TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Constantly Evolving Refund Fraud Patterns Require Continued Refinement and Development of Detection Initiatives

July 10, 2020

Reference Number: 2020-40-040

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Constantly Evolving Refund Fraud Patterns Require Continued Refinement and Development of Detection Initiatives

Final Audit Report issued on July 10, 2020
Reference Number 2020-40-040

Why TIGTA Did This Audit

This audit was initiated because identifying and reducing individual tax refund fraud, including fraud resulting from identity theft, continues to be a major management challenge for the IRS. In addition, provisions in the Taxpayer First Act, signed into law on July 1, 2019, allow for more information sharing between the IRS and industry partners, to identify more cases of identity theft and tax refund fraud. Our overall objective of this review was to assess the IRS's Service-wide revenue protection strategy.

Impact on Taxpayers

The IRS defines tax refund fraud as an intentional wrongdoing, on the part of a taxpayer, with the specific purpose of evading a tax known or believed to be owed in an attempt to obtain a refund that the taxpayer is not entitled to receive. For example, a taxpayer fraudulently adjusts his or her income or withholding. Identity theft tax refund fraud involves individuals who use another person's name and Taxpayer Identification Number to file a fraudulent tax return reporting false income and withholding in an effort to receive a fraudulent tax refund.

What TIGTA Found

The IRS continues to evaluate and expand on successful fraud detection initiatives, while also piloting new fraud detection initiatives. The actions taken on the part of the IRS have been extremely effective in addressing the identity theft epidemic and reducing its negative impact on tax administration. For example, the IRS actively works with the Security Summit partners to continue to improve its identification of fraudulent tax returns. As a result of this collaborative effort, the IRS used 50 of 61 identified data elements in its fraud detection filters and models and protected approximately $18.6 million in tax refunds as of December 2019. In addition to its partnership with external stakeholders, the IRS continues to expand successful initiatives previously piloted (*e.g.*, the External Leads Program).

Provisions in the Taxpayer First Act are directed toward assessing efforts to reduce identity theft tax refund fraud. For example, the Taxpayer First Act requires that the IRS develop performance metrics to measure the success of the Information Sharing and Analysis Center (ISAC) in detecting and preventing identity theft tax refund fraud. Currently, the only measure the IRS has relative to the ISAC is the level of participation. The IRS reports that this provision has been implemented, yet has not developed metrics to quantitatively measure the success of the ISAC in detecting and preventing identity theft tax refund fraud (*i.e.*, reporting number of tax returns stopped and refunds protected).

Finally, in its most recent *Identity Theft Taxonomy Report*, for Processing Year 2018, the IRS estimates it prevented the issuance of between $6.03 billion and $6.08 billion in fraudulent tax refunds (referred to as protected revenue). However, the IRS also reported that identity thieves were still successful in receiving an estimated $90 million to $380 million in fraudulent tax refunds (referred to as unprotected revenue). As part of the Department of the Treasury's Agency Priority Goals, the IRS set a goal to reduce the amount of unprotected identity theft tax refunds paid by 2 percent by December 31, 2019, and 1 percent thereafter until December 31, 2024.

What TIGTA Recommended

TIGTA recommended that the Commissioner, Wage and Investment Division, develop measures to report on the success of the ISAC in identifying and detecting fraudulent tax returns.

IRS management agreed with this recommendation and plans to take appropriate corrective actions. However, management can only commit to measuring IRS outcomes, as the reporting of State and industry outcomes is not under IRS control.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

July 10, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Constantly Evolving Refund Fraud Patterns Require Continued Refinement and Development of Detection Initiatives (Audit # 201940003)

This report presents the results of our review to assess the Internal Revenue Service's (IRS) Service-wide revenue protection strategy for individual tax returns. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenges of *Addressing Emerging Threats to Tax Administration* and *Reducing Fraudulent Claims and Improper Payments*.

Management's complete response to the draft report is included as Appendix II.

Copies of this report are also being sent to the IRS managers affected by the report's recommendation. If you have any questions, please contact me or Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services).

