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 trails[2] 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 logs[7] – 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 (31of 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 (141of 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 Logs[10]

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 Act[11] 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 law[17] 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.

- The Automated Underreporter function contacted taxpayers multiple times for the same compliance issues even though these taxpayers' cases were previously marked as closed for identity theft. The Automated Underreporter function is a compliance function using third-party information returns to identify income and deductions that were not reported on tax returns.[18]
- The Withholding Compliance function unnecessarily contacted taxpayers for withholding issues because the function does not consider the Identity Theft Closing codes used by the Automated Underreporter function's computer system. The Withholding Compliance function ensures that taxpayers who have serious under-withholding problems are brought into compliance with Federal income tax withholding requirements. The function uses Form W-2 information to identify taxpayers with insufficient withholding and attempts to correct withholding to ensure that taxpayers have enough income tax withheld to meet their tax obligations.

In January 2008, the IRS implemented the universal identity theft indicator. The effective use of this universal identity theft indicator should reduce the number of multiple contacts made with taxpayers who have been victims of identity theft. Once a taxpayer has been coded as an identity theft victim, he or she should no longer be selected and contacted by the various IRS functions for compliance issues that resulted from the identity theft.

The IRS advised TIGTA that it is implementing a five-year strategy for its Privacy, Information Protection, and Data Security Office that will include identity theft issues. However, it did not state when this strategy will be implemented, what milestones will be established, and how its success will be measured.

The IRS has also indicated that it is collaborating with the FTC on outreach activities. It is also using extracts of general information from the Identity Theft Clearinghouse to track trends and develop process improvements and outreach initiatives for victim assistance. Yet, the IRS has concluded that the FTC data are not useful in evaluating or investigating tax fraud or employment-related identity theft, even though the Identity Theft Clearinghouse is the sole national repository of consumer identity theft complaints and should be an important source of data for the Criminal Investigation Division.

Identity Theft and the Questionable Refund Program

The QRP, which was established to identify and prevent the issuance of fraudulent refunds, received harsh criticism from the National Taxpayer Advocate as a program that was inefficient, ineffective, and did not afford taxpayers their rights. In 2006, the IRS re-evaluated its processes and procedures to address the Taxpayer

[18] The annual underreporter process begins when the IRS creates an inventory list of potential underreporter cases by matching taxpayer return data against the data in the third-party information return database, identifying taxpayers with discrepancies. The first match occurs between July and September of each year; a second match, picking up additional filers, occurs during January and February of each year.

Advocate's concerns. Yet, TIGTA believed that several of these changes might adversely affect the IRS's ability to prevent the issuance of millions of dollars in potentially fraudulent refunds.

The Growing Problem of Identity Theft and Tax Return Fraud

Of the 44,788 tax refunds verified as fraudulent by the IRS's QRP through September of Processing Year 2006, the Criminal Investigation Division indicated that approximately 18 percent involved identity theft.[19] However, the QRP processing changes made in 2006 could have resulted in a burden on the victims of identity theft, lost revenue, and additional IRS resources to resolve these accounts.

The IRS's policy prior to Processing Year 2006 was to freeze both the current and future years' tax accounts when the QRP found fraud. This automatically prevented the issuance of any refunds to these taxpayers for their current and subsequent tax years, including identify theft victims. The 2005 National Taxpayer Advocate's Report highlighted the automatic freezing of future years' refund returns as a significant problem with the QRP because it caused significant and continuing inconvenience to identity theft victims whose refund returns in those future years were legitimate.[20] As a result of the Advocate's report, the IRS decided in 2006 to discontinue freezing the future years' accounts when fraud is found.

TIGTA reported a concern with this revised procedure because the future year freeze was an effective means for protecting revenue, when considered along with other changes that included notifying taxpayers that their refunds had been frozen and minimizing the time that refunds are frozen. These additional changes minimized the burden on taxpayers and allowed the IRS to systemically protect the government's revenue. A sample of fraudulent refund returns filed during Processing Year 2004 identified that 42 percent of those accounts had a repeat incident of refund fraud the following year.

