HEARING BEFORE THE
COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON FINANCIAL SERVICES
AND GENERAL GOVERNMENT
U.S. HOUSE OF REPRESENTATIVES

"Oversight Hearing – Internal Revenue Service"

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

May 23, 2017

Washington, D.C.

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES

"Oversight Hearing – Internal Revenue Service"
May 23, 2017

Chairman Graves, Ranking Member Quigley, and Members of the Subcommittee, thank you for the opportunity to testify on the status of the 2017 Filing Season and some of the significant challenges currently facing the Internal Revenue Service (IRS).

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 and is mandated to ensure integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. 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 the key role of ensuring that the approximately 83,000 IRS employees[1] who collected more than $3.3 trillion in tax revenue, processed more than 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2016,[2] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and abuse.

TIGTA's Office of Audit (OA) reviews all aspects of the Federal tax administration system 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 OA 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

---

[1] Total IRS staffing as of January 7, 2017. Included in the total are approximately 16,200 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2016*.
[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.).

Treasury, the Commissioner of Internal Revenue, and other key stakeholders. The OA has examined 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. The OI investigates misconduct by IRS employees which manifests itself in many ways, including extortion, theft, taxpayer abuses, false statements, financial fraud, and identity theft. The Office of Investigations places a high priority on its statutory responsibility to protect all IRS employees located in over 670 facilities nationwide. In the last several years, threats directed at the IRS have remained the second largest component of the 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 committed to ensuring the safety of IRS employees and the taxpayers who conduct business in IRS facilities. As will be discussed in more detail later in the testimony, over the past several years, the OI has been conducting an investigation of a massive IRS impersonation scam that has impacted close to 2 million people.

TIGTA's Office of Inspections and Evaluations (I&E) provides responsive, timely, and cost-effective inspections and evaluations of challenging areas within the IRS, providing TIGTA with additional flexibility and capability to produce value-added products and services to improve tax administration. The I&E's work is not a substitute for audits and investigations. In fact, its findings may result in subsequent audits and/or investigations. Inspections are intended to monitor compliance with applicable law, regulation, and/or policy; assess the effectiveness and efficiency of programs and operations; and inquire into allegations of waste, fraud, abuse, and mismanagement. Evaluations, on the other hand, are intended to provide in-depth reviews of specific management issues, policies, or programs.

FY 2018 IRS BUDGET

As of May 19, 2017, the President had not submitted the IRS's detailed FY 2018 budget to Congress. The IRS's FY 2017 appropriated funding level was set at $11.2 billion in the Consolidated Appropriations, 2017[4] which was signed by the

[4] Consolidated Appropriations Act of 2017, Pub. L. No. 115-31, div. E., tit. I,.

President on May 5, 2017. The FY 2017 funding level represents no change from the IRS's FY 2016 enacted budget of $11.2 billion. For FY 2017, the IRS had requested appropriated funds of $12.3 billion.

In addition, similar to FY 2016, the IRS's appropriated funding level for FY 2017 includes $290 million in supplemental funding specifically for the IRS to make measurable improvements in the areas of customer service, identification and prevention of refund fraud and identity theft, and cybersecurity and the safeguarding of taxpayer data.

CHALLENGES FACING THE IRS

In this section of my testimony, I will briefly discuss the status of the 2017 Filing Season and several of the key challenges now facing the IRS as it administers our Nation's tax laws.

STATUS OF THE 2017 FILING SEASON

The annual tax return filing season 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) 2017, the IRS expects to receive approximately 152 million individual income tax returns (approximately 17 million paper-filed and 134.3 million electronically-filed (e-filed)). The IRS plans to process individual income tax returns at five Wage and Investment Division Submission Processing sites[5] during the 2017 Filing Season. In addition, the IRS expects to provide assistance to millions of taxpayers via the telephone, e-mail, website, social media, and face-to-face assistance.

The IRS began accepting and processing individual tax returns on January 23, 2017, as scheduled. As of April 28, 2017, the IRS received approximately 137.5 million tax returns – 122.8 million (89.3 percent) were filed electronically and 14.7 million (10.7 percent) were filed on paper. The IRS has issued 100.1 million refunds totaling approximately $276.8 billion.