Table of Contents

Appendices

Background

Identifying and reducing individual tax refund fraud, including fraud resulting from identity theft, continues to be a major management challenge for the Internal Revenue Service (IRS). The IRS defines tax refund fraud as an intentional wrongdoing, on the part of a taxpayer, with the specific purpose of evading a tax known or believed to be owed in an attempt to obtain a refund that the taxpayer is not entitled to receive. For example, a taxpayer fraudulently adjusts his or her income or withholding. Identity theft tax refund fraud involves individuals who use another person's name and Taxpayer Identification Number[1] to file a fraudulent tax return reporting false income and withholding in an effort to receive a fraudulent tax refund. The IRS uses the following systems to identify potentially fraudulent tax returns during tax return processing:

- **Return Review Program** – includes the use of predictive analytics, models, business rules, and selection groups to identify and score suspected identity theft and fraudulent tax returns.
- **Dependent Database** – is a rules-based system that incorporates information from many sources that include the Department of Health and Human Services, the Social Security Administration (SSA), and the IRS. The system includes identity theft rules to identify potentially fraudulent tax returns involving identity theft.

In addition to these systems, analysts in the IRS's Fraud Referral and Evaluation Group manually review tax returns to identify suspicious patterns and trends that the Return Review Program or the Dependent Database potentially does not identify. Once a potentially fraudulent tax return is identified, those involving potential identity theft are held during processing until the IRS can verify the taxpayer's identity. If the IRS cannot confirm the individual's identity, the IRS removes the tax return from processing to prevent the issuance of a fraudulent refund.

For other types of potentially fraudulent tax returns identified, the IRS in Processing Year (PY) 2019 implemented a new process to suspend tax returns identified by the IRS's Return Review Program. The IRS suspends these tax returns to provide additional time for the IRS to receive third-party income documents (*i.e.*, Form W-2, *Wage and Tax Statement*). These documents are used to verify the income and withholding reported on the tax returns identified as potentially fraudulent. The suspended tax returns are held until either the IRS receives third-party documents and the income and withholding is verified or the tax return is sent for further review if the income and withholding did not match. For those tax returns for which no third-party income document(s) are received by June 15, the IRS will send the tax returns to its Integrity and Verification Operations for screening and verification.

The IRS continues to participate in two data sharing arrangements with public and private sector partners:

[1] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, it can be an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.

- **Security Summit**[2] – In March 2015, the IRS convened a coalition of State tax agencies and private-sector tax industry officials to assist in the fight against the filing of fraudulent tax returns. Each year, industry partners have worked to improve the coverage, completeness, and quality of information provided for the identified data elements, increasing the information available to combat identity theft. The IRS and participating members continue to meet monthly (more often when necessary) to discuss emerging trends in tax refund fraud and discuss improvements to detection efforts.
- **Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC)** – First piloted in January 2017, the ISAC is a highly secure web-based portal operated by the Trusted Third Party[3] for States, industry, and the IRS to share and exchange information related to fraudulent tax return filings. The IRS and State tax agencies use the shared information to assist in their efforts to detect, deter, and prevent tax-related identity theft. As of January 2020, the ISAC reported that 72 organizations were participating with 432 users.

Results of Review

New fraud patterns are constantly evolving and as such, the IRS needs to adapt its detection and prevention processes. Our review found that the IRS continues to evaluate and expand on successful fraud detection initiatives, while also piloting new fraud detection initiatives. The actions taken on the part of the IRS have been extremely effective in addressing the widespread identity theft problem and reducing its negative impact on tax administration. The IRS's multi-faceted approach has significantly reduced losses to the Government from the $5.2 billion reported for PY 2010 that the Treasury Inspector General for Tax Administration (TIGTA) first estimated in July 2012[4] to the IRS's most recent measurement of estimated losses for PY 2018 of between $90 million and $380 million. For PY 2019, as of December 7, 2019, the IRS reported that its fraud and identity theft filters identified and confirmed:

- 438,580 fraudulent tax returns (*i.e.*, non–identity theft) and prevented the issuance of approximately $1.76 billion in refunds.
- 442,991 fraudulent tax returns, as a result of identity theft filters, and prevented the issuance of approximately $1.87 billion in refunds.

Figure 1 shows a comparison of tax returns identified and confirmed as fraudulent using its identity theft filters for PYs 2018 and 2019.

