

**HEARING BEFORE THE
U.S. SENATE
COMMITTEE ON FINANCE**



April 10, 2008

Washington, DC

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

**STATEMENT OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
U.S. SENATE
COMMITTEE ON FINANCE**

April 10, 2008

Chairman Baucus, Ranking Member Grassley, and Members of the Committee, thank you for the opportunity to testify on the growing problem of the threat identity theft poses to the administration of our nation's tax system. My comments will focus on the Internal Revenue Service's (IRS) efforts to protect the personally identifiable information of millions of taxpayers, the IRS's efforts to assist taxpayers who have been victimized by identity theft, and its ability to identify fraudulent returns. My closing comments will briefly address the status of the 2008 Filing Season.

In the context of this testimony, as is generally agreed, identity theft occurs when someone steals and uses someone else's personally identifiable information (PII) – his or her name, Social Security Number, credit card numbers, or other forms of financial information.

There are two primary types of identity theft related to tax administration: The first involves an individual who steals another person's name and Social Security Number to file a fraudulent tax return in order to steal a tax refund. The second type – employment identity theft – involves an individual who uses someone else's identity to obtain employment which results in taxable income reported to the wrong taxpayer. The Federal Trade Commission (FTC), the primary Federal agency responsible for receiving identity theft complaints, reported that in 2007, more than 56,000 people complained that they had been victimized by one of these two types of identity theft.¹

The IRS's identity theft program has primarily focused on public outreach and education. At the same time, however, its processes and procedures have been inadequate in reducing the burden for taxpayers who have been victimized.

When the IRS becomes aware of employment-related identity theft, it does not take action unless the case directly relates to a substantive tax or conspiracy violation. The IRS cannot notify employers when it has information which indicates that an employee may be using another person's identity to obtain employment. Internal Revenue Code confidentiality and disclosure provisions restrict the IRS's ability to share employee information with his or her employer. However, there are exceptions in the Internal Revenue Code that allow disclosure of tax information to other Federal agencies

¹ *Consumer Fraud and Identity Theft Complaint Data, January – December 2007*, FTC, dated February 2008; FTC's public Internet Web site, FTC.gov and Consumer.gov/sentinel.

with jurisdiction over certain non-tax criminal matters. The Treasury Inspector General for Tax Administration (TIGTA) believes the IRS should use these exceptions to the fullest extent possible in combating identity theft related to tax administration and work with the Office of the Assistant Secretary of the Treasury for Tax Policy to seek additional exceptions or clarify policy as needed.

Other systemic problems also hamper the IRS's ability to ensure the security of sensitive taxpayer information. For example, the IRS does not collect all transactions and audit trails² on its modernized systems, including the Customer Account Data Engine (CADE). This type of review is needed to determine whether IRS employees are illegally browsing through taxpayer files. While it may be understandable that legacy systems could not log these transactions due to older computer technology, there is no excuse for modernized systems not to have this capability.

Essentially, the IRS has failed to address these requirements during development of its modernized systems. As a result, it is deploying several new systems that lack detection capabilities. Without these audit trail logs, the IRS does not know what configuration changes are made or who makes them. Intruders and ill-intended IRS employees who have access to these components could steal taxpayer information with little chance of detection.

In addition, the IRS's Questionable Refund Program (QRP), which identifies and prevents fraudulent refund claims from being paid, has faced its own challenges. In May 2007, TIGTA reported that the IRS did not respond to various warning signs – including five previous TIGTA audit reports--that the QRP had problems and was becoming unmanageable.³ In 2006, the IRS had quickly responded to a National Taxpayer Advocate's recommendation that certain changes be made to the QRP to restore a better balance between taxpayer rights and effective tax administration. However, some of those procedural changes may have adversely affected the IRS's ability to prevent potentially fraudulent refunds from being issued, possibly placing millions of dollars at risk. For example, TIGTA found that the use of criminal refund freezes, if implemented correctly and reviewed in a timely manner, could have prevented the issuance of over 20,000 fraudulent refunds totaling \$71.7 million during Processing Year 2005.⁴

Overall, the IRS not only lacks the comprehensive data needed to determine the impact of identity theft on tax administration, it faces enormous challenges in securing the vast amount of personally identifiable taxpayer information that it stores.