One of the continuing challenges the IRS faces each year in processing tax returns is the implementation of new tax law changes and changes resulting from

---

[5] IRS Submission Processing sites in Fresno, California; Kansas City, Missouri; and Austin, Texas, will process paper-filed and e-filed tax returns. Sites in Andover, Massachusetts, and Philadelphia, Pennsylvania, will process only e-filed tax returns.

expired tax provisions. Before the filing season begins, the IRS must identify the tax law and administrative changes affecting the upcoming filing season. Once it has identified these, the IRS must revise the various affected tax forms, instructions, and publications. 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 2017 Filing Season, tax law changes include the continued implementation of the Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act of 2010[6] (collectively referred to as the Affordable Care Act or ACA), and those provisions of the Protecting Americans from Tax Hikes Act of 2015[7] (PATH Act) specifically intended to reduce fraudulent and improper refundable credit claims. For example, these provisions modify the filing dates for income and withholding documents to January 31st.[8] The PATH Act also contains a number of provisions referred to as "program integrity provisions" that were intended to reduce fraudulent and improper payments for the Earned Income Tax Credit (EITC),[9] Child Tax Credit (CTC),[10] Additional Child Tax Credit (ACTC),[11] and American Opportunity Tax Credit (AOTC)[12]. In addition, the PATH Act includes provisions to prevent EITC, CTC, ACTC, and AOTC claims by individuals filing tax returns for years prior to when a Taxpayer Identification Number[13] was issued.

The majority of the program integrity provisions were effective January 1, 2016, and affect the processing of Tax Year (TY) 2016 returns. According to the House Committee on Ways and Means, these integrity provisions are projected to save roughly

---

[6] Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.
[7] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, Div. Q, (2015).
[8] Previously, employers who filed paper Forms W-2 were not required to file these forms until February of each year. Employers who e-file Forms W-2 had until the end of March each year to file.
[9] The EITC is used to offset the impact of Social Security taxes on low-income families and to encourage them to seek employment.
[10] A tax credit for families with dependent children that is used to reduce the individual income tax burden for families, better recognize the financial responsibilities of raising dependent children, and promote family values.
[11] The ACTC (the refundable portion of the CTC) is used to adjust the individual income tax structure to reflect a family's reduced ability to pay taxes as family size increases.
[12] A partially refundable Federal tax credit used to help parents and college students offset the costs of college.
[13] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the taxpayer, the number can be an Employer Identification Number, a Social Security Number (SSN), or an Individual Taxpayer Identification Number.

$7 billion over 10 years by reducing fraud, abuse, and improper payments in refundable credit programs.

TIGTA has multiple ongoing reviews[14] to evaluate IRS actions to implement key provisions of the PATH Act. To date, our work has found that the IRS has held refunds as required for returns with an EITC or ACTC claim and has released those returns as required if they were not identified for additional review. In addition, IRS management informed us that all EITC and ACTC claims will be verified against Forms W-2, *Wage and Tax Statement*, data to identify claims that have unsupported income. Those that are identified as potentially fraudulent will be addressed as part of the IRS's fraud prevention programs. The remaining returns with an income discrepancy will be addressed as part of the IRS's overall Questionable Refund Program. In September 2014, TIGTA identified 677,000 TY 2012 tax returns for which third-party Forms W-2 were not sent to the IRS by the employer for either the taxpayer and/or spouse listed on the tax return. These tax returns claimed EITCs totaling more than $1.7 billion.

In response to the January 20, 2017, Affordable Care Act Executive Order directing Federal agencies to exercise authority and discretion available to them to reduce potential burden on taxpayers, the IRS changed its processes and procedures on February 3, 2017. These changes will now allow electronic and paper-filed tax returns to be accepted for processing in instances in which taxpayers do not indicate their health care coverage status. At the start of the filing season, processes and procedures were developed to reject e-filed tax returns from taxpayers that did not report full-year insurance coverage, claim an exemption from coverage or self-report a Shared Responsibility Payment (SRP).[15] For those taxpayers that filed a paper tax return, the IRS would hold their tax return and correspond with the taxpayer. If the taxpayer did not respond or provide adequate documentation, the IRS would assess the SRP.

As of May 4, 2017, the IRS processed over 5 million tax returns that reported $23.9 billion in the Premium Tax Credits[16] that were either received in advance or claimed at the time of filing. As of May 4, 2017, approximately 4.1 million taxpayers

---

[14] TIGTA, Audit No. 201640031, *Implementation of Refundable Credit Integrity Provisions*, report planned for May 2017; TIGTA, Audit No. 201640023, *Individual Taxpayer Identification Number Deactivation Process*, report planned for Aug. 2017; TIGTA, Audit No. 201740005, *2017 Filing Season*, report planned for Sept. 2017; TIGTA, Audit No. 201740031, *Implementation of Refundable Credit Integrity Provisions Phase 2*, report planned for Oct. 2017.
[15] A payment based on each month that individuals or their dependents are without Minimum Essential Coverage and do not qualify for an exemption.
[16] A refundable tax credit to assist individuals and families in purchasing health insurance coverage through an Affordable Insurance Exchange.