In a March 2008 congressional statement, the National Taxpayer Advocate described that in a typical identity theft refund fraud situation, the perpetrator submits a fraudulent tax return early in the filing season using the personal information of an innocent taxpayer before the actual owner of the Social Security Number has an opportunity to file a legitimate tax return. Because the IRS does not know that this is a return involving identity theft, any refund due is issued to the perpetrator. When the identity theft victim later attempts to file his or her tax return, the IRS flags it as a duplicate return and prevents any refund claimed on the true return from being issued.[21]

---

[19] *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).
[20] *National Taxpayer Advocate's 2005 Annual Report to Congress* (Publication 2104, Rev. 12-2005).
[21] Written Statement of Nina E. Olson, National Taxpayer Advocate, before the Subcommittee on Oversight Committee on Ways and Means, U.S. House of Representatives Hearing on: The 2008 Tax Return Filing Season, IRS Operations, FY 2009 Budget Proposals, and The National Taxpayer Advocate's 2007 Annual Report to Congress (March 13, 2008).

When this occurs, the identity theft victim will likely contact the IRS to ask what happened to his or her refund.

This contact would have also likely occurred if the IRS had frozen the subsequent year account of a prior identity theft victim. The identity theft victim would contact the IRS asking about his or her refund that had been frozen. However, the advantage of having the refund already frozen is that it allows the IRS to identify these cases upfront. It can then be proactive through a timely determination of whether the taxpayer is again the victim of identity theft – or if the refund is valid – and notifying the victim of a delay in receiving his or her refund.

With the high risk of repeat problems for innocent taxpayers, a future year automatic freeze on at least one subsequent tax return might help reduce the adverse effects of identity theft by allowing the IRS a brief window of time to prevent a fraudulent tax return from being processed. If the Criminal Investigation Division properly identifies identity theft freezes, notifies the taxpayers of the freezes, and resolves the freezes in a timely manner, the IRS will be providing a valuable service to innocent taxpayers, while also protecting Federal revenue and minimizing taxpayer burden if the return does not involve a repeat occurrence of identity theft.

The Role of the Questionable Refund Program in Identifying and Preventing Fraud

The IRS relies on the QRP to identify and prevent fraudulent refund claims from being paid. Over the past several years, TIGTA has reported that the QRP was becoming increasingly unmanageable due to the growing number of fraudulent claims and the IRS's lack of resources to combat the fraud.[22] In addition, the QRP was severely curtailed when the IRS and its information technology contractors failed to launch a Web-based version of its primary information system, the Electronic Fraud Detection System, during Processing Year 2006. Unfortunately, this resulted in dramatic decreases in the amount of refund fraud the IRS identified and stopped that year. For Processing Years 2007 and 2008, the IRS reverted to a legacy version of the Electronic Fraud Detection System.

In May 2007, TIGTA reported that the IRS did not respond to various warning signs, including five previous audit reports, that the QRP was facing problems and becoming unmanageable.[23] Nevertheless, the IRS quickly responded to the National Taxpayer Advocate's Report and made changes to the QRP in Processing Year 2006 that were intended to address the Advocate's concerns and reduce the burden on taxpayers. While TIGTA is encouraged by the IRS's actions to address stakeholder concerns and restore balance between taxpayer rights and effective administration of the tax laws, some procedural changes may have adversely affected the IRS's ability to prevent potentially fraudulent refunds from being issued in the future, possibly placing millions of dollars at risk. For example, TIGTA found that the use of criminal refund freezes, if

[22] *The Internal Revenue Service Needs to Do More to Stop the Millions of Dollars in Fraudulent Refunds Paid to Prisoners* (Reference Number 2005-10-164, dated September 28, 2005).
[23] *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).

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.

Additionally, the IRS needed to be more aggressive in adjusting accounts with frozen refunds to either recover fraudulent refunds that were issued or to prevent repeat fraud. TIGTA estimated that had the IRS taken action on earlier fraudulent returns, it could have prevented $27.5 million of future potentially fraudulent refunds.

Identifying prisoner refund fraud continues to be a problem. In the 2007 report, TIGTA found that only 4,235 prisoner returns claiming approximately $19 million in refunds were identified as fraudulent in Processing Year 2006 and only $11.5 million in refunds were stopped. In contrast, during Processing Year 2004, 18,159 prisoner returns claiming $68.2 million in fraudulent refunds were identified and 14,033 refunds totaling $53.5 million were stopped. This indicates the potential magnitude of the IRS's lost ability to detect and stop fraudulent prisoner refunds during Processing Year 2006 when the Electronic Fraud Detection System was not available.