[2] The Security Summit convened in Calendar Year 2015 and includes IRS officials, representatives from State Departments of Revenue, the Chief Executive Officers of leading tax preparation firms, software developers, and payroll and tax financial product processors.
[3] The Trusted Third Party is an IRS Federally Funded Research and Development Center that facilitates information sharing among members of the ISAC.
[4] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

Figure 1: Comparison of PYs 2018 and 2019 IRS Fraud and Identity Theft Filters

	PY 2018 (as of December 8, 2018)		PY 2019 (as of December 7, 2019)	
	Tax Returns	Tax Refunds	Tax Returns	Tax Refunds
Confirmed Non-Identity Theft Fraud	427,380	$1.73 billion	438,580	$1.76 billion
Confirmed Identity Theft Fraud	648,808	$3.10 billion	442,991	$1.87 billion
Totals	1,076,188	$4.83 billion	881,571	$3.63 billion

Source: The IRS Global Identity Theft Report for December 2018 and 2019.

New and Expanded Tax Refund Fraud Detection Initiatives Result in Continued Improvement

As previously noted, the IRS actively works with the Security Summit partners to continue to improve its identification of fraudulent tax returns. One such initiative involves identifying data elements included on electronically filed (e-filed) tax returns that can be used for fraud detection. As a result of this collaborative effort, the Security Summit identified 61 data elements for evaluation in detecting tax refund fraud.[5] During PY 2019, the IRS incorporated 50 of these data elements into its fraud detection filters and models. The IRS reported that as of December 2019, incorporation of these data elements in detection filters and models identified 9,385 confirmed fraudulent tax returns and protected approximately $18.6 million in tax refunds. The IRS continues to analyze the remaining data elements for use in future filters or models.

In addition to its partnership with external stakeholders, the IRS continues to expand successful initiatives previously piloted. These initiatives include:

- **Deposit Account Verification Program** – The IRS first began this initiative in January 2017, and partnered with a Security Summit industry provider of debit cards.[6] Under this initiative, when the IRS identifies a potentially fraudulent tax return, in which the refund was to be deposited on a debit card associated with this industry provider, the IRS sends certain information to this provider. Once received, the debit card provider evaluates the information it has for the individual associated with the debit card account to provide the IRS with a risk level associated with the recipient's account. For example, **********2********** **********2********** at the time of the IRS inquiry or whether additional verification is suggested.

  During PY 2018, the IRS expanded this pilot to include two debit card providers. The IRS sent 293,074 inquiries to the debit card providers as of December 12, 2018. For PY 2019, as of December 11, 2019, the IRS increased the inquiries sent to these debit card

[5] As of PY 2020, the IRS did not use the data element associated with the W-2 Verification Program because it discontinued the program.
[6] Taxpayers can have their tax refunds deposited directly onto a debit card.

providers to 428,679 inquires. The IRS used responses from these providers to confirm 131,431 tax returns as having fraudulent refunds and protected more than $483 million in refunds. When we asked IRS management why it had not continued to expand to additional providers as noted in our prior report,[7] IRS management stated they plan to finalize their pilot results after July 2020. Ongoing efforts include possible sharing of additional information with the debit card providers and analyzing the tax returns identified as fraud by the debit card providers to adjust fraud detection filters.

- **External Leads Program** – This initiative is a partnership between the IRS and various financial institutions (*i.e.*, banks) to identify questionable Federal tax refunds. A questionable refund can include a name mismatch between the tax return and the bank account receiving the refund or other account characteristics that indicate that the deposit is questionable, invalid, or has been fraudulently obtained. Once a refund is identified as questionable, the financial institution notifies the IRS and sends the refund back to the IRS for additional review. As of December 2019, the External Leads Program has resulted in the protection of refunds totaling approximately $294 million, compared to $112 million for the same period in PY 2018. IRS management noted that they are evaluating additional initiatives that could be used to further leverage relationships with financial institutions in detecting fraudulent refunds. These include expanding the use of deposit reject codes used by financial institutions and the deposit account verification program discussed previously.
- **Deceased Tax Account Lock** – This initiative blocks fraudulent tax returns from entering the tax processing system. As of December 26, 2019, the IRS has locked the tax accounts of more than 42.9 million deceased individuals. This compares to approximately 36.7 million tax accounts locked as of December 27, 2018. When tax accounts are locked, e-filed tax returns are rejected and paper-filed tax returns are prevented from posting to the Master File.[8] According to the IRS, as of December 31, 2019, it rejected 73,414 fraudulent e-filed tax returns and stopped 129,480 paper tax returns (as of December 27, 2019) from posting to the Master File.