reported a SRP, for a decrease of 27.2 percent from the prior year. However, the amount of SRPs reported increased 16.6 percent over the prior year to nearly $2.9 billion. It should be noted that, by statute, the amount of the SRP has increased in each of the prior years.[17]

As they have in past filing seasons, taxpayers have multiple options to choose from when they need assistance from the IRS, including assistance through the toll-free telephone lines,[18] 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 its trend to depend more on technology-based services and external partners by directing 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. By using this approach, the IRS believes that it is able to improve its service to taxpayers by addressing and resolving more complex matters, such as assistance to identity theft victims and people with tax account issues.

The most notable self-assistance option is the IRS's public Internet site, IRS.gov. The IRS has been actively steering taxpayers to its website as the best source for answers to their tax questions. The IRS reports 321.7 million visits to IRS.gov this filing season, as of April 29, 2017. Taxpayers can also interact with the IRS using IRS2Go, which is a mobile application that lets taxpayers access information and a limited number of IRS online tools. As of May 4, 2017, the IRS reports that the IRS2Go mobile application had 4.8 million active users. In addition, the IRS uses various forms of social media including YouTube, Twitter, Tumblr, and Facebook. As of May 4, 2017, there have been 1,555,275 new views of IRS YouTube videos and, as of May 9, 2017, a total of 140,198 Twitter followers.

During the 2017 Filing Season, the IRS has continued to increase its toll-free telephone level of assistance. As of April 29, 2017, taxpayers made approximately 53.9 million total attempts to contact the IRS seeking help to understand the tax law and meet their tax obligations. Of the 53.9 million total attempts reported by the IRS,

---

[17] The maximum Shared Responsibility Payment increased significantly from TY 2015 to TY 2016 and will continue to increase as the payment is indexed for inflation. For example, the family maximum increased from $975 in TY 2015 to $2,085 in TY 2016.
[18] The IRS refers to the suite of 29 telephone lines to which taxpayers can make calls as "Customer Account Services Toll-Free."

38.8 million net attempts[19] were made by taxpayers to contact the IRS by calling the various customer service toll-free telephone assistance lines. The IRS reports that 18.9 million calls had been answered with automation, and telephone assistors had answered over 10.4 million calls and provided a 79 percent Level of Service[20] with a 6.7 minute Average Speed of Answer. The Level of Service for the 2016 Filing Season was 72 percent. The IRS forecasts a 75 percent Level of Service for the 2017 Filing Season.

Besides telephone assistance, each year many taxpayers also seek assistance from one of the IRS's 376 TAC walk-in offices. Although the IRS reports that it has 376 TACs for the 2017 Filing Season, 24 TACs are not open because they have not been staffed. The IRS estimates that the number of taxpayers it will assist at its TACs will continue to decrease this fiscal year. The IRS plans to assist approximately 3.4 million taxpayers at the TACs in FY 2017, which represents an approximately 23.6 percent decrease from FY 2016. The IRS indicated that budget cuts and its strategy of appointment service at the TACs, along with continued promotion of alternative service options, will result in the reduction of the number of employees available to assist taxpayers at the TACs.

However, the IRS has implemented initiatives in an effort 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 April 29, 2017,[21] IRS employees answered over 2.1 million calls from taxpayers seeking to make an appointment, resulting in approximately 945,000 that necessitated an appointment. The IRS notes that taxpayers that travel to a TAC without an appointment are assisted if there is availability. As of April 29, 2017, the IRS reported that they provided a walk-in exception to the requirement for an appointment to nearly 264,000 taxpayers.

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 2017 Filing Season, the IRS is offering Virtual Service Delivery at 28 partner site locations, which is a decrease from the previous year when this service was offered at

[19] Total call attempts represent calls received during open and after hours. Total net call attempts represent calls received during open hours.
[20] The primary measure of service to taxpayers. It is the relative success rate of taxpayers who call for live assistance on the IRS's toll-free telephone lines.
[21] For FY 2017 – October 1, 2016, through April 29, 2017.

35 locations.[22] The IRS reports that as of April 29, 2017,[23] 1,673 taxpayers have used the service. Finally, the IRS has an initiative to co-locate staff with the Social Security Administration to better assist taxpayers. For the 2017 Filing Season, the IRS has placed employees in four Social Security Administration locations. TIGTA is planning a follow-up audit to assess the IRS's efforts to expand customer service options to taxpayers seeking face-to-face assistance.

