



*Partnership With State and Industry
Leaders Is a Key Focus in Further
Reducing Tax-Related Identity Theft*

December 27, 2018

Reference Number: 2019-40-012

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:

2 = Law Enforcement Techniques/Procedures and Guidelines for Law Enforcement Investigations or Prosecutions.

Phone Number / 202-622-6500

E-mail Address / TIGTACommunications@tigta.treas.gov

Website / <http://www.treasury.gov/tigta>



To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.



HIGHLIGHTS

PARTNERSHIP WITH STATE AND INDUSTRY LEADERS IS A KEY FOCUS IN FURTHER REDUCING TAX-RELATED IDENTITY THEFT

Highlights

**Final Report issued on
December 27, 2018**

Highlights of Reference Number: 2019-40-012 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Identity theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number to file a fraudulent tax return. In its most recent Identity Theft Taxonomy report for Processing Year 2016, the IRS estimates that it prevented the issuance of between \$10.56 billion and \$10.61 billion in fraudulent tax refunds. However, the IRS also reported that identity thieves were successful in receiving an estimated \$1.68 billion to \$2.31 billion in fraudulent tax refunds.

WHY TIGTA DID THE AUDIT

This audit was initiated to assess the effectiveness of the IRS's ongoing efforts to detect and prevent tax-related identity theft, measure undetected identity theft, and coordinate identity theft information with other Government agencies and tax industry partners.

WHAT TIGTA FOUND

The IRS continues to expand its efforts to detect and prevent identity theft. For Processing Year 2018, the IRS is using 200 identity theft filters to identify potentially fraudulent tax returns at the time returns are filed and prior to issuance of the refund. As of December 31, 2017, the IRS had identified 652,119 fraudulent returns and prevented more than \$7.2 billion in fraudulent tax refunds as a result of these filters.

The IRS continues to work with the Security Summit to explore programs and processes to improve the extent of sharing identity theft information in an effort to further improve the

detection and prevention of tax-related identity theft through the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC). The IRS and its partners launched the ISAC as a pilot in January 2017.

According to the April 2018 *Identity Theft Tax Refund Fraud ISAC Annual Report*, participation in the ISAC has increased from 18 participating organizations in Calendar Year 2017 to 60 participating organizations and more than 400 registered users in Calendar Year 2018. The report also states that alert and data contributions by participating organizations have increased by more than six times since January 2017.

In addition, the IRS developed additional filters in response to TIGTA recommendations to improve the detection of fraudulent tax returns that use Schedule C, *Profit or Loss From Business (Sole Proprietorship)*, income and foreign addresses. However, because of programming errors and the use of a dollar tolerance, 28,092 potentially fraudulent tax returns with refunds totaling more than \$4.4 million were not identified.

Finally, the IRS began the Form W-2, [Wage and Tax Statement] Verification Code initiative in Processing Year 2016 as a pilot program. IRS management informed us that Processing Year 2018 is the last year it will operate as a pilot program. However, the passage of legislation as well as significant payroll provider data breaches warrant ensuring that there is continued business value before the IRS expands the Verification Code initiative.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS revise identity theft detection filters to eliminate specific dollar tolerances and ensure that the reduction in the risk of tax-related identity theft warrants full implementation of the Form W-2 Verification Code Program. The IRS disagreed with one of the two recommendations. The IRS does not believe eliminating the dollar tolerances from filters would be a wise use of its resources. TIGTA believes that, at a minimum, the IRS should consider reducing the dollar tolerance to reduce the known risk in this area.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

December 27, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft
(Audit # 201740007)

This report presents the results of our review to determine the effectiveness of the Internal Revenue Service's ongoing efforts to detect and prevent identity theft. This audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Identity Theft and Impersonation Fraud.

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

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



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Table of Contents

<u>Background</u>	Page 1
<u>Results of Review</u>	Page 4
<u>Participation and Use of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Is Increasing</u>	Page 4
<u>The Use of a Dollar Tolerance and Programming Error Resulted in Some Potentially Fraudulent Returns Not Being Identified</u>	Page 8
<u>Recommendation 1:</u>	Page 9
<u>Cost-Benefit Analysis Should Be Performed to Ensure That Expansion of the Form W-2 Verification Code Initiative Is Warranted</u>	Page 10
<u>Recommendation 2:</u>	Page 12
<u>Adding Social Security Records That Are Currently Excluded From the Death Master File Could Further Reduce Risk of Misuse of Deceased Individuals’ Identities to File Fraudulent Tax Returns</u>	Page 12
Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 14
<u>Appendix II – Major Contributors to This Report</u>	Page 18
<u>Appendix III – Report Distribution List</u>	Page 19
<u>Appendix IV – Outcome Measures</u>	Page 20
<u>Appendix V – Prior TIGTA Audit Reports on Identity Theft</u>	Page 23
<u>Appendix VI – Management’s Response to the Draft Report</u>	Page 24



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Abbreviations

DDb	Dependent Database
e-file(d)	Electronically file(d)
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
OMM	Operation Mass Mailing
SSA	Social Security Administration
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Background

Identity theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number¹ to file a fraudulent tax return. Specifically, these individuals use the stolen identities to submit tax returns with false income and withholding documents to the Internal Revenue Service (IRS) for the sole purpose of receiving a fraudulent tax refund.

Detection of tax returns involving identity theft

The IRS reported that for Processing Year² 2017, as of December 31, 2017, it identified 652,119 fraudulent tax returns and prevented the issuance of more than \$7.2 billion in fraudulent tax refunds as a result of its identity theft filters. For Processing Year 2018, the IRS is using 200 identity theft filters to identify potentially fraudulent tax returns at the time tax returns are processed and prior to the issuance of fraudulent tax refunds. Identity theft filters incorporate criteria based on characteristics of confirmed identity theft tax returns, including amounts claimed for income and withholding, filing requirements, prisoner status, taxpayer age, and filing history. These filters are incorporated into the following systems the IRS uses during tax return processing to identify fraudulent tax returns involving identity theft:

- **Return Review Program** – The Return Review Program uses predictive analytics, models (*i.e.*, filters), clustering, a scoring system, business rules, and selection groups to identify suspected identity theft and fraudulent tax returns.
- **Dependent Database (DDb)** – The DDb 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 IRS implemented identity theft rules within the DDb system in Processing Year 2012. Tax returns are analyzed to identify potentially fraudulent tax returns involving identity theft.

