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"

November 4, 2011

Washington, D.C.

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

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"

November 4, 2011

Chairman Platts, Ranking Member Towns and Members of the Subcommittee, thank you for the invitation to speak before you today on the subject of identity theft and its impact on the Internal Revenue Service's (IRS) function of administering the Nation's tax laws. My comments will focus on the ongoing work that the Treasury Inspector General for Tax Administration (TIGTA) has underway to evaluate the IRS's efforts in identifying and preventing identity theft relating to tax administration and to assist taxpayers who have been victims of identity theft.

There are two primary types of identity theft that relate to tax administration: the first type involves an individual using another person's name and/or Social Security Number (SSN) to file a fraudulent tax return to generate a tax refund. I will refer to this form of identity theft as "tax fraud identity theft." The second type involves using another person's identity (*e.g.,* name, SSN, or both) to obtain employment. I will refer to this form of identity theft as "employment-related identity theft."

In April 2008, I testified on the growing threat of identity theft to tax administration. At that time, we reported that the IRS had not placed sufficient emphasis on developing strategies to address either form of identity theft, whether employment- or tax-fraud-related. The IRS lacked the comprehensive data needed to determine the impact of identity theft on tax administration. Its prevention strategy did not include pursuing individuals using another person's identity, unless a case directly related to a substantive tax violation. According to IRS policy at that time, identity theft crimes were investigated by the IRS's Criminal Investigation Division if the crime was committed in conjunction with other criminal offenses having a large tax effect.

In 2008, TIGTA recommended that the IRS develop and implement a strategy to address both employment-related and tax-fraud identity theft.[1] We recommended that this strategy include coordinating with other Federal agencies, such as the Federal Trade Commission and Social Security Administration, to evaluate and investigate identity-theft allegations related to tax administration. We also recommended improvements in the use of an identity theft closing codes in the IRS's compliance functions.[2]

At that time, it was the IRS's position that it did not have sufficient enforcement resources to address most identity-theft cases. Moreover, it stated that employment-related identity theft cases were not the responsibility of the IRS and that it would not be worthwhile to pursue employment-related identity theft cases for unreported tax liabilities because the taxes owed on most of these cases were not significant. We expressed concern that if the IRS did not take additional action to stem the problem, there would be no deterrent effort to keep the problem from spreading.

Since 2008, the number of tax-related identity-theft incidents impacting tax administration has grown significantly. Although the IRS acknowledges that it does not know for certain the number of open or closed identity-theft cases, as of August 31, 2011, IRS incident tracking reports indicate that 582,736 taxpayers were affected by identity theft in Calendar Year 2011. In Calendar Year 2008, the IRS reported 254,079 taxpayers were affected.

IRS's Assistance to Victimized Taxpayers

The impact of identity theft on taxpayers is profound and can have major consequences. Employment-related identity theft can affect taxpayers when the IRS attempts to take enforcement actions for what appears to be unreported income. Refund fraud using another person's identity has a more substantial effect. After an identity thief has successfully committed this crime and is enjoying the benefits, the victim begins to realize the harm. It affects lawful taxpayers' ability to file their tax returns and can significantly delay their tax refunds.

TIGTA is currently evaluating whether the IRS is effectively providing assistance to victims of identity theft.[3] To date, auditors have analyzed identity theft cases, reviewed all significant guidance and procedures dealing with identity theft, and conducted interviews with more than 200 IRS employees who work identity theft issues. TIGTA interviewed employees in all aspects of the Identity Theft Program, including assistors, technicians, case reviewers, quality team

[1] TIGTA, Ref. No. 2008-40-086, *Outreach Has Improved, But More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft* (March 2008).
[2] A closing code is entered on an account when the case is closed and identifies the type of case.
[3] TIGTA, Audit No. 201140042, *Effectiveness of Assistance Provided to Victims of Identity Theft* (planned report issuance in May 2012).

managers, production monitors, tax examiners, analysts, managers, and executives.

