HEARING BEFORE THE
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES

"The 2016 Tax Filing Season"

Testimony of
Timothy P. Camus
Deputy Inspector General for Investigations
Treasury Inspector General for Tax Administration

April 19, 2016

Washington, D.C.

TESTIMONY
OF
TIMOTHY P. CAMUS
DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES

"The 2016 Tax Filing Season"
April 19, 2016

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to testify on the topic of tax scams and schemes faced by the Internal Revenue Service (IRS) during the 2016 tax return filing season.

The Treasury Inspector General for Tax Administration (TIGTA) is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of IRS operations, including the IRS Chief Counsel. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays a critical role in ensuring the approximately 86,000 IRS employees[1] who collected over $3.3 trillion in tax revenue, processed over 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2015,[2] have done so in an effective and efficient manner while minimizing the risks of waste, fraud, and abuse.

TIGTA's Office of Audit (OA) reviews all aspects of Federal tax administration and provides recommendations to improve IRS systems and operations; ensure the fair and equitable treatment of taxpayers; and detect and prevent waste, fraud, and abuse in tax administration. The Office of Audit places an emphasis on statutory coverage required by the IRS Restructuring and Reform Act of 1998 (RRA 98)[3] and other laws, as well as on areas of concern raised by Congress, the Secretary of the Treasury, the Commissioner of Internal Revenue, and other key stakeholders. The OA has examined

[1] Total IRS staffing as of October 3, 2015. Included in the total are approximately 15,400 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2015*.
[3] Pub. L. No. 105-206, 112 Stat. 685 (1998) (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

specific high-risk issues such as identity theft, refund fraud, improper payments, information technology, security vulnerabilities, complex modernized computer systems, tax collections and revenue, and waste and abuse in IRS operations.

TIGTA's Office of Investigations (OI) protects the integrity of the IRS by investigating allegations of IRS employee misconduct, external threats to IRS employees and facilities, and other attempts to impede or otherwise interfere with the IRS's ability to collect taxes. Specifically, OI investigates misconduct by IRS employees which manifests itself in many ways, including unauthorized access to taxpayer information and the use of the information for the purposes of identity theft; extortion; theft of government property; Section 1203 taxpayer abuses; false statements; and other financial fraud. For example, as will soon be reported in our upcoming Semiannual Report to Congress, in the past six months, TIGTA investigations resulted in Federal prosecution action on six IRS employees whose criminal activity impacted over 240 taxpayers and cost the Government the payment of hundreds of thousands of dollars in fraudulent refunds. Although the six IRS employees involved in this criminal activity represent a very small percentage of the total IRS employee population, their actions negatively impacted the public's perception of the integrity of the Federal tax system; therefore, allegations of IRS employee misconduct will remain one of our primary investigative priorities.

Since the summer of 2013, a significant amount of OI's workload has consisted of investigating a telephone impersonation scam in which more than one million intended victims have received unsolicited telephone calls from individuals falsely claiming to be IRS or Department of the Treasury employees. The callers demand money under the pretense that the victim owes unpaid taxes. To date, over 5,700 victims have purportedly paid more than $31 million to these criminals.

In the last several years, threats directed at the IRS have remained the second largest component of OI's work. Physical violence, harassment, and intimidation of IRS employees continue to pose challenges to the implementation of a fair and effective system of tax administration. The Office of Investigations is statutorily charged to investigate threats made against IRS employees, facilities, and data and is committed to ensuring the safety of IRS employees as well as the taxpayers who conduct business at the approximately 550 IRS offices[4].

In this section of my testimony, I will briefly discuss the status of the 2016 tax return Filing Season and the tax scams and schemes that the IRS is currently facing as

[4] IRS, *Management's Discussion & Analysis, Fiscal Year 2015*.

it administers our Nation's tax laws.

STATUS OF THE 2016 FILING SEASON

The annual tax return filing season[5] is a critical time for the IRS as this is when most individuals file their income tax returns and contact the IRS if they have questions about specific tax laws or filing procedures. During Calendar Year (CY) 2016, the IRS expects to receive more than 150 million individual income tax returns, approximately 19 million paper filed and 131 million filed electronically (e-filed).

Among the continuing challenges the IRS faces each year in processing tax returns are the implementation of new tax law changes and changes resulting from expired tax provisions. Before the filing season begins, the IRS must identify the tax law and administrative changes affecting the upcoming filing season. Once these have been identified, the IRS must revise the various tax forms, instructions, and publications affected by the changes. It also must reprogram its computer systems to ensure that tax returns are accurately processed based on changes in the tax law. Errors in the IRS's tax return processing systems may delay tax refunds, affect the accuracy of taxpayer accounts, or result in incorrect taxpayer notices.