In addition to the previously mentioned systems, Fraud Referral and Evaluation analysts manually review tax returns to identify suspicious patterns and trends that potentially have not been identified by the Return Review Program or the DDb. The detection systems and filters use a myriad of data to evaluate tax returns for potential identity theft. The data include:

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.

² The calendar year in which the IRS processes the tax return or document.



Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft

- Data elements from electronically filed (e-filed) tax returns.** As a result of the Security Summit,³ the IRS used 23 data elements from e-filed tax returns provided by e-file return transmitters during Processing Year 2017 to detect potential identity theft. *****2*****
*****2*****
24 *****2*****.⁵ The IRS reported that as of December 2017, it identified 4,649 potentially fraudulent tax returns claiming \$20.9 million in tax refunds as a result of these data elements. It should be noted that e-file transmitters are providing an additional 37 return elements to the IRS for use during Processing Year 2018.
- Forms W-2, Wage and Tax Statement.** On December 18, 2015, the President signed the Consolidated Appropriations Act of 2016,⁶ which contained provisions to help combat identity theft. The Act requires employers to submit third-party income and withholding information, *i.e.*, Forms W-2, and any returns or statements required to report nonemployee compensation on or before January 31 of the following tax year.⁷ In addition, the IRS continued its voluntary program in which 18 payroll providers were requested to submit Forms W-2 directly to the IRS by January 31, 2018.
- Leads of potential identity theft tax returns from State tax agencies and tax industry partners.** The IRS has developed two voluntary information sharing programs (*State Suspicious Filer Program* and *Industry Leads Program*). The *State Suspicious Filer Program* enables participating States to provide the IRS referrals of potential and confirmed identity theft, tax return preparers connected to the filing of potential identity theft tax returns, and other fraudulent activities that the States identify during the processing of the State tax returns. The *Industry Leads Program* enables industry partners such as tax return preparers, software developers, and return transmitters to report suspicious activity to the IRS.⁸ According to the IRS, it selected 135,104 tax returns with approximately \$1.13 billion in refunds claimed as of December 31, 2017, as a result of the State and industry leads programs.

³ The unprecedented partnership between the IRS, State tax agencies, and the private-sector tax industry to form a united and coordinated front against identity theft tax refund fraud.

⁴ *****2*****
*****2*****

⁵ *****2*****

⁶ Pub. L. No. 114-113, 129 Stat. 2242 (2015).

⁷ A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.

⁸ In August 2015, the IRS modified the *Industry Leads Program* to require participating e-file return transmitters that transmit more than 2,000 individual income tax returns per year to perform post-filing analytics. These return transmitters are also required to provide the results of their analytics to the IRS annually.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

This review was performed at the Austin Submission Processing Campus⁹ in Austin, Texas; the New Carrollton Federal Building in Lanham, Maryland; and the *****2*****
*****2***** In addition, we used information obtained from the IRS Wage and Investment Division Accounts Management and Return Integrity and Compliance Services functions in Atlanta, Georgia, during the period March 2017 through May 2018. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

⁹ The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Results of Review

The IRS continues to expand its efforts to detect and prevent identity theft. In its most recent Identity Theft Taxonomy report for Processing Year 2016, the IRS estimates it prevented the issuance of between \$10.56 billion and \$10.61 billion in fraudulent tax refunds, *i.e.*, protected revenue. However, the IRS also reported that identity thieves were still successful in receiving an estimated \$1.68 billion to \$2.31 billion in fraudulent tax refunds, *i.e.*, unprotected revenue. Figure 1 shows estimated protected and unprotected tax revenue for Processing Years 2015 and 2016.

**Figure 1: Estimated Revenue Protected and Unprotected
for Processing Years 2015 and 2016**

Processing Year	Protected Tax Revenue		Unprotected Tax Revenue	
	Tax Returns (Millions)	Tax Refunds (Billions)	Tax Returns (Millions)	Tax Refunds (Billions)
2015	2.38 – 2.47	\$12.35 – \$12.88	0.86 – 1.03	\$2.24 – \$3.34
2016	1.98 – 1.99	\$10.56 – \$10.61	0.74 – 0.81	\$1.68 – \$2.31

Source: The IRS Return Integrity and Compliance Services Division analysis of identity theft, dated October 31, 2016, and October 19, 2017.

Participation and Use of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Is Increasing

The IRS continues to work with its Security Summit partners to refine sharing and coordination processes in an effort to continue to improve the detection and prevention of tax-related identity theft. 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. A primary initiative of the Security Summit is the creation of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC). The ISAC was launched as a pilot on January 23, 2017. The IRS reports that the ISAC is a highly secure web-based portal operated by the Trusted Third Party¹⁰ for States, industry, and the IRS to share and exchange information. The ISAC facilitates the sharing of information among participating organizations for the purpose of detecting, deterring, and preventing tax-related identity theft. In April 2018, the IRS

¹⁰ The Trusted Third Party is an IRS Federally Funded Research and Development Center that facilitates information sharing among members of the Identity Theft Tax Refund Fraud ISAC.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

reported that more than 60 organizations were participating in the ISAC with more than 400 users. The ISAC consists of two parts:

- ***The ISAC Partnership*** – is made up of representatives from the IRS, States, and tax industry. The ISAC Partnership is governed by the 15 member ISAC Senior Executive Board.¹¹ The Senior Executive Board is principally responsible for the mission and vision statements for the ISAC Partnership, recommending ISAC operating procedures, nominating new ISAC Operational Platform participants, and recommending the removal of such participants. Each member shares in the financial responsibility for the Senior Executive Board activities. For example, each member’s organization pays for the member to attend Board meetings.
- ***The ISAC Operational Platform*** – is the information sharing and analysis element of the ISAC.¹² The operational platform provides different levels of participation. For example, all users can post alerts to share information on identity theft schemes they have identified and can view alerts posted by other users. State and industry partners who have signed an information sharing agreement with the ISAC Trusted Third Party can also access data (including confirmed identity theft),¹³ analytical products, and analysis tools.¹⁴

Unlike the ISAC Partnership, the IRS operates and fully funds the ISAC Operational Platform. According to the IRS, it awarded the Trusted Third Party more than \$6.3 million to develop and maintain the ISAC through November 26, 2017. In addition, the IRS signed an additional \$6 million contract with the Trusted Third Party in September 2017 for the administration of the ISAC during Fiscal Year¹⁵ 2018. Although the IRS solely funds this initiative, Internal Revenue Code Section 6103¹⁶ currently prohibits the IRS from sharing tax return information with ISAC partners. Congress is currently considering legislation authorizing the IRS to share limited relevant tax return data with ISAC participants.¹⁷

¹¹ Five representatives each from the IRS, States, and industry.

¹² It also includes an early warning alarm system that allows States and industry partners to share information related to identity theft refund fraud and schemes more quickly to better defend against fraud.

¹³ Record-level data may include Personally Identifiable Information or other details about suspected fraud. States and industry partners share record-level data with the ISAC; however, according to IRS officials, the IRS does not due to legal restrictions.

¹⁴ The Trusted Third Party analyzes identity theft leads to identify fraud patterns and trends. State and industry partners who have signed an information sharing agreement with the Trusted Third Party have access to these analytics.

¹⁵ Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government’s fiscal year begins on October 1 and ends on September 30.

¹⁶ 26 U.S.C. § 6103.

¹⁷ H.R. 5445.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Participation and use of the ISAC is increasing

Most States did not participate in the ISAC during its initial rollout for the 2017 Filing Season.¹⁸ For the 11 States that were registered during the 2017 Filing Season, users from only two States posted information to the ISAC. We surveyed the 42 States that have an individual income tax to obtain their input as to why they did not use the ISAC during the 2017 Filing Season. Of the 15 States that responded to our survey, seven stated concerns with the ISAC being duplicative of other tools and processes already available or commented on the difficulty of sharing data on the ISAC platform.

Recognizing the low participation in the ISAC, the IRS and Security Summit partners conducted outreach and education subsequent to the 2017 Filing Season on the use and benefits of the ISAC to combat identity theft. According to the April 2018 *Identity Theft Tax Refund Fraud ISAC Annual Report*, participation in the ISAC increased from 18 organizations participating in Calendar Year 2017 to more than 60 organizations (includes 28 States)¹⁹ with more than 400 registered users for Calendar Year 2018. The report also states that alert and data contributions by participating organizations have increased by more than six times since January 2017, which has increased the volume of data sharing as well as the quality of the ISAC's data analytics.

As with other participating organizations, the IRS's use of the ISAC has increased

For the 2017 Filing Season as of June 9, 2017, the IRS had used only three of the 40 alerts posted to the ISAC. IRS management informed us that it had already received information directly from the States or industry partners as part of other processes for the remaining 37 alerts. However, for the 2018 Filing Season as of April 30, 2018, the IRS used 37 of the 78 alerts posted to the ISAC to identify potentially fraudulent tax return schemes, some of which were previously unknown. The IRS reviewed the remaining 41 alerts; however, not all of the alerts provided actionable information for the IRS. The IRS reports that use of these alerts resulted in the identification of 2,637 potentially fraudulent tax returns with nearly \$13.5 million in refunds in the 2018 Filing Season.

In addition, to assist detection efforts by ISAC participants, the IRS posted 11 alerts to the ISAC since January 2017. These alerts relate to the IRS's identification of suspicious device identifications, dark web intelligence, fraudulent third-party authorizations, telephone schemes, and cyber alerts. Figure 2 shows the increase in usage of the ISAC by the IRS and State tax agencies between the 2017 and 2018 Filing Seasons.

¹⁸ The period from January through mid-April when most individual income tax returns are filed.

¹⁹ States with access to both ISAC data analytics and ISAC Collaboration space.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

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

Metric	2017 Filing Season	2018 Filing Season
State Partners ²⁰	20	28
Industry Partners	17	17
Registered Users	264	426
Alerts Posted	40 ²¹	78
Alerts Used by the IRS	3	37

Source: ISAC Program Update as of September 19, 2017, and April 30, 2018. Identity Theft Tax Refund Fraud ISAC as of May 10, 2018.

Figure 3 provides a further breakdown by submitter of alerts posted during the 2018 Filing Season.

**Figure 3: Alerts Posted to the ISAC
by Submitter for the 2018 Filing Season**

Submitter	Number of Alerts
State Partners	39
Tax Industry Partners	14
Submitter Blank	13
Other	5
IRS	6
Financial Industry Partners	1
Total	78

Source: Identity Theft Tax Refund Fraud ISAC as of May 10, 2018.

Expansion of the Deposit Account Verification Tool

In January 2017, the IRS partnered with a Security Summit industry provider of debit cards to implement and test an initiative called the *Deposit Account Verification Tool*. As part of this initiative, the IRS sends limited information to the debit card partner related to refunds claimed on identified potentially fraudulent tax returns that have a bank routing number belonging to a debit card issued by this partner’s organization. The debit card provider then evaluates the

²⁰ States with access to both the ISAC data analytics and the ISAC Collaboration space.

