HEARING BEFORE THE
COMMITTEE ON FINANCE
UNITED STATES SENATE

"Internal Revenue Service Data Breach Affecting Taxpayer Information"

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

June 2, 2015

Washington, D.C.

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON FINANCE
UNITED STATES SENATE

"Internal Revenue Service Data Breach Affecting Taxpayer Information"

June 2, 2015

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, thank you for the opportunity to testify on the data breach that occurred at the Internal Revenue Service (IRS).

The Treasury Inspector General for Tax Administration, also known as "TIGTA," is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of the IRS. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 91,000[1] IRS employees, who collected over $3.1 trillion in tax revenue, processed over 242 million tax returns and other forms, and issued $374 billion in tax refunds[2] during Fiscal Year 2014, perform their duties in an effective and efficient manner while minimizing the risks of waste, fraud, or abuse. This includes investigating individuals who use the IRS as a means of furthering fraudulent, criminal activity that negatively impacts the operations of the IRS, as well as investigating allegations of serious misconduct by IRS employees and threats of violence against the IRS, its employees, and facilities. Over the past year, a significant part of our workload has been devoted to investigating scams that can negatively impact the integrity of tax administration.

OVERVIEW OF THE RECENT IRS DATA BREACH

On May 26, 2015, the IRS announced that criminals had used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on

[1] Total IRS staffing as of January 24, 2015. Included in the total are approximately 19,000 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2014*, page 2.

approximately 100,000 tax accounts through the IRS's "Get Transcript" application.[3] TIGTA's Office of Investigations continues to investigate this incident, coordinating with other Federal law enforcement agencies. We ask for patience while we gather the evidence we need to determine who is responsible for this intrusion so they can be brought to justice. In addition, the evidence we are gathering is also critically important for us to understand the impact on the victims as well as to document exactly how this happened so it can be prevented in the future.

According to reports we received from the IRS, which we have not yet validated, an individual or individuals succeeded in clearing an authentication process that required knowledge of information about the taxpayer, including Social Security information, date of birth, tax filing status, and street address. In addition, it appears that these third-parties had access to private personal information that allowed them to correctly answer questions which typically only the taxpayer would know. This type of information can be purchased from illicit sources or fee-based databases, or obtained from social media sites.

The proliferation of data breaches reported in recent years and the types of information available on the Internet has resulted in a degradation of controls used to authenticate individuals accessing personal data in some systems. The expansion of e-commerce services often conflicts with the tenets of strict security standards. Providing taxpayers more avenues to obtain answers to their tax questions or to access their own tax records online also creates greater risk to an organization and provides more opportunities for exploitation by hackers and other fraudsters.

In its most recent Strategic Plan,[4] the IRS acknowledged that the current technology environment has raised taxpayers' expectations for online customer service interactions and it needs to meet these expectations. However, the risk for this type of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering taxpayers self-assisted interactive online tools. The Commissioner of Internal Revenue's vision is to provide taxpayers and tax professionals with electronic products and services that they desire to enable them to interact and communicate with the IRS. This includes more robust online services, based on the idea of accessing Government services anywhere, any time, on any device, in three to five years. For example, the IRS is acquiring software and contractor services for a Secure Messaging Pilot Program to be launched in Fiscal Year 2016 that will lay the foundation for a

[3] Information available on the "Get Transcript" application can include account transactions, line-by-line tax return information and income reported to the IRS.
[4] *Internal Revenue Service Strategic Plan – FY 2014-2017* (IRS Publication 3744), pgs. 6-7 (June 2014).

broader taxpayer digital communication rollout in the future.

In addition to the IRS's "Get Transcript" application, the IRS also requires taxpayers to authenticate their identities for certain other services on its public Internet site or its toll-free customer service lines, which could also pose a risk for unauthorized access. In June 2014, the IRS established its Authentication Group to provide oversight and facilitate the development and implementation of authentication policies and processes across the IRS's business functions. Due to the significant risks in this area, we currently have an audit underway to assess the IRS's processes for authenticating taxpayers at the time tax returns are processed and when accessing IRS services.[5]

DATA SECURITY REMAINS A TOP CONCERN OF TIGTA

Since Fiscal Year 2011, TIGTA has designated the security of taxpayer data as the top concern facing the IRS based on the increased number and sophistication of threats to taxpayer information and the need for the IRS to better protect taxpayer data and improve its enterprise security program. In addition, the IRS has declared its Information Security program as a "significant deficiency" from a financial reporting standpoint, which means weaknesses in its internal control environment are important enough to merit the attention of those charged with IRS governance.