For the 2016 Filing Season, the IRS was challenged by the late passage of legislation that extended a number of expired tax provisions.[6] To reduce the impact on the filing season, the IRS monitored the status of the legislation and took steps to implement the extension of these provisions prior to their enactment. These efforts enabled the IRS to begin accepting and processing individual tax returns on January 19, 2016, as scheduled. As of March 4, 2016, the IRS had received more than 66.7 million tax returns—more than 62.6 million (93.9 percent) of which were e-filed and more than 4 million (6.1 percent) of which were filed on paper. The IRS has issued more than 53.5 million refunds totaling more than $160 billion.

Implementation of provisions of the Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act of 2010[7] (collectively referred to as the Affordable Care Act or ACA) will also continue to present challenges for the IRS in the 2016 Filing Season. As of February 25, 2016, the IRS had processed 1.4 million tax returns that reported $4.4 billion in Premium Tax Credits that were either received

---

[5] The period from January 1 through mid-April when most individual income tax returns are filed.
[6] TIGTA, Ref. No. 2016-40-034, *Interim Results of the 2016 Filing Season* (Mar. 2016).
[7] Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the Internal Revenue Code and 42 U.S.C.), as amended by the Heath Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

in advance or claimed at the time of filing. As of March 3, 2016, the IRS had received approximately 47 million tax returns reporting that all members of the taxpayer's family maintained minimum essential coverage as required by the ACA. In addition, more than 2.7 million taxpayers reported shared responsibility payments totaling $1 billion for not maintaining the required health insurance coverage.

For the 2016 Filing Season, taxpayers have several options to choose from when they need assistance from the IRS, including assistance through the toll-free telephone lines,[8] face-to-face assistance at the Taxpayer Assistance Centers (TAC) or Volunteer Program sites, and self-assistance through IRS.gov and various other social media channels (*e.g.*, Twitter, Facebook, and YouTube). The IRS continues to increase its dependence on technology-based services and external partners that direct taxpayers to the most cost-effective IRS or partner channel available to provide the needed service. The IRS notes that this approach allows it to focus limited toll-free and walk-in resources on customer issues that can be best resolved with person-to-person interaction. However, the cuts made by the IRS in its traditional services continue to significantly affect a number of areas.

For example, the IRS reports that, as of March 5, 2016, approximately 46.1 million attempts had been made to contact the IRS via its toll-free assistance lines for the 2016 Filing Season. Assistors have answered approximately 7.3 million calls and have achieved a 72.8 percent Level of Service[9] with a 9.6 minute Average Speed of Answer.[10] As a result of the IRS receiving additional funding for customer service in FY 2016, the IRS is forecasting a 65 percent Level of Service for the 2016 Filing Season, which is an increase from the 38 percent it originally forecasted. Overall, the IRS is forecasting a 47 percent Level of Service for the full fiscal year, which is an increase from its original forecast of 34 percent. We are currently assessing the IRS's process for allocating its Customer Service budget.

In addition, each year many taxpayers seek assistance from one of the IRS's 376 walk-in offices, called TACs. However, the IRS estimates that the number of taxpayers it will assist at its TACs will continue to decrease. The IRS assisted 5.6 million taxpayers in FY 2015 and plans to assist 4.7 million taxpayers in FY 2016, which represents a 16 percent decline from FY 2015.

---

[8] The IRS refers to the suite of 29 telephone lines to which taxpayers can make calls as "Customer Account Services Toll-Free".
[9] The primary measure of service to taxpayers. It is the relative success rate of taxpayers who call for live assistance on the IRS toll-free telephone lines.
[10] The average number of seconds taxpayers waited in the assistor queue (on hold) before receiving services.

However, the IRS has implemented initiatives to better assist those individuals seeking assistance from a TAC. For example, in CY 2015, the IRS began providing services at selected TACs by appointment, in an attempt to alleviate long lines that sometimes occur at many TACs and to help ensure that taxpayers' issues are resolved. The IRS reports that as of February 29, 2016,[11] 166,569 taxpayers had scheduled an appointment. The IRS also offers Virtual Service Delivery, which integrates video and audio technology to allow taxpayers to see and hear an assistor located at a remote TAC. For the 2016 Filing Season, the IRS is offering Virtual Service Delivery at 35 locations, which include 24 TACs and 11 Volunteer Program sites. The IRS reports that 8,137 taxpayers had used the service as of February 29, 2016.