  As we previously reported,[9] in September 2016, the SSA's Office of the Inspector General identified that the SSA excluded approximately 8.7 million individuals for whom it had a date of death from the SSA Death Master File. The IRS obtains and uses the SSA Death Master File to update tax accounts associated with deceased individuals to set a deceased tax account lock. Beginning March 2018, the SSA started the process of updating the Death Master File with the missing dates of death associated with these 8.7 million individuals and sending the updates to the IRS with their normal weekly file submission. IRS management indicated that they had received updated dates of death for all 8.7 million taxpayers during 2018.

  However, the IRS discovered that approximately 1.6 million of these updates did not post to the Master File because the Master File cannot post transactions dated prior to 1962 or dates with invalid days. IRS management stated that they updated their programming to identify invalid dates received from the SSA before sending to the

[7] TIGTA, Ref. No. 2019-40-012, *Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft* (Dec. 2018).
[8] The IRS database that stores various types of taxpayer account information.
[9] TIGTA, Ref. No. 2019-40-012, *Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft* (Dec. 2018).

Master File, so that accounts of decedents update appropriately when received in future SSA files. As of December 2019, the IRS resolved the 1.6 million unposted transactions.

The IRS continues to pilot new fraud detection initiatives

During the 2019 Filing Season,[10] the IRS partnered with the Bureau of Fiscal Services (BFS) on an initiative that **********2********** maintained by the BFS. This match is performed only for those **********2**********. The results of the pilot confirmed that tax returns that were initially identified as potentially fraudulent in which the **********2********** are in fact likely not to be fraudulent tax returns.

As of November 13, 2019, the IRS sent to the ****2********** related to 1.3 million potential identity theft related tax returns. As previously noted, the IRS's pilot focused on tax returns in which **********2********** with the BFS. The BFS identified 45,703 tax returns that met the criteria. For 12,750 of these tax returns, the taxpayers had not authenticated their identity when the IRS originally stopped their tax returns and sent notification. The IRS sent a second notification informing the filers that they need to authenticate themselves with the IRS in order to receive their tax refund. These efforts resulted in the IRS authenticating 5,960 taxpayers who would have otherwise not received their tax refund. The IRS reported that it confirmed 4,275 were identity theft tax returns and protected $197 million[11] in refunds.

As a result, during the 2020 Filing Season, in an effort to assist taxpayers entitled to a refund whose tax returns are identified and held as potentially fraudulent, the IRS will send a second authentication letter to the taxpayer if the IRS has not received a response to its first letter. The IRS hopes the additional contact will improve the identity theft determinations made by the Taxpayer Protection Program[12] for the 2020 Filing Season. The IRS also stated that, similar to other pilots and initiatives, it plans to continue to evaluate additional uses of the BFS **********.

The Taxpayer First Act Requires Development of Performance Metrics to Measure Success of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center

Provisions in the Taxpayer First Act,[13] signed into law on July 1, 2019, allow for more information sharing to assist with reducing identity theft and tax refund fraud. One of the key provisions included in this Act is the expansion of the IRS's authority to share fraudulent tax return data with ISAC partners. Specifically, the Act now permits the IRS to share information from potential identity theft tax returns including the Internet Protocol address, device identification, e-mail domain name, speed of completion, method of authentication, refund method, Preparer

[10] The period from January through mid-April when most individual income tax returns are filed.
[11] The IRS confirmed that one tax return had a refund of more than $187 million.
[12] The Taxpayer Protection Program is responsible for authenticating a taxpayer's identity when the Dependent Database or Return Review Program selects their tax return as potential identity theft.
[13] Pub. L. No. 116-25, 133 Stat. 981 (2019).