²¹ ISAC members posted an additional 31 alerts after the filing season as a result of their post-filing analysis.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

information it has for the individual associated with the debit card account to provide the risk level associated with the recipient account. For example, the debit card provider would indicate whether the recipient account has been verified and is in good standing at the time of the IRS inquiry or whether additional verification is suggested. As of April 25, 2018, the debit card provider responded to 158,447 IRS inquiries indicating that it would accept the deposit for 142,110 (89.7 percent) refunds and reject the deposit for with 13,656 (8.6 percent) refunds.²² Reasons the debit card provider rejects a deposit include that an existing bank account was not located, the taxpayer's last name and last four digits of the Social Security Number (SSN) did not match, the account is blocked or closed, the account type is not eligible to receive deposits, or the debit card is expired.

According to the IRS, participation in the *Deposit Account Verification Tool* initiative was expanded in Processing Year 2018, making the tool available to 12 States and two financial institutions. IRS management indicated that the Security Summit plans to further expand the use of this tool for Processing Year 2019 to additional Security Summit participants as well as expanding the number of financial institutions that participate.

The Use of a Dollar Tolerance and Programming Errors Resulted in Some Potentially Fraudulent Returns Not Being Identified

Our review identified that the IRS developed additional detection filters in response to prior Treasury Inspector General for Tax Administration (TIGTA) recommendations. For example:

- The IRS expanded the filters used to detect identity theft involving the use of Schedule C, *Profit or Loss From Business (Sole Proprietorship)*, income. In April 2015, we reported that existing filters did not detect 175,191 potentially fraudulent returns with refunds totaling \$611 million.²³ Our review of the expanded Schedule C filters found that they address our recommendation. For Processing Year 2017, the IRS reports that 87,489 returns were selected for review using the expanded Schedule C filters. As a result, the IRS protected \$289.4 million in revenue.
- The IRS modified its identity theft filters to no longer exclude returns with foreign addresses from potential identity theft detection. In April 2015, we reported that the IRS excluded tax returns with foreign addresses from the criteria used by its clustering tools. According to the IRS, it began using confirmed instances of identity theft with foreign addresses to refine its filters in Processing Year 2015. Our review of tax returns filed during Processing Year 2017 with a foreign address found that these tax returns were no longer excluded from detection filters. The IRS reports that 20,299 returns were selected

²² The remaining 2,681 (1.7 percent) refunds were still being verified by the debit card provider.

²³ TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

for review as of December 31, 2017. As a result, the IRS protected more than \$71.2 million in revenue.

However, exclusionary criteria associated with a filter developed in response to prior TIGTA recommendations,²⁴ as well as programming errors associated with another filter, resulted in 28,092 potentially fraudulent Tax Year 2016 tax returns as of May 25, 2017, with refunds totaling more than \$4.4 million, not being identified. The 28,092 returns include:

- 27,566 potentially fraudulent tax returns with refunds totaling almost \$1.3 million that were not selected for review despite using a same *****2*****
*****2***** that was used on at least one IRS-confirmed identity theft return. The filter,²⁵ implemented in June 2016, selects returns for review if the refund meets specific dollar tolerances. However, the tax returns we identified were below the refund dollar tolerances. IRS management indicated that the tolerances used in the filter are consistent with the tolerances used for IRS math error processing. It should be noted that between May 23, 2017, and August 7, 2017, six alerts were posted to the ISAC alerting the IRS and other ISAC users to an identity theft scheme involving refund amounts below the IRS's refund dollar tolerance amount.
- 526 potentially fraudulent tax returns with refunds totaling more than \$3.1 million that contain at least one confirmed Operation Mass Mailing (OMM)²⁶ characteristic and were not identified for review. We notified the IRS of our concerns on November 20, 2017. IRS management indicated that computer programming errors resulted in 473 (90 percent) tax returns with refunds totaling \$2.9 million not being identified for review. The IRS corrected the programming errors in January 2018. As of June 7, 2018, the IRS reports that 319 returns were selected for review using the confirmed OMM characteristic criteria. As a result, the IRS protected \$1.9 million in revenue. IRS management indicated that they were unable to determine why the remaining 53 returns with refunds totaling \$187,278 were not identified.

Recommendation

Recommendation 1: The Commissioner, Wage and Investment Division, should revise identity theft detection filters to eliminate specific refund dollar tolerances when identifying potentially fraudulent returns.

²⁴ 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 Improvement* (Feb. 2017).

²⁵ *****2*****
*****2*****

²⁶ In Processing Year 1999, the IRS Fraud Detection Center at the Brookhaven Campus first identified a scheme, known as the OMM scheme, in which unscrupulous individuals use the identities of residents of U.S. possessions, *i.e.*, Puerto Rico, Guam, and American Samoa, to obtain fraudulent tax refunds.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Management’s Response: The IRS disagreed with this recommendation. IRS management reviewed the 27,566 returns on which this recommendation was based and determined that only 388 of the returns were potentially fraudulent. IRS management does not believe elimination of the threshold criteria would be a wise use of resources considering the very low dollar amount of the refunds at stake, the additional burden placed on the other 27,178 taxpayers in this population whose returns did not have the potential for tax-related identity theft, and the cost of treating this group of returns. IRS management also responded that they have the ability to conduct detailed analyses on these returns outside the mainstream processes when an emerging trend is identified.

Office of Audit Comment: We believe that, at a minimum, the IRS should consider reducing the dollar tolerance. The IRS attributes continued improvement in its detection and prevention of identity theft tax returns to the Security Summit and most recently to the ISAC. However, IRS management is not acting on information from these valued partners alerting the IRS of a confirmed identity theft scheme: the filing of fraudulent returns with refund amounts below dollar tolerances for fraud detection and selection. The lack of action with regard to this known scheme increases the risk that fraudsters will continue to exploit weaknesses in IRS detection processes to obtain fraudulent refunds.

