Congress of the United States
U.S. House of Representatives
Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515–0315

To: Members, Committee on Small Business
From: Committee Staff
Date: April 4, 2017
Re: Hearing: "Scam Spotting: Can the IRS Effectively Protect Small Business Information?"

On Thursday, April 6, 2017, at 10:00 a.m. in Room 2360 of the Rayburn House Office Building, the Committee on Small Business will meet with the Treasury Inspector General for Tax Administration (TIGTA) to examine the IRS' performance with regard to protecting small businesses from tax identity theft and fraudulent tax filings.

As tax filing season heats up, so does fraud season at the IRS. Identity theft and fraudulent tax returns have been a growing problem for individuals and small businesses alike. The TIGTA is charged with overseeing the IRS in the conduct of its job to ensure the integrity of the tax collection system, including protecting taxpayers from identity theft, putting systems into place to identify fraudulent returns, and ensuring quality customer service. The Committee will meet with the current Inspector General to discuss the findings of their recent audits of the IRS' performance in addressing these issues.

I. Introduction

The Treasury Inspector General for Tax Administration was created by the IRS Restructuring and Reform Act of 1998.[1] The TIGTA's mandate is to oversee the IRS and promote the integrity of the U.S. tax system by providing independent audit and investigative services.[2] The TIGTA's audit activities are designed to objectively evaluate the IRS' performance, focusing on systemic inefficiencies and weaknesses in tax administration.[3] Its resulting recommendations are intended to ensure effective, efficient tax administration, minimizing the risks of waste, fraud, and abuse.[4]

As identity theft grows and evolves, it is important to note that identity theft not only affects individuals, it can also affect businesses.[5] The IRS defines business identity theft as "creating,

---

[1] Pub. L. No. 105–206, 112 Stat. 685 (July 22, 1998).
[2] *Examining the IRS's Customer Service Challenges: Joint Hearing before the Subcomm. on Health Care, Benefits, and Admin. Rules and Subcomm. on Gov't Operations of the House Comm. on Oversight and Gov't Reform*, 115th Cong., 1st Sess. 1 (2017) (testimony of Russell P. Martin, Assistant Inspector General for Audit, TIGTA).
[3] *Id.*
[4] *Id.*
[5] TREAS. INSP. GEN. FOR TAX ADMIN., 2015-40-082, PROCESSES ARE BEING ESTABLISHED TO DETECT BUSINESS IDENTITY THEFT; HOWEVER, ADDITIONAL ACTIONS CAN HELP IMPROVE DETECTION 1 (2015).

using, or attempting to use businesses' identifying information without authority to obtain tax benefits."[6] In the context of small businesses, individual identity theft is also relevant, since approximately 95 percent of small businesses are organized as pass-through entities, which means that the business' income and expenses run directly through to the taxpayer's personal tax return.

The IRS has been battling the issues of tax identity theft and fraudulent filings with varying degrees of success. The TIGTA has audited their processes and results, and the Committee hearing will feature the current Inspector General, J. Russell George, who will discuss the findings of their recent investigations and their recommendations for continued improvement.

II. Processes to Detect Business Identity Theft

In November of 2014, the IRS Advisory Council (IRSAC) observed that business identity theft can be more complex than individual identity theft.[7] They cited the fact that individual identity theft generally involves filing one fraudulent return at a time, but there are more options in the realm of business identity theft.[8] Larger refunds can be obtained on business entity tax returns because of the availability of refundable business tax credits.[9] Plus, fraudulent W-2 forms may be filed with fictitious withholding that will be later claimed as a refund through a subsequent fraudulent individual income tax return.[10] These potentially larger pay-offs are giving rise to an increase in business identity theft.[11] The IRSAC made several recommendations to head off business identity theft, which were met with mixed reception by the IRS.[12] The TIGTA audit report noted the IRSAC recommendations prior to moving on to its own review.

Both individual and business identity theft are constantly evolving, and the IRS must continuously adapt its detection and prevention processes to keep up.[13] The IRS had taken the following steps as of the TIGTA's September 2015 audit report:

- Defined business identity theft.
- Implemented internal procedures to follow when IRS employees become aware of potential identity theft.
- Created Form 14039-B to collect information to determine whether a business' identity has been stolen.
- Conducted a Business Identity Theft Project aimed at detecting business identity theft based on overpayments reported on Form 1120 and claiming refundable credits.[14]

In addition, the IRS maintains a database of suspicious employer identification numbers (EINs), which basically means that the business associated with the EIN has been determined to be

[6] *Id*.
[7] *Id*. at 2.
[8] *Id*.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *Id*. at 3.
[13] *Id*. at 5.
[14] *Id*.