TAX REFUND FRAUD

The IRS is continuing to expand its efforts to detect tax-refund fraud. The IRS reports that, as of March 5, 2016, it had identified 42,148 tax returns with nearly $227 million claimed in fraudulent refunds. Moreover, it had prevented the issuance of $180.6 million (79.6 percent) in fraudulent refunds and also identified 20,224 potentially fraudulent tax returns filed by prisoners during this year's filing season. The IRS also reports that, as of February 29, 2016, it had identified and confirmed 31,578 fraudulent tax returns and prevented the issuance of $193.8 million in fraudulent tax refunds as a result of its identity-theft filters. Finally, the IRS is continuing to expand on its use of controls to identify fraudulent refund claims before they are accepted into the processing system. As of February 29, 2016, it had identified approximately 35,000 fraudulent e-filed tax returns and approximately 741 fraudulent paper tax returns.

TIGTA continues to identify fraudulent claims as an IRS major management challenge. As such, we continue to evaluate the IRS's efforts to improve fraudulent tax return filing detection processes, including its efforts to implement TIGTA's recommendations.

In November 2015,[12] TIGTA reported that a programming error resulted in over $27 million in refunds being erroneously issued for more than 13,000 Tax Year (TY) 2013 returns before the income and withholding had been screened and verified. Each of these tax returns was identified by the IRS as potentially fraudulent. In addition,

---

[11] For Fiscal Year 2016 – October 1, 2015 through February 29, 2016.
[12] TIGTA, Ref. No. 2016-40-006, *Improvements Are Needed to Better Ensure That Refunds Claimed on Potentially Fraudulent Tax Returns Are Not Erroneously Released* (Nov. 2015).

TIGTA reported that ineffective monitoring of potentially fraudulent tax returns had resulted in the erroneous release of $19 million in refunds for 3,910 TY 2013 tax returns. Each of these returns was selected by the IRS; however there was no indication that tax examiners had verified the returns prior to the refund being issued. The IRS agreed with TIGTA recommendations to address the concerns identified.

Clearly, tax-related identify theft is a major challenge still facing the IRS. Since 2012, TIGTA has issued a series of reports assessing the IRS's efforts to detect and prevent fraudulent tax refunds resulting from identity theft. In July 2012, we reported that the impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents. Our analysis of TY 2010 tax returns identified approximately 1.5 million undetected tax returns with potentially fraudulent tax refunds, totaling in excess of $5.2 billion, which had the characteristics of identity theft confirmed by the IRS.[13]

For example, in response to our reporting that the IRS did not have a process to measure the impact of identity theft, the IRS initiated a research project in CY 2012 to develop a measurement process to assess its efforts to defend against identity theft and identify areas that require additional effort. For the 2014 Filing Season, the IRS reported that identity thieves had been successful in receiving approximately $3.1 billion in fraudulent tax refunds. TIGTA is evaluating the accuracy of the IRS's measurement process and expects to issue its report early next fiscal year.

The IRS has implemented many of TIGTA's recommendations and has continued in its efforts to improve its detection processes. In the 2014 Filing Season, the IRS reported that it had detected and prevented approximately $21.5 billion in identity theft refund fraud.

The IRS is locking the tax accounts of deceased individuals to prevent others from filing a tax return using their names and Social Security Numbers (SSN). The IRS locked approximately 30.2 million taxpayer accounts between January 2011 and December 31, 2015. For Processing Year 2015, the IRS rejected approximately 77,000 fraudulent e-filed tax returns and prevented about 16,000 paper-filed tax returns through the use of these locks as of April 30, 2015.

The IRS also continues to expand the number of filters it uses to detect identity theft refund fraud at the time tax returns are processed. Those filters increased from

---

[13] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

11 filters for the 2012 Filing Season to 183 filters for the 2016 Filing Season. Tax returns identified by these filters are held during processing until the IRS can verify the taxpayers' identities. As of December 31, 2015, the IRS reported that it had identified and confirmed more than one million fraudulent tax returns and prevented the issuance of nearly $6.8 billion in fraudulent tax refunds as a result of the identity theft filters.

After TIGTA continued to identify large volumes of undetected potentially fraudulent tax returns with tax refunds issued to the same address or deposited into the same bank account, the IRS developed and implemented a clustering filter tool during the 2013 Filing Season. This tool groups tax returns based on characteristics that include address and bank routing numbers. Tax returns identified are held from processing until the IRS can verify the taxpayer's identity. As of December 31, 2015, the IRS reported that, using this tool, it identified 835,183 tax returns claiming approximately $4.3 billion in potentially fraudulent tax refunds.