In addition, in their response, IRS management informed us that the primary factor considered when assessing the fraud potential of the 27,566 returns we identified was the existence of a wage or withholding reporting discrepancy. Other factors were disregarded, such as *****2***** In fact, the assessment performed by the IRS is not consistent with its statements in its *Fiscal Year 2018 Management’s Discussion and Analysis*²⁷ that “the profile of tax-related identity theft has changed and continues to grow more sophisticated. Today, identity theft returns often mirror the actual taxpayer’s return. This is due to the efforts by identity thieves to acquire actual federal tax information, such as employees’ Forms W-2, through phishing schemes targeting employers and/or payroll providers.” During Calendar Year 2017, the IRS received more than 450 reports of external data breaches that involved Form W-2 information.

We will continue to quantify the potential identity theft associated with this scheme during the 2019 Filing Season.

**Cost-Benefit Analysis Should Be Performed to Ensure That Expansion of
the Form W-2 Verification Code Initiative Is Warranted**

Beginning in Processing Year 2016, the IRS piloted the use of a Form W-2 verification code in

²⁷ Issued on November 20, 2018, the IRS Management’s Discussion and Analysis provides select IRS statistics for the fiscal year and discusses the IRS’s efforts during the fiscal year toward achieving its strategic plan.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

an effort to verify that Forms W-2 reported on tax returns were issued by a third-party payroll provider. The IRS initially partnered with four large payroll providers to test the use of a 16-digit code. For the 2018 Filing Season, the IRS expanded the initiative to partner with 10 payroll providers. These providers placed a verification code on approximately 61 million Forms W-2 for Tax Year 2017, representing 885,000 employers. The IRS provides the specifications required to generate the code to participating payroll providers in September prior the filing season, *e.g.*, in September 2017 for the 2018 Filing Season. The payroll providers are responsible for placing the unique verification code on each of their issued Forms W-2. The taxpayer or their tax return preparer is asked to provide the verification code when entering their Form W-2 information into an e-filed return.

However, changes to the Form W-2 filing requirements, as well as increased payroll provider and tax return preparer data breaches, justify additional evaluation to ensure that there is a continued business value in further expanding the Verification Code initiative. For example:

- Subsequent to the IRS piloting this initiative, Congress enacted the Protecting Americans from Tax Hikes Act,²⁸ which changed the filing date by which employers must file Forms W-2 with the SSA to January 31 (making them available for use by the IRS at the time tax returns are filed). Prior to the 2017 Filing Season, the due date for a paper Form W-2 was February 28; for an e-filed Form W-2, the due date was March 31.
- Attempts by unscrupulous individuals to obtain Form W-2 information from employers, payroll providers, and tax professionals significantly increase the risk that the verification code is compromised, thus reducing its usefulness. For example, the verification code is present on the Forms W-2 provided to employees. Employees also provide the code to their tax return preparer when they provide a copy of their Form W-2 for use in preparing their tax return. As such, Forms W-2 stolen from employers, their employees, or the tax professionals who prepare these individuals' tax returns would contain the verification code. Once obtained, identity thieves can use the "valid" verification code on the fraudulent tax return, thus adding one more factor to authenticate the return. In Calendar Year 2017, the IRS received more than 450 reports of data breaches involving Forms W-2 from external entities.

IRS management informed us that Processing Year 2018 will be the last year the Form W-2 Verification Code Program will operate as a pilot program. IRS management stated that they will assess the results of the W-2 Verification Code pilot and determine whether the program should be implemented for all payroll providers and employers. IRS management also informed us that, if they determine that the Form W-2 Verification Code Program should be implemented, additional resources will need to be expended to ensure that the program complies with the security standards required by the National Institute of Standards and Technology before it can

²⁸ Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015).



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

be implemented. The IRS estimated resources of \$220,174 would be needed to develop and continue the Form W-2 Verification Code Program as a pilot program in Filing Season 2018.

Recommendation

Recommendation 2: The Commissioner, Wage and Investment Division, should conduct an analysis to determine whether the reduction of the risk of tax-related identity theft resulting from the use of the Form W-2 verification code justifies the cost to fully implement the Form W-2 Verification Code Program.

Management's Response: The IRS agreed with this recommendation and has initiated an analysis to determine the future use of the Form W-2 Verification Code Program.

Adding Social Security Records That Are Currently Excluded From the Death Master File Could Further Reduce Risk of Misuse of Deceased Individuals' Identities to File Fraudulent Tax Returns

In September 2016, the SSA Office of the Inspector General reported that the SSA excluded approximately 8.7 million individuals for whom it has a date of death from the SSA Death Master File.²⁹ The IRS obtains and uses the SSA Death Master File to identify tax accounts associated with deceased individuals. In fact, the SSA Death Master File is the basis for one of the IRS's key efforts to prevent identity theft tax return filings using the Taxpayer Identification Number of a deceased individual – locking of the deceased individual's tax account. For example, as of May 15, 2017, the IRS locked approximately 33.9 million tax accounts of deceased individuals. The locking of a tax account results in the rejection of an e-filed tax return and prevention of a paper-filed tax return from posting to the IRS's Individual Master File³⁰ if the SSN associated with a locked tax account is used to file a tax return. However, the IRS's efforts to detect and prevent tax-related identity theft using deceased individuals' identities may be substantially incomplete as a result of incomplete SSA Death Master File data.

The SSA explained that these records were not previously added to the Death Master File because of its concerns regarding the accuracy of the information used to create death claim records prior to the creation of the electronic Numident Database³¹ in the early 1970s. However, on April 9, 2018, the SSA confirmed that it is undertaking an initiative to confirm the date of death information for individuals included on the Numident Database and update the Death Master File with these records. Once the records are added to the Death Master File, the IRS

²⁹ SSA Office of the Inspector General, A-06-16-50069, *Numident Death Information Not Included on the Death Master File* (Sept. 2016).

³⁰ The IRS database that maintains transactions or records of individual tax accounts.