² An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

³ *Actions Have Been Taken to Address Deficiencies in the Questionable Refund Program; Many Concerns Remain, With Millions of Dollars at Risk* (Reference Number 2007-10-076, dated May 31, 2007).

⁴ A processing year is the year in which tax returns and other tax data are processed by the IRS.

Security and Identity Theft

Each year, millions of taxpayers entrust the IRS with their sensitive financial and personal data that are stored in and processed by IRS computer systems. The risk that this sensitive data could be compromised and computer operations disrupted continues to increase. Both internal factors, such as the increased connectivity of computer systems and greater use of portable laptop computers, and external factors, such as the volatile threat environment related to increased phishing scams and hacker activity, contribute to these risks.

Phishing

Phishing is a deceptive practice by which an unsolicited e-mail directs unsuspecting victims to a fraudulent Web site that requests PII, such as credit card or bank account numbers, or other sensitive financial information. These scams continue to be a serious problem for the IRS.

The online phishing scam epidemic is growing exponentially. In Calendar Year 2007, an average of 2.46 host Web sites surfaced each day. That number has risen to 8.82 per day as of March 31, 2008 – a 359 percent increase over 2007.⁵

The IRS and TIGTA have coordinated efforts to thwart IRS-related phishing scams and minimize their impact on tax administration by leveraging the resources of both agencies. Since November 2005, TIGTA has identified phishing scams originating in 68 different countries. From March 2007 through February 2008, 1,418 phishing Web sites have been taken off the Internet. There has also been a dramatic increase in “Get Your Refund” phishing sites, and TIGTA anticipates that the economic stimulus payments this year will lead to new “Get Your Rebate” sites as well.

Although the volume of IRS-related phishing scams remains high, as of March 31, 2008, TIGTA has identified only seven phishing sites related to electronic tax return filing compared to 39 in all of 2007. These sites are designed to lure taxpayers into believing that they are filing their Federal income tax returns electronically with the IRS when, in fact, they are not. Criminals could be using different techniques this year that have not yet been identified, or they could be waiting until later in the filing season to establish the sites.

Insider attacks by employees and contractors continue to be a concern, because employees are more familiar with the IRS network than outsiders and can potentially do more harm. TIGTA’s penetration tests on the IRS’s internal network have shown that disgruntled employees and contractors could gain unauthorized access to employees’ passwords and sensitive system data due to high-risk vulnerabilities, which are well-known to the hacker community. These vulnerabilities include blank and default passwords that system administrators failed to change when installing databases.

⁵ Based on coordinated data tracking maintained by the TIGTA Strategic Enforcement Division and the IRS Computer Security Incident Response Center.

Personally Identifiable Information

Whether the attacks on security come from outside intruders or insiders, the target in the IRS is PII. TIGTA investigates individuals who attempt to steal PII and conducts proactive security assessments of IRS data systems to identify potential vulnerabilities that could be exploited by intruders. TIGTA also coordinates activities with the IRS Computer Security Incident Response Center (CSIRC) to reduce or eliminate any negative impact on tax administration by providing daily downloads to the CSIRC, informing the IRS of any potentially lost and/or stolen information technology assets.

The IRS stores PII for more than 130 million individual taxpayers who file annual Federal income tax returns. Each tax return includes the filer's name, address, Social Security Number, and other personal information. Approximately 30 percent of the tax returns also include the names and Social Security Numbers of at least one dependent. In addition, the IRS maintains PII on its employees and contractors.

The challenge of protecting this information from unauthorized disclosure is related not only to the volume of the data but also the complexity of ever-changing technology, which includes the IRS's more than 240 computer systems and 1,500 databases. Most of the IRS's approximately 100,000 employees and contractors have access to at least some of this information on a daily basis. Similar to recent news reports of breaches involving the improper browsing of presidential candidates' passport files, the IRS faces the risk of employees improperly accessing personal data contained in IRS computer systems.