A new process, also implemented during the 2015 Filing Season, limits the number of direct deposit refunds that can be sent to a single bank account to three deposits. The IRS converts the fourth and subsequent direct deposit refund requests to a specific account to a paper refund check and mails the check to the taxpayer's address of record. In August 2015, we reported that programming errors resulted in some direct deposit refunds not converting to a paper check as required.[14]

As noted earlier in my testimony, unfortunately, tax refund fraud and identity theft is not limited to unscrupulous individuals operating from outside of the IRS; there is also an insider threat posed by IRS employees who use their official positions and access to IRS information in furtherance of these schemes. For example, one of the most significant recent cases involved an IRS employee who, through their access to IRS data, stole the IRS information of hundreds of taxpayers, and then used that information in an attempt to obtain between $550,000 and $1.5 million in fraudulent refunds. The employee was able to successfully steal over $438,000 in fraudulent refunds.[15] We detected this criminal activity through our ability to review the audit trails of accesses made by IRS employees to the IRS computer systems. We remain very concerned that as the IRS has modernized its systems over the last several years, it has not built in adequate audit trails that would allow us to detect an IRS employee's unauthorized access to taxpayer information. Although we are discussing this vulnerability with the IRS Information Technology leadership, the pace of progress is not acceptable. For example, currently only 12 of the 82 applications subject to the risk

[14] TIGTA, Ref. No. 2015-40-080, *Results of the 2015 Filing Season* (Aug. 2015).
[15] N.D. Ala. Plea Agreement Nakeisha Hall filed Feb. 8, 2016.

of unauthorized access and theft of taxpayer information are currently transmitting accurate and complete audit trail data. The IRS estimates that it will have this vulnerability addressed between FY 2021 and FY 2027.

In December 2015, Congress passed legislation to address TIGTA's ongoing concern about limitations in the IRS's ability to prevent the continued issuance of billions of dollars in fraudulent tax refunds.[16] We reported that the IRS did not have timely access to third-party income and withholding information needed to make substantial improvements in its fraud detection efforts. The recently enacted legislation now requires the annual filing of income and withholding information by January 31, beginning in 2017.[17] Access to this information at the beginning of the filing season is the single most important tool to detect and prevent tax fraud-related identity theft. TIGTA will be reviewing the IRS's use of the income and withholding information returns as part of its FY 2017 assessment of efforts to detect and prevent identity theft.

Identity theft also affects businesses. In September 2015, TIGTA determined that processing filters could be developed to identify business tax returns containing certain characteristics that could indicate potential identity-theft cases.[18] TIGTA also reported that State information sharing agreements do not address business identity theft and that actions are needed to better promote awareness of business identity theft. The IRS agreed with our recommendations.

In order to continue to improve its detection efforts, the IRS needs expanded capabilities in its fraud detection system. The IRS's current fraud detection system does not allow the IRS to change or adjust identification filters throughout the processing year. The IRS is developing and testing a replacement fraud detection system, called the Return Review Program (RRP), which the IRS believes will provide new and improved capabilities that advance its fraud detection and prevention to a higher level.

The IRS conducted a pilot test of the RRP scoring and models during Processing Year 2014 to assess its effectiveness in identifying potential identity-theft tax returns. In December 2015, TIGTA reported that although the pilot successfully identified tax returns involving identity theft that were not identified by the IRS's other

---

[16] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. Q, § 201 (2015).
[17] *Id*.
[18] TIGTA, Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).

fraud detection systems, it did not detect all the fraudulent tax returns identified by its existing fraud detection systems.[19]

IRS ASSISTANCE TO VICTIMS OF IDENTITY THEFT

TIGTA has identified continuing issues with victim assistance. In September 2013, TIGTA reported that, on average, it took the IRS 312 days to resolve tax accounts of identity-theft victims due a refund in FY 2012.[20] In March 2015, we reported that taxpayers were still experiencing long delays in resolving their tax accounts and that the IRS continued to make errors on the victims' tax accounts.[21] Our review of a statistically valid sample of 100 identity-theft tax accounts resolved by the IRS during FY 2013 identified that the IRS took an average of 278 days to resolve the tax accounts and did not correctly resolve 17 of the 100 accounts (17 percent) we reviewed. We estimate that of the 267,692 taxpayer cases resolved during this period, 25,565 (10 percent) may have been resolved incorrectly resulting in delayed or incorrect refunds and requiring the IRS to reopen cases to resolve the errors.