Understandably, the IRS made processing decisions in the context of balancing available resources with workload, but concerns remain that those decisions could have a negative impact on effective tax administration. Continuing to freeze the subsequent year's return, when properly controlled, is an efficient and effective means of identifying repeat fraud, protecting revenue, and protecting innocent taxpayers who are victims of identity theft. The IRS has continued to advise us that it does not have sufficient resources to effectively and promptly deal with a rapidly growing fraudulent refund problem. Recognizing the challenge of limited resources, TIGTA recommended that the Criminal Investigation Division take a leading role in pursuing legislation that would change current legal procedures that would allow the IRS to reverse fraudulent tax return information. This would streamline account resolutions while still protecting taxpayer rights.

TIGTA has an ongoing audit focused on the QRP to evaluate the impact of the failure of the Electronic Fraud Detection System on the IRS's ability to identify and stop questionable refunds during Processing Year 2006 (for example, the amount of fraudulent refunds that were issued) and to determine the effectiveness of the IRS's QRP processes during Processing Year 2007. Among other issues, the current audit will also estimate the impact that the higher dollar threshold had on stopping fraudulent refunds during Processing Year 2007. The IRS advised TIGTA that the need to implement thresholds to exclude tax returns occurred because of limited IRS resources available to process fraudulent tax returns identified through the QRP.

The IRS was more successful in stopping fraudulent refund claims during Processing Year 2007 than in past years. According to the IRS Criminal Investigation Division, over $1.2 billion in fraudulent tax refunds were stopped during Processing Year 2007. This amount represents a 152 percent increase over Processing Year 2005. Also, according to Division data, the QRP became more effective in stopping fraudulent refund

claims because only those returns with the highest potential for fraud were verified. TIGTA will continue to monitor this very important area as the IRS seeks additional solutions to combat the rapidly growing problem of fraudulent tax refunds.

2008 Filing Season

The 2008 Filing Season appears to be progressing without major problems. As of March 29, 2008, the IRS reported it had received approximately 86.8 million tax returns. Of those, approximately 62.2 million were filed electronically (e-filed) (an increase of 9.3 percent from this time in 2007), and approximately 24.6 million were filed on paper (an increase of 4.8 percent from this time in 2007). Additionally, nearly 69.8 million refunds totaling approximately $172 billion had been issued. Of these, 50.8 million (73 percent of all refunds) were directly deposited to taxpayer bank accounts, an increase of 7.3 percent compared to 2007.

Use of the IRS's free online filing program had been declining in prior years. However, based on the current volume, it appears that taxpayers are increasingly taking advantage of this option; the number has increased by 17.4 percent from 2007. Additionally, the number of taxpayers who e-file from their home computers has increased by 17.3 percent this filing season.

Due to late passage of the Tax Increase Prevention Act of 2007,[24] which provides relief to taxpayers who would have been subject to the Alternative Minimum Tax, five tax forms that were affected by the legislation could not be processed until February 11, 2008. The February 11 date allowed the IRS enough time to update and test its systems without major disruptions to other return processing operations. The week ending February 15, 2008, was the first week for processing returns with the five affected forms. As a result, receipts increased by 20.9 percent over the same week last year. TIGTA is evaluating the effect on taxpayers of the delay in processing the five tax forms related to the Alternative Minimum Tax legislation.

The latest release of the CADE, Release 3.0, was originally developed to deliver 17 new functions and capabilities. The IRS divided Release 3.0 into two sub-releases. CADE Release 3.1 contained four major functions and was deployed between August and October 2007. CADE Release 3.2 included seven major functions and was delivered in February 2008. The major functions delivered include the capability of processing tax returns with a disaster area designator; processing tax returns claiming the Earned Income Tax Credit, Credit for Child and Dependent Care, and requests for Split Refunds; providing address change service requests; and validating tax balances. The remaining six functions will be determined for delivery in future releases of the CADE. These additional capabilities were expected to significantly increase the volume of returns posting to the CADE from the approximately 11.2 million returns posted during Calendar Year 2007. As of March 28, 2008, about 21.1 million tax returns had been posted to the CADE.[25]

[24] Tax Increase Prevention Act of 2007, Pub. L. No. 110-166 Stat 2461 (2007).
[25] TIGTA has not evaluated the accuracy of the postings.

