TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Successful Detection and Assistance Processes Used to Combat Individual Identity Theft Should Be Implemented for Business Identity Theft

July 27, 2022

Report Number: 2022-40-041

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Successful Detection and Assistance Processes Used to Combat Individual Identity Theft Should Be Implemented for Business Identity Theft

Final Audit Report issued on July 27, 2022 **Report Number 2022-40-041**

Why TIGTA Did This Audit

Identity theft patterns are constantly evolving and, as such, the IRS needs to continually adapt its detection and prevention processes by adjusting its existing filters and expanding its detection processes to include additional business tax return types. Our overall objective was to assess the IRS's continued efforts to detect and prevent business identity theft.

Impact on Tax Administration

The IRS published its first Business Taxonomy Report and reported protecting almost $3.8 billion in fraudulent tax refunds from being issued since Tax Year 2016. The IRS also reported that identity thieves successfully received fraudulent refunds ranging between about $6 million and $3.2 billion.

Furthermore, the IRS has not adequately addressed the risk of unsupported [redacted] related to business tax returns. TIGTA's review identified 3,243 [redacted], filed as of December 31, 2020, with refunds totaling approximately $17.2 million with characteristics of confirmed fraudulent tax returns, including [redacted], which were not selected by the IRS's filters.

What TIGTA Found

The IRS continues to improve and expand its detection capabilities to include additional types of business tax returns. During Processing Year 2021, the IRS used 84 selection filters to identify business tax returns claiming refunds for potential fraud. Filters identified and selected for review 60,296 business returns as potentially fraudulent.

In addition to the continued expansion of its business identity theft detection filters, the IRS continues to take actions to address deficiencies reported in prior reviews. These actions include developing procedures to promptly review business tax returns with high-dollar refunds and implementing a selection filter that identifies discrepancies with the reporting of estimated tax payments. The IRS also continues to use information from partners, *i.e.*, the States, and information provided on a newly released affidavit form to further expand its detection efforts.

However, our assessment of the IRS's efforts to combat business identity theft and assist these types of victims identified that efforts can be improved if the IRS adopts successful taxpayer detection and assistance options, similar to those it provides to individual taxpayers. These include developing clustering filters for business identity theft detection and expanding Identity Protection Personal Identification Numbers to business taxpayers.

Finally, the IRS is in the process of developing a new Form 1099 intake system and plans to incorporate the same controls into the new system as the IRS agreed to implement in the prior intake system. The new Form 1099 intake system is scheduled for implementation by January 2023.

What TIGTA Recommended

TIGTA made four recommendations to improve the identification of business identity theft including evaluating the expansion of clustering in business identity theft filters; continuing research to make the Identity Protection Personal Identification Number program available to businesses; and developing a program to identify and verify [redacted] that are potentially fraudulent.

The IRS agreed with three of the four recommendations; however, the IRS did not agree to develop a program to identify and verify [redacted]. TIGTA continues to believe that a prerefund process is needed to prevent the issuance of potentially fraudulent refunds.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20224

July 27, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Successful Detection and Assistance Processes Used to Combat Individual Identity Theft Should Be Implemented for Business Identity Theft (Audit # 202140019)

This report presents the results of our review to assess the Internal Revenue Service's continued efforts to detect and prevent business identity theft. This review is part of our Fiscal Year 2022 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 III.

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 Diana M. Tengesdal, Acting Assistant Inspector General for Audit (Returns Processing and Account Services).

Table of Contents

Appendices

Background

The Internal Revenue Service (IRS) defines business identity theft as creating, using, or attempting to use a business's identifying information without authority to obtain tax benefits. Examples include the following:

- An identity thief files a business tax return, [redacted], using the Employer Identification Number (EIN)[1] of an active or inactive business without the permission or knowledge of the EIN's owner to obtain a fraudulent refund.
- An identity thief, using the EIN of an active or inactive business without the permission or knowledge of the EIN's owner, files [redacted], claiming a fraudulent refund.
- An identity thief applies for and obtains an EIN using the name and Social Security Number[2] of another individual as the responsible party (fraudulently obtained EIN) without their approval or knowledge to file fraudulent tax returns, [redacted], avoid paying taxes, obtain a refund, or further perpetuate individual identity theft or refund fraud.