Taxpayer Identification Number,[14] and Electronic Filer Identification Number.[15] In addition, the Act also permits the IRS to share the following tax return information for confirmed identity theft tax returns: taxpayer name, Taxpayer Identification Number, bank account, and routing number. For the 2020 Filing Season, the IRS plans to launch a new platform to share this information with select ISAC participants as required by the Taxpayer First Act. As of March 2020, the IRS and the Trusted Third Party, which operates the ISAC, have completed the necessary agreements and the platform to share tax return data. The IRS anticipates sharing data before the end of the 2020 Filing Season. TIGTA has initiated a separate review to assess the IRS's implementation of the ISAC provision included in the Taxpayer First Act.[16]

Section 2003 of the Taxpayer First Act requires the IRS to develop performance metrics to measure the success of the ISAC in detecting and preventing identity theft tax refund fraud

Currently, the only measure the IRS has relative to the ISAC is level of participation. IRS management stated that the increase in the participation results in more alerts posted, which shows the success of the ISAC. Management also stated that participants would not continue to participate if the ISAC was not helpful to their organizations. The IRS reports that this provision has been implemented yet has not developed metrics to quantitatively measure the success of the ISAC in detecting and preventing identity theft tax refund fraud (*i.e.*, reporting number of tax returns stopped and refunds protected). When we met with IRS management to discuss our concerns about not having quantitative measures, management stated that developing such measures could be difficult. Management also noted that quantitative measures might not provide an accurate measurement of success of the ISAC, as there are intangible benefits to the ISAC (*e.g.*, future year tax returns or fraudster deterrence) that cannot be measured.

For the 2019 Filing Season, the IRS internally published an ISAC cost-benefit analysis reporting the potential to protect $2.53 million in fraudulent tax returns. During the 2019 Filing Season, the IRS used 20 of the 171 alerts posted to the ISAC and as of December 2019, the IRS confirmed 680 tax returns as identity theft and protected approximately $1.9 million in fraudulent tax refunds.

To assist detection efforts by ISAC participants, the IRS posted 25 alerts to the ISAC for the 2019 Filing Season. These alerts provide information relating to the IRS's identification of suspicious device identification numbers, dark web intelligence, fraudulent third-party authorizations, telephone schemes, and cyber alerts. Figure 2 shows the increase in use of the ISAC by the IRS and State tax agencies from the 2017 through 2019 Filing Seasons.

[14] A nine-digit number issued by the IRS that is required if an individual prepares or assists in preparing tax returns for compensation.
[15] A six-digit number assigned to Providers to identify businesses that have completed the IRS e-file application to become an authorized Provider and allows them to e-file tax returns.
[16] TIGTA, Audit Number 202020010, *Data Protection at the Information Sharing and Analysis Center*.

Figure 2: ISAC Metrics for the 2017, 2018, and 2019 Filing Seasons

	2017 Filing Season	2018 Filing Season	2019 Filing Season
State Partners	42	46	47
Industry Partners	17	18	19
Organizations Submitting Alerts	20	24	30
Alerts Posted	71	142	171
Alerts Used by the IRS	1	47	20

Source: ISAC reports on metrics for December 2017, 2018, and 2019.

The ISAC partnership noted in its 2019 Annual Report[17] that it does not comprehensively measure amounts of identity theft tax refund fraud stopped because ownership of those measures resides with the IRS and the State tax and revenue departments. Further, the 2019 Annual Report noted that the ISAC is evaluating metrics that better quantify the value of the ISAC as its data are one of many cumulative factors used in detecting identity theft tax refund fraud.

The IRS operates and fully funds the ISAC Operational Platform

The IRS awarded a Trusted Third Party approximately $5.3 million to develop and maintain the ISAC through December 31, 2017. Since then, the IRS has expended approximately $18.9 million for the Trusted Third Party to administer the ISAC for Filing Seasons 2018, 2019, and 2020. During the 2020 Filing Season, the IRS incurred an additional $629,000 to fund an additional platform within the ISAC to share tax return information with ISAC partners in addition to the normal cost to maintain the existing platform, which increased in cost for the 2020 Filing Season to $6.2 million. Figure 3 shows the project costs the IRS paid for the 2018 through the 2020 Filing Seasons.