Economic Stimulus Act of 2008[26]

In keeping with the intent of the Economic Stimulus Act of 2008, the IRS expects to issue over $100 billion in stimulus payments (often referred to as rebates) and is trying to ensure that everyone who is entitled to the rebates knows what to do to receive it. The IRS sent Economic Stimulus Payment Notices (Notice 1377) to more than 130 million taxpayers who filed a Tax Year 2006 income tax return. These notices were mailed from March 4 to March 21, 2008, and cost an estimated $45 million to print and mail. The notice was informational only and did not require a response from the taxpayer. Beginning in May 2008, an additional notice will be mailed to those taxpayers eligible for the payments to explain the payment amount and how it was calculated. The IRS believes it will receive significantly fewer calls to its toll-free telephone information line as a result of issuing these notices.[27]

The IRS also created a new tax package *Information About Economic Stimulus Payments for Social Security, Veterans, and Other Beneficiaries* (Package 1040A-3) to be mailed to more than 20 million individuals who normally do not have to file tax returns but might qualify for the stimulus payments (for example, those who receive Social Security Administration and Department of Veterans Affairs benefits). The law provides for payments to these individuals if they have a total of $3,000 or more in qualifying income. Qualifying income is earned income, certain Social Security Administration, Railroad Retirement, and Department of Veterans Affairs benefits, and non-taxable combat pay.

As of March 28, 2008, the IRS had received an estimated 1.4 million tax returns from individuals who filed them solely to receive the rebates. Since these are tax returns that would normally not have to be filed, the normal IRS refund controls are not geared for this situation. The IRS is evaluating alternatives to identify any of these tax returns that are fraudulent so it can prevent any associated fraudulent stimulus payments. TIGTA is currently evaluating the controls over the processing of these tax returns and monitoring their volume and effect on the 2008 Filing Season.

Since the Economic Stimulus Act of 2008 was enacted, the IRS has been averaging more than 63,000 calls per day beyond the normal volume to its toll-free telephone lines related to the upcoming rebates. However, for the one week ending March 29, 2008, the IRS averaged more than 144,000 calls per day to its toll-free telephone lines related to the rebates. At peak, the IRS plans to use 1,067 Automated Collection System[28] telephone assistors to take rebate telephone calls during their regular tours of duty and has also trained more than 500 tax examiners and assistors (who

[26] Economic Stimulus Act of 2008, Pub. L. No. 110-185 (2008).
[27] The IRS estimates one telephone contact with an IRS assistor costs almost $20. Mailing one stimulus payment notice costs approximately 35 cents.
[28] The Automated Collection System is an integral part of the IRS process for collecting unpaid taxes and securing unfiled tax returns from both individual and business taxpayers. When taxpayers do not comply with the IRS's computer-generated notices, Automated Collection System tax examiners attempt to contact them by telephone to secure payments or unfiled returns. The Automated Collection System is the computer system that assigns these cases to the individual tax examiners.

normally work taxpayer correspondence and paper casework) to answer general rebate calls. Additionally, 2,100 Automated Collection System assistors will be offered the opportunity to work weekday overtime on an "as needed" basis. The IRS will also utilize overtime and extend the employment of its seasonal hires.

The IRS stopped the issuance of Automated Collection System enforcement tools (systemic notices and letters were stopped on February 22 and systemic levies on February 29). Issuance of regular delinquency notices on accounts not yet assigned to the Automated Collection System has not been stopped, and the IRS expects to reserve 40 percent to 50 percent of the available Automated Collection System staff to answer calls from taxpayers who respond to these notices. The IRS plans to restart the notices when telephone demand decreases. The IRS reports that the foregone revenue associated with these actions could be as high as $666 million.