Our preliminary observations are that the IRS is not effectively providing assistance to victims of identity theft and its processes are not adequate to communicate identity-theft procedures to taxpayers. This results in increased burden for the victims of identity theft.

We have analyzed recent identity theft cases to evaluate the IRS process for assisting victims and have found that the process is very lengthy. While we cannot provide specific case examples due to privacy and disclosure laws, the following timeline illustrates a composite for an identity theft refund fraud case.

February The identity thief files a fraudulent tax return and obtains a tax refund. Subsequently, the lawful 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 customer service assistor. The assistor, after authenticating the taxpayer, researches his tax account and determines a tax return has already been filed using that name and SSN. The assistor advises the taxpayer to file a paper tax return, attaching an Identity Theft Affidavit (Form 14039, which is attached to the testimony) 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 mail it to the IRS.

The IRS receives the paper tax return in one of its processing sites and a technician enters the data into the IRS's computer system.[4] It is rejected. A technician determines it is a duplicate tax return and inputs the appropriate transaction code. The duplicative 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 he may receive correspondence requesting additional information. The assistor also advises the taxpayer to visit the IRS's 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 duplicative 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 alleged identity thief and the taxpayer to attempt to determine who the legitimate taxpayer is. The legitimate taxpayer responds, confirming that he did not file the first tax return the IRS received.

[4] The paper tax return with all attachments is sent to the Files Unit, which is a repository where paper tax returns and related documents are stored.

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

November The assistor determines which is the legitimate taxpayer, 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 legitimate taxpayer advising him he has been a victim of identity theft and his account has been flagged.

December The legitimate 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 legitimate taxpayer's account and the refund is released. He receives another letter advising him he has been a victim of identity theft and his account has been flagged. A tax account for the person who committed the identity theft is also established.[5]

The above illustration provides a "best case" resolution of an identity theft case. 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 determine who the legitimate taxpayer is. With other cases we have reviewed, taxpayers claimed to be victims of identity theft after receiving refunds for which 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.

Standard IRS processes and organizational structure hinder timely and effective case resolution. Demanding telephone schedules, resource restraints, and a large identity-theft inventory make it difficult for assistors to prioritize identity theft cases. Assistors who work the majority of identity-theft cases also work the IRS's toll-free telephones responding to taxpayer inquiries. Identity theft cases are not always priority, even though an untimely case resolution could result in significant taxpayer burden and an improper payment.

Identity-theft case processing is highly decentralized. Coordination among the IRS functions is limited. Procedures pertaining to identity theft are not arranged for efficient access, are inconsistent, and are scattered throughout the Internal Revenue Manual. The different systems used by the various functions prevent accurate tracking and reporting of identity theft workloads and their affect on tax administration. There is no mechanism or system in place to track cases in process or time spent working cases.

[5] 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.

The majority of identity theft cases are worked by telephone assistors. Total time spent on a case can vary significantly and sometimes cases can stay open for months with little or no activity as assistors answer calls or work other types of cases.

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. When victims are asked numerous times to prove their identities, although they had previously followed IRS instructions and sent in Identity Theft Affidavits and copies of identification with their tax returns, this adds to taxpayer burden.

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 actions have been taken on a case, such as, 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 auditors reviewed a sample of cases, they could not determine if some of the cases had been resolved or why the cases were still open. In most cases, TIGTA auditors had to reconstruct the cases to determine if all actions had been appropriately taken to resolve them.

The IRS's standard processes and procedures are not conducive to timely working identity theft cases and need to be streamlined. Victims who contact the IRS when their tax returns are rejected are instructed to mail a paper tax return to an IRS processing site and attach a completed Identity Theft Affidavit along with copies of identification. These tax returns, with the Affidavit and identifying documents attached, are added to the normal processing stream for processing tax returns and casework. They are merely identified as a duplicate tax return and are put in the queue to be worked after the filing season. After the cases are identified as identity theft cases, they then await assignment. This process can take from four to five months.

Transactions to adjust the victims' tax accounts and release the tax refunds can take from 2 to 12 weeks to post, yet the victims may have already received letters advising them that their cases have been resolved. This can lead to additional taxpayer contacts and wasted IRS resources.