To compound the risk that this information could be lost or stolen, some IRS employees regularly take laptop computers containing PII outside their offices to carry out their audit or collection duties and assignments. In March 2007, a TIGTA audit found that IRS employees reported the loss or theft of at least 490 computers and other sensitive data in 387 separate incidents.⁶ Employees reported 296 (76 percent) of the incidents to TIGTA but not to the CSIRC. In addition, employees reported 91 of the incidents to the CSIRC; however, 49 of these were not reported to TIGTA.

The PII of at least 2,359 individuals in 126 of these incidents was lost. A test of 100 laptop computers used by IRS employees found that 44 of the computers contained unencrypted sensitive data, including taxpayer data and employee personnel data. Thus, it is likely that a large number of the lost computers contained similar unencrypted data. Employees did not follow encryption procedures because they were either unaware of security requirements or did so for their own convenience. As required by the Office of Management and Budget, the IRS has taken actions to encrypt data on all laptop computers, and TIGTA plans to determine the effectiveness of these corrective actions.

To address these challenges, security must become part of the fabric of the IRS. That is, all managers and employees must consider security ramifications along with

⁶ *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007).

productivity and quality concerns in their day-to-day activities. For years, however, IRS managers and employees have perceived security to be the responsibility of security professionals in the Modernization and Information Technology Services organization and the former Mission Assurance and Security Services organization. This cultural mindset limits the IRS's ability to strengthen overall security activities and controls within the organization and to provide assurance to the American taxpayers that their tax information is protected. While the IRS continues to remind executives that all managers and employees are responsible for the security of PII, TIGTA audit results reflect that managers and employees are not being held accountable for their lack of attention to their security responsibilities.

Weaknesses in two key areas – access controls and audit logs⁷ – continue to plague the IRS.

Access Controls

In September 2007, TIGTA reported that managers continue to give employees access to systems they do not need to carry out their job responsibilities.⁸ For example, systems administrators must be given total control over computer systems. Due to the sensitive nature of this position, the IRS must have proper controls in place to ensure that: 1) only appropriate employees have administrator rights and privileges; 2) administrator user accounts are reviewed annually for continued business needs; 3) user accounts are protected with strong passwords; and 4) user actions on computer systems are monitored for questionable activities. In the audit, covering five systems in several IRS offices, TIGTA could not find authorization and approval documentation for five percent of system administrator accounts (31 of 607) for the five applications reviewed. Thirteen percent of active user accounts (79 of 607) were not needed because the employees no longer had a business need to administer their respective computer systems. In addition, weak passwords on user accounts existed on all five applications reviewed.

Because the IRS sends sensitive taxpayer and administrative information across its networks, routers on the networks must have sufficient security controls to detect and deter unauthorized use. TIGTA found that access controls for IRS routers were not adequate, and reviews to monitor security configuration changes were not conducted to identify inappropriate use. The IRS uses the terminal control system to administer and configure routers and switches, and users of this system must be authorized by managers. The IRS had authorized 374 accounts for employees and contractors that could be used to access routers and switches to perform system administration duties.

⁷ Access controls limit access to systems and accounts to only authorized users. An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

⁸ *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved* (Reference Number 2007-20-161, dated September 19, 2007).

In March 2008, TIGTA reported that managers had not authorized 38 percent of the accounts (141 of 374) used to administer key network components.⁹ Over 84 percent of the configuration changes were made to the components using accounts shared by administrators so that accountability for the changes could not be established. Essentially, the IRS had no idea who had access to the network components.

Audit Trail Logs¹⁰

Because the IRS logs transactions on so few applications, it has no way to conduct the type of proper intrusion investigations that are needed to hold individuals accountable for unauthorized transactions and disclosures. The IRS has failed in prior attempts to provide a reasonable audit log process and does not expect to have one in place until 2014. This is an unacceptable major control weakness. The IRS cannot determine if, when, or where its sensitive data have been exposed.