Figure 3: ISAC Cost Benefit for the 2018 through 2020 Filing Seasons

	2018 Filing Season	2019 Filing Season	2020 Filing Season
Project Costs	$6.0 million	$6.0 million	$6.9 million
Potential Value	$2.82 million	$2.53 million	

Source: The IRS ISAC Cost-Benefit Analysis report as of November 2019 and IRS reported cost for the 2020 Filing Season.

Recommendation 1: The Commissioner, Wage and Investment Division, should, as required by the Taxpayer First Act, develop measures to report on the success of the ISAC in identifying and detecting fraudulent tax returns.

Management's Response: The IRS agreed with this recommendation. However, IRS management can only commit to measuring IRS outcomes, as the reporting of State and industry outcomes is not under IRS control. The IRS plans to use the annual IRS cost

[17] The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Partnership 2019 Annual Report.

benefit analysis report that is developed each fall after the filing season as the metric for determining the success of the ISAC in identifying and detecting fraudulent tax returns.

Actions Taken to Address a Prior Recommendation Regarding Low-Dollar Refunds

In December 2018, we reported[18] that the IRS's use of a refund dollar tolerance resulted in the IRS excluding potentially fraudulent tax returns from its detection process. The IRS's filter implemented in June 2016 selects tax returns for review only if the amount of the refund is in excess of a specific dollar amount. This resulted in 27,566 potentially fraudulent tax returns we identified with refunds totaling almost $1.3 million that were not selected for review despite the tax returns having the **********2********** ****2**** that was used on at least one IRS-confirmed identity theft tax return. IRS management indicated that the refund dollar tolerance used in their fraud filters are consistent with the tolerances used for IRS math error processing. We further reported that the ISAC received and posted six alerts detailing an identity theft scheme involving refund amounts below the IRS's refund dollar tolerance.

We recommended that the IRS evaluate the use of refund dollar tolerances in the identity theft detection filters. IRS management disagreed, stating that elimination of the threshold criteria would not be a wise use of resources considering the very low-dollar amount of the refunds at stake, the additional burden placed on taxpayers whose tax returns did not have the potential for tax-related identity theft, and the cost of treating this group of tax returns. IRS management also stated that they have the ability to conduct detailed analyses on these tax returns outside the mainstream processes when an emerging trend is identified.

Although management, in its response to our recommendation, cited its ability to identify emerging trends associated with low-dollar refunds, they did not timely identify a low-dollar refund scheme that resulted in the loss of $14 million in fraudulent refunds. During the 2019 Filing Season, the IRS's Criminal Investigation Division became aware of a scheme, similar to what TIGTA previously reported, that involved the filing of fraudulent tax returns with low-dollar refunds in an attempt to bypass IRS reviews to steal estimated tax payments. As of April 19, 2019, the IRS identified 2,882 tax returns meeting the low-dollar refund scheme characteristics, in which the associated tax accounts contained approximately $33.3 million in estimated tax payments that could be refunded. The IRS identified and stopped 1,559 tax returns during processing. However, it was unable to stop the other 1,323 potentially fraudulent tax returns with refunds totaling $14 million. On May 31, 2019, the IRS implemented a programming change to update its fraud detection filters to systemically identify fraudulent tax return filings that met the characteristics of this scheme.

When we discussed the scheme with IRS management, they noted that during PY 2019, the IRS selected approximately 130,000 potentially fraudulent tax returns with refunds under the dollar tolerance. As of February 2020, the IRS identified approximately 62,000 tax returns as confirmed identity theft and protected approximately $12 million in refunds. Additionally, the IRS has developed a new filter for the 2020 Filing Season to identify tax returns below the dollar tolerances, which has resulted in the selection of an additional 5,040 tax returns as of

[18] TIGTA, Ref. No. 2019-40-012, *Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft* (Dec. 2018).

February 20, 2020. IRS management stated that they would continue to monitor and evaluate the data to determine if the IRS needs additional measures or if a threshold change is appropriate.

