TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts

October 21, 2020

Reference Number: 2021-40-004

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

HIGHLIGHTS: Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts

Final Audit Report issued on October 21, 2020
Reference Number 2021-40-004

Why TIGTA Did This Audit

This audit was initiated because new fraud patterns are constantly evolving, and as such, the IRS needs to adjust its existing filters and continue to expand 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 Taxpayers

Identity theft not only affects individuals, it can also affect businesses. The IRS defines business identity theft as creating, using, or attempting to use businesses' information without authority to obtain tax benefits. For example, an identity thief files a business tax return using the Employer Identification Number of an active or inactive business without the permission or knowledge of the owner to obtain a fraudulent refund.

What TIGTA Found

The IRS continues to take actions to improve its detection of business identity theft, including expanding the number of identity theft filters from 35 in Processing Year 2018 to 84 in Processing Year 2020. However, continued expansion of detection capabilities, to include other business return types, is needed. For example, TIGTA found that 36 business return types with refunds issued totaling $10.5 billion in Processing Year 2019 were not evaluated for potential identity theft.

In addition, our review identified 11,908 **********2********** **********2**********, with refunds totaling almost $63.2 million for which the amount of ******2****** reported on the tax return differed from the amount reported to the IRS by a third party. However, the IRS's existing identity theft filters do not evaluate *****2***** for this characteristic. In addition, our review identified 3,283 Form *****2***** with refunds totaling almost $21 million that should have been identified by the IRS's business identity theft filters but instead were excluded from filter evaluation.

The IRS also continues to use processes that do not protect potentially fraudulent refunds from erroneous release. Our review identified that 1,966 of the 6,110 *****2***** the IRS's frivolous filters selected as potentially fraudulent had their associated refunds, totaling almost $110.4 million, erroneously released before a tax examiner confirmed the validity of the refund. The erroneous release of these refunds results from a process that allows other functional areas to erroneously release refunds associated with returns the Return Integrity and Compliance Services function identified and selected for review as potentially fraudulent.

Finally, the IRS is not timely releasing refunds once a non–identity theft determination is made. Our analysis identified 821 taxpayer accounts for which the associated refund freeze was released 21 or more calendar days after a tax examiner determined that the return was valid. These delays resulted in additional interest paid totaling more than $1.3 million.

What TIGTA Recommended

TIGTA made four recommendations to the Commissioner, Wage and Investment Division, to improve the identification of business identity theft. These recommendations include expanding the *******2******* business identity theft filters; revising filters to use **********2******* *****2***** that posted to the taxpayer's account; and establishing procedures to ensure the prompt release of refunds once a determination is made that they are not the result of identity theft.

IRS management agreed with all four recommendations and plans to take appropriate corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

October 21, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts (Audit # 201940020)

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 was part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Addressing Emerging Threats to Tax Administration*.

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 Russell P. Martin, 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 businesses' identifying information without authority to obtain tax benefits. Examples include the following:

- An identity thief files a business tax return, **********2********** ***2***, 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 bogus **********2********** **********2**********, 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, *********2********** **********2**********, avoid paying taxes, obtain a refund, or further perpetuate individual identity theft or refund fraud.

Processes to identify potential business tax return identity theft

The IRS systemically evaluates business tax returns claiming refunds for potential fraud during tax return processing using business identity theft filters included in the Dependent Database (DDb).[3] For Processing Year (PY)[4] 2019, the IRS used 77 filters in an effort to identify tax return filings involving business identity theft. In addition to the filters, the IRS also used 10 *Dynamic Selection Lists*. These lists include unique identifiers, such as a Taxpayer Identification Number, that the IRS uses to identify business tax returns that include one or more of these identifiers.

When a tax return is identified as potential 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 manually screen selected tax returns that meet certain criteria or have a high-dollar refund[5] to determine whether they are identity theft tax returns. This includes researching the associated tax account to determine if the taxpayer ****2********* *******2******* and evaluating whether ********2******** of the tax return are *********2********* **********2**********. These characteristics may indicate that the filing was a legitimate business filing.