fictitious.[15] The TIGTA's analysis of the business returns filed during the 2014 tax season identified 233 returns using a suspicious EIN, 97 of which claimed refunds totaling over $2.5 million.[16] The IRS put programming into place as of July 2016 to better match database entries against filed returns.[17] This system, in conjunction with other processing filters, would greatly increase the IRS' ability to proactively ensure the legitimacy of business filings.[18]

The IRS also maintains information-sharing agreements with a number of states in order to exchange suspicious filer information.[19] However, these agreements cover only individual return information.[20] These programs have been successful, enabling the IRS to identify 2,600 questionable returns totaling $16 million in refunds, claimed just from calendar year 2014 referrals from 19 states.[21] The TIGTA recommended expanding this program to also identify potentially fraudulent business tax return filings.[22]

Finally, the IRS needs to do a better job of public outreach. The TIGTA found that the IRS was providing only minimal information to businesses to let them know how to identify potential identity theft, how to prevent it, and what to do if it happens to them.[23] The IRS responded to this criticism by adding information to its website to assist practitioners who spot potential identity theft.[24] However, not all businesses use tax practitioners, particularly small businesses, and information aimed directly at these taxpayers should be provided as well.[25]

III. Processes to Identify Individual Identity Theft

Tax identity theft is defined as an individual using another person's name and Taxpayer Identification Number (usually a Social Security Number) to file a fraudulent tax return for the sole purpose of receiving a fraudulent tax refund.[26] The IRS is using a variety of detection systems to identify potentially fraudulent tax returns, and its success is steadily improving.[27] However, its efforts to quantify identity theft are substantially lacking, and the impact of identity theft on tax administration is significantly greater than IRS estimates.[28] The IRS implemented an Identify Theft Taxonomy research project to:

- Provide the IRS with a quantifiable measure of overall identity theft detection and prevention efforts; and

---

[15] *Id*. at 6.
[16] *Id*.
[17] *Id*.
[18] *Id*. at 8.
[19] *Id*.
[20] *Id*.
[21] *Id*. at 9.
[22] *Id*. at 10.
[23] *Id*.
[24] *Id*. at 11.
[25] *Id*.
[26] TREAS. INSP. GEN. FOR TAX ADMIN., 2017-40-017, EFFORTS CONTINUE TO RESULT IN IMPROVED IDENTIFICATION OF FRAUDULENT TAX RETURNS INVOLVING IDENTITY THEFT; HOWEVER ACCURACY OF MEASURES NEEDS IMPROVEMENT 1 (2017).
[27] *Id*.
[28] *Id*.

- Identify and quantify identity theft not caught by its filters.[29]

The initial report was published on September 15, 2014, and it is annually updated.[30]

The initial report found that the IRS prevented between $22 billion and $24 billion in fraudulent refunds from being issued during the 2013 filing season.[31] However, identity thieves were still successful in receiving around $5.75 billion in fraudulent refunds.[32] While the IRS' methodology is a reasonable one to identify and quantify both successful and unsuccessful identity theft, the accuracy needs improvement.[33] For example, the IRS is using estimates where actual numbers are available, assuming an average refund amount even for returns with a balance due or zero balance, and engaging in various instances of double-counting.[34] The IRS is modifying its methodology to address these concerns.[35]

The IRS is continuing to adapt its strategies and identity thieves become ever more sophisticated.[36] Two examples of new initiatives to assist in detection and prevention efforts are:

- Earlier access to Forms W-2; and
- Exchanging information with state tax agencies.[37]

The TIGTA reported in its July 2012 audit that "access to third-party income and withholding information at the time tax returns are processed is the single most important tool that the IRS needed to further its efforts to identify and prevent tax refund fraud."[38] The TIGTA has also found that "false reporting of wages and withholding continues to account for the largest amount of undetected potentially fraudulent tax returns."[39] Until this year, the IRS did not have timely access to third-party income and withholding information. Previously, information returns were required to be filed with the Social Security Administration by March 31 of the following year, so the IRS did not get access to this information until well after tax filing season had begun.[40] However, the Consolidated Appropriations Act of 2016, enacted on December 18, 2015, now requires employers to submit this information by January 31 of the following year.[41] The IRS should now be able to significantly reduce the number of potentially fraudulent tax returns processed for refund by comparing Form W-2 information to the return at the time of processing.[42] Equally important, the IRS should also be able to exclude more returns from identity theft treatment in cases where this information matches.[43]

---

[29] *Id*. at 1-2.
[30] *Id*.
[31] *Id*. at 2.
[32] *Id*.
[33] *Id*. at 10.
[34] *Id*. at 10-13.
[35] *Id*. at 13.
[36] *Id*. at 5.
[37] *Id*. at 5-6.
[38] *Id*. at 3.
[39] *Id*. at 7.
[40] *Id*.
[41] *Id*.
[42] *Id*.
[43] *Id*. at 5.