In October 2008, the IRS formed the Identity Protection Specialized Unit (IPSU) as part of its strategy to reduce taxpayer burden caused by identity theft. The IPSU is a dedicated unit for victims of identity theft to have their questions answered and obtain assistance in resolving their identity-theft issues quickly and effectively. In October 2015, we reported that the majority of identity-theft victims are no longer provided with an IPSU single point of contact.[22] The IRS indicated that budgetary constraints did not allow for a single employee to be assigned to each identity-theft victim. However, the IRS has stated that it remains committed to providing identity-theft victims with the centralized IPSU hotline to obtain assistance. The IRS noted that obtaining assistance via contact with the hotline does not depend on the availability of a single IRS representative, who may be unavailable because he or she is performing other casework. We also found that the IPSU's process does not ensure that taxpayers are timely informed about the IRS's receipt of their supporting documentation or the status of their identity-theft claims.

---

[19] TIGTA, Ref. No. 2016-40-008*, Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection* (Dec. 2015).
[20] TIGTA, Ref. No. 2013-40-129, *Case Processing Delays and Tax Account Errors Increased Hardship for Victims of Identity Theft* (Sept. 2013).
[21] TIGTA, Ref. No. 2015-40-024, *Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds* (Mar. 2015).
[22] TIGTA, Ref. No. 2016-40-003, *Improvements Are Needed in the Identity Protection Specialized Unit to Better Assist Victims of Identity Theft* (Oct. 2015).

On May 4, 2015, the IRS announced the final phase of its plan to consolidate its identity-theft assistance and compliance activities into a new organization called the Identity Theft Victim Assistance Directorate. The IRS indicated that this new directorate aims to provide consistent treatment to victims of tax-related identity theft. We plan to review the IRS's implementation of this organization as part of our FY 2016 audit coverage.

IRS "GET TRANSCRIPT" DATA BREACH

The risk of unauthorized access to tax accounts and the potential theft of taxpayer information from the IRS will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers. The IRS plans to increase the availability and quality of self-service interactions, allowing it to free up in-person resources for taxpayers who truly need them. The IRS's goal is to eventually provide taxpayers with dynamic online account access that includes viewing their recent payments, making minor changes and adjustments to their accounts, and corresponding digitally with the IRS. As tax administration evolves, the challenge of providing adequate data security will continue.

In a report issued in November 2015, TIGTA found that although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, it has not established a Service-wide approach to managing its authentication needs.[23] As a result, the level of authentication the IRS uses for its various services is not consistent. The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system.

Unscrupulous individuals constantly seek to identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information. For example, on May 26, 2015, the IRS announced that individuals using taxpayer-specific data had attempted to gain unauthorized access to tax information[24] through the e-authentication portal and into the Get Transcript application. According to the IRS, one or more individuals succeeded in clearing the IRS's authentication process, which required knowledge of information about individual taxpayers, including

---

[23] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).

[24] The tax information that can be accessed on the Get Transcript application can include the current and three prior years of tax returns, nine years of tax account information, and wage and income information.

Social Security information, date of birth, tax filing status, and street address. The unauthorized accesses resulted in the IRS disabling the application.

Office of Management Budget (OMB) standards require Federal agencies to conduct an assessment of the risk of authentication error for each online service or application they provide. An authentication error occurs when an agency confirms the identity provided by an individual, despite the fact that the individual is not who he or she claims to be. In addition, the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Special Publication 800-63 establishes specific requirements that agencies' authentication processes must meet to provide a specific level of authentication assurance. However, we found that, although the IRS has established processes and procedures to authenticate individuals requesting online access to IRS services, these processes and procedures do not comply with Government standards for assessing authentication risk and establishing adequate authentication processes.

The IRS assessed the risk of the Get Transcript application as required. However, the IRS determined that the authentication risk associated with Get Transcript was low to both the IRS and taxpayers. The IRS defines a low risk rating as one in which the likelihood of an imposter obtaining and using the information available on an application is low. In addition, a low risk rating indicates that controls are in place to prevent, or at least significantly impede, an imposter from accessing the information. As a result, the IRS has implemented single-factor authentication to access the Get Transcript application.

In August 2015, the IRS indicated that unauthorized users had been successful[25] in obtaining information on the Get Transcript application for an estimated 334,000 taxpayer accounts. TIGTA's current review[26] of the Get Transcript breach has identified additional suspicious accesses to taxpayers' accounts that the IRS had not identified. Based on TIGTA's analysis of Get Transcript access logs, the IRS reported on February 26, 2016 that potentially unauthorized users had been successful in obtaining access to an additional 390,000 taxpayer accounts, for a total of over 724,000 stolen transcripts. The IRS also reported that an additional 295,000 taxpayer transcripts had been targeted but the access attempts had not been successful. TIGTA was able to identify these additional unauthorized accesses due to our use of advanced analytics and cross-discipline approaches. The IRS had not

[25] A successful access is one in which the unauthorized users successfully answered identity proofing and knowledge-based authentication questions required to gain access to taxpayer account information.
[26] TIGTA, Audit No. 201540027, *Evaluation of Assistance Provided to Victims of the Get Transcript Data Breach*, report planned for May 2016.

previously identified these accesses because of limitations in the scope of its analysis, including its method of identifying suspicious e-mail accounts and the timeframe it analyzed.