[1] A Federal Tax Identification Number used to identify a taxpayer's business account. The EIN is a nine-digit number (in the format of xx-xxxxxxx) assigned by the IRS and used by employers, sole proprietors, corporations, partnerships, nonprofit associations, trusts and estates, government agencies, certain individuals, and other types of businesses.
[2] A nine-digit number assigned by the Social Security Administration and used as the account number of a taxpayer on the Individual Master File.
[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 returns daily and selects questionable returns for audit.
[4] The calendar year in which the IRS processes the tax return or document.
[5] The IRS defines a high-dollar refund amount as a refund that is **********2**********.

For those returns determined to be legitimate, the IRS releases the hold and the tax return continues to process. For the screened returns that remain as potential identity theft, taxpayers are sent Letter 6042C, *Entity Verification for Business*. For those returns associated with a response to Letter 6042C, the IRS evaluates the response and takes one of the following actions:

- For those responses that support the legitimacy of the business, the IRS removes the hold to release the refund and post the return when necessary.
- For those responses that confirm identity theft, the IRS will place an identity theft indicator on the account confirming that the return is an identity theft filing. In addition, the IRS will deactivate, *i.e.,* lock, the associated tax account when it determines the entity associated with the return was fabricated. Once an account is locked, no future tax returns will be accepted for processing using that EIN.[6]

For those instances in which no response is received, the IRS does not process the tax return[7] and continues to hold the refund until either a response is received or for one year after the filing of the return. For those returns that have not posted and the refund is being held after the one-year period expires, the IRS removes the return from further processing to permanently prevent the refund from being issued. If the tax return has posted[8] to the Business Master File[9] and no response is received, the IRS maintains the hold on the tax account to prevent the refund from issuing.

Results of Review

This report presents the results of our continued evaluation of the IRS's efforts to combat business identity theft. Our review of the IRS's business identity theft inventory showed that, between January 1, 2019, and December 31, 2019, the IRS identified 31,272 business returns[10] with characteristics of identity theft that had associated refunds totaling $9.7 billion.[11] In addition, the IRS identified another 140,529 **********2**********, with potentially fraudulent losses reported totaling $93.8 billion. The IRS has filters to identify these types of *****2***** return filings because fraudsters may use **********2********** **********2**********. However, due to the closing of Tax Processing Center operations in response to COVID-19, the IRS has a backlog of potentially fraudulent business tax returns that it has identified but not yet evaluated. As of June 30, 2020, there are 7,605 (24.3 percent) business tax returns identified as potential identity theft with

[6] 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.
[7] **********2********** selected by business identity theft filters are prevented from posting to the Master File.
[8] **********2********** **********2********** **********2********** selected by business identity theft filters are posted to the Business Master File.
[9] 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.
[10] This includes **********2**********. This does not include *****2***** as those returns generally do not claim refunds and are shown separately.
[11] This excludes six outlier returns with total refunds claimed of more than $18 trillion.

refunds claimed totaling more than $1 billion and another 20,679 (14.7 percent) *******2******** returns with losses reported totaling $17.8 billion that remain to be evaluated by tax examiners in the RICS function.

In response to recommendations included in a prior Treasury Inspector General for Tax Administration (TIGTA) audit,[12] the IRS continues to take actions to improve its detection of business identity theft and to prevent the issuance of fraudulent refunds. The IRS's actions include expanding the number of identity theft filters from 35 in PY 2018 to 84 in PY 2020, increasing the number of *Dynamic Selection Lists*, and increasing detection coverage to include nine types of business tax returns up from three types. For example, the IRS:

- Expanded detection to include Form 940, **********2********** **********2********** beginning in PY 2019. The IRS developed 22 DDb identity theft filters to detect potentially fraudulent returns. For PY 2019 through December 31, 2019, these filters identified 6,709 *******2******** as potential identity theft returns for RICS function screening with refunds claimed totaling almost $392.7 million.[13] As of June 30, 2020, the IRS has confirmed **********1********** **********1**********. A total of 2,249 (33.5 percent) tax returns with refunds claimed totaling more than $241 million are still being worked. The remaining cases selected were determined to be legitimate returns.
- Expanded detection to include **********2********** **********2**********, for use in PY 2020. The IRS developed 12 DDb identity theft filters to detect potentially fraudulent returns. As of June 30, 2020, these filters identified 169 **********2********** as potential identity theft for RICS function screening with refunds claimed totaling almost $9.7 million.[14] As of this same time, 133 (78.7 percent) returns with refunds claimed totaling more than $7.7 million are still being worked. The remaining cases selected were determined to be legitimate returns.
- Developed seven additional *Dynamic Selection Lists* for use during PYs 2018 and 2019. These lists include **********2**********,[15] **********2**********,[16] **********2********** that the IRS previously identified as questionable or were associated with a business that was part of a reported data breach.
- Developed and added eight business tax return filters to the Return Review Program (RRP) selection models to assist with evaluating how these filters will identify potentially fraudulent business tax return filings. The RRP is the IRS's primary individual tax refund fraud selection system. The RRP uses predictive analytics, models, filters, clustering, a scoring system, business rules, and selection groups to identify suspected identity theft.