TIGTA is reviewing the IRS's planning and preparation for issuing the stimulus payments. TIGTA will continue to closely monitor the issuance of the payments and their effect on customer service and enforcement activities. Future reviews are planned on the accuracy of the payments, costs of distribution, and effects the payments might have, if any, on Tax Year 2008 tax returns and the 2009 Filing Season.

Providing Quality Customer Service

Providing quality customer service to the American taxpayer will always be a challenge for the IRS. Nevertheless, it has made consistent progress. In April 2007, the IRS issued the Taxpayer Assistance Blueprint Phase 2 report, which presents the IRS's guiding principles and Strategic Plan for taxpayer services. The Strategic Plan includes performance measures, service improvement portfolios, and an implementation strategy.

IRS.gov

IRS.gov continues to be one of the most visited Web sites in the world, especially during filing seasons. As of March 22, 2008, the IRS reported more than 111 million visits to IRS.gov, a 16.7 percent increase over last year. Almost 25 million taxpayers went to IRS.gov to obtain their refund information via the "Where's My Refund?" option, a 20.2 percent increase over last year.

Taxpayer Assistance Centers

Taxpayer Assistance Centers are walk-in sites where taxpayers can receive answers to account and tax law questions, as well as assistance in preparing their tax returns. As of March 22, 2008, the Centers had served approximately 1.8 million taxpayers this filing season.

In Fiscal Year 2007, the IRS implemented a standardized quality measurement system to measure the quality of taxpayer service at the Centers. As of March 22, 2008,

the IRS had reported a 59 percent accuracy rate for tax law questions and an 83 percent accuracy rate for tax account questions for this fiscal year.

Toll-Free Operations

The IRS expects increased demand this year for its toll-free telephone assistance lines related to the upcoming stimulus payments. However, all planning for the 2008 Filing Season was completed before the economic stimulus legislation was passed, and calls related to the upcoming rebates have affected service. The IRS had planned to provide an 82 percent Level of Service for Fiscal Year 2008, but has projected the Level of Service could be as low as 74 percent. The Level of Service is the primary measure of service to taxpayers. It is the relative success rate of taxpayers who call for services on the IRS toll-free telephone lines.

For the 2008 Filing Season (as of March 29, 2008), the IRS had already answered about 112 percent of the planned 10.9 million assistor-answered calls. Its 80.0 percent Level of Service is 4.5 points lower than the actual 2007 Filing Season Level of Service of 84.5 percent. Additionally, the IRS had planned to answer 14.8 million automated calls but had answered 16.1 million automated calls.

The IRS expects to receive approximately 1.8 million calls from March through April 2008 related to rebates and additional calls in May through July after the IRS mails detailed notices to taxpayers. To ensure that taxpayers are able to call the toll-free lines, the IRS states that it is maximizing availability of the telephone lines and the assistors. In late January 2008, the IRS began receiving higher volumes of calls from taxpayers inquiring about the stimulus payments. To reduce the demand on assistors, the IRS implemented an automated message on the 1-800-829-1040 and 1-800-829-4933 toll-free telephone lines. On February 19, 2008, the IRS dedicated a separate telephone line (Rebate Hotline) to the automated message on the rebates. From the end of January through March 29, 2008, the IRS has received 2.2 million calls to all automated rebate lines. In addition to the 2.2 million automated calls, IRS assistors have answered 572,000 calls about the stimulus payments.

The IRS has also extended its toll-free telephone service by opening it on March 29, 2008, for Super Saturday. Super Saturday is the day the IRS opened 320 Taxpayer Assistance Centers to help reach Americans who are eligible for the stimulus payments, but who normally are not required to file income tax returns. The IRS opened the toll-free Rebate Hotline on Super Saturday between 9 a.m. and 3 p.m. local time.

Volunteer Program

Each year, more taxpayers choose to have volunteers prepare their tax returns. So far this filing season, almost two million tax returns have been prepared by volunteers, an increase of 17 percent over the 2007 Filing Season. The IRS's Volunteer Program is playing an increasingly important role in the IRS's efforts to improve taxpayer service

and facilitate participation in the tax system. The Program provides no-cost Federal tax return preparation and electronic filing to underserved taxpayer segments, including low-income, elderly, disabled, and limited-English-proficient taxpayers. These taxpayers are frequently involved in complex family situations that increase the difficulty of correctly understanding and applying tax laws.