Processes to identify potentially fraudulent business tax returns as a result of identity theft

The IRS systemically evaluates business tax returns claiming refunds for potential fraud during tax return processing by using business identity theft filters included in the Dependent Database.[3] During Processing Year (PY) 2018, the IRS used 35 filters to detect business identity theft. This expanded to 84 filters for PY 2020. For the majority of PY 2021, the IRS had 84 filters; however, these filters are different from PY 2020 as the IRS added seven new filters, disabled eight filters, and re-enabled an old filter based on emerging identity theft schemes and the IRS's evaluation of the filters. The IRS also has nine filters that use the *Dynamic Selection List*.[4] Based on these filters, when a tax return is identified as potentially fraudulent resulting from business identity theft, the IRS places a hold on the associated tax account to prevent the refund from issuing. Tax analysts in the Return Integrity and Compliance Services (RICS) function then manually screen the identified tax returns that meet a certain criterion, *e.g.*, refunds at a certain dollar tolerance, to determine whether they are identity theft tax returns. This includes researching the associated tax account to determine if the taxpayer made payments and

[1] A unique, nine-digit number used to identify a taxpayer's business account.

[2] A nine-digit number issued to an individual by the Social Security Administration. The IRS uses this number to process tax documents and returns.

[3] An IRS system that uses a set of sophisticated rules and scoring models along with internal and external data to evaluate tax returns to validate taxpayers' entitlement to refunds. This system scores tax returns and selects questionable returns for audit.

[4] A list of EINs, bank routing and account numbers, preparers, *etc.*, that the IRS has determined to be suspicious. The IRS selects tax returns for potential identity theft treatment if the tax return characteristics match to the *Dynamic Selection List*.

evaluating whether the characteristics of the tax return [redacted].

For those tax returns determined to be legitimate, the IRS releases the refund hold and the tax return continues to process with any associated refund being issued. For the tax returns that remain as potential identity theft, business filers are sent Letter 6042C, *Entity Verification for Business*. This letter requests that the business or associated business owner provide additional information about the business that will assist the IRS in authenticating the tax return filed. The IRS evaluates the responses received and takes one of the following actions:

- If the taxpayer's response supports the legitimacy of the business, the IRS removes the hold on the refund and posts the tax return for continued processing.
- If the taxpayer's response confirms the business filer is a victim of identity theft, the IRS will place an identity theft indicator on the associated business tax account confirming that the tax return is an identity theft filing. For those confirmed identity theft filings associated with a fabricated entity,[5] the IRS will deactivate the associated tax account, *i.e.*, lock the tax account. Once a tax account is locked, no future tax returns will be accepted for processing using that EIN.

If the business tax return filing is a [redacted] and no response is received, the IRS does not process the tax return. For these tax returns, the IRS maintains the refund hold until either a response is received, *i.e.*, to confirm a legitimate tax return filing, or for one year after the filing of the tax return. After the one-year hold expires, the IRS removes the tax return from further processing to permanently prevent the issuance of the refund, *i.e.*, the tax return will not be posted to the Master File. Beginning in PY 2022, the IRS will also follow the same process for business tax returns in the [redacted],[6] [redacted]. Additionally, the refund hold is now three years. The IRS extended the refund hold requirement to three years to [redacted].

The IRS developed Form 14039-B, *Business Identity Theft Affidavit*, for business taxpayers to report suspected identity theft

On August 1, 2020, the IRS released Form 14039-B, which allows taxpayers to report that they suspect their business entity, estate, trust, or exempt organization has been a victim of identity theft. Form 14039-B is used to obtain necessary information from the taxpayer to attest that they have been a victim of business identity theft. Once the IRS receives Form 14039-B, the taxpayer is sent an acknowledgement letter within 30 calendar days of receipt. The IRS will input an identity theft indicator on the associated business taxpayer's tax account. This indicator marks the tax account as potential identity theft so other business units within the IRS are aware of the potential identity theft issue. The account is then referred to either the Return Integrity Verification Operations or Accounts Management Identity Theft Victims Assistance group to

[5] A fabricated entity is an entity that was established for the sole purpose of defrauding the Federal Government through the filing of false individual and business refund returns or income documents.

[6] This includes a [redacted].

conduct research to close the case using the appropriate closing actions, *e.g.*, reverse the identity theft indicator, input a fabricated EIN indicator, or mark the account as confirmed identity theft.

Results of Review

This report presents the results of our continued evaluation of the IRS's efforts to combat business identity theft. As we have reported in our prior reviews, the IRS continues to improve and expand its detection capabilities to include additional types of business tax returns. Figure 1 provides a comparison of the IRS's business identity theft filter results, by return type, for Calendar Years 2020 and 2021.

Figure 1: Comparison of Business Identity Theft Filter Results (Calendar Years 2020 and 2021)

	[redacted]	[redacted][7]	[redacted][8]	Total Refund Returns[9]
Calendar Year 2021				
Selected	10,887	11,015	19,105	41,007
Confirmed Identity Theft	54	179	48	281
Refunds Protected	$23 million	$53 million	$2.3 trillion[10]	$2.3 trillion
Calendar Year 2020				
Selected	11,177	12,030	12,609	35,816
Confirmed Identity Theft	45	394	33	472
Refunds Protected	$41 million	$172 million	$7.3 trillion[11]	$7.3 trillion

Source: Business Master File Identity Check Database Inventory Summary by Form Type for Calendar Years 2020 and 2021, as of December 23, 2021.