Most notably, the IRS is not reviewing transactions on its modernized systems, including the CADE. The IRS could review limited audit trail information on the CADE, but it does not do so on a regular basis. In addition, some of the information and transactions on the CADE are not captured in an audit trail, thus, they cannot be reviewed. While it may be understandable that older legacy systems could not log transactions due to computer equipment available at the time, there is no excuse for modernized systems to not have this capability. Essentially, the IRS has failed to address these requirements during the development stages of its modernized systems. As a result, it is deploying new systems that lack detection capabilities. Any effort to install logging capabilities after deployment will likely cost significantly more than if the security capabilities had been designed into the systems during the system development phase.

TIGTA also raised concerns in the September 2007 report that audit trails were not being reviewed for four of the five applications tested. Although the IRS was capturing every key stroke from administrator user accounts and sending the data offsite for backup purposes for three of the four applications, it was not conducting required regular audit trail reviews. In a more recent audit, audit trail logs were not reviewed to monitor configuration changes. Without audit logs, the IRS did not know what configuration changes were being made or who made the changes. Intruders and malicious employees who had access to these components could steal taxpayer information with little chance of detection.

UNAX

Logging these transactions is vitally important because the Taxpayer Browsing Protection Act¹¹ mandates that the IRS identify and penalize employees who access

⁹ *Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information* (Reference Number 2008-20-071, dated March 26, 2008).

¹⁰ An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

¹¹ Taxpayer Browsing Protection Act, Pub. L. No. 105-35, 111 Stat. 1104.

taxpayer accounts without authorization. The legacy computer system currently used to update taxpayers' accounts does, in fact, maintain an audit log enabling TIGTA to proactively identify IRS employees who commit unauthorized accesses (UNAX) of confidential taxpayer information.

TIGTA operates the UNAX detection program that identifies IRS employees who access taxpayer information without authorization. Whether the intent is fraud or simply curiosity, the potential exists for unauthorized accesses to tax information of high profile individuals and other taxpayers based on the volume of PII the IRS collects and stores. The competing goals of protecting this information and achieving workplace efficiencies become even more difficult as technology becomes faster and more complex.

For example, one recent prosecution involved an IRS employee who inspected the return information of a Certified Public Accountant (CPA) who had been preparing the former employee's tax returns for the past 30 years. The employee also inspected the tax returns and/or tax return information of approximately 56 clients of the CPA, a former employer, friends and relatives, and her friends' relatives. The employee was sentenced to four years of probation, six months of home confinement, and was fined \$10,000.

Another IRS employee pleaded guilty to unauthorized access of a government computer. While an employee of the IRS, this individual accessed an IRS computer database containing taxpayer information and used a computer search function to search for taxpayers with the same first and last name as one of her relatives. The search resulted in a list of dozens of taxpayers with that name and also displayed the corresponding Social Security Number for each name. The employee provided the list to her relative, knowing that he intended to use the information to commit financial fraud through identity theft for private financial gain.

Since Fiscal Year 1998, the annual number of UNAX cases has increased from 430 to 521 in Fiscal Year 2007. Since Fiscal Year 1998, 471 employees have been removed, 452 have been suspended, and 934 have resigned for UNAX violations. In addition, since Fiscal Year 1998, TIGTA investigations have resulted in 185 prosecutions.

Sharing Federal Government Information

The IRS provides vast amounts of sensitive taxpayer data to U.S. Federal and State agencies and to contractors such as those associated with the IRS's Private Debt Collection initiative. TIGTA has evaluated the security of sensitive data at the private collection agencies during two audits. In March 2007, TIGTA reported several security weaknesses in the program but found that in Fiscal Year 2008 the two contractors had taken adequate corrective actions.¹² In particular, files were securely transmitted from the IRS to the contractors and adequately secured on the contractors' systems. Workstations

¹² *The Private Debt Collection Program Was Effectively Developed and Implemented, but Some Follow-up Actions Are Still Necessary* (Reference Number 2007-30-066, dated March 27, 2007); *Private Collection Agencies Adequately Protected Taxpayer Data* (Reference Number 2008-20-278, dated March 26, 2008).

used by contractor collection personnel were adequately controlled to prevent unauthorized copying of taxpayer information to removable media or transferring via e-mail. The contractors also maintained adequate audit trails and performed periodic reviews, including reviews to identify unauthorized access to taxpayer data. In addition, all contractors were subject to background investigations.