During this filing season, TIGTA auditors are visiting 36 Volunteer Income Tax Assistance and Tax Counseling for the Elderly sites across the United States. The auditors pose as taxpayers to determine whether taxpayers are receiving quality service, including the accurate preparation of their individual income tax returns. Auditors developed scenarios designed to test quality controls and present volunteers with a wide range of tax law topics that taxpayers may need assistance with when preparing their tax returns. These scenarios include the characteristics (for example, income level, credits claimed) of tax returns typically prepared by Volunteer Program volunteers based on an analysis of the Tax Year 2007 volunteer-prepared tax returns.

As of March 28, 2008, 30 tax returns had been prepared with a 67 percent accuracy rate, which is an increase over the 56 percent accuracy rate TIGTA reported for the 2007 Filing Season. Volunteers are doing a better job of using the tax tools and information available when preparing tax returns.

Paid Preparers

Paid preparers are an important source in assisting taxpayers in filing their tax returns on time, paying their taxes, and receiving refunds. During this filing season, TIGTA conducted an audit to determine whether taxpayers receive accurate preparation of their income tax returns when using commercial chain preparers and unenrolled paid preparers.[29] In Tax Year 2006, paid preparers prepared over 85 million individual Federal income tax returns, which was a 9 percent increase above the nearly 78 million tax returns prepared by paid preparers in Tax Year 2005. Currently, there are no national standards that a preparer is required to satisfy before selling tax preparation services to the public. Anyone – regardless of training, experience, skill, or knowledge – may prepare Federal income tax returns for others for a fee.

Paid preparers who are authorized to represent taxpayers in matters before the IRS are called practitioners. They include attorneys, CPAs, enrolled agents, and actuaries. These practitioners, who can legally represent taxpayers, serve as a conduit to the IRS on account-related matters and are regulated by the IRS Office of Professional Responsibility.

All paid preparers are subject to Internal Revenue Code penalties – both civil and criminal. For example, civil penalties apply if paid preparers do not sign the tax returns they prepare, do not provide the taxpayers with copies of the tax returns, or deliberately understate a taxpayer's tax liability. Criminal penalties apply when a paid preparer

[29] Accuracy of Tax Returns Prepared by Unenrolled Paid Preparers (Audit Number 200840009).

willfully prepares or makes a false statement regarding a false or fraudulent tax return or knowingly provides fraudulent tax returns to the IRS.

In February and March 2008, TIGTA auditors posed as taxpayers in one large metropolitan area and had 27 tax returns prepared by individuals employed at both commercial chains and small independently owned tax preparation offices. The tax returns were not filed. Auditors explained to preparers that they would file the tax returns themselves.

Auditors used five scenarios with income ranging from $16,000 to $85,000. One scenario had self-employment income. The filing statuses ranged from Single or Married Filing Jointly to Head of Household. The issues included, for example, dependency exemptions, child care expenses, early withdrawal from a retirement plan, the Earned Income Tax Credit, and business expenses. TIGTA also used two of these scenarios in its filing season review of the Volunteer Program.

In its visits to tax preparation offices, TIGTA found that only 41 percent (11 of 27) of tax returns were considered to be prepared accurately. Among the inaccuracies, TIGTA found:

- 11 of 27 tax returns contained mistakes and omissions believed to be caused by human error and/or the complexity of the tax laws; and
- 5 of 27 tax returns contained misstatements and omissions that significantly affected the tax liability believed to be caused by willful or reckless conduct.

For six tax returns prepared inaccurately, taxpayers would have received unjustifiable refunds of $6,318. In 10 instances, taxpayers would have owed taxes of $6,472. In one case, a correctly prepared tax return would have resulted in a refund of $98, but instead resulted in a balance due of more than $6,000.

Refund Anticipation Loans

During the 2008 Filing Season, TIGTA also conducted an audit to determine the impact of Refund Anticipation Loans (RAL) on taxpayers and tax administration.[30] A RAL is a short-term loan based on a taxpayer's expected income tax refund and is a contract between the taxpayer and a lender. The lender is a bank and the facilitator is usually the tax preparer or tax preparation company. The bank first deducts fees for tax return preparation, e-filing, finance charges, and processing. The taxpayer receives the balance of the refund by check, direct deposit, debit card, or as a down payment on a good or service. Once the IRS processes the tax return that generated the refund, the IRS transfers the funds directly to the bank to repay the loan. The IRS is not involved in the contract, cannot grant or deny the loan, and cannot answer any questions about it.