In addition to tax forms detailed in Figure 1, the IRS's business identity theft filters also identify [redacted]. The taxpayer's reporting of [redacted] then either result in the taxpayer

[7] This includes [redacted].

[8] This includes [redacted].

[9] As of December 23, 2021, the IRS still had 43,625 potentially fraudulent business tax returns that remained to be evaluated by tax examiners in the RICS function. This backlog of potentially fraudulent tax returns to be evaluated results from the closing of the Tax Processing Centers in response to the Coronavirus Disease 2019 pandemic.

[10] This includes [redacted].

[11] This includes [redacted].

fraudulently reducing their tax owed or in the fraudulent issuance of a refund. As of December 23, 2021, the IRS reports that it identified:

- 21,194 potentially fraudulent [redacted] in Calendar Year 2020 resulting in 14 tax returns being confirmed as identity theft with the fraudulent reporting of $5.6 million [redacted].
- 19,289 potentially fraudulent [redacted] in Calendar Year 2021 resulting in 10 confirmed identity theft tax returns with the fraudulent reporting of $404,309 [redacted].

In addition to the continued expansion of its business identity theft detection filters, our review also identified that the IRS continues to take actions to address deficiencies reported in prior Treasury Inspector General for Tax Administration (TIGTA) reviews.[12] These actions include:

- Developing procedures to review business tax returns with high-dollar refunds that were identified as potential identity theft. In our August 2018 review, we identified 25 tax returns with [redacted] that were not promptly reviewed resulting in unnecessarily paid interest totaling more than $4 million. As a result, the IRS now has a process to monitor these cases to avoid paying interest unnecessarily.
- Providing additional training to RICS function employees to ensure that cases are timely reviewed, refunds are promptly released once a non-identity theft determination is made, and that other functions are not releasing refunds controlled by RICS. This included resubmitting a request for programming updates to prevent other functions from erroneously releasing refunds on RICS-controlled cases. Although this programming has not been completed, our testing shows that outreach performed by the RICS function has resulted in a significant reduction of potentially fraudulent refunds from being released erroneously. For example, our review identified four cases that potentially had their refunds released erroneously during PY 2020 and PY 2021 compared to 1,966 cases we identified during PY 2018 and PY 2019.
- Implementing processes to monitor and update the *Suspicious EIN Listing*.[13] Once an EIN is on the list, the IRS reviews future tax returns filings associated with these EINs to identify additional fraudulent tax returns. As of December 29, 2020, the *Suspicious EIN Listing* included 8,388 EINs. Moreover, the IRS will lock those EINs on the list determined to be fabricated.[14] As of August 2021, there are 47,669 EINs locked as fabricated EINs.[15] The IRS uses the fabricated entity indicator on the business's account and the fabricated indicator on information returns[16] to identify potentially fraudulent tax return filings by

[12] TIGTA, Report No. 2018-40-061, *Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft* (Aug. 2018) and TIGTA, Report No. 2021-40-004, *Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts* (Oct. 2020).

[13] The *Suspicious EIN Listing* contains EINs that the IRS has determined to have suspicious activity as a result of fraudulent tax return filing or identified through the IRS's Criminal Investigation.

[14] A fabricated EIN is established for the sole purpose of defrauding the Government through the filing of false individual and business refund tax returns or information returns.

[15] Some of these EINs are included on the *Suspicious EIN Listing*.

[16] Information returns include Form 1099 series and Form W-2 documents.

individuals. Our testing confirmed that the IRS is appropriately selecting tax returns being filed using fabricated EINs.

- Implementing a filter that identifies discrepancies with [redacted]. During PY 2020, the [redacted] filter selected 5,857 tax returns, of which 1,171 tax returns were confirmed identity theft. The remaining 4,686 tax returns were determined to not be identity theft. There are additional controls in place to identify tax returns with [redacted] and [redacted] to ensure the accuracy of the tax return filing.