Goals to Reduce Unprotected Identity Theft Tax Refunds Have Been Established

In its most recent *Identity Theft Taxonomy Report,*[19] for PY 2018, the IRS estimates it prevented the issuance of between $6.03 billion and $6.08 billion in fraudulent tax refunds (referred to as protected revenue).[20] However, the IRS also reported that identity thieves were still successful in receiving an estimated $90 million to $380 million in fraudulent tax refunds (referred to as unprotected revenue). Figure 4 shows estimated protected and unprotected tax revenue for PY 2017 and PY 2018.

Figure 4: Estimated Revenue Protected and Unprotected for PY 2017 and PY 2018

Processing Year	Protected Tax Revenue		Unprotected Tax Revenue	
	Tax Returns	Tax Refunds	Tax Returns	Tax Refunds
2017	1.619 – 1.623 million	$11.78 – $11.81 billion	27,900 – 137,000	$110 - $600 million
2018	1.46 – 1.48 million	$6.03 - $6.08 billion	22,200 – 94,400	$90 - $380 million

Source: The IRS Return Integrity and Compliance Services Division Taxonomy analysis of identity theft dated September 30, 2019.

As part of the Department of the Treasury's Agency Priority Goals, the IRS set a goal to reduce the amount of unprotected identity theft tax refunds paid by 2 percent by December 31, 2019, and 1 percent thereafter until December 31, 2024. Figure 4 shows that the IRS estimated unprotected revenue at between $110 million to $600 million in PY 2017, and between $90 million and $380 million in PY 2018. Although the IRS has met its goal to reduce the amount paid by 2 percent, management acknowledges that challenges remain due to increases in the sophistication of identity theft, including fraudsters filing high consistency tax returns[21] that appear to be filed by legitimate taxpayers. Even still, the IRS remains committed to this goal by continuing to develop and retrain detection models using new elements and using data analytics and enhanced filters to detect and prevent identity theft. This also includes monitoring filter performance to ensure a continuous cycle of improvement.

[19] The *Identity Theft Taxonomy Report* provides strategic insight, including the amount of identity theft protected and unprotected. The insight helps the IRS better understand the effectiveness of the identity theft initiatives when viewed collectively.
[20] The protected revenue includes additional controls to the fraud and identity theft filters, *i.e.*, e-file business rules, date of death locks.
[21] Fraudulent tax returns that contain information that is very similar to the legitimate tax return.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the IRS's Service-wide revenue protection strategy for individual tax returns. To accomplish our objective, we:

- Determined if the IRS's Taxonomy analysis is accurate and identified the IRS's plan to continue to decrease the amount of undetected tax returns resulting from identity theft. We obtained the PY 2017 and PY 2018 Taxonomy reports and compared the methodologies to identify how the IRS is combating identity theft. We interviewed IRS management on the Taxonomy analysis and how the IRS uses the analysis to reduce undetected identity theft refunds.
- Determined if the IRS took actions to update its fraud detection filters based upon the results of several IRS initiatives. We reviewed the Security Summit data elements available to the IRS to expand tax refund fraud coverage and the results of the Deposit Account Verification Program. We assessed the IRS process to use the ISAC alerts to improve fraud detection. We reviewed the IRS's process to lock deceased taxpayers' tax accounts through the SSA Death Master File.
- Assessed the effectiveness of the IRS's filters in identifying instances of tax return filing fraud. We reviewed the population of tax returns identified by the IRS Criminal Investigation Division that fit the criteria of the estimated tax payment scheme and IRS actions taken to address tax returns filed below the refund dollar tolerance.
- Reviewed the Taxpayer First Act Provisions 2001, 2002, and 2003 and determined their implementation status.

Performance of This Review

This review was performed with information obtained from the Wage and Investment Division, Return Integrity and Compliance Services Division in Atlanta, Georgia, during the period June 2019 through March 2020. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Major contributors to the report were Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services); Diana M. Tengesdal, Director; Jonathan W. Lloyd, Audit Manager; David P. Robben, Lead Auditor; Alexis E. Gomez, Auditor.

Validity and Reliability of Data From Computer-Based Systems

During this review, we relied on data extracted by TIGTA's Strategic Data Services from the IRS's Individual Return Transaction File[1] for PY 2019 and Form W-2 data from the IRS's Information

[1] Contains data transcribed from initial input of the original individual tax returns during tax return processing.