³¹ The SSA Numident Database is used to create the Death Master File. Death information for approximately 8.7 million individuals was included on the Numident Database but was not included in the Death Master File.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

receives them through a secure data transfer process. The first update of 10,000 death records was included in the Death Master File data sent to the IRS during the weekend of March 17, 2018. The IRS received 999,998 additional death record updates during the weekend of April 7, 2018. SSA officials indicated that the SSA will complete updating the Death Master File by the end of Fiscal Year 2018 through a series of monthly updates.

The IRS updates its records weekly upon receipt of Death Master File information from the SSA. For those tax accounts added to the Death Master File as part of the previously mentioned SSA initiative, the IRS has processes in place to identify tax returns using the SSNs associated with these deceased individuals during processing. Once identified, error codes are added to the tax account, and the tax return will be suspended from processing while the IRS corresponds with the filer of the return to determine if the death information is incorrect or if the filer is authorized to claim a refund on behalf of the decedent. The taxpayer has 20 calendar days to respond to the IRS. If the taxpayer does not reply or the response is insufficient, the tax return is removed from processing. When an account has been locked erroneously due to incorrect death information, taxpayers are advised to resolve the error with the SSA. Upon receipt of the correction in the weekly Death Master File updates, the IRS record will be systemically corrected.

On May 30, 2018, we received more than 7.7 million SSNs from the SSA Office of the Inspector General for individuals for whom the SSA has a date of death on the Numident Database but the date of death was omitted from the Death Master File. Our analysis of tax returns filed in Processing Years 2015 through 2018 found that 2,807 of the 7.7 million SSNs were used 3,783 times on 3,596 tax returns. Of the 3,596 returns, 2,490 (69 percent) claimed refunds totaling more than \$8 million.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine the effectiveness of the IRS's ongoing efforts to detect and prevent identity theft. To accomplish our objective, we:

- I. Determined whether the IRS implemented corrective actions to address prior TIGTA recommendations¹ and assess the methodology to ensure the Identity Theft Taxonomy report provides accurate and reliable information.
 - A. Determined whether the IRS effectively used information received as part of the Form W-2, *Wage and Tax Statement*, verification code pilot during Processing Year² 2017.
 1. Met with IRS officials to determine how the IRS used this information during Processing Year 2017.
 2. Identified any changes the IRS will make to this program for Processing Year 2018 based on results from Processing Year 2017.
 - B. Identified potential Tax Year³ 2016 tax returns filed by identity thieves using criteria used in the prior TIGTA audit report based on Schedule C, *Profit or Loss From Business (Sole Proprietorship)*, income claimed on the tax return. Our analysis identified undetected tax returns using an SSN.
 - C. Assessed the IRS's efforts to develop criteria to identify and evaluate potentially fraudulent tax returns below the refund dollar tolerance for Processing Year 2017.
 1. Reviewed the DDb⁴ to identify the new business rule implemented to select potentially fraudulent tax returns when the refund claimed was below the dollar tolerance.

¹ 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 Improvement* (Feb. 2017).

TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).

² The calendar year in which the tax return or document is processed by the IRS.

³ A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.

⁴ A rules-based system that incorporates information from many sources that include the Department of Health and Human Services, the SSA, and the IRS. The IRS implemented identity theft rules within the DDb system in Processing Year 2012. Tax returns are analyzed to identify potentially fraudulent tax returns involving identity theft.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

2. Analyzed Processing Year 2017 tax return information to determine whether the DDb business rule accurately identified tax returns below the refund dollar tolerance.
 3. If applicable, provided examples of the cases identified in Step I.C.2. to the IRS for its review and determination as to how the tax returns bypassed IRS controls.
- D. Assessed the IRS's efforts to develop criteria to identify and evaluate potential identity theft tax returns filed using foreign address in Processing Year 2017.
- E. Assessed the IRS's efforts to develop a process to timely use State lead data as another characteristic to evaluate tax returns during processing potential identity theft tax returns.
- II. Determined the effectiveness of the IRS's continued efforts to detect and prevent identity theft, including ongoing efforts to measure undetected identity theft and coordinate information with other Government agencies and tax industry partners.
- A. Assessed the effectiveness of the ISAC.
1. Met with IRS officials to discuss how they used the information received as part of the Identity Theft Tax Refund Fraud ISAC in Processing Year 2017.
 2. Discussed how the IRS plans to change/improve this initiative in Processing Year 2018.
- B. Determined whether the records missing a date of death identified by the SSA Office of the Inspector General have been locked in IRS records.
1. Determined whether the IRS received a date of death for all identified individuals.
 2. Obtained the list of records missing a date of death from the SSA Office of the Inspector General.
 3. Analyzed SSA data and identified tax returns filed using the identities of individuals who had a date of death that was omitted from the Death Master File.⁵ For those individuals who are not on the active Individual Master File,⁶ we determined whether sufficient controls are in place to prevent future misuse.

⁵ The IRS obtains and uses the SSA Death Master File to identify tax accounts associated with deceased individuals.

⁶ The IRS database that maintains transactions or records of individual tax accounts.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

- III. Determined the effectiveness of the IRS's efforts to detect and prevent OMM tax returns posting to the Master File.
- A. Reviewed the Internal Revenue Manual, desk procedures, and other internal IRS resources and evaluated the sufficiency of IRS return processing and identity theft filters and procedures intended to prevent the erroneous refunds on OMM returns.
- B. Analyzed Processing Year 2017 tax returns to identify tax returns that meet the characteristics of the OMM matrix.
1. Determined whether the tax returns identified in Step III.B. have been identified by any IRS processes as potential identity theft.
 2. Provided examples of the cases identified in Step III.B. to the IRS for its review and determination as to how the refund bypassed IRS controls.
- C. Quantified the impact of weaknesses in the IRS's controls to detect and prevent the erroneous issuance of refunds on OMM tax returns.