Finally, the IRS continues to use information from partners and information provided on a newly released affidavit form to further expand its detection efforts. Specifically:

- **Information Sharing and Analysis Center (ISAC) alerts are used to identify business identity theft.** The ISAC is a web-based portal operated by a Trusted Third Party[17] for States, industry, and the IRS to share information related to fraudulent tax return filings. The IRS receives alerts via the ISAC, which the IRS reviews to determine if the alerts are applicable to the filing of Federal tax returns. The IRS uses the alerts to update its *Dynamic Selection List* with information, such as an EIN, to improve fraud detection. During PY 2020, the *Dynamic Selection List* identified 31 tax returns that were confirmed as business identity theft or as a frivolous filer.[18] For PY 2021, the *Dynamic Selection List* identified 61 tax returns that were confirmed fraudulent, *i.e.*, identity theft[19] or frivolous filer, and protected refunds totaling $256 billion, as of October 9, 2021.[20]
- **Business Identity Theft Affidavits are used by businesses to report suspected business identity theft.** Between August 1, 2020, and May 21, 2021, the IRS received a total of 135 Forms 14039-B, of which 15 have been confirmed as business identity theft. Based on these forms, the IRS marked these accounts as confirmed identity theft to help protect against future fraudulent filings. The remaining Forms 14039-B have been determined not to be identity theft or are still being reviewed by the IRS.

Additional Business Identity Theft Detection and Prevention Capabilities, Similar to Those Used for Individual Tax Returns, Are Needed

As we have reported previously,[21] the IRS's efforts to detect fraudulent individual tax returns involving identity theft have continued to significantly reduce the losses associated with this type of fraud. Similarly, we have also reported on the various increased protections the IRS

[17] The Trusted Third Party is an IRS Federally Funded Research and Development Center that facilitates information sharing among members of the ISAC.

[18] A frivolous tax argument is based on a frivolous or incorrect interpretation of the Federal tax law. The IRS continues to identify frivolous tax arguments and reports these arguments annually on the "Dirty Dozen Tax Scams" list. Individuals and businesses use these frivolous tax arguments to support their claims that they are not subject to Federal tax laws.

[19] Confirmed identity theft includes cases in which the taxpayer did not respond to authentication letters.

[20] There were [redacted] with refunds [redacted]. Without [redacted], the IRS protected [redacted] in refunds.

[21] TIGTA, Report No. 2020-40-040, *Constantly Evolving Refund Fraud Patterns Require Continued Refinement and Development of Detection Initiatives* (July 2020).

offers to assist individual taxpayer identity theft victims. This includes the implementation of provisions outlined in the *Taxpayer First Act*,[22] which includes the IRS participating in the ISAC and expansion of the Identity Protection Personal Identification Number (IP PIN).

However, our assessment of the IRS's efforts to combat business identity theft and assist these types of victims identified that efforts can be improved if the IRS adopts successful individual taxpayer detection and assistance options, similar to what it provides to individual taxpayers. This includes:

- **Developing clustering filters for business identity theft detection.** As we have reported, one of the characteristics of potentially fraudulent individual identity theft tax returns is the use of the [redacted]. In response to recommendations we made, the IRS developed a filtering tool for individual tax returns to identify groups of tax returns based upon [redacted], known as clusters. Since we first reported on these characteristics in July 2012,[23] the IRS has continued to expand its clustering filters to include additional commonality criterion such as [redacted]. Clustering filters are currently part of both the Dependent Database and the Return Review Program,[24] which are the primary detection systems for individual tax returns. Although development has stopped on the Return Review Program, as of March 2022, the IRS has identified the Return Review Program as a potential area to expand business identity theft detection. The IRS is evaluating the available resources to determine what capabilities can be developed into the Return Review Program.

  These types of filters are not being used to identify potential business identity theft tax returns. IRS management indicated that they were developing clustering filters to identify business tax returns. However, in November 2019, the IRS ceased the continued development of not only clustering filters, but also additional business fraud filters in the Return Review Program as a result of funding constraints. Although the IRS stopped the development of enhanced business identity theft detection capabilities in its Return Review Program, as noted previously, the IRS should evaluate how it can implement these filters in the Dependent Database similar to what is used for individual tax returns.

- **Expanding IP PIN to business taxpayers.** The IRS began issuing IP PINs to eligible taxpayers in Fiscal Year 2011. Use of an IP PIN provides relief to taxpayers because it allows the IRS to process their tax returns without delay and helps prevent the misuse of the taxpayers' Social Security Number on fraudulent tax returns. Each December, the IRS mails IP PINs to taxpayers who are confirmed by the IRS as victims of identity theft. The IRS also proactively provides an IP PIN to taxpayers via its *Opt-In Program*. The *Opt-In Program* enables taxpayers who are concerned about becoming a victim of identity theft to proactively request an IP PIN.

  However, there is no such program for businesses to protect their tax account from fraudulent filings. IRS management stated that research to determine the feasibility of

[22] Pub. L. No. 116-25, 133 Stat. 981.

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

[24] 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.

expanding the IP PIN to business taxpayers started in late Calendar Year 2019. However, due to the Coronavirus Disease 2019 pandemic and redirected resources, the research was placed on hold. The IRS plans to report on this feasibility by December 2022.