Returns Master File.[2] We relied on IRS-provided data from the Taxpayer Protection Program, Return Review Program, and the Dependent Database systems for PY 2018 and PY 2019. To assess the reliability of computer-processed data, programmers within TIGTA's Strategic Data Services validated the data extract files. Additionally, we reviewed judgmental samples of the extracts to ensure that the data matched to the IRS Master File.[3] To assess the reliability of the data received from the IRS, we compared the data to the IRS's Master File transaction codes and selected judgmental samples of each extract to verify against the IRS's Master File. Based on the results of our testing, we believe that the data used in our review were reliable.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Return Review Program and Dependent Database procedures used to select tax returns for fraud and identity theft treatment and IRS processing procedures on posting deceased transaction codes to the Master File. We evaluated these controls by reviewing Internal Revenue Manuals, interviewing management, and reviewing program reports.

[2] An IRS database that contains third-party information returns documents for taxpayers such as Form W-2.
[3] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Appendix II

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

June 22, 2020

MEMORANDUM FOR MICHAEL E MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin David P. Alito Digitally signed by David P. Alito Date: 2020.06.22 15:32:30 -04'00'
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – *Constantly Evolving Refund Fraud Patterns Require Continued Refinement and Development of Detection Initiatives* (Audit #201940003)

We appreciate your support of the IRS' multi-faceted approach in detecting and mitigating identity theft and non-identity theft tax refund fraud. The IRS strives to protect taxpayers, while simultaneously working to decrease their burden. We are proud of our achievements in the reduction of revenue losses associated with identity theft tax refund fraud, which is estimated to be $5.2 billion since 2012. We also recognize that we must continue in our efforts to prevent these revenue losses in the future. As noted in the report, the IRS continues progressive efforts to leverage external stakeholders and government agencies in our efforts to combat identity theft. We recognize that those we are combating are sophisticated perpetrators and so we must continue to evaluate and refine our processes to identify fraudulent tax returns and protect revenue.

As you noted, the Taxpayer First Act (TFA) expands the IRS's authority to share fraudulent tax return data with our Information Sharing and Analysis Center (ISAC) partners. In response, we have developed a three-phase approach to implementing TFA Section 2003. The first phase consisted of the IRS sharing potential identity theft data with ISAC partners. The second phase expanded our information sharing to include confirmed identity theft data with ISAC partners. Finally, the third phase will consist of the creation of ISAC Federal Tax Information Analytical Reports to measure ISAC success.

Thus far, we have implemented Phase 1 of our three-phase plan. We have begun sharing potential identity theft data with our ISAC partners and successfully deployed a secure environment on the ISAC platform to receive, store, and share federal tax information with authorized ISAC partners. In addition, in order to improve reporting, we have enhanced the ISAC alerts process to gather more meaningful data around identity

theft activities. We also continue in our efforts to optimize the use of data currently available to ISAC partners, so we have created new data dashboards for their use. We continue to explore relevant and new information and data sources, including other potential ISAC partners and other government agencies, to improve detection or false detection.

Attached are our comments and proposed actions to your recommendation. If you have any questions, please contact me, or a member of your staff may contact Michael Beebe, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (470)-639-3250.

Attachment

Attachment

Recommendation

RECOMMENDATION 1
The Commissioner, Wage and Investment Division, should, as required by the Taxpayer First Act, develop measures to report on the success of the ISAC in identifying and detecting fraudulent tax returns.

CORRECTIVE ACTION
We will develop measures which would report on the success of the ISAC in identifying and detecting fraudulent tax returns. However, we can only commit to measuring IRS outcomes, as the reporting of state and industry outcomes is not under IRS control. Our metric will be the annual IRS cost benefit analysis report we currently use that is developed each fall after the filing season.

IMPLEMENTATION DATE
April 15, 2022

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification Program Management, Return Integrity and Compliance Services, Wage and Investment Division

Appendix III

Abbreviations

BFS	Bureau of Fiscal Services
e-file(d)	Electronically file(d)
IRS	Internal Revenue Service
ISAC	Identity Theft Tax Refund Fraud Information Sharing and Analysis Center
PY	Processing Year
SSA	Social Security Administration
TIGTA	Treasury Inspector General for Tax Administration