The IRS is not able to effectively report on its Identity Theft Program, which inhibits it from taking appropriate actions to reduce identity theft affecting tax administration. The IRS reports cases only for accounts with identity theft indicators.[6] 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 tax administration. However, the procedures are inconsistent and complex. Potential identity theft cases in process do not have indicators and are not counted. There are approximately 200,000 cases in the Duplicate function inventory that are not being counted. Cases being reviewed, which at any one time can be more than 15,000, may be counted twice. Additionally, identity theft indicators have not been consistently inputted, reversed when necessary, or inputted at all.

The IRS has guidelines to assign temporary Internal Revenue Service Numbers[7] for identity theft cases, but procedures are inconsistent. It does not track or identify which Internal Revenue Service Numbers are created for identity thieves. The IRS also does not classify identity theft cases by employment or refund fraud.

In Fiscal Year 2011, the IRS began issuing Identity Protection Personal Identification Numbers (PIN) to taxpayers who have previously been identified by the IRS as victims of identity theft (when the identity theft affected the filing or processing of their tax return and an identity theft indicator was placed on their account). The PIN 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 Identity Protection PIN correctly inputted at the time of filing will be processed as the valid tax return using standard processing procedures. A new Identity Protection PIN will be issued each subsequent year in January for the new filing season for as long as the taxpayer remains at risk for identity theft – which depends on whether there are additional fraudulent returns filed using the taxpayer's identity.

Currently, the IRS offers the Identity Protection PIN only to taxpayers who have been a victim of identity theft that has affected the filing or processing of their Federal tax return. It does not offer the Identity Protection PIN to all taxpayers, even if they have reported that they believe they have been a victim of identity theft, but have not had problems filing their tax returns. The financial

[6] Identity theft indicators were developed to track identity theft incidents. Each indicator is input as a transaction code with action code and displayed on the affected taxpayer's account. There are various codes that distinguish the type of identity theft incident. For example, a code can indicate (1) the taxpayer identified that they are a victim of identity theft; (2) the IRS identified the taxpayer is a victim and notified the taxpayer; and (3) the taxpayer has submitted the required documentation (Form 14039 and government-issued identification).

[7] This number is created by the IRS for internal processing problems only and is not considered a valid SSN. Tax returns with Internal Revenue Service Numbers are considered invalid by the IRS and as such, the individual is unable to claim personal exemptions, deductions, and credits.

sector offers customers the option of providing additional protection on their accounts. The IRS should consider adopting such practices.

The IRS has an IRS-wide Authentication Strategy, and its goals are to enhance an IRS-wide authentication internal-control framework to address risk, deter fraudulent access, and institutionalize a common set of principles for authenticating taxpayers when contacting the IRS. As the IRS moves forward with this strategy, it should consider controls to prevent fraudulent tax returns from being filed. Providing protection only after the taxpayer has been victimized is a dereliction of its obligation and is not serving the American taxpayer well.

In January 2011, the IRS began working on its latest effort to address the challenges involving identity theft. The Identity Theft Assessment and Action Group was formed in June 2011 to analyze current identity theft operations, identify key pain points and quick actions to improve them, determine a future structure for improving taxpayer service and case resolution, and recommend a plan to achieve these goals. The IRS plans to issue two reports – one on its assessment of the current state of the Identity Theft Program and one on the future state of the program.

Detection and Prevention of Identity Theft During Tax Return Processing

A substantial number of unscrupulous taxpayers submit tax returns with false income documents to the IRS for the sole purpose of receiving a fraudulent tax refund from the Federal Government. For Processing Year 2011[8] (through September 10, 2011), the IRS reported that it had identified over 1.6 million tax returns with more than $12 billion claimed in fraudulent tax refunds and it prevented the issuance of more than $11.5 billion (94 percent) of the refunds.[9]

The fraudulent tax returns are identified through the IRS's Electronic Fraud Detection System as well as through the manual screening of paper tax returns. Individual tax returns are sent through the IRS's Electronic Fraud Detection System and are scored based on the characteristics of the tax return and other data. The higher the score, the greater the probability that the tax return is fraudulent. For those tax returns meeting a certain score, the tax return is sent to an IRS employee to screen for fraud potential. If a tax return is selected for further verification, a hold is placed on the tax account for two weeks to prevent the issuance of any tax refund. This delay is to provide IRS tax examiners time to evaluate the tax return for fraud potential, including contacting employers or third parties to verify wage information on the tax return.