Identity Theft and Its Effect on Tax Administration

Recent reports of identity theft from both the private and public sectors have heightened awareness of the need to protect taxpayers' sensitive financial and personal data. There are two primary types of identity theft relating to tax administration:

- The first type involves an individual using another person's identity (name and Social Security Number) to file a fraudulent tax return to steal a tax refund. The individual committing this type of fraud frequently files the fictitious tax return electronically, early in the filing season.

The individual whose identity was stolen later files his or her tax return and the IRS identifies it as a duplicate tax return. When this happens, the IRS freezes the second tax return, including any tax refunds due, and begins a process of corresponding with the individuals involved in the duplicate filing. This requires considerable time and effort by the legitimate taxpayer to prove he or she is a victim of identity theft. The victim's tax refund, if frozen, will not be issued until the matter is resolved.

- The second type involves using another person's identity (name, Social Security Number, or both) to obtain employment. This frequently involves undocumented workers. The wage information is reported to the Social Security Administration by the employer on the Wage and Tax Statement (Form W-2) under the stolen identification information (the victim's name and Social Security Number).

According to the FTC, 22 percent (56,125 of 258,427) of all reported identity theft complaints in Calendar Year 2007 resulted from either the filing of a fraudulent tax return or the misuse of someone's identity to obtain employment. This is up 10 percent from 2006. The FTC reports that the number of fraudulent tax returns filed as a result of identity theft increased 579 percent – from over 3,000 in Calendar Year 2002 to almost 21,000 in 2007.¹³

In July 2005, TIGTA reported that the IRS lacked a corporate strategy to adequately address identity theft issues.¹⁴ In response to some of TIGTA's recommendations, the IRS agreed to develop: (1) updated agency-wide communication tools for educating and assisting taxpayers with information about identity theft; (2) agency-wide standards to ensure that the information taxpayers were asked to provide

¹³ *Consumer Fraud and Identity Theft Complaint Data, January – December 2007*, FTC, dated February 2008; FTC's public Internet Web site, FTC.gov and Consumer.gov/sentinel.

¹⁴ *A Corporate Strategy Is Key to Addressing the Growing Challenge of Identity Theft* (Reference Number 2005-40-106, dated July 22, 2005).

to substantiate identity theft claims is consistent throughout the IRS; (3) specific closing codes for cases involving identity theft that would allow the IRS to track and monitor the effect of identity theft on tax administration; and (4) processes to proactively identify instances of identity theft.

In October 2005, the IRS established the Identity Theft Program Office to provide centralized development of policy and procedural guidance within tax administration and to implement an agency-wide strategy composed of three components: outreach, prevention, and victim assistance. The Office was established in the Wage and Investment Division to facilitate cross-functional coordination. In 2007, the IRS moved the Identity Theft Program Office from the Wage and Investment Division to the Mission Assurance and Security Services (Mission Assurance) organization. According to the December 21, 2006, Memorandum of Understanding between Mission Assurance and the Wage and Investment Division, “...*Identity Theft will be incorporated as part of enterprise information protection and will not be managed as a stand alone program office.*” In July 2007, responsibility for the Identity Theft Program was assigned to the Deputy Commissioner for Operations Support. According to the IRS, “. . . reporting directly to a Deputy Commissioner will provide this program the ability to reach across all IRS organizations to ensure that proper attention and discipline is given . . .” to this important issue.