[12] TIGTA, Ref. No. 2018-40-061, *Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft* (Aug. 2018).
[13] This excludes six outlier returns with total refunds claimed of more than *******1********.
[14] This excludes **********1**********.
[15] **********2********.
[16] **********2**********.

Filters added were to evaluate **********2**********2**********2**********, for fraud potential. Currently, the IRS is not using the RRP to select returns for potential business identity theft because the filters are still being refined.

In addition to these actions, the IRS established a new inventory control system, the *Business Master File Identity Check*, to more effectively process and document the actions taken to resolve business identity theft cases. Our review of a statistical sample of 95[17] case selections determined by the IRS to be legitimate tax return filings between October 29, 2019, and December 7, 2019, identified that case processing, including the documentation of the basis for IRS decisions of non–identity theft determination, has improved since our last review. Our review determined that, in 93 (98 percent) of the 95 cases, the case files adequately supported the tax examiners determination. This is an improvement from our prior audit in which we determined that, in 21 (23 percent) of the 91 cases reviewed, the IRS had either incomplete information to make a proper determination, improperly disclosed taxpayer information, and/or made procedural case processing errors.[18]

Finally, the IRS is continuing to actively work with Security Summit partners in an effort to improve the identification of fraudulent tax returns during tax return processing. The Security Summit 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. The IRS and participating members continue to meet monthly (more often when necessary) to discuss emerging trends in tax refund fraud and improvements to detection efforts. For example, one such initiative is the evaluation of specific data elements from electronically filed (e-filed) tax returns for use in systemically identifying fraudulent business tax returns. In PY 2017, the IRS began receiving 30 business authentication elements as part of a business tax return e-file record. The IRS is assessing the use of these 30 elements to identify trends and patterns of business identity theft. In fact, one of the data elements was included in its filters used to identify fraudulent ******2******. The IRS's use of this data element in PY 2019 resulted in the selection of 1,660 ******2****** with refunds claimed totaling more than $2 billion.

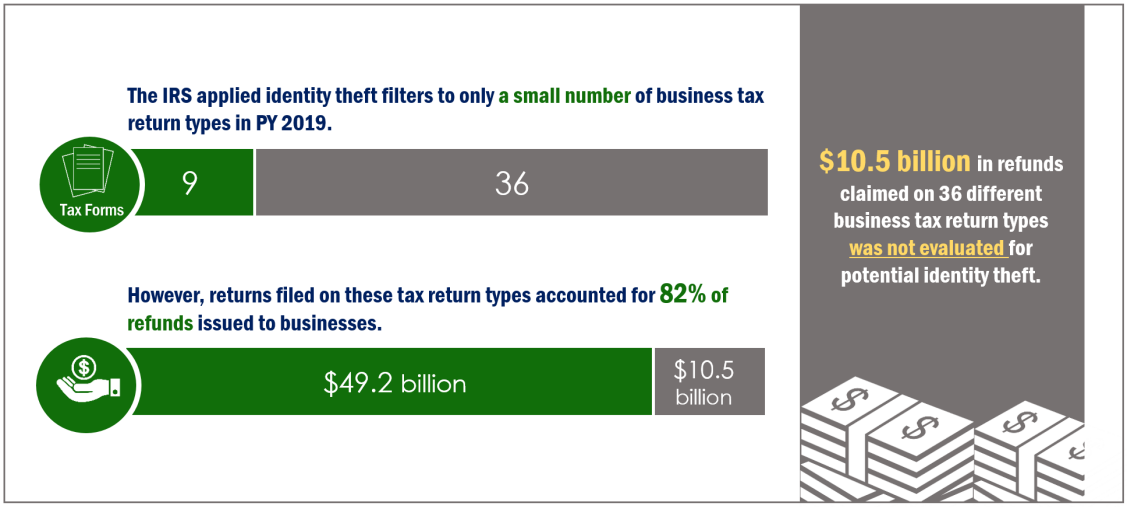
Continued Expansion of Detection Capabilities, to Include Other Business Return Types, Is Needed to Address Constantly Evolving Fraud Patterns