In response to TIGTA's identification of the additional accesses, the IRS started mailing notification letters on February 29, 2016 to the affected taxpayers and placing identity-theft markers on their tax accounts. It should be noted that the actual number of individuals whose personal information was available to the potentially unauthorized individuals accessing these tax accounts is significantly larger than the number of taxpayers whose accounts were accessed in that these tax accounts include certain information on individuals other than the taxpayers listed on these tax returns (*e.g.*, spouses and dependents).

We are currently evaluating the appropriateness of the IRS's response to the Get Transcript incident and the IRS's proposed solutions to address the authentication weakness that allowed the incident to occur.[27] To date, we have learned that the IRS is working with the U.S. Digital Service[28] on its new e-authentication and authorization policies and procedures.

In addition, TIGTA is participating in a multi-agency investigation into this matter, and we have provided the IRS with some of our investigative observations to date in order to help them secure the e-authentication environment in the future. During its investigation, TIGTA has observed that the unauthorized accesses and the thefts of tax transcripts from the Get Transcript application have been occurring for some time, not long after the application was initially made available to the public until the IRS disabled it in May 2015. In addition to the investigative activity based on the May 2015 data breach, TIGTA is also investigating an additional 22 other cases involving transcripts that were stolen from the Get Transcript application and then used to file fraudulent refund tax returns.

For example, in one case, our investigation revealed that the defendant broke into the Get Transcript application and obtained 22 transcripts. He then filed over 100 fraudulent tax returns seeking $500,000 in fraudulent IRS refunds.[29] In a separate case, the defendant and co-conspirators stole over 1,200 transcripts from the Get Transcript application. They then used the stolen information to file over 2,900

---

[27] TIGTA, Audit No. 201520006, *Review of Progress to Improve Electronic Authentication*, report planned for July 2016.
[28] The U.S. Digital Service is part of Executive Office of the President. Its goal is to improve and simplify the digital services that people and businesses have with the Government.
[29] Department of Justice Press Release, S.D. Fla dated Mar. 1, 2016.

fraudulent tax returns seeking $25 million in refunds. The IRS stopped most of the fraudulent refunds, but ultimately paid $4.7 million in fraudulent refunds to the defendant and his co-conspirators.[30] In both cases, the Get Transcript information was stolen from between early February 2015 and April 30, 2015.

Finally, we also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its online Identity Protection Personal Identification Number (IP PIN)[31] application. On January 8, 2016, we recommended that the IRS not reactivate its online IP PIN application for the 2016 Filing Season, due to concerns that the IP PIN authentication process requires knowledge of the same taxpayer information that was used by the individuals who breached the Get Transcript application. Notwithstanding our recommendation, the IRS reactivated the application on January 19, 2016. We issued a second recommendation to the IRS on February 24, 2016, advising it to disable the IP PIN application from its public website to prevent any further abuse.

On March 7, 2016, the IRS reported that it was temporarily suspending use of the IP PIN application as part of an ongoing security review. The IRS also reported that 800 stolen IP PINs had been used to file fraudulent refund returns. The IRS advised that it is conducting a further review of the application that allows taxpayers to retrieve their IP PINs online and is looking at further strengthening its security features. The IRS does not anticipate having the technology in place to provide multifactor authentication capability for either the Get Transcript or IP PIN application before the summer of 2016.

No single authentication method or process will prevent criminals from filing identity-theft tax returns or attempting to inappropriately access IRS services. However, strong authentication processes can reduce the risk of such activity by making it harder and more costly for individuals to gain unauthorized access to resources and information. Therefore, it is important that the IRS ensure that its authentication processes are in compliance with NIST standards to provide the highest degree of assurance that valuable taxpayer information is protected from criminals.

---

[30] D. Or. Indictment Michael O. Kazeem filed Feb. 4, 2016.

[31] To provide relief to tax-related identity-theft victims, the IRS issues IP PINs to taxpayers who are confirmed by the IRS as victims of identity theft, taxpayers who are at a high risk of becoming a victim such as taxpayers who call reporting a lost or stolen wallet or purse, as well as taxpayers who live in three locations that the IRS has identified as having a high rate of identity theft (Florida, Georgia and the District of Columbia).