Finally, for the 2017 Filing Season the IRS has transitioned fraud detection and selection capabilities from the Electronic Fraud Detection System (EFDS) to the Return Review Program (RRP). The IRS states that the RRP provides new and improved capabilities in its fraud detection and prevention processes. The RRP has real-time filtering capabilities and is designed to improve the IRS's ability to detect, resolve, and prevent fraud. It should be noted that the IRS did not fully retire the EFDS, as it continues to use the EFDS case management functionality because the RRP does not have this capability. We have an ongoing review to ensure that the EFDS fraud detection capabilities were incorporated into the RRP.[24]

SECURITY OVER TAXPAYER DATA

As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS. According to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, Federal agencies reported 77,183 cyberattacks in FY 2015, an increase of approximately 10 percent from FY 2014.[25] The increasing number of data breaches in the private and public sectors means more personally identifying information than ever before is available to unscrupulous individuals.

Much of the data is detailed enough to enable circumvention of most authentication processes. Therefore, it is critical that the methods the IRS uses to authenticate individuals' identities promote a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them. In March 2017, the IRS announced that it was deactivating its online Data Retrieval Tool due to privacy concerns and to protect sensitive taxpayer data. The

---

[22] For the 2017 Filing Season, the IRS is no longer offering Virtual Service Delivery at IRS locations. Access to this service is only available through external partner locations.
[23] For FY 2017 – October 1, 2016, through April 29, 2017.
[24] TIGTA, Audit No. 201740029, *Processing Year 2017 Fraud Detection Activities*, report planned for Jan. 2018.
[25] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Modernization Act* (Mar. 2016).

online Data Retrieval Tool allows students and parents to access their adjusted gross income (AGI) information from the IRS to complete the Free Application for Federal Student Aid (FAFSA) by transferring the data directly into their FAFSA application form from the IRS web site. Identity thieves may have used personal information of individuals which they obtained outside the tax system to start the FAFSA application process form in an attempt to secure the AGI tax information through the Data Retrieval Tool. TIGTA is conducting a joint investigation of this exploitation with IRS Criminal Investigation and the Department of Education Inspector General. In addition, TIGTA is planning to initiate an audit to review this issue.

As we have reported, the risk of unauthorized access to tax accounts will continue to be significant as the IRS proceeds with its Future State initiative[26] and focuses its efforts on delivering online tools to taxpayers. 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. 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. By using this approach, the IRS believes that it is able to improve its service to taxpayers by addressing and resolving more complex matters such as assistance to identity theft victims and people with tax account issues.

TIGTA reported in November 2015 that the IRS had not established effective authentication processes and procedures for its online services.[27] As such, the level of authentication that the IRS used for its various services was not consistent, increasing the risk of unscrupulous individuals accessing and obtaining personal taxpayer information and/or defrauding the tax system. This was one of the main factors in the Get Transcript incident, in which hundreds of thousands of accounts were accessed by unauthorized users.

We also reported in November 2015 that the IRS did not complete the required authentication risk assessment for its Identity Protection Personal Identification Numbers (IP PIN)[28] application. In addition, on January 8, 2016, we recommended that

---

[26] Preparing the IRS to adapt to the changing needs of taxpayers is described generally as the IRS Future State initiative. A key part of this effort is for taxpayers to have a more complete online experience for their IRS interactions.

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

[28] An IP PIN is a six-digit number assigned to taxpayers that allows their tax returns/refunds to be processed without delay and helps prevent the misuse of their SSNs to file fraudulent Federal income tax returns.

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 unscrupulous individuals to breach the Get Transcript application. However, the IRS reactivated the application on January 19, 2016. We issued a second recommendation to the IRS on February 24, 2016, advising it to remove the IP PIN application from its public website.

In March 2017, we reported that, in addition to not completing the required risk assessment when the IP PIN application was brought online, the IRS also did not complete a sufficient risk assessment for the IP PIN application after discovering this application had been breached by unauthorized individuals.[29] The National Institute of Standards and Technology requires organizations, including the IRS, to complete an authentication risk assessment after it identifies a system security breach to mitigate the risks of known security vulnerabilities. The authentication risk assessment should be documented and include identified weaknesses, risks arising from the weaknesses, mitigation actions considered, and costs and resources required for the mitigation actions. Had the IRS conducted this required risk assessment, it may have concluded that the risk to victims and the IRS of having their IP PINs compromised warranted taking the application offline until authentication processes and procedures could be strengthened.