[8] A Processing Year is the year that the tax return is processed.
[9] There has been a substantial increase in the number of these fraudulent claims identified. In Processing Year 2008, the IRS identified 381,000 tax returns with $2 billion claimed in fraudulent tax refunds and it prevented the issuance of $1.7 billion of the refunds.

In addition, the tax returns identified included individuals who used another person's identity (name and SSN) to file a fraudulent tax return in an attempt to steal a tax refund. The IRS reported that of the 1.6 million tax returns identified as fraudulent for Processing Year 2011, a total of 851,602 of these tax returns, with $5.8 billion in associated fraudulent tax refunds, involved identity theft. These fraudulent tax returns are part of an extensive tax refund scheme that typically involves the submission of paper tax returns using SSNs from individuals who are unlikely to have to file a tax return. The IRS attempts to identify these tax returns through manual screening when tax returns are received and before the tax return is processed. Our preliminary analysis indicates that this fraud scheme has since expanded to include tax returns submitted through electronic filing.

Overall, the IRS does not know how many identity thieves are filing fraudulent tax returns and how much revenue is being lost. However, there are actions that the IRS can take to improve its identification of fraudulent tax returns. In September 2010, we reported that expanded and expedited access to wage and withholding information would significantly increase the IRS's ability to more efficiently and effectively verify wage and withholding information reported on a tax return at the time the return is processed.[10] The Social Security Act[11] limits the IRS's access to the Department of Health and Human Services national repository of wage and employment information. The data contain quarterly wage information submitted by Federal agencies and State workforce agencies. The law limits the IRS's use of the data solely for purposes of administering the Earned Income Tax Credit, and "verifying a claim with respect to employment in a tax return."[12]

In addition, the IRS has not developed processes to expedite the use of wage and withholding data received from the Social Security Administration. We recommended that the IRS develop a process to expedite the availability of wage and withholding information for use in identifying potentially fraudulent tax returns. IRS management agreed with this recommendation, noting that they continue to take strategic steps to accelerate access to information return data with the goal of refund verification at the time of tax return filing and upfront issue detection. The IRS initiated a pilot project to accelerate its access to Social Security Administration wage data. The IRS is working with the Social Security Administration to analyze the costs and benefits of accelerated transfer, perfection, and integration of Social Security Administration data into IRS systems.

[10] TIGTA, Ref. No. 2010-40-129, *Expanded Access to Wage and Withholding Information Can Improve Identification of Fraudulent Tax Returns* (September 2010).
[11] 42 U.S.C. § 653(i)(3).
[12] *Id.*

We are currently evaluating the effectiveness of the IRS's efforts to identify and prevent fraudulent tax returns resulting from identity theft.[13] However, at this point, we are in the early stages of our audit of this area. As part of our assessment, we will identify and quantify potential tax refund losses resulting from identity theft. This will involve researching the characteristics of both the stolen identities used and tax returns filed that were confirmed to be fraudulent. We will apply these characteristics to the population of tax returns filed to identify other potential fraudulent tax returns involving identity theft that were not identified by the IRS and to quantify the associated potential tax refund losses.

We are evaluating tax filing authentication processes and the ability of the IRS to prevent identity thieves from filing fraudulent tax returns. Currently, taxpayers who want to file electronically must select a PIN in order to electronically submit their tax return. In an attempt to authenticate an individual's identity, the IRS requires Personally Identifiable Information to be provided, which can include name, SSN, date of birth, and prior year Adjusted Gross Income, to obtain the PIN necessary to sign their electronic tax return.