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Evaluate various business tax return common characteristics, *i.e.*, [redacted], which can be used to develop clustering filters to be added to the Dependent Database.

Management's Response: The IRS agreed with this recommendation and plans to evaluate various common tax return characteristics to determine if clustering filters should be developed.

Recommendation 2: Develop processes to assign an IP PIN to business taxpayers that are confirmed victims of tax-related identity theft for use in filing of business tax returns and for business taxpayers to proactively request an IP PIN if they are concerned about becoming a victim of business identity theft.

Management's Response: The IRS agreed with this recommendation and is currently completing an analysis to determine the feasibility of assigning the IP PINs to business taxpayers. IRS management stated that assigning an IP PIN to a business entity presents numerous challenges that are not associated with assignment to individual taxpayers. However, management will consider the next steps for the business entity IP PIN based on this analysis.

Management Needs to Develop a Fraud Program to Identify and Verify [redacted], a Known Characteristic of Fraudulent Business Tax Returns

In October 2020, we reported that the IRS needed to evaluate and adjust its detection filters to address ever-changing business tax return filing fraud patterns.[25] Specifically, our review identified 11,908 [redacted], filed as of December 31, 2019, with refunds totaling almost $63.2 million whereby the [redacted]. Unlike for individual tax returns, IRS filters do not identify this as a characteristic of a potentially fraudulent [redacted]. To address this concern, we recommended that the IRS expand the [redacted] business identity theft filters to include [redacted]. The IRS agreed and stated it would conduct an analysis to determine the effectiveness of incorporating this as a characteristic in its detection filters.

Based upon its analysis, the IRS determined that it was not necessary to expand its business identity theft filters for [redacted] to include [redacted]. IRS management indicated that their review of the tax returns from our prior audit did not identify any indications

[25] TIGTA, Report No. 2021-40-004, *Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts* (Oct. 2020).

of identity theft resulting in the potentially fraudulent filing but agreed that these tax returns may involve a fraudulent business tax return filing. The IRS noted that due to the increasing complexity of [redacted] is not a reliable element to include in its business identity theft filters. For example, IRS management explained that the [redacted]. Additionally, information returns report income on a calendar year resulting in mismatches with tax returns that are not filed by calendar year.

The increasing complexity to [redacted] is a key reason why the IRS should develop processes to identify and review these tax returns. Fraudsters familiar with this complexity could exploit this fact to obtain a fraudulent refund. Furthermore, our analysis continues to identify [redacted] that have characteristics of confirmed fraudulent filings. Specifically, as of December 31, 2020, we identified 3,243 [redacted] with refunds totaling approximately $17.2 million not selected by the IRS's fraud filters in which we could not verify $23 million [redacted].

Finally, the IRS's 2021 Fraud Risk Profile, dated October 2021, identified both business tax fraud and business identity theft tax refund fraud as one of the top 12 risks affecting its operations. This document notes that the Coronavirus Disease 2019 pandemic-related tax relief introduced new opportunities and incentives for fraud. As we have noted previously, fraud patterns change and evolve, and the IRS needs to ensure that it is continually evaluating this scheme, and others, to make appropriate updates to its detection efforts when warranted.

Recommendation 3: The Commissioner, Wage and Investment Division, should develop a program to identify and verify [redacted] business tax returns to prevent the issuance of potentially fraudulent refunds.

Management's Response: The IRS disagreed with this recommendation. IRS management stated that prior analyses outlined the complexity surrounding [redacted] business tax returns prior to return processing and issuance of refunds. Additionally, IRS compliance organizations have active business rules in place to identify these tax returns and select them for treatment, when appropriate, in a post-processing environment to address potential fraud or [redacted].

Office of Audit Comment: We continue to believe that a prerefund process to prevent the issuance of potentially fraudulent refunds is needed. As stated previously, the complexities of [redacted] is a key reason in support of developing a prerefund program intended to prevent exploitation of this vulnerability. Further, prerefund programs result in increased revenue protection as potentially fraudulent refunds are not issued to taxpayers, which must then be subsequently recovered.

First Annual Business Taxonomy Report Released in December 2021 Outlined Efforts to Protect Fraudulent Tax Refund Issuance

On December 12, 2021, the IRS published its first Business Taxonomy Report and reported that the IRS's efforts protected almost $3.8 billion in fraudulent tax refunds from being issued since Tax Year 2016. However, the IRS also reported that identity thieves were successful in receiving between about $6 million and $3.2 billion in fraudulent refunds since Tax Year 2016. The IRS refers to this as "unprotected revenue." The IRS uses estimates of unprotected revenue to analyze the associated tax return filings in an effort to continue to refine its existing detection filters or to develop new identity theft detection filters. Much like the Individual Identity Theft Taxonomy, the Business Taxonomy Report provides the IRS with strategic insight that will help assess the effectiveness of its business identity theft refund fraud detection and protection efforts.