In response to TIGTA recommendations, the IRS has undertaken a number of steps to provide for more secure authentication, including strengthening application and network controls.[30] However, we continue to have concerns about the IRS's logging and monitoring abilities over all connections to IRS online systems. We are currently assessing the IRS's efforts to improve its authentication. This includes evaluating whether the IRS has properly implemented secure eAuthentication in accordance with Federal standards for public access to IRS online systems and has effectively resolved identified control weaknesses. We expect to issue the final report in September 2017.

Protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS. The IRS relies extensively on its computer systems to support both its financial and mission-related operations. These computer systems collect and process extensive amounts of taxpayer data.

---

[29] TIGTA, Ref. No. 2017-40-026, *Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers* (Mar. 2017).
[30] TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).

DETECTION AND PREVENTION OF IDENTITY THEFT

Identity-theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number to file a fraudulent tax return. Unscrupulous individuals steal identities for use in submitting tax returns with false income and withholding documents to the IRS for the sole purpose of receiving a fraudulent tax refund. Identity-theft tax refund fraud affects both individuals and businesses.

Since May 2012, my office has issued a number of reports that address the IRS's efforts to detect and prevent the filing of fraudulent individual and business tax returns by identity thieves, as well as the IRS's efforts to assist victims. In July 2012,[31] TIGTA issued its first report on our assessment of IRS efforts to detect and prevent fraudulent tax refunds resulting from identity theft. We reported that the impact of identity theft on tax administration is significantly greater than the amount that the IRS detects and prevents. For example, our analysis of TY 2010 tax returns identified approximately 1.5 million undetected individual tax returns that had the characteristics of identity theft confirmed by the IRS, with potentially fraudulent tax refunds totaling in excess of $5.2 billion.

Our ongoing audit work shows that the IRS is making progress in detecting and resolving identity-theft issues and providing victim assistance. We have continued to perform follow-up reviews evaluating the IRS's efforts to improve detection processes, including its implementation of TIGTA recommendations. Most recently, we reported in February 2017 that IRS efforts are resulting in improved detection of identity-theft individual tax returns at the time returns are processed and before fraudulent tax refunds are released.[32] For example, the IRS reported in its October 2016 Identity Theft Taxonomy Analysis that, for TY 2014, it had detected and prevented approximately $12 billion in identity-theft refund fraud.

For the 2017 Filing Season, the IRS is using 197 identity-theft filters to identify potentially fraudulent individual tax returns and prevent the issuance of fraudulent tax refunds. These filters incorporate criteria based on characteristics of confirmed identity-theft tax returns, including characteristics such as amounts claimed for income and withholding, filing requirements, prisoner status, taxpayer age, and filing history. Tax returns identified by these filters are held during processing until the IRS can verify

---

[31] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).
[32] TIGTA, Ref. No. 2017-40-017, *Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvements* (Feb. 2017).

the taxpayer's identity. The IRS attempts to contact the individual who filed the tax return and, if the individual's identity cannot be confirmed, the IRS removes the tax return from processing. This prevents the issuance of many fraudulent tax refunds. As of April 29, 2017, the IRS reported that it had identified and confirmed 75,797 fraudulent tax returns and prevented the issuance of $581.6 million in fraudulent tax refunds as a result of the identity-theft filters.

To prevent fraudulent tax returns from entering the tax processing system, the IRS continues to expand its processes to reject e-filed tax returns and prevent paper tax returns from posting. For example, as of April 17, 2017, the IRS locked approximately 33.5 million taxpayer accounts of deceased individuals. The locking of a tax account results in the rejection of an e-filed tax return and the prevention of a paper-filed tax return from posting to the Master File if the Social Security Number (SSN) associated with a locked tax account is used to file a tax return. According to the IRS, as of March 31, 2017, it had rejected 17,461 fraudulent e-filed tax returns and, as of May 4, 2017, it had stopped 4,672 paper-filed tax returns from posting to the Master File.

In addition, in response to concerns raised by TIGTA regarding multiple refunds going to the same address or bank account, the IRS now uses a clustering filter tool to group tax returns based on characteristics that include address, zip code, and bank routing numbers. For the tax returns identified, the IRS uses criteria designed to ensure that legitimate taxpayers are not included. Tax returns identified are withheld from processing until the IRS can verify the taxpayer's identity. As of May 4, 2017, the IRS reports that, using this tool, it has identified 93,633 tax returns and prevented the issuance of approximately $449.9 million in fraudulent tax refunds.