In addition, we are assessing the IRS's process to ensure the refund is being deposited in an account that belongs to the taxpayer. In 2008, we reported that the IRS had not developed processes to ensure that more than 61 million Filing Season 2008 tax refunds were deposited to an account in the name of the filer, as required by Federal direct-deposit regulations.[14] Analysis of IRS direct deposit data identified bank accounts receiving multiple (three or more) tax refunds. For Calendar Year 2007, more than 700,000 bank accounts received three or more tax refunds totaling approximately $8.14 billion. Direct deposit, which now includes debit cards, is frequently the payment method used by individuals who attempt to commit filing fraud. Direct deposit provides the ability to receive quickly fraudulent tax refunds without the difficulty of having to negotiate a tax refund paper check.

To improve IRS conformance with direct-deposit regulations and to help minimize fraud, we recommended that the IRS: (1) coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that direct deposit payments are made only to a deposit account held in the name of the recipient; and (2) take action to limit the number of tax refunds being sent to the same account. While such a limit would not ensure that all direct deposits are in the name of the filer, it would help limit deposits going to a single account, which could help reduce fraud. The IRS responded that the Federal direct deposit regulations do not specify that the IRS is responsible for ensuring compliance with these regulations. IRS officials believe that coordinating a

[13] TIGTA, Audit No. 201140044, *Efforts to Identify and Prevent Fraudulent Tax Returns Resulting From Identity Theft* (planned report issuance in May 2012).
[14] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (September 2008).

recommendation of this type is beyond their jurisdiction. The IRS was also 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.

We are also evaluating the effectiveness of identity-theft indicators in identifying potentially fraudulent tax returns for review. In January 2008, the IRS began placing identity theft indicators on taxpayer accounts, which they determined had current or potential identity-theft issues. For these accounts, any incoming tax returns using the taxpayers' SSNs are to be systemically screened using a series of filters in an attempt to distinguish legitimate tax returns from fraudulent returns. If the tax return is deemed to be potentially fraudulent, processing of the tax return is halted and sent to a tax examiner for review. Furthermore, we are assessing whether tax returns with a valid Identity Protection PIN are processed correctly.

Title 26 United States Code Section 6103

TIGTA's Office of Investigations has the unique responsibility to conduct investigations that protect the IRS's ability to collect tax revenue. These investigations involve violations of Federal criminal statutes and/or standards of ethical conduct. Regarding the coordination of investigating and prosecuting crimes such as identity theft, the ability for the IRS and TIGTA to disclose tax return and/or return information to other Federal, State, or local law enforcement agencies for use in their investigations is controlled by the provisions of Title 26 United States Code (U.S.C.) Section (§) 6103. More specifically, § 6103 restricts access to, and disclosure of, tax information by providing that returns and return information are confidential and are not subject to disclosure except in limited situations as expressly authorized by the Internal Revenue Code.

Section 6103 protects the following information: (1) returns (*i.e.*, tax or information returns as well as attachments, schedules, or supplements) filed with the Secretary of the Treasury (Secretary) and (2) return information. Return information is defined broadly by § 6103(b)(2) but generally includes any information collected by the Secretary with respect to determining liability under Title 26. For example, return information includes a taxpayer's identity, taxpayer identifying number (*e.g.*, SSN or Employer Identification Number), nature, source or amount of income, payments, deductions, and an investigation into an alleged violation of a Title 26 criminal offense (*e.g.*, filing a fraudulent tax return or false statement under penalty of perjury).

Section 6103 contains a number of provisions that authorize the IRS, on behalf of the Secretary, to disclose returns and return information to a State agency or to a local law enforcement agency. For example, § 6103(i) authorizes, in situations involving imminent danger of death or physical injury, disclosure of returns and return information to a State law enforcement agency. In addition, § 6103(d) authorizes disclosure of returns and return information to a State tax

official or State or local law enforcement agencies for the purpose of enforcing State tax laws. Further, § 6103 authorizes disclosure of return information to State or local child support enforcement agencies to facilitate collection or enforcement of child support obligations upon written request of the agency. Lastly, § 6103(c) contains a consent provision that enables individuals or entities to consent to the disclosure of their return or return information. In addition to the previous examples, several other § 6103 provisions authorize disclosure to a State or local law enforcement agency (*e.g.*, information relating to terrorist activity, alcohol fuel producers, and/or investigative disclosures).

