleen Lance was a public accountant and president of her company. In this capacity, Lance obtained and used the identification of six of her clients to change the direct deposit account information on clients' tax returns before she electronically submitted their returns to the IRS. Lance thereby diverted funds from the clients' bank accounts and redirected the deposits to her personal and business bank accounts. Lance also assumed and disclosed the identity of those six clients and fraudulently opened credit card accounts in her name. On May 24, 2010, she was sentenced to serve 64-months imprisonment and three-years supervised probation for wire fraud, theft of Government funds, use of unauthorized access devices, and aggravated identity theft.

Impersonation of the IRS as part of an identity theft scheme takes many forms. Often, the IRS is impersonated by individuals who seek to trick unsuspecting taxpayers into revealing their personal information. The details of each scheme tend to vary, but the common thread is the use of the IRS name to lure recipients into accessing links or providing sensitive information.

- Victims are told that they are either due a refund or that a tax payment was rejected and the taxpayer needs to click on a link which either opens an attached form or takes them to a website where they enter their Personally Identifiable Information (PII), Federal tax information, and credit card information; or

- Victims are told that they are being investigated by the IRS and need to immediately respond by clicking on a link which opens an attached form or takes them to a website, where they are prompted to provide their PII to verify the status of their tax matter.

In both of these situations, the victim is presented with a website which is designed to replicate a legitimate IRS.gov website, often by using authentic IRS images and seals. The case below is an example wherein an individual impersonated the IRS to commit identity theft:

Godspower Egbufor, together with co-conspirators, operated a scheme and stole the identities of numerous individuals and defrauded them out of more than $1 million through Internet solicitations. Egbufor obtained massive e-mail distribution lists containing thousands of e-mail addresses and sent unsolicited e-mails falsely informing targeted victims that they had won a lottery or had inherited money from a distant relative. E-mails to victims falsely indicated that a government or quasi-governmental entity, such as the IRS or the United Nations, prevented the money due to them from being awarded because advance payment of taxes and other fees were required. Follow-up e-mails instructed the victims to provide their personal and bank account information in order to receive their lottery winnings or inheritance. On December 19, 2011, Egbufor was sentenced to 108 months of imprisonment and five years of supervised release for violations of Aggravated Identity Theft and Conspiracy to Commit Wire Fraud.

In conclusion, we at TIGTA continue to be very concerned about the scope of this problem and will provide continuing audit coverage of IRS actions taken to stem tax fraud-related identity theft and to provide prompt resolution to taxpayers who are 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. I hope my discussion of our work assists you with your oversight of the IRS on this issue.

Chairman Boustany, Chairman Johnson, Ranking Member Lewis, Ranking Member Becerra, and Members of the Subcommittees, thank you for the opportunity to address this important topic 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.