New fraud patterns are constantly evolving, and as such, the IRS needs to adjust its existing filters and continue to expand its detection processes to include additional business tax return types. Our analysis of business tax returns filed during PY 2019 identified 45 different types of business tax returns (including nonprofit) with refunds issued; however, 36 of these business return types are not evaluated for potential identity theft.[19] Refunds issued relative to these

[17] Our sample of 95 cases was randomly selected from a total population of 3,476 cases, following the guidance of our contract statistician. The sample was selected with an unknown expected error rate, a ±10 percent precision rate, and a 95 percent confidence interval.
[18] TIGTA, Ref. No. 2018-40-061, *Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft* (Aug. 2018).
[19] As noted, the IRS is testing the use of the RRP for business tax returns but is not making selections with the RRP.

36 business tax return types totaled almost $10.5 billion in PY 2019. Figure 1 summarizes the IRS's use of identity theft filters on business tax return types.

Figure 1: Identity Theft Filters for Business Tax Return Types



Source: TIGTA analysis of the Business Master File for PY 2019 as of December 31, 2019, and IRS business identity theft filters through PY 2020.

Detection filters need to be constantly evaluated and adjusted to address ever-changing fraud patterns

Our review found that the effectiveness of the IRS's detection filters is directly related to its ability to improve or develop additional filters as fraud patterns change. For example, our review identified 11,908 *****2***** returns, filed as of December 31, 2019, with refunds totaling almost $63.2 million whereby the amount of ******2****** reported on the tax return differed from the amount reported to the IRS by a third party.[20] The IRS's existing identity theft filters do not evaluate *****2***** for this characteristic. We analyzed these types of return filings in response to a referral we received from our Office of Investigations which identified that an unscrupulous individual filed a *****2***** claiming a $5 million refund by fraudulently reporting a large amount of unsupported ********2********.

When we brought to management's attention our concerns about the returns we identified with *****2***** discrepancies, they indicated that they use prerefund Frivolous Return Program[21] filters to identify unsubstantiated **********2**********. Further, they stated that they reviewed a sample of our exceptions and noted that these returns did not meet their criteria for identity theft or frivolous intent. In addition, the IRS indicated that its review of these returns did not identify any indications of identity theft. However, the IRS has identified refund schemes whereby fraudsters become aware of the use of a specific dollar tolerance and submit tax returns below these thresholds knowing the IRS will not review these returns. The returns we identified not only had *****2***** discrepancies but also included characteristics similar to

[20] These tax returns were for Tax Years 2017 and 2018 and processed during PY 2019.

[21] Generally, a frivolous tax argument is based on a frivolous or incorrect interpretation of the Federal tax laws. Individuals and businesses use these incorrect interpretations to support their claims that they are not subject to Federal tax laws. The Frivolous Return Program is responsible for determining if identified potentially frivolous returns meet frivolous return criteria.

those that the IRS's existing identity theft filters use to identify individual tax returns as potentially fraudulent, *i.e.*, *****2***** discrepancies **********2**********. As such, the IRS needs to update its detection filters to take into account previous fraud patterns.

IRS filters have not been updated to identify business returns with inconsistencies in reported **********2********** as potentially fraudulent even though this is a characteristic of known refund fraud schemes

Similar to the prior example, the IRS is not taking proactive actions to identify and stop known identity theft refund schemes. Our review identified 3,283 ****2**** returns with refunds totaling almost $21 million that should have been identified by the IRS's business identity theft filters but instead were excluded from filter evaluation because the refund amounts (and in some instances balances due) were below the filter's threshold amount. The IRS's filter selects tax returns for review only if the amount of the refund per the tax return is in excess of a specific dollar amount. For example, each of these returns had refunds and **********2********** reported on the tax return of *****2*****,[22] yet the associated tax accounts reflected ******2****** ****2**** credited to the tax account ranging from $660 to almost $1.8 million.