In October 2020, we reported that the IRS had yet to develop a Taxonomy Report related to its efforts to protect against business identity theft.[26] IRS management stated that they are seeking to expand the use of business identity theft filters to other business tax return types. Management indicated that they recognize the need to assess which remaining refund-eligible business tax forms present the greatest risks for potential business identity theft. In an effort to develop a Business Taxonomy Report, IRS management noted that they analyzed 35 business tax returns as part of the IRS's risk assessment.[27] The purpose of the risk assessment was to identify the risks associated with each business return, such as the potential of identity theft, fraudulent refunds, and refundable credits. Based upon the results of the risk assessment, the IRS determined that the [redacted], the IRS has developed filters that will be implemented for the [redacted] during the 2022 Filing Season. For example, the [redacted] will be compared against the *Dynamic Selection List* for potential identity theft treatment.

Recommendation 4 (Information Request): On May 14, 2021, we reported to the IRS that our analysis of the risk assessment identified the [redacted], is at potential risk for refund fraud and should be included in the IRS's risk assessment.

> **Management's Response to Information Request:** RICS agreed, and the [redacted] was included in the October 2021 risk assessment. Upon further evaluation as part of the risk assessment process, the [redacted].

[26] TIGTA, Report No. 2021-40-004, *Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts* (Oct. 2020).

[27] See Appendix II for list of 35 business tax returns included in the IRS risk assessment.

Management Indicated That Development of a New Information Return Intake System Will Include Controls to Detect and Prevent Fraudulent Information Return Submissions

The *Taxpayer First Act* requires the IRS to develop an Internet website by January 1, 2023, that will allow issuers to prepare, file, distribute, and maintain a record of Forms 1099.[28] The purpose of the new Internet website is to provide a simple and secure manner for small businesses to file Forms 1099. The new system is to be modeled after the Social Security Administration's *Business Services Online*, *i.e.*, the portal used to file Forms W-2 with the Social Security Administration. This system will supplement the IRS's existing Form 1099 submission portal referred to as the *Filing Information Returns Electronically* (FIRE).[29] The IRS is planning for this new intake system to potentially replace FIRE.

In September 2019, we reported that the FIRE system's authentication criteria are inconsistent with processes to validate employers submitting Forms W-2.[30] Additionally, filters need to be expanded to identify questionable information return submissions in FIRE. We made several recommendations to improve the detection and prevention of fraudulent information return submissions using the FIRE system and to address the need to strengthen authentication of web-based users. The IRS has begun the process to strengthen authentication of users, evaluate potential business rules or filters to identify questionable information return submissions, and ensure that entities that received the account lock are not allowed to access FIRE to file information returns.

The IRS is still in the process of developing the new Form 1099 intake system, but plans to incorporate the same controls into the new system as the IRS agreed to implement in the FIRE system to improve on the detection and prevention of fraudulent information return submissions. Also, the IRS plans to deploy and test some of the functionality associated with the new intake system in mid-Calendar Year 2022. In addition, the IRS indicated it is still on track to complete the requirements outlined in the *Taxpayer First Act* by the January 2023 due date. We are planning to conduct an audit to assess the IRS's implementation of the information returns modernization platform in accordance with the provisions of the *Taxpayer First Act*.

[28] Forms 1099 comprise a series of documents the IRS refers to as information returns. There are a number of different Forms 1099 that report various types of payments taxpayers receive throughout the year other than wages.

[29] FIRE allows payers to submit bulk file uploads of Forms 1099. Payers who file 250 or more Forms 1099 are required to submit these forms to the IRS using the FIRE portal.

[30] TIGTA, Report No. 2019-40-071, *Strengthened Validation Controls Are Needed to Protect Against Unauthorized Filing and Input of Fraudulent Information Returns* (Sept. 2019).

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to assess the IRS's continued efforts to detect and prevent business identity theft. To accomplish our objective, we:

- Evaluated the IRS's use of fabricated entity indicators to detect potentially fraudulent individual tax returns.
- Evaluated the IRS's process to allow taxpayers to proactively report business identity theft and protect their tax account. We determined that current individual identity theft criteria, *e.g.*, clustering, is applicable to identify potential business identity theft tax returns.
- Evaluated the IRS's efforts to measure and quantify the risk of identity theft on the various business tax return types.
- Evaluated the IRS's implementation of corrective actions to address concerns raised in the prior TIGTA business identity theft report, Report No. 2021-40-004, *Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts*.
- Evaluated the IRS's implementation plan for the new Form 1099 Platform, mandated by the *Taxpayer First Act*, to ensure that fraud/identity theft concerns are addressed.