Validity and reliability of data from computer-based systems

During this review, we relied on data extracted from the TIGTA Data Center Warehouse⁷ of the IRS's Individual Master File⁸ for Tax Year 2016, the Individual Return Transaction File⁹ for Processing Year 2017, the Modernized Tax Return Database¹⁰ for Processing Year 2017, the National Account Profile database,¹¹ and the Form W-2 File¹² for Tax Years 2015 and 2016. We obtained from the SSA Office of the Inspector General an electronic download of records for deceased individuals contained in the SSA Numident Database.¹³ Before relying on the data, we ensured that each file contained the specific data elements we requested. In addition, we reviewed judgmental samples of the data extracted and verified that the data in the extracts were the same as the data captured in the IRS's Integrated Data Retrieval System.¹⁴ These tests demonstrated that the data were sufficiently reliable and could be used to meet the objectives of this audit.

⁷ A collection of IRS databases containing various types of taxpayer account information that is maintained by TIGTA for the purpose of analyzing data for ongoing audits.

⁸ The IRS database that maintains transactions or records of individual tax accounts.

⁹ This file contains data transcribed from initial input of the original individual tax returns during return processing.

¹⁰ The Modernized Tax Return Database is the legal repository for original electronically filed returns received by the IRS through the Modernized e-File system.

¹¹ A compilation of selected entity data from various Master Files that also includes data from the SSA.

¹² The Form W-2 database is created by TIGTA using IRS information reported on Forms W-2 for each tax year.

¹³ The SSA Numident Database is used to create the Death Master File. Death information for approximately 8.7 million individuals was included on the Numident Database but was not included in the Death Master File.

¹⁴ IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

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: the IRS's return processing, identity theft filters, and identity theft procedures intended to prevent issuance of refunds on potential identity theft tax accounts. We evaluated these controls by interviewing employees and management, analyzing data and reviewing tax returns identified by the system, and reviewing policies and procedures.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Deann L. Baiza, Director
Linna K. Hung, Audit Manager
Jane G. Lee, Lead Auditor
Jeffrey D. Cullum, Senior Auditor
Joyce L. Bruggisser, Auditor
Brieane K. Hamaoka, Auditor



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Appendix III

Report Distribution List

Deputy Commissioner for Services and Enforcement
Commissioner, Wage and Investment Division
Deputy Chief Information Officer for Operations
Deputy Commissioner, Wage and Investment Division
Associate Chief Information Officer, Applications Development
Chief Research and Analytics Officer
Director, Customer Account Services, Wage and Investment Division
Director, Operations Support, Wage and Investment Division
Director, Return Integrity and Compliance Services, Wage and Investment Division
Director, Submission Processing, Wage and Investment Division
Director, Office of Audit Coordination



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Revenue Protection – Actual; \$360,604,677 in confirmed fraudulent refunds resulting from the IRS’s use of expanded identity theft filters (see page 8).

Methodology Used to Measure the Reported Benefit:

In response to prior TIGTA recommendations,¹ the IRS:

- Expanded the filters used to detect identity theft involving the use of Schedule C, *Profit or Loss From Business (Sole Proprietorship)*, income. For Processing Year 2017, the IRS reports that 87,489 returns were selected for review using the expanded Schedule C filters. As a result, the IRS protected \$289,402,267 in revenue.
- Modified its identity theft filters to no longer exclude returns with foreign addresses from selection for review. For Processing Year 2017, the IRS reports that 20,299 returns were selected for review using the expanded clustering tool criteria. As a result, the IRS protected \$71,202,410 in revenue.

We first reported concerns with the IRS’s identity theft detection filters in July 2012.² We recommended that the IRS develop processes to analyze characteristics of fraudulent tax returns resulting from identity theft and continue to refine and expand the IRS’s tax processing filters used to detect and prevent the issuance of fraudulent tax refunds resulting from identity theft. We estimated the IRS could have protected more than \$5.2 billion in revenue in Tax Year 2010 as a result of our recommendation. We also forecast that the IRS would not detect more than \$20.7 billion in identity theft in Tax Years 2010 through 2014 as a result of these weaknesses.

¹ TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).

² TIGA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).



Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft

Type and Value of Outcome Measure:

- Revenue Protection – Potential; 2 potentially fraudulent returns with refunds totaling \$2 that were not selected for review as a result of the IRS’s use of dollar tolerances (see page 8).

Methodology Used to Measure the Reported Benefit:

We previously reported concerns with the IRS’s selection of below the dollar tolerance returns for review in February 2017.³ We recommended that the IRS develop criteria to identify and evaluate for fraud potential tax returns below the refund dollar tolerance amount for the entire processing year. On June 13, 2016, the IRS implemented a new business rule within the DDb that selected potentially fraudulent returns when the claimed refund was below the dollar tolerance. However, the revised filters do not ensure that all potentially fraudulent returns with refunds below the dollar tolerance are selected for review.

Our analysis of Tax Year 2016 returns identified 2 potentially fraudulent tax returns with refunds totaling \$2 that were not selected for additional review because the refund amount was \$2. These returns had the following characteristics: [REDACTED]

Type and Value of Outcome Measure:

- Revenue Protection – Actual; 473 potentially fraudulent returns with refunds totaling \$2,942,496 that were not selected for review despite having characteristics of a known identity theft fraud scheme (see page 8).

Methodology Used to Measure the Reported Benefit:

We reported concerns with the IRS’s processes to detect and prevent fraudulent refunds resulting from the OMM scheme in July 2012. We recommended that the IRS develop processes to analyze characteristics of fraudulent tax returns resulting from identity theft and continue to refine and expand the IRS’s tax processing filters used to detect and prevent the issuance of fraudulent tax refunds resulting from identity theft.

The IRS implemented filters to systemically identify tax returns with the characteristics of the OMM scheme. However, our analysis of Tax Year 2016 returns identified 526 potentially fraudulent returns with refunds totaling \$3,129,774 that were not identified for review despite containing at least one confirmed OMM characteristic. IRS management indicated that 473 (90 percent) of the 526 returns resulted from programming errors. The IRS corrected the

³ 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 Improvement* (Feb. 2017).