To the extent that the IRS determines that an individual has filed a Federal tax return utilizing the SSN of another individual (*i.e.*, possible tax fraud identity theft), § 6103 protects the confidentiality of the potentially false or fraudulent tax return. The IRS is authorized to release such tax return only as authorized by § 6103. Without the consent of the "taxpayer" (*i.e.*, the individual who filed the potentially false or fraudulent tax return), the IRS is prohibited by § 6103 from disclosing the return for purposes of enabling a State or local investigation and/or prosecution of a State criminal statute involving identity theft.

The IRS's Criminal Investigation Division is responsible for investigating allegations of violation of Federal substantive tax-related statutes, including the filing of a fraudulent tax return (26 U.S.C. § 7207) and fraud and false statements under penalty of perjury (26 U.S.C. § 7206). To the extent that the IRS investigates the alleged crime described above, its investigation of the potential violation of a Title 26 criminal offense is "return information" as that term is defined in § 6103(b)(2) and is subject to the same confidentiality provisions referenced above (*i.e.*, without the consent of the subject of the investigation, the IRS cannot disclose the investigation to a State or local law enforcement agency for investigation and/or prosecution of a State law prohibiting identity theft).

TIGTA Provides Investigative Oversight of Taxpayer Information

Under the Internal Revenue Service Restructuring and Reform Act of 1998,[15] TIGTA was created and charged with protecting Federal tax administration. TIGTA carries out this legal mandate by focusing on three core components that expose the IRS to risk: IRS employee integrity; IRS employee and infrastructure security; and external attempts to corrupt tax administration. TIGTA's responsibility is substantially broader than that of most other Offices of Inspector General. While all Offices of Inspector General combat fraud, waste, and abuse, TIGTA is also charged with protecting the integrity of Federal tax administration. A component of protecting Federal tax administration is the investigation of criminal activity as it relates to identity theft and fraud within the tax system. TIGTA's jurisdiction in this area includes the investigation of identity

[15] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

theft that is committed by an IRS employee, an individual impersonating the IRS (primarily phishing and spam e-mail schemes), and tax preparers who steal a client's tax information and disclose it to others or use it themselves for the purpose of committing the identity theft.

Over the past three years, TIGTA pursued 102 investigations of possible or potential identity theft. I will now provide examples of each of the categories that TIGTA investigates to combat identity theft.

Employee Integrity

In order to perform their duties, IRS employees have access to taxpayer information. Identity theft initiated by IRS employees most often occurs as a result of an IRS employee who steals taxpayer information from IRS records. TIGTA investigates the unauthorized access or disclosure of tax information by IRS employees. An example was when an IRS employee accessed the accounts of multiple taxpayers for the purpose of appropriating dependent information which he then sold to others who used such confidential tax information to obtain fraudulent tax refunds.[16]

Another example of IRS employee misconduct as it relates to identity theft is an IRS employee who, while employed as a data entry clerk, stole information of other taxpayers, listed on various IRS forms, including Form 1099-B.[17] This particular form lists a taxpayer's income received and withholdings withheld from interest and dividend earnings. The employee then falsified and forged Forms 1099-B to reflect her own personal information. Using the falsified and forged 1099s as support, the employee then filed her own personal tax return claiming the fraudulent information provided on the forged 1099, specifically, the excessive withholdings to obtain a larger tax refund. The employee filed false tax returns for taxable years 2006, 2007 and 2008, and was able to obtain refunds from the IRS in the amount of $175,143.99. In addition, the employee illegally acquired 68 tax returns of taxpayers, which had been received by the IRS but had not yet been entered into the IRS's computer system. The employee then electronically filed fraudulent tax returns for her benefit using the means of identification of some of these taxpayers. Again, in order to increase the amount of refunds the employee could receive, she filed fraudulent tax returns claiming excessive withholdings from dividends and interest income.[18]