The IRS recognizes that new identity-theft patterns are constantly evolving and that, as a result, it needs to continuously adapt its detection and prevention processes. These evolving identity-theft patterns affect not only individuals, but also businesses. The IRS defines business identity theft as creating, using, or attempting to use a business's identifying information without authority, in order to claim tax benefits. For example, in order to obtain a fraudulent refund, an identity thief files a business tax return (*e.g.*, Form 1120, *U.S. Corporation Income Tax Return*, Form 720, *Quarterly Federal Excise Tax Return,* or Form 941, *Employer's QUARTERLY Federal Tax Return*) using the Employer Identification Number (EIN)[33] of an active or inactive business without the permission or knowledge of the EIN's owner. As another example, an identity thief applies for and obtains an EIN using the name and SSN of another individual as the responsible party (*i.e.*, fraudulently obtained EIN), without that individual's approval or knowledge, and uses it to create fictitious Forms W-2 and bogus Forms 1040, *U.S. Individual Income Tax Return*, which the thief then files to claim a fraudulent refund.

In September 2015, we reported that the IRS recognized the growing threat of business-related identity theft and, in response, was implementing processes to detect identity theft on business returns at the time tax returns are processed.[34] These efforts included conducting a *Business Identity Theft Project* to detect potential business identity theft relating to the filing of Forms 1120 reporting overpayments and claiming refundable credits.

However, TIGTA also found that the IRS is not using data that it has readily available to proactively identify potential business identity theft. For example, the IRS maintains a cumulative list of suspicious EINs that it has determined to be associated with fictitious businesses. In response to TIGTA's recommendations, the IRS is expanding its filters to identify business identity theft. For the 2017 Filing Season, the IRS is using 25 identity-theft filters to identify potentially fraudulent business tax returns and prevent the issuance of fraudulent tax refunds. TIGTA is planning a follow-up audit to assess the IRS's efforts to expand on its processes and procedures to detect business identity theft.

While the IRS's identification and detection strategies have led to many notable improvements, it recognizes the need to continue to explore other initiatives that would assist with its overall detection and prevention efforts. These initiatives include a collaborative effort among IRS officials, representatives from leading tax preparation firms, software developers, payroll and tax financial product processors, and representatives from the State Departments of Revenue to discuss common challenges and ways to leverage collective resources and efforts for identity theft detection and prevention. Additionally, the IRS obtains leads about potential identify-theft tax returns from State tax agencies via its State Suspicious Filer Exchange Initiative, and is

---

[33] An EIN is a Federal Tax Identification Number used to identify a taxpayer's business account. The EIN is a nine-digit number (in the format of xx-xxxxxxx) assigned by the IRS and used by employers, sole proprietors, corporations, partnerships, nonprofit associations, trusts and estates, government agencies, certain individuals, and other types of businesses.

[34] TIGTA Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).

conducting a pilot initiative with select payroll providers to test the feasibility of using a verification code to authenticate Form W-2 data at the time tax returns are processed.

IRS ASSISTANCE TO VICTIMS OF IDENTITY THEFT

Tax-related identity theft adversely affects the ability of innocent taxpayers to file their tax returns and timely receive their tax refunds, often imposing significant financial and emotional hardships. Many taxpayers learn that they are a victim of tax-related identity theft when they attempt to file their electronic tax return and the IRS rejects it because someone else (an identity thief) has already filed a return using the same SSN. Individuals can also learn that they are victims of employment-related identity theft if they receive a notification from the IRS of an income discrepancy between the amounts reported on their tax returns and the amounts employers reported to the IRS. This can occur when an innocent taxpayer's stolen identity is used by someone else to gain employment. It can cause a significant burden, due to the incorrect computation of taxes and Social Security benefits based on income that does not belong to the taxpayer.

TIGTA has reported that the IRS does not always effectively provide assistance to taxpayers who report that they have been victims of identity theft, which causes increased burden for those victims. Specifically, TIGTA reviews have identified long delays in case resolution and account errors, and have found that not all tax-related identity-theft victims receive IP PINs. For example, in March 2015,[35] we reported that victims continue to experience long delays while waiting for the IRS to resolve their cases and issue their refunds. Our report also found that IRS employees did not correctly resolve taxpayer accounts, resulting in a delayed issuance of refunds to some victims or in some victims receiving an incorrect refund amount.