To provide oversight of the IRS's Information Security program, TIGTA completes approximately seven audits each year on various security programs, systems, and solutions. As of March 2015, these audits have resulted in 44 recommendations that have yet to be implemented. While most of these recommendations are based on recent audits, there are 10 recommendations from five audits that are over three years old. In addition, the IRS has disagreed with 10 of 109 recommendations from 19 audits relating to security that we performed during the period of Fiscal Year 2012 through Fiscal Year 2014.

We have identified a number of areas in which the IRS could better protect taxpayer data and improve its overall security posture. Most recently, we found two areas that did not meet the level of performance specified by the Office of Management and Budget and the Department of Homeland Security: (1) Identity and Access Management, and (2) Configuration Management.[6]

---

[5] TIGTA, Audit No. 201440016, *Efforts to Authenticate Individual Income Tax Return Filers Before Tax Returns Are Processed*, report planned for August 2015.
[6] TIGTA, Ref. No. 2014-20-090, *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2014* (Sept. 2014).

Identity and Access Management ensures that only those with a business need are able to obtain access to IRS systems and data. However, we found that the IRS needs to fully implement unique user identification and authentication that complies with Department of Homeland Security directives, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

Configuration Management ensures that settings on IRS systems are maintained in an organized, secure, and approved manner, including timely updating patches to known security vulnerabilities. We found that the IRS needs to improve enterprise-wide processes for assessing configuration settings and vulnerabilities by means of automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

Patch[7] management is an important element in mitigating the security risks associated with known vulnerabilities to computer systems. This is critical to prevent intrusions by unauthorized individuals or entities. Due to its importance, TIGTA evaluated the effectiveness of the IRS security patch management process, which has been an ongoing challenge for the IRS.[8] We found that the IRS has made progress in automating installation and monitoring in a large segment of its computers, but it has not yet implemented key patch management policies and procedures needed to ensure that all IRS systems are patched timely and operating securely. Any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control over vulnerable computers and get access to the sensitive data the computer systems may contain, including taxpayer data.

We have also identified other areas that would improve the IRS's ability to defend its systems against cyberattacks. Monitoring IRS networks 24 hours a day year-round for cyberattacks and responding to various computer security incidents is the responsibility of the IRS's Computer Security Incident Response Center (CSIRC). TIGTA evaluated the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data.[9] We found that the CSIRC is effectively performing most of its responsibilities for preventing, detecting, and responding to computer security incidents. However, further

---

[7] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.
[8] TIGTA, Ref. No. 2012-20-112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012).
[9] TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012).

improvements could be made. At the time of our review, the CSIRC's host-based intrusion detection system was not monitoring a significant percentage of IRS servers, which leaves that portion of the IRS network and data at risk. In addition, the CSIRC was not reporting all computer security incidents to the Department of the Treasury, as required. Finally, incident response policies, plans, and procedures were either nonexistent, inaccurate, or incomplete.

One of the Federal Government's latest security initiatives is the implementation of information security continuous monitoring, which is defined as maintaining ongoing, real-time awareness of information security, vulnerabilities, and threats to support organizational risk decisions. While the IRS has made progress and is in compliance with Department of Homeland Security and Department of the Treasury guidelines, we have found that, based on the large scale of the IRS's computer environment, a one-size-fits-all approach does not provide the best security for the IRS.[10]

We have also previously raised concerns over the remediation of security weaknesses identified in our audits. Management controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are achieved. We have reviewed closed corrective actions to security weaknesses and findings reported by TIGTA and identified weak management controls in the IRS over its closed planned corrective actions for the security of systems involving taxpayer data.[11] During our audit, TIGTA determined that eight (42 percent) of 19 planned corrective actions that were approved and closed by the IRS as fully implemented in response to reported security weaknesses from prior TIGTA audits were only partially implemented.

Management control also involves the use of risk-based decisions by IRS management to make an exception to its own policies and requirements based on suitable justification and a thorough assessment of evident and potential risks. For decisions related to the security of information systems, exceptions are allowed if meeting the requirement is: 1) not technically or operationally possible, or 2) not cost effective. We found that these risk-based decisions were not adequately tracked and documented. Without required supporting documentation, we could not determine why decisions were made and whether the information technology risks were appropriately

[10] TIGTA, Ref. No. 2014-20-083, *The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs* (Sept. 2014).
[11] TIGTA, Ref. No. 2013-20-117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).

accepted and approved.[12]

ATTEMPTS TO DEFRAUD TAX ADMINISTRATION ARE INCREASING

Due to its mission, the trillions of dollars that flow through the IRS each year, and the hundreds of millions of taxpayer data sets used and maintained by the IRS, the IRS is continuously under attack by criminals using the tax administration system for personal gain in various ways. These scams, and the methods used to perpetrate them, are constantly changing and require constant monitoring by the IRS. For at least the last decade, the IRS has provided the public with information about what it sees as the "Dirty Dozen" tax scams on its website. These scams range from offshore tax avoidance to fake charities, and inflated refund claims. Compiled annually, the "Dirty Dozen" lists a variety of common scams that taxpayers may encounter.