TELEPHONE IMPERSONATION SCAM

As noted earlier in my testimony, the telephone impersonation scam continues to be one of TIGTA's top priorities; it has also landed at the top of the IRS's **"**Dirty Dozen**"** tax scams. The numbers of complaints we have received about this scam continues to climb, cementing its status as the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims, including victims in every State represented on this committee, with reported losses totaling more than $31 million to date.

We started receiving reports of this particular phone scam in August 2013. As the reporting continued through the Fall, we started to specifically track this crime in October 2013. TIGTA currently receives between 10,000 and 19,000 reports of these calls each week. To date, TIGTA has received more than one million reports of these calls. As of April 4, 2016, 5,770 victims of this scam have reported to TIGTA they have collectively paid a total of more than $31 million, an average of approximately $5,370 per victim. The highest reported loss by any one individual exceeded $500,000. In addition, more than 1,275 of these victims reported that they also provided sensitive identity information to the scammers.

Here is how the scam works: The intended victim receives an unsolicited telephone call from a live person or from an automated call dialer. The caller, using a fake name and sometimes a fictitious employee badge number, claims to be an IRS or Treasury employee. The scammers use Voice over Internet Protocol technology to hide their tracks and create false telephone numbers that show up on the victim's caller ID system. For example, the scammers may make it appear as though the calls are originating from Washington, D.C., or elsewhere in the U.S.

The callers may even know the last four digits of the victim's SSN or other personal information about the victim. The caller claims that the intended victim owes the IRS taxes and that, if those taxes are not paid immediately, the victim will be arrested or charged in a lawsuit. Other threats for non-payment include the loss of a driver's license, deportation, or loss of a business license. They often leave "urgent" messages to return telephone calls and they often call the victim multiple times.

According to the victims we have interviewed, the scammers who made the threatening statements as described above then demanded that the victims immediately pay the money using prepaid debit cards, wire transfers, Western Union payments or MoneyGram payments in order to avoid being immediately arrested. They are typically warned that if they hang up, local police will come to their homes to arrest them immediately. Sometimes the scammers also send bogus IRS e-mails to

support their claims that they work for the IRS. By the time the victims realize that they have been scammed, the funds are long gone.

Over time, the scam has evolved from live callers demanding payment using prepaid debit cards to scammers using automated call dialers, or "robo-dialers," to place thousands of calls very rapidly. When the intended victim answers the phone, the automated voice states that the victim owes the IRS taxes. The victims are informed that if they do not immediately call a telephone number provided in the message, they will face arrest and possibly a lawsuit.

TIGTA has made several arrests in connection with this scam and has numerous investigations underway. In one of the largest prosecutions on this scam that we have had to date, in July 2015, an individual plead guilty to organizing an impersonation scam ring and was sentenced to over 14 years of incarceration and a $1 million dollar forfeiture. While we cannot provide specific details of our additional ongoing investigations out of concern that it will hinder our ability to prosecute those responsible, we can describe for you some of the other steps TIGTA is taking to combat this scam.

To thwart scammers using robo-dialers, we have created and instituted an "Advise and Disrupt" strategy. The strategy involves cataloguing the telephone numbers that were reported by intended victims. We then use our own automated call dialers to make calls to those telephone numbers to advise the scammers that their activity is criminal and to cease and desist their activity. As of April 8, 2016, we have placed more than 59,000 automated calls back to the scammers.

Also, we are working with the telephone companies to have the scammers' telephone numbers shut down as soon as possible. Of the 626 telephone numbers that have been reported by victims, we have successfully shut down over 75 percent of them, some of them within one week of the number's being reported to us.

TIGTA is also publishing those telephone numbers that have been used by the scammers on the Internet. This provides intended victims an additional tool to help them determine if the call is part of a scam. All they have to do is type the telephone number in any search engine, and the response will indicate whether the telephone number has been identified as part of the impersonation scam. These efforts are producing results: our data show it now takes hundreds of calls to defraud one victim, whereas in the beginning of the scam it took only double digit attempts.

In addition, TIGTA is engaged in public outreach efforts to educate taxpayers

about the scam. These efforts include publishing press releases, granting television interviews, issuing public service announcements, and providing testimony to the Congress. The criminals view this scam as they do many others; it is a crime of opportunity. Unfortunately, while we plan on arresting and prosecuting more individuals, the scam will not stop until people stop paying the scammers money. Our best chance at defeating this crime is to educate people so they do not become victims in the first place. Every innocent taxpayer we protect from this crime is a victory.