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

error in January 2018. IRS management indicated that they were unable to determine why the remaining 53 returns were not identified.



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Appendix V

Prior TIGTA Audit Reports on Identity Theft

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 Improvement* (Feb. 2017).

TIGTA, Ref. No. 2016-40-008, *Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection* (Dec. 2015).

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

TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).

TIGTA, Ref. No. 2013-40-122, *Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds* (Sept. 2013).

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



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Appendix VI

Management's Response to the Draft Report

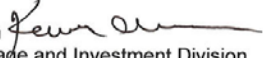


COMMISSIONER
WAGE AND INVESTMENT DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

NOV 08 2018

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin 
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Partnership With State and Industry Leaders
Is a Key Focus in Further Reducing Tax-Related Identity Theft
(Audit #201740007)

Thank you for the opportunity to review and comment on the subject draft report. We appreciate your acknowledgement of the positive results we have accomplished with our Security Summit partners in combatting tax-related identity theft at the state and federal levels. The creation of the Information Sharing and Analysis Center (ISAC), which is a vehicle through which information on known and emerging threats is shared among participants, is a hallmark achievement of the Security Summit. The creation of the ISAC and its use by participating members benefits tax administration by improving the timeliness in which taxing authorities may become aware of the ever-evolving tactics employed by the perpetrators of tax-related identity theft and fortify their defenses against it. The value of the ISAC is illustrated by the expanded participation it experienced in 2017, growing from 18 participating organizations to more than 60 by year-end.

Tax-related identity theft occurs when an individual uses another person's name and Taxpayer Identification Number to file a fraudulent tax return. The detection of tax-related identity theft can be challenging in that one of the goals of a fraudster is to learn controls, such as detection thresholds, and develop schemes that bypass those controls and, thus, detection. During and since 2017, we continued to expand and improve our identity theft detection and prevention capabilities. The report notes our use of 200 identity theft filters to identify potentially fraudulent tax returns when they are filed and stop the payment of claimed refunds. The 652,119 fraudulent tax returns, claiming over \$7.2 billion in refunds, that are reported as having been identified through December 31, 2017, do not include those cases that were identified but not yet resolved at year-end. As of June 14, 2018, the number of returns received during 2017 and determined to be



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

2

tax-related identity theft attempts had increased to 670,857, with associated refunds totaling more than \$8.8 billion that were stopped before payment.

We also appreciate your acknowledgement that modifications we made to our business income and address filters identified almost 108,000 returns for review and protected over \$360 million. We agree that exclusionary criteria based on threshold tolerance levels does not capture and suspend questionable returns with very low refund amounts. We disagree, however, with the conclusion that the threshold tolerance criteria should be removed from the filters. We also disagree with the reported outcome measure associated with this finding. Of the ***2*** returns identified as potentially fraudulent returns because a filter data element matched at least one other return that had been determined as fraudulent, none claimed a refund above **2**. The average refund amount for the population was ***2***. When we reviewed the ***2*** returns only ***2*** (0.014 percent) were determined to be potentially fraudulent. Introducing these returns into our primary treatment processes would not only significantly increase the burden to legitimate taxpayers whose returns are identified, but the cost of treatment, in most cases, would exceed the amount protected. When an emerging issue is identified, our Fraud Risk Evaluation process can select these returns for closer evaluation and consider their attributes when determining if filter selection criteria should be modified.

We agree with your recommendation to assess the benefits of continuing the Form W-2, Wage and Tax Statement, Verification Code (VC) program. As initially conceived, it was believed the VC could be used to authenticate taxpayers when their returns were filed; however, as noted in the report, the high levels of data breaches experienced by employers and other third-parties in possession of payroll information have rendered the VC ineffective as an identity authenticator and we no longer use it for that purpose. In 2018, the VC was useful in confirming the accuracy of Form W-2 data transcribed by taxpayers or return preparers on electronic returns. There is a short period of time, early in the year, when an electronic return may be filed with the IRS but Form W-2 data from the Social Security Administration has not yet been received or available to our systems. In that instance, the VC will confirm that the wage and withholding information presented on the return reconciles with the information reported by the employer and will satisfy non-identity theft validation processes.

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

Attachment



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

Attachment

Recommendations

RECOMMENDATION 1

The Commissioner, Wage and Investment Division, should revise identity theft detection filters to eliminate specific refund dollar tolerances when identifying potentially fraudulent returns.

CORRECTIVE ACTION

We disagree with this recommendation. Our analysis of the ***2*** returns upon which the recommendation is based found that only **2** were potentially fraudulent. When considering the very low dollar amount of the refunds at stake, the additional burden placed on the other **2** taxpayers in this population whose returns were found not to have potential for tax-related identity theft, and the cost of treating this group of returns, we do not believe elimination of the threshold criteria would be a wise use of resources. Further, we do have the ability to do detailed analyses on these returns outside the mainstream processes when an emerging trend is identified.

IMPLEMENTATION DATE

N/A

RESPONSIBLE OFFICIAL

N/A

CORRECTIVE ACTION MONITORING PLAN

N/A

RECOMMENDATION 2

The Commissioner, Wage and Investment Division, should conduct an analysis to determine whether the reduction of the risk of tax-related identity theft resulting from the use of the Form W-2 verification code justifies the cost to fully implement the Form W-2 Verification Code Program.

CORRECTIVE ACTION

We agree with this recommendation and have initiated an analysis to determine the future use of the Form W-2, Wage and Tax Statement, Verification Code Program.

IMPLEMENTATION DATE

May 15, 2019

RESPONSIBLE OFFICIAL

Director, Return Integrity Operations, Return Integrity and Compliance Services, Wage and Investment Division



*Partnership With State and Industry Leaders Is a
Key Focus in Further Reducing Tax-Related Identity Theft*

2

CORRECTIVE ACTION MONITORING PLAN

We will monitor this corrective action as part of our internal management control system.