In addition to the data breach discussed previously, two of the most pervasive frauds currently being perpetrated that impact tax administration are the phone impersonation scheme and identity theft.

Phone Impersonation Scam

The phone impersonation scam has proven to be so large that it is one of TIGTA's Office of Investigation's top priorities**,** and it has also landed at the top of the IRS's **"**Dirty Dozen**"** tax scams this year. It has proven to be a surprisingly effective and fast way to steal taxpayers' money, and in this fast-paced electronic environment, the money can be gone before the victims ever realize that they have been scammed. The number of complaints we have received about this scam makes it the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims with reported losses totaling almost $19 million to date.

We first started seeing concentrated reporting of these calls in August 2013. As the reporting continued through the fall, in October 2013 we started to specifically track this crime. To date, we have received hundreds of thousands of complaints about these calls. According to the victims, the scam artists made threatening statements and then demanded that the victims immediately put money on prepaid debit cards in order to avoid being arrested. The callers often warned the victims that if they hung up, local police would come to their homes to arrest them. The scammers may also send bogus IRS e-mails to support their scam. Those who fell for the scam withdrew thousands of

[12] TIGTA, Ref. No. 2014-20-092, *The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions* (Sept. 2014).

dollars from their bank accounts and then purchased the prepaid debit cards as instructed by the callers. Once the prepaid debit cards were purchased, the perpetrators instructed the victims to call them back and read them the numbers on the prepaid card. By the time the victims realized they had been scammed, the perpetrators had negotiated the prepaid cards and the money was gone.

To date, TIGTA has received over 525,000 reports of these calls. We continue to receive between 9,000 and 12,000 reports of these calls each week. As of May 25, 2015, 3,700 individuals have been victimized by this scam and have paid a total of almost $19 million, an average of approximately $5,100 per victim. The highest reported loss by one individual was over $500,000. In addition, 296 of these victims also provided sensitive identity information to these scammers.

The perpetrators do not discriminate; they are calling people everywhere, of all income levels and backgrounds. Based on a review of the complaints we have received, we believe the calls are now being placed from more than one source. This scam is the subject of an ongoing multi-agency investigation. There is much that we are doing to apprehend the perpetrators, but TIGTA is not at liberty to disclose specifically what is being done as it may impede our ability to successfully bring these criminals to justice. I can tell you that it is a matter of high priority for law enforcement.

However, there is much more that needs to be done, as these examples are part of a broader ring of scam artists operating beyond our borders. This is unfortunately similar to most of the cybercrime we are seeing today – it is international in nature and committed by means of technology (*e.g.*, in the case of the phone fraud scam, the use of Voice over Internet Protocol technology), and much of it originates from computers outside the United States. To further deceive their intended victims, by using this technology, the criminals create false telephone numbers that show up on the victim's caller ID system. For example, the criminals make it appear as though the calls are originating from Washington, D.C. or elsewhere in the United States.

Identity Theft

Another challenging area impacting tax administration is the growth in identity theft. At the same time the IRS is operating with a reduced budget, it continues to dedicate significant resources to detect and review potential identity theft tax returns as well as to assist victims. Resources have not been sufficient for the IRS to work identity theft cases dealing with refund fraud, which continues to be a concern. A critical component of preventing and combating identity theft refund fraud is the authentication of a taxpayer's identity at the time tax returns are processed.

During the past several years, the IRS has continued to take steps to more effectively detect and prevent the issuance of fraudulent refunds resulting from identity theft tax return filings. The IRS reported that in Filing Season 2013, its efforts prevented between $22 billion and $24 billion in identity theft tax refunds from being issued.[13] This is a result of the IRS's continued enhancement of filters used to detect tax returns that have a high likelihood of involving identity theft at the time the returns are processed. For example, the IRS used 11 filters in Processing Year (PY) 2012 to identify tax returns with a high likelihood of involving identity theft, compared to the 114 filters it used in PY 2014. The use of these filters assists the IRS in more effectively allocating its resources to address identity theft tax refund fraud.