As of March 28, 2008, approximately 18.6 million taxpayer accounts for Tax Year 2007 included RAL indicators. This includes 10 million taxpayers who filed tax

[30] Assessment of Refund Anticipation Loans (Audit Number 200840012).

returns claiming the Earned Income Tax Credit.[31] The IRS explained that preparers input the RAL indicator on the accounts when taxpayers apply for the loans.

As part of the audit, TIGTA conducted a telephone survey of 350 taxpayers whose Tax Year 2007 accounts contained RAL indicators. The survey was designed to gain an understanding of why taxpayers obtain RALs and determine the taxpayers' experiences during the process and the cost of the loans.

Of the 350 taxpayers surveyed, 81 percent (284) stated that they were unaware of IRS's free tax return preparation services for which they qualified. Seventy-one percent of respondents (250) stated that they had actually received RALs. The other 29 percent (100) did not apply for a RAL, applied but did not obtain the loan, or received a Refund Anticipation Check. A Refund Anticipation Check is a non-loan alternative to RALs. With a Refund Anticipation Check, the bank sets up a temporary account to receive the refund. Once the refund is deposited into this account, the bank deducts return preparation, filing, and bank processing fees before disbursing the remainder of the funds to the taxpayer.

Of the 250 respondents who stated that they had received RALs, 85 percent (213) stated that they understood they were receiving loans and that their preparers explained the fees – although most could not tell auditors the annual percentage rate they were charged for the loans.

Eighty-five percent (213) of respondents stated that they obtained the loans to more quickly receive their refunds and most used the funds to pay bills. About one-half received their loans within two business days. Additionally, 64 percent (159) stated that they had a checking or savings account in a financial institution.

IRS records show that some respondents who stated they did not receive a RAL might have received one, while other respondents who stated they received a RAL might not have received one. TIGTA is conducting additional research to resolve the discrepancies, as well as analyzing, for example, the amount of time it took the refunds to be deposited into the banks, whether the tax returns were posted on the CADE, and whether there were debt indicators or freezes on the respondents' accounts. In addition, selected demographics will be identified and analyzed.

Conclusion

Overall, the 2008 Filing Season appears to be progressing without major problems. The IRS has taken positive actions to prepare for the issuing of over $100 billion in stimulus payments beginning in May. In addition, the IRS has improved its quality customer service by creating a strategic plan to focus on service improvement and performance measures.

[31] The Earned Income Tax Credit is a refundable Federal tax credit for low-income working individuals and families.

However, TIGTA is concerned about the proliferation of phishing scams that attempt to trick taxpayers into providing sensitive tax information. Insider attacks by IRS employees and contractors continue to be a concern. Because of their familiarity with the IRS network, they can potentially do more harm than outsiders. Whether the attacks come from outside intruders or inside the IRS, the target is personal and financial information. While the IRS relies on its QRP to identify fraudulent refund claims and prevent them from being paid, TIGTA is concerned that the QRP is becoming increasingly unmanageable due to the growing number of fraudulent claims and the IRS's lack of resources to combat the fraud.

Furthermore, the IRS has placed only limited emphasis on employment-related and tax fraud identity theft. Although the Internal Revenue Code currently permits the referral of tax information to certain Federal law enforcement agencies, the IRS does not appear to be fully utilizing this authority. The IRS Criminal Investigation Division investigates identity theft crimes only if they are committed in conjunction with other criminal offenses having a large tax effect. As a result, the IRS has mainly focused on combating identity theft through public outreach. In addition, current processes have been inadequate in reducing burden for taxpayers victimized by identity theft. The IRS still lacks the comprehensive data needed to determine the impact identity theft is having on tax administration.

I hope that my discussion of tax-related identity theft and the 2008 Filing Season will assist you with your oversight of the IRS. Mr. Chairman and Members of the Committee, thank you for the opportunity to share my views.