In March 2008, however, TIGTA reported that the IRS has not placed sufficient emphasis on employment-related and tax fraud identity theft strategies.¹⁵ The IRS currently lacks the comprehensive data needed to determine the impact of identity theft on tax administration. Its prevention strategy does not include pursuing individuals using another person’s identity, unless a given case directly relates to a substantive tax or conspiracy violation. According to IRS policy, the actual crime of identity theft will only be investigated by its Criminal Investigation Division if the crime is committed in conjunction with other criminal offenses having a large tax effect. In Fiscal Years 2005 and 2006, the IRS recommended only 45 and 55 cases, respectively, for prosecution that included charges of identity theft.

Due to the IRS’s lack of information related to identity theft, it is not clear whether the IRS Criminal Investigation Division evaluated or investigated any of these complaints. According to the IRS, the Criminal Investigation Division does not use FTC Identity Theft Clearinghouse data.¹⁶

In addition, actions taken in response to employment-related identity theft are not adequate to stop the unlawful use of the identity. Although the Social Security Administration notifies employers of mismatches between names and Social Security Numbers, the IRS does not notify them when their employees are using someone else’s

¹⁵ *Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft* (Reference Number 2008-40-086, dated March 25, 2008).

¹⁶ The Identity Theft Clearinghouse is the sole national repository of consumer complaints about identity theft. The database is maintained on the FTC Consumer Sentinel Network, a secure, encrypted Web site for use by law enforcement agencies.

identity. Social Security Number/name mismatches are indeed a significant problem for the IRS and the Social Security Administration; however, a more serious problem develops for the lawful taxpayers when both their names and Social Security Numbers are used by others to gain employment. Because the IRS and the Social Security Administration assume that the information on the *Employee's Withholding Certificate* (Form W-2) is accurate, the earnings resulting from the identity theft will be attributed to the lawful taxpayers for determining both Social Security benefits and tax liabilities.

IRS officials explained that the Internal Revenue Code confidentiality and disclosure provisions prevent the agency from taking actions to stop continued use of another person's identity for employment, and that it is broadly restricted from sharing taxpayer information with third parties. The IRS also does not pursue the taxes that might be due on income earned using a stolen identity because it does not have sufficient enforcement resources to address most of the identity theft cases.

Additionally, the IRS does not believe that it is worthwhile to pursue employment-related identity theft cases for unreported tax liabilities because the taxes owed on most of these cases are not significant. TIGTA is concerned that if the IRS takes no additional action to address the misreporting of income resulting from identity theft, there is no deterrent to keep the problem from spreading.

Use of another person's identity for employment results in the misreporting of income which affects income tax and Social Security tax as well as other employment taxes. Agencies with jurisdiction over these matters include the IRS and the Social Security Administration. Consequently, coordination between these agencies is important to ensure that Federal records related to income earned by a taxpayer are correct and to ensure appropriate law enforcement. Federal law¹⁷ allows the Social Security Administration to pursue criminal penalties for an individual who fraudulently obtains, uses, or represents a Social Security Number to be theirs. There are exceptions in the Internal Revenue Code that allow disclosure of tax information to other Federal agencies with jurisdiction over certain non-tax criminal matters. If the IRS believes these exceptions are not adequate for the purposes of combating identity theft, IRS management should seek legislative remedy through the Office of the Assistant Secretary of the Treasury for Tax Policy. The IRS provided a copy of TIGTA's report to the Office of the Assistant Secretary of the Treasury for Tax Policy to evaluate whether a legislative remedy should be sought for this issue.

The IRS has primarily focused on identity theft through public outreach and education. This included revising widely used documents to include information on identity theft, creating and maintaining the Identity Theft Web page on IRS.gov, and giving numerous identity theft presentations to the tax preparer community. Nonetheless, its current processes and procedures have been inadequate in reducing the burden for taxpayers who are victimized by identity theft. For example:

¹⁷ 42 U.S.C. § 408 provides for criminal penalties for an individual who fraudulently buys, sells, or possesses a Social Security card with intent to sell or alter or who discloses, uses, or compels the disclosure of the Social Security Number of any person in violation of the laws of the United States.