The IRS has also taken steps to more effectively prevent the filing of identity theft tax returns by locking the tax accounts of deceased individuals to prevent others from filing a tax return using their names and Social Security Numbers. The IRS has locked approximately 26.3 million taxpayer accounts between January 2011 and December 31, 2014. In addition, the IRS issues an Identity Protection Personal Identification Number (IP PIN) to any taxpayer who is a confirmed victim of identity theft or who has reported to the IRS that he or she could be at risk of identity theft. However, we reported that the IRS did not provide an IP PIN to 557,265 eligible taxpayers for Processing Year 2013.[14] Once the IRS confirms the identity of a victim or "at-risk" taxpayer, the IRS will issue the taxpayer an IP PIN for use by the taxpayer when filing his or her tax return. The presence of a valid IP PIN on the tax return tells the IRS that the rightful taxpayer filed the tax return, thus reducing the need for the IRS to screen the tax return for potential identity theft. The IRS has issued more than 1.5 million IP PINs for PY 2015.

---

[13] IRS Identity Theft Taxonomy, dated September 15, 2014, page 1.
[14] TIGTA, Ref. No. 2014-40-086, *Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers* (Sept. 2014).

Despite these improvements, the IRS recognizes that new identity theft patterns are constantly evolving and that consequently, it needs to adapt its detection and prevention processes. The IRS's own analysis estimates that identity thieves were successful in receiving over $5 billion in fraudulent tax refunds in Filing Season 2013.

In summary, the IRS faces the daunting task of protecting its data and IT environment from the ever-changing and rapidly-evolving hacker world. This incident provides a stark reminder that even security controls that may have been adequate in the past can be overcome by hackers, who are anonymous, persistent, and have access to vast amounts of personal data and knowledge. The IRS needs to be even more vigilant in protecting the confidentiality of sensitive taxpayer information. Otherwise, as shown by this incident, taxpayers can be exposed to the loss of privacy and to financial damages resulting from identity theft or other financial crimes.

We at TIGTA are committed to our mission of ensuring an effective and efficient tax administration system and preventing, detecting, and deterring waste, fraud, and abuse. As such, we plan to provide continuing audit and investigative coverage of the IRS's efforts to effectively protect sensitive taxpayer data and investigate any instances of attempts to corrupt or otherwise interfere with tax administration.

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, thank you for the opportunity to share my views.

J. Russell George

Treasury Inspector General for Tax Administration

Following his nomination by President George W. Bush, the United States Senate confirmed J. Russell George in November 2004, as the Treasury Inspector General for Tax Administration. Prior to assuming this role, Mr. George served as the Inspector General of the Corporation for National and Community Service, having been nominated to that position by President Bush and confirmed by the Senate in 2002.

A native of New York City, where he attended public schools, including Brooklyn Technical High School, Mr. George received his Bachelor of Arts degree from Howard University in Washington, DC, and his Doctorate of Jurisprudence from Harvard University's School of Law in Cambridge, MA. After receiving his law degree, he returned to New York and served as a prosecutor in the Queens County District Attorney's Office.

Following his work as a prosecutor, Mr. George joined the Counsel's Office in the White House Office of Management and Budget where he was Assistant General Counsel. In that capacity, he provided legal guidance on issues concerning presidential and executive branch authority. He was next invited to join the White House Staff as the Associate Director for Policy in the Office of National Service. It was there that he implemented the legislation establishing the Commission for National and Community Service, the precursor to the Corporation for National and Community Service. He then returned to New York and practiced law at Kramer, Levin, Naftalis, Nessen, Kamin & Frankel.

In 1995, Mr. George returned to Washington and joined the staff of the Committee on Government Reform and Oversight, where he served as the Staff Director and Chief Counsel of the Government Management, Information and Technology subcommittee (later renamed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations), chaired by Representative Stephen Horn. There he directed a staff that conducted over 200 hearings on legislative and oversight issues pertaining to Federal Government management practices, including procurement policies, the disposition of government-controlled information, the performance of chief financial officers and inspectors general, and the Government's use of technology. He continued in that position until his appointment by President Bush in 2002.

In addition to his duties as the Inspector General for Tax Administration, Mr. George serves as a member of the Recovery Accountability and Transparency Board, a non-partisan, non-political agency created by the American Recovery and Reinvestment Act of 2009 to provide unprecedented transparency and to detect and prevent fraud, waste, and mismanagement of Recovery funds. There, he serves as chairman of the Recovery.gov committee, which oversees the dissemination of accurate and timely data about Recovery funds.