Performance of This Review

This review was performed with information obtained from the IRS Wage and Investment Division in Atlanta, Georgia, and the Tax Processing Center in Ogden, Utah, during the period July 2021 through March 2022. 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.

Major contributors to the report were Russell Martin, Assistant Inspector General for Audit (Returns Processing and Account Services); Diana Tengesdal, Director; Jonathan Lloyd, Audit Manager; Jennifer Bailey, Lead Auditor; Michael Russell, Senior Auditor; Ryan Kenaley, Auditor; and Dallin West, Auditor.

Validity and Reliability of Data From Computer-Based Systems

During this review, we relied on the Business Master File[1] data stored on the TIGTA Data Center Warehouse.[2] We also relied on data extracted from the IRS's Business Master File Identity Check

[1] The IRS database that consists of Federal tax-related transactions and accounts for businesses. These include employment taxes, income taxes on businesses, and excise taxes.

[2] A TIGTA repository of IRS data.

inventory database[3] that was provided by programmers from the TIGTA Data Center Warehouse. To assess the reliability of the computer-processed data, we ensured that each data extract contained specific data we needed and that the data were accurate. In addition, we selected judgmental samples from the extracts and verified that the data in the extracts were the same as the data captured in the IRS's Integrated Data Retrieval System.[4] 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: the Internal Revenue Manual,[5] other policies and procedures followed when processing business identity theft tax returns, and the systems/programming used to process the tax returns. We evaluated the controls by reviewing the IRS's internal guidelines,[6] interviewing IRS management, and evaluating applicable documentation and management information reports.

[3] A web application used to track and monitor cases that have been marked fraudulent by the Entity Fabrication and Business Master File Identity Theft programs used to track letters, responses, calls, research, and determinations of case legitimacy.

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

[5] The primary, official source of IRS instructions to staff related to the organization, administration, and operations of the IRS.

[6] Internal guidelines include the Internal Revenue Manual, desk guides, *etc*.

Appendix II

Forms Included in IRS Risk Assessment

Form	Form Name
Form 1041	U.S. Income Tax Return for Estates and Trusts
Form 1041-QFT	U.S. Income Tax Return for Qualified Funeral Trusts
Form 1042	Annual Withholding Tax Return for U.S. Source Income of Foreign Persons
Form 1065	U.S. Return of Partnership Income
Form 1120	U.S. Corporation Income Tax Return
Form 1120-REIT	U.S. Income Tax Return for Real Estate Investment Trusts
Form 1120-C	U.S. Income Tax Return for Cooperative Associations
Form 1120-F	U.S. Income Tax Return for a Foreign Corporation
Form 1120-FSC	U.S. Income Tax Return for a Foreign Sales Corporation
Form 1120-H	U.S. Income Tax Return for Homeowners Associations
Form 1120-ND	Return for Nuclear Decommissioning Funds and Certain Related Persons
Form 1120-PC	U.S. Property and Casualty Insurance Company Income Tax Return
Form 1120-RIC	U.S. Income Tax Return for Regulated Investment Companies
Form 1120-S	U.S. Income Tax Return for an S Corporation
Form 1120-SF	U.S. Income Tax Return for Settlement Funds (Under Section 468B)
Form 11-C	Occupational Tax and Registration Return for Wagering
Form 2290	Heavy Highway Vehicle Use Tax Return
Form 4720	Return of Certain Excise Taxes Under Chapters 41 and 42 of the Internal Revenue Code
Form 5330	Return of Excise Taxes Related to Employee Benefit Plans
Form 706	United States Estate (and Generation-Skipping Transfer) Tax Return
Form 706-GS(D)	Generation-Skipping Transfer Tax Return For Distributions
Form 706-GS(T)	Generation-Skipping Transfer Tax Return For Terminations
Form 709	United States Gift (and Generation-Skipping Transfer) Tax Return
Form 720	Quarterly Federal Excise Tax Return
Form 730	Monthly Tax Return for Wagers
Form 8752	Required Payment or Refund Under Section 7519
Form 8804	Annual Return for Partnership Withholding Tax (Section 1446)
Form 940	Employer's Annual Federal Unemployment (FUTA) Tax Return
Form 941	Employer's QUARTERLY Federal Tax Return
Form 943	Employer's Annual Federal Tax Return for Agricultural Employees
Form 944	Employer's ANNUAL Federal Tax Return
Form 945	Annual Return of Withheld Federal Income Tax
Form 990-PF	Return of Private Foundation or Section 4947(a)(1) Trust Treated as Private Foundation
Form 990-T	Exempt Organization Business Income Tax Return (and proxy tax under section 6033(e))
Form CT-1	Employer's Annual Railroad Retirement Tax Return