In July 2015, the IRS created the Identity Theft Victim Assistance (IDTVA) Directorate to combine into one directorate the skills of employees working tax-related identity-theft cases in multiple functions. The goal is to improve the taxpayer's experience when working with the IRS to resolve his or her tax-related identity-theft case. Approximately 1,300 employees work in the IDTVA Directorate to resolve identity-theft cases. TIGTA's current review[36] of cases closed from August 1, 2015, through May 25, 2016, identified improvements in case-closure timeframes and a

---

[35] TIGTA, Ref. No. 2015-40-024, *Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds* (Mar. 2015).
[36] TIGTA, Audit No. 201640015, *Identity Theft Victim Assistance Directorate*, report scheduled for May 2017.

reduction in case closing errors in comparison to our prior audit completed before the IDTVA Directorate was created. The IRS's efforts to centralize operations under a unified leadership, along with its enhanced procedures and processes, have contributed to the improvements identified since our prior audit. We plan to issue our final report in May 2017.

To provide relief to tax-related identity-theft victims, the IRS began issuing IP PINs to eligible taxpayers in FY 2011. For Processing Year 2016, the IRS issued more than 2.7 million IP PINs to taxpayers for use in filing their tax returns. In March 2017, TIGTA reported that some process improvements are needed.[37] Specifically, TIGTA found that taxpayer accounts were not always consistently updated to ensure that IP PINs were generated for taxpayers as required. For example, the IRS did not generate IP PINs for more than 2 million taxpayers for whom the IRS resolved an identity-theft case by confirming that the taxpayer was a victim.

This results from inconsistent processes and procedures between the different functional areas when closing resolved identity-theft cases. These inconsistent procedures will create burden for the 2 million taxpayers who do not have the marker on their account. For example, while these individuals do not have a marker that will result in the generation of an IP PIN, they do have an identity theft indicator on their tax account because they are a confirmed victim of identity theft. As such, the IRS will identify future filings by the legitimate taxpayer as a potential identify theft return which will result in delays while the IRS manually reviews and processes their returns.

In August 2016, we reported that, during the period February 2011 to December 2015, the IRS identified almost 1.1 million taxpayers who were victims of employment-related identity theft, but were not notified of that fact.[38] During this audit, the IRS announced that it would begin notifying newly identified victims of employment identity theft in January 2017. The notification letter describes steps the taxpayers could take to prevent further misuse of their personal information, including reviewing their earnings with the Social Security Administration to ensure that their records are correct. Because this letter provides victims with useful information and assistance, we recommended the IRS issue it to all victims, including those whose identity was stolen prior to January 2017. However, the IRS responded that, after the first year of its new systemic notification process, it will evaluate the results and determine an appropriate

[37] TIGTA, Ref. No. 2017-40-026, *Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers* (Mar. 2017).
[38] TIGTA, Ref. No. 2016-40-065, *Processes Are Not Sufficient to Assist Victims of Employment-Related Identity Theft* (Aug. 2016).

course of action with respect to the previously identified potential victims. TIGTA is currently conducting a review to assess the IRS's actions to notify victims of identity theft, and we plan to issue our draft report in November 2017.[39]

We have an ongoing audit that is evaluating the IRS's processes to identify and mark victims' tax accounts and to notify the Social Security Administration to ensure that individuals' Social Security benefits are not affected by others who are misusing their identities to gain employment.[40] Our audit has identified that the number of employment-related identity theft victims is significantly greater than identified. For example, IRS processes do not identify employment identity theft when processing paper tax returns. TIGTA reviewed a statistically valid sample of 292 paper tax returns filed in Processing Year 2015 by individuals with an Individual Taxpayer Identification Number (ITIN).[41] These tax return filers reported wages on 150 (51.4 percent) of the returns and attached Form W-2, *Wage and Income Statement*, indicating they used someone's SSN to gain employment. As a result, TIGTA projects that the IRS did not identify 272,416 victims of employment identity theft for the 685,737 paper tax returns filed by ITIN holders reporting wages in Processing Year 2015. In addition, IRS does not have a process to notify the Social Security Administration of employment identity theft when both the victim's name and SSN are used by another person to gain employment. TIGTA expects to issue its report in May 2017.

TELEPHONE IMPERSONATION SCAM

Since the fall of 2013, a significant amount of our Office of Investigations' workload has consisted of investigating a telephone impersonation scam in which more than 1.9 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 10,300 victims have reported that they paid more than $55 million to these criminals.

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 have cemented its status as the largest,

---

[39] TIGTA, Audit No. 201740033, *Notification Letters to Victims of Employment Identity Theft*, report scheduled for November 2017.
[40] TIGTA, Audit No. 201640028, *Employment Related Identity Theft – Returns Processing*, report scheduled for May 2017.
[41] In Calendar Year 1996, the IRS created the ITIN to provide Taxpayer Identification Numbers, when needed for tax purposes, to individuals who do not have and are not eligible to obtain an SSN.

most pervasive impersonation scam in the history of our agency. It has claimed victims in every State.