Phishing

The increase in electronic tax return filing and the migration of Federal tax administration operations into an electronic environment brings an increase to both internal and external vulnerabilities that can be exploited by criminals. An

[16] N.D. Ga. Indict. filed Feb. 22, 2005.
[17] E.D. Cal. Indict. filed Apr. 14, 2011.
[18] *Id.*

example deals with an individual who participated with others to defraud the IRS and taxpayers by fraudulently obtaining income tax returns before they were filed electronically with the IRS.[19] Without the permission of the taxpayers, this individual and the co-conspirators fraudulently changed the income tax returns in order to redirect the tax refund payments to bank accounts controlled by them. The individual and his co-conspirators engaged in a form of phishing by creating fake websites that misrepresented themselves as accredited and authorized to electronically file Federal tax returns. They advertised these bogus websites on the Internet and electronic mail.[20] The individuals received Federal income tax returns prepared for electronic filing by taxpayers who were misled by the fraudulent websites or electronic mail. In addition, the taxpayers' information was changed so that any refunds issued by the IRS would be sent to bank accounts opened by the individual and his co-conspirators. The investigation into the individual and his co-conspirators had identified 44 phishing websites and a total of 27 different bank accounts, which received diverted tax refunds totaling $647,987.[21] Some of these funds were withdrawn by debit and check cards and by automatic teller machines in the United States and elsewhere.

Tax Preparers

An increasing number of taxpayers are turning to tax preparers for assistance in preparing their tax returns. Tax preparers can potentially engage in several types of identity theft schemes. An example involved a man who offered to prepare tax returns for free as a service to the community.[22] He filed over 66 tax returns for persons living in Miami-Dade County, Florida, many of whom were members of two churches. He was not affiliated with any IRS-sponsored programs. He was not a certified public accountant nor did he have any formal accounting or tax preparation training. The scheme involved preparation of returns by inflating the deductions and credits on these returns without the filer's knowledge. He had the IRS send the refund money to bank accounts he controlled. In some instances, the tax filers received an amount that they were expecting, while the tax preparer kept the difference. However, in other circumstances, he kept the entire refund money. In total, the tax filings sought tax refunds over $272,000, in fraudulent tax refunds while depositing $206,000 of this amount into accounts he controlled.[23]

Conclusion

Tax fraud perpetrated by identity theft is a growing concern, despite the IRS's efforts to address this serious problem. For Calendar Year 2011, the IRS estimates the number of taxpayers impacted by identity theft – just through the

[19] S.D. Cal. Indict. filed Apr. 16, 2009.
[20] *Id.*
[21] *Id.*
[22] S.D. Fla. Plea Agr. Filed Feb. 27, 2009.
[23] I*d.*

August timeframe – is more than twice the annual estimate for Calendar Year 2008. Whenever identity theft permits criminals to commit tax fraud, law-abiding taxpayers are too often harmed, both financially and personally. Further, the essential trust and reliability of the Nation's tax administration system is eroded.

It is critical for the IRS to deter and detect identity theft before it occurs within the tax return process. Further, the IRS needs a better process to identify and respond whenever tax fraud occurs as a result of identity theft. While the IRS has undertaken important steps and initiatives to prevent the occurrence of identity theft and associated tax fraud, additional controls could help to minimize or prevent future incidences. TIGTA continues to address this escalating problem through audits and investigations that assist the IRS in its efforts to strengthen critical programs, processes, and controls needed to protect sensitive taxpayer data. Moreover, we believe that the escalating rate of identity theft across the Nation warrants additional safeguards and response capabilities that will enable the IRS to avoid unacceptable future losses due to the consequences of tax fraud perpetrated through identity theft.

Thank you, Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, for the opportunity to address this important topic and to share TIGTA's view of specific efforts by the IRS to combat tax fraud perpetrated by identity theft.