Source: RICS/RAAS IDT Detection Business Form Risk Assessment published September 21, 2020.
RAAS = Research, Applied Analytics, and Statistics; IDT = Identity Theft.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

June 29, 2022

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: *for* Kenneth C. Corbin /s/ David P. Alito
Commissioner, Small Business/Self-Employed Division

SUBJECT: Draft Audit Report – Successful Detection and Assistance Processes Used to Combat Individual Identity Theft Should Be Implemented to Improve Business Identity Theft (Audit # 202140019)

Thank you for the opportunity to review and provide comments on the subject draft report. We are proud of the work we have done to expand identity theft (IDT) protections to more business return filers. During processing year 2021 there were 84 pre-refund identity theft filters being used to identify suspected IDT return filings. This resulted in revenue protection of $7.3 trillion in calendar year 2020 and $2.3 trillion in calendar year 2021. These amounts include revenue protected from potentially fraudulent refund claims associated with returns filed by suspected identity thieves attempting to obtain refundable credits intended to help businesses struggling with the economic effects of the COVID-19 pandemic. In addition to implementing new filters, we acted on recommendations from previous Treasury Inspector General for Tax Administration audits, which include enhancements to training and IDT detection methods, and increased monitoring and control activities. As a result, we have reduced unnecessary interest payments, improved quality, increased efficiency, and improved identity theft detection.

We understand the vulnerability of taxpayers [redacted] when tax returns are filed. Specifically, we evaluated over 31,000 [redacted] in processing year 2020. Approximately 33 percent of the [redacted] matched the [redacted], with an additional 37 percent matching [redacted]. Among the [redacted] amounts, there were approximately 13,000 refunds claimed. The incidence of identity theft among this population was extremely low, with [redacted] as potential identity theft. The risk of

[redacted] is not one of identity theft but, rather, first-party fraud. When [redacted], filtering in a [redacted] is extremely complicated. There are multiple sources from which [redacted] a variety of information returns upon which [redacted]. These information returns have varying filing due dates and the [redacted]. Treating this type of discrepancy in a pre-refund environment raises issues of increased taxpayer burden and business costs, such as interest paid on delayed refunds. For this reason, any [redacted] must be performed in a post-refund environment, challenges still exist with respect to the identification and selection of those returns where additional scrutiny is warranted. Our compliance organizations, as part of their post-refund reviews, have processes in place to identify [redacted] and other returns.

Our responses to your specific recommendations are enclosed. If you have any questions, please contact me, or a member of your staff may contact, Mike Beebe Director, Return Integrity and Compliance Services, Wage and Investment Division, at 470-639-3250.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1:
Evaluate various business tax return common characteristics, [redacted], which can be used to develop clustering filters to be added to the Dependent Database.

CORRECTIVE ACTION
We will evaluate various common tax return characteristics to determine if clustering filters should be developed.

IMPLEMENTATION DATE
February 15, 2023

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

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 2:
Develop processes to assign an IP PIN to business taxpayers that are confirmed victims of tax-related identity theft for use in filing of business tax returns and for business taxpayers to proactively request an IP PIN if they are concerned about becoming a victim of business identity theft.

CORRECTIVE ACTION
We are currently completing an analysis to determine the feasibility of assigning Identity Protection Personal Identification Numbers (IP PINs) to business taxpayers. Assigning an IP PIN to a business entity presents numerous challenges that are not associated with assignment to individual taxpayers. We will consider the next steps for the business entity IP PIN based on this analysis.

IMPLEMENTATION DATE
March 15, 2023

RESPONSIBLE OFFICIAL
Director, Accounts Management

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendations

RECOMMENDATION 3:
The Commissioner, Wage and Investment Division, should develop a program to identify and verify [redacted] business tax returns to prevent the issuance of potentially fraudulent refunds.

CORRECTIVE ACTION
Prior analyses outlined, the complexity surrounding [redacted], tax returns prior to return processing and issuance of refunds. Additionally, our compliance organizations have active business rules in place to identify these returns and select them for treatment, when appropriate, in a post-processing environment to address potential fraud or [redacted].

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 4 (Information Request):
On May 14, 2021, we reported to the IRS that our analysis of the risk assessment identified the [redacted], is at potential risk for refund fraud and should be included in the IRS's risk assessment.

CORRECTIVE ACTION
[redacted], was included in the 2021 Business Identity Theft Risk Assessment.

IMPLEMENTATION DATE
Implemented

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

3

CORRECTIVE ACTION MONITORING PLAN
N/A

Appendix IV

Abbreviations

EIN	Employer Identification Number
FIRE	Filing Information Returns Electronically
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
PY	Processing Year
RICS	Return Integrity and Compliance Services
TIGTA	Treasury Inspector General for Tax Administration

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

(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.