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 IRS 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 United States, when in fact they may be originating from a call center located in India.

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, these scammers then demanded that the victims immediately pay the money using Apple iTunes® gift cards, Target gift cards, 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.

TIGTA has made several arrests in connection with this scam and has numerous investigations underway. In July 2015, in one of the largest prosecutions on this scam that we have had to date, an individual pled guilty to organizing an impersonation scam ring. He was sentenced to over 14 years of incarceration and ordered to forfeit $1 million. In October of 2016, after an extensive three-year investigation, TIGTA, the Department of Justice and the Department of Homeland Security announced the indictment of 56 individuals and five call centers located in India. Although the investigations and prosecutions have reduced by over 90 percent the number of scam calls being placed, we are still receiving reports that between 5,000 and 10,000 people are receiving calls each week.

In addition to the criminal prosecutions, to thwart scammers using robo-dialers, we have created and instituted an "Advise and Disrupt" strategy. The strategy involves cataloguing the telephone numbers that have been 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. Utilizing this technique, we have placed more than 142,000 automated calls back to the scammers. We are also working with the telephone companies to have the scammers' telephone numbers shut down as soon as possible. Of the 1,160 telephone numbers that have been reported by victims, we have successfully shut down 94 percent of them, some of them within one week of the numbers having been reported to us.

TIGTA is also publishing those scam-related telephone numbers 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 that it now takes hundreds of calls to defraud one victim, whereas in the beginning of the scam it took only a double-digit number of attempts.

Further, 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 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.

PRIVATE DEBT COLLECTION

In 2015, a law was enacted that mandated the IRS's use of private collection agencies (PCAs) to collect certain "inactive receivables."[42] Certain inventories were specifically excluded from the definition of inactive receivables.[43] TIGTA initiated an

---

[42] Fixing America's Surface Transportation Act, Pub. L. No. 114-94, Div. C, Title XXXII, § 32102,129 Stat. 1312, 1733-36 (2015), codified in Internal Revenue Code (I.R.C.) Section (§) 6306. The term "inactive receivables" means: receivables removed from active inventory due to inability to locate the taxpayer, inventory in which one-third of the collection statute of limitations has expired, or assigned inventory in which more than 365 days have passed since contact with the taxpayer occurred.

[43] I.R.C. § 6306(d) excludes inventory that is: subject to a pending or active offer-in-compromise or installment agreement; is classified as an innocent spouse case; or involves a taxpayer identified

audit soon after the enactment of the legislation to evaluate the IRS's establishment of policies, procedures, and other infrastructure necessary to operate this program, as well as to assess the IRS's efforts to mitigate risks to the program.[44] We have identified numerous concerns during our audit, including the IRS's lack of commitment to assist taxpayers concerned that the PCAs are part of an impersonation scam, as well as our concerns related to the IRS's process for receiving taxpayer complaints about PCAs. In addition, TIGTA is planning a future audit related to the operations of the program, as well as a review evaluating the PCA contractors' performance.

Further, TIGTA's Office of Investigations provided the IRS with insight on how the widespread IRS impersonation scam might impact the Private Debt Collection program. Specifically, based on what TIGTA learned during its investigation of the impersonation scam, the Office of Investigations provided the IRS with different ways it could consider notifying taxpayers about the program and that their accounts have been assigned to the PCAs. In addition, the Office of Investigations has provided integrity and safety briefings to the PCAs' employees. TIGTA will closely monitor incoming impersonation complaints involving the PCAs, and we will work to take appropriate action and notify the IRS, the PCAs and the public if we identify an impersonation scheme growing within the Private Debt Collection program.

We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. Accordingly, we plan to provide continuing audit coverage of the IRS's efforts to operate efficiently and effectively and to investigate any instances of IRS employee misconduct.

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

---

as deceased, under the age of 18, in a designated combat zone, a victim of tax-related identity theft, is currently under examination, litigation, criminal investigation, or levy, or is currently subject to a proper exercise of a right of appeal.

[44] TIGTA, Audit No. 201630029, *Planning and Implementation of the IRS's Private Debt Collection Program*, report scheduled for September 2017.

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 and 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.

Mr. George also served as a member of the Integrity Committee of the Council of Inspectors General for Integrity and Efficiency (CIGIE). CIGIE is an independent entity within the executive branch, statutorily established by the Inspector General Act, as amended, to address integrity, economy, and effectiveness issues that transcend individual Government agencies and to increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General. The CIGIE Integrity Committee serves as an independent review and investigative mechanism for allegations of wrongdoing brought against Inspectors General.