ADVANCE FEE "LOTTERY WINNING" SCAMS AND PHISHING

We continue to receive reports of people who have become victims of lottery winnings scams and we are also seeing an uptick in the number of reported phishing attempts. The lottery scam is a continuation of an older scam and it starts with an unsolicited e-mail or telephone call from an impersonator to an unsuspecting victim. The caller tells the intended victim that they have won a lottery or other valuable prize, however; in order to collect the prize, the victim must send money to prepay the tax on the winnings to the IRS. The lottery scam often, but not always, originates from outside of the U.S., and it continues to be a successful crime because it capitalizes on a very common dream: getting rich quick and hitting the jackpot.

In a recent investigation, one individual was sentenced after pleading guilty to money laundering[32] and another individual was sentenced to 33 months of incarceration after pleading guilty to conspiracy to commit mail and wire fraud for their roles in a lottery scheme.[33] Overall, the scammers defrauded approximately $380,000 from at least 20 victims.[34]

In another case in the District of Nevada, on March 16, 2016, three individuals were indicted for conspiracy, mail fraud, wire fraud, and money laundering in connection with a telemarketing lottery scheme that was intended to target victims over the age of 55. Under the guise of collecting money for the Federal taxes associated with a lottery prize, the defendants and others called at least 66 victims in 22 states. The defendants caused the victims to send approximately $97,000 via MoneyGram and at least $366,000 via Western Union wire transfers. The defendants also caused victims to send at least $389,000 in fraudulently induced payments through the U.S. mail, UPS and FedEx. As a result of the scheme, the defendants

[32] N.D. Ga. Judgment Kecia Place filed Nov. 19, 2015.
[33] N.D. Ga. Amended Judgment Kenneth Kaufman filed Jan. 7, 2016.
[34] N.D. Ga. Indictment Kenneth Kaufman and Kecia Place filed Mar. 18, 2015.

and others collected over $1 million in fraudulently obtained funds from their victims.[35] Prosecution action is ongoing.

In yet another case, we were successful in having a defendant extradited from the United Kingdom for his role in a lottery scheme where he targeted and victimized a citizen in West Virginia.[36]

This year, we have also seen a resurgence of criminals using a technique called phishing to swindle and victimize taxpayers into paying money or providing financial information by tricking the victims into believing they are receiving an e-mail from the IRS. In one current version, taxpayers are receiving e-mails purporting to be from the IRS which asks the taxpayers to confirm their tax return information. This information will then more than likely be used to file fraudulent refund returns or to commit other forms of identity theft.

A new phishing scheme involves scammers sending e-mails purporting to be a business's Chief Executive or Financial Officer. These e-mails notify the employees there has been a mistake on their Form W-2, *Wage and Tax Statement*, and directs the employees to either e-mail their Form W-2 to the sender, or to provide information that was on the Form W-2 for verification. Both approaches result in the theft of the employee's identity information.

As with the other scams, the phishing scam preys on people who simply want to comply with the law and other requests. The IRS will not send e-mails to taxpayers requesting their personal or financial information. If someone receives an e-mail of this nature, they should forward it to phishing@irs.gov prior to clicking on any links that may be contained in the e-mail.

We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. As such, we plan to provide continuing audit and investigative coverage of the IRS's efforts to operate efficiently and effectively and to expand our oversight related to cybersecurity.

Chairman Roskam, Ranking Member Lewis, and Members of the Subcommittee, thank you for the opportunity to share my views.

---

[35] D. Nev. Indictment Willie Montgomery, Tanika Armstrong, and Reginald Lowe filed Mar. 16, 2016.
[36] N.D. W.Va. Indictment Davel Young filed Sep. 4, 2013.

Timothy P. Camus
Deputy Inspector General for Investigations

Mr. Timothy P. Camus has served in the Treasury Inspector General for Tax Administration (TIGTA) and the Internal Revenue Service Inspection Service, TIGTA's predecessor organization, as a Special Agent, for 25 years.

After an exemplary investigative career, Mr. Camus was promoted into TIGTA management. In June 2003, Mr. Camus became a member of the Senior Executive Service, and in January 2011, he was promoted to the position of the Deputy Inspector General for Investigations for TIGTA. As the Deputy Inspector General for Investigations, Mr. Camus is responsible for overseeing and leading all aspects of TIGTA's law enforcement mission.

During his law enforcement career, Mr. Camus has successfully investigated domestic terrorism, death threats made against public officials, bribery and extortion cases, as well as thefts of Government property and all other facets of white collar crime and fraud that impact the IRS. In 2008, Mr. Camus was awarded the Presidential Rank Award for Meritorious Service.