Cooperation with states, as mentioned above, is another very useful tool. The IRS piloted the State Suspicious Filer Exchange in 2013, through which states provide information to the IRS with regard to potential and confirmed identity theft, suspect tax return preparers, and other fraudulent activity identified by the state during its processing of returns.[44] Unfortunately, information is only as good as one's ability to use it, and the IRS has not been processing these leads fast enough to use the data for the current filing season.[45] The IRS responded to this flaw in its system by implementing new programming on January 8, 2017, that allows it to consider this data in a more timely fashion.[46]

IV. Processes to Address and Prevent Identity Theft

In an effort to help tax identity theft victims, the IRS began issuing Identity Protection Personal Identification Numbers (IP PINs) in Fiscal Year 2011.[47] This six-digit number helps taxpayers in two ways. First, it allows the taxpayer's tax returns and refunds to be processed without delay.[48] Second, it helps prevent future misuse of the taxpayer's Social Security Number to file additional fraudulent tax returns.[49] The IRS issues a new IP PIN to affected taxpayers before each filing season to confirm the taxpayer's identity on the tax return, whether electronic or paper.[50] In addition to offering IP PINs to taxpayers already affected by tax identity theft, the IRS also proactively offers them to taxpayers who are at risk, e.g., if a taxpayer reports a lost or stolen wallet.[51]

Unfortunately, implementation of the IP PIN program is characterized by several problems. First, the IRS did not complete an authentication risk assessment when the program was first brought online.[52] While recognizing that multifactor authentication should be used for the IP PIN application, the IRS was concerned that such a system would further burden identity theft victims, so they instead implemented a single-factor authentication.[53] On May 17, 2015, it was discovered that the system had been breached by unauthorized individuals.[54] Despite numerous warnings, the IRS allowed the application to remain active after the breach was discovered.[55] It was not taken offline until November 21, 2015, for system maintenance.[56] When the system was brought back online on January 19, 2016, the IRS did implement additional procedures to mitigate IP PIN authentication risks.[57] Unfortunately, these were enough to protect taxpayers. The IRS was alerted to the problem and urged by the TIGTA to take the application offline in February 2016, but it was

[44] *Id*. at 6.
[45] *Id*. at 9.
[46] *Id*. at 10.
[47] TREAS. INSP. GEN. FOR TAX ADMIN., 2017-40-026, INCONSISTENT PROCESSES AND PROCEDURES RESULT IN MANY VICTIMS OF IDENTITY THEFT NOT RECEIVING IDENTITY PROTECTION PERSONAL IDENTIFICATION NUMBERS 1 (2017).
[48] *Id*.
[49] *Id*.
[50] *Id*.
[51] *Id*. at 2.
[52] *Id*. at 4.
[53] *Id*.
[54] *Id*.
[55] *Id*.
[56] *Id*.
[57] *Id*. at 5.

not actually deactivated until March 7, 2016.[58] The TIGTA reviewed the potential effect of the IRS' delay and found that of the 100,463 tax returns with an IP PIN claiming a refund, 23,991 (24 percent) were potentially fraudulent.[59] The IRS improved the security of the IP PIN application, including multifactor authentication, and brought the application back online on July 19, 2016.[60]

A second problem is that not all victims of identity theft were issued an IP PIN.[61] This resulted from inconsistent guidance within the IRS based on whether the tax identity theft case was resolved by the Identity Theft Victim Assistance Directorate or the Taxpayer Protection Program.[62] The IRS was made aware of the inconsistent instructions and is establishing a standard process across functional units.[63]

Finally, taxpayers that were issued IP PINs were provided erroneous instructions by the IRS.[64] The IRS mailed approximately 2.7 million notices for 2016 incorrectly instructing them not to use their IP PIN if being claimed as a dependent on a tax return.[65] Of 1.4 million rejected tax returns with an IP PIN, 127,273 were rejected because of a missing dependent IP PIN.[66] The notice also stated the wrong year for which the IP PIN was to be used.[67] The IRS was unable to change the language of the notice and attempted to address taxpayer confusion by updating its website to notify IP PIN recipients of the errors.[68]

V. Conclusion

Tax-related identity theft continues to be one of the biggest challenges facing the IRS. This problem plagues individuals and businesses alike. The IRS is adapting to continually changing and increasingly sophisticated methods used by tax identity thieves, and it is making progress. However, there is still room for substantial improvement. The Committee is committed to tracking the IRS' progress on this front and to defending small businesses affected by this problem.

[58] *Id*. at 6.
[59] *Id*.
[60] *Id*. at 7.
[61] *Id*.
[62] *Id*.
[63] *Id*. at 9.
[64] *Id*.
[65] *Id*.
[66] *Id*.
[67] *Id*.
[68] *Id*.