The returns we identified are similar to a scheme the IRS identified related to the fraudulent filing of individual tax returns. In that scheme, IRS Criminal Investigation became aware of the filing of fraudulent individual tax returns with *****2***** refunds in an attempt to bypass the IRS's filters and steal the **********2**********. When we brought our concern to IRS management's attention, they indicated that our analysis supports the IRS's position that **********2********** discrepancies are not contributing to business identity theft. They also indicated that the IRS does not need to filter for these types of cases because, during processing, discrepancies in **********2********** for business taxpayers are identified for further review. However, as our analysis showed, these are **not** **********2********** discrepancies when considering the actual **********2********** that posted to the taxpayer's account rather than the amount reported on the tax return. Resulting refunds issued for these returns ranged from $1,000 to $1.7 million due to the refunding of the **********2********** reflected on the associated tax account.

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Expand the ****2**** business identity theft filters to include the use of ****2**** reported on third-party information documents as a characteristic of potential identity theft.

> **Management's Response:** The IRS agreed with this recommendation and plans to conduct an analysis to determine the effectiveness of incorporating *********2********* discrepancies in its filtering process as a characteristic of potential identity theft.

Recommendation 2: Revise the ****2**** business identity theft filters to use ******2********* ****2**** that post to the taxpayer's account.

> **Management's Response:** The IRS agreed with this recommendation and plans to conduct an analysis to determine the effectiveness of using **********2********** that

[22] This includes returns that had a balance due and returns that claimed no **********2**********.

post to the taxpayer's account in its filtering process for the ****2**** business identity theft filters.

The IRS Continues to Use Processes That Do Not Prevent the Erroneous Release of Potentially Fraudulent Refunds

Our review identified that 1,966 of the 6,110 ****2**** the IRS's frivolous filters selected as potentially fraudulent had their associated refunds totaling almost $110.4 million erroneously released before a tax examiner confirmed the validity of the refund. When a tax return is identified as potential identity theft, the IRS places a hold on the associated tax account to prevent issuance of the refund. The erroneous release of these refunds results from the IRS's continued use of an ineffective process for holding refunds associated with potentially fraudulent returns. As we have previously reported to management, this process allows other functional areas within the IRS to erroneously release refunds associated with returns the RICS function identified and selected for review as potentially fraudulent.

In August 2018, we reported that 872 business identity theft tax returns with refunds totaling more than $61 million appear to have been released in error. This occurred because the process the RICS function established was to first process and then post the potential business identity theft tax returns to the business's tax account. At the time the return posted, the refund was also frozen. However, this process created a situation in which other functional areas within the IRS could erroneously release the refund without notifying the RICS function.[23] Management acknowledged the risk associated with the erroneous release of refunds on business tax returns identified as potential identity theft and changed its procedures for PY 2017. However, when identity theft detection coverage was expanded to include six additional types of business tax returns, procedures were established to post the potential business identity theft tax returns to the business tax account. The RICS function requested changes to the programming to ensure that the refunds could not be released, but this request was denied due to a lack of resources. The IRS selected the ****2**** refund returns we identified as potential frivolous cases, and similar to business identity theft, the IRS should hold these refunds until a full determination is made as to whether the taxpayer is submitting a fraudulent refund claim.

When we brought our concerns to RICS function management's attention, they agreed with what we found and stated that, although the tax accounts show the returns are being evaluated by either the RICS or Frivolous Filer Program functions, IRS employees are not always following their procedures to contact the RICS or Frivolous Filer Program functions prior to taking actions to release the refund. RICS function management also noted that they resubmitted a work request for Fiscal Year 2021 consideration on January 31, 2020. However, the programming request was denied due to COVID-19 priorities and will require resubmission for Fiscal Year 2022.

Recommendation 3: The Commissioner, Wage and Investment Division, should analyze the 1,966 accounts we identified to detect any trends regarding the IRS functional areas releasing the refunds and send alerts targeted at those functions emphasizing that refunds associated with returns under RICS function control are not to be released.

[23] TIGTA, Ref. No. 2018-40-061, *Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft* (Aug. 2018).

Management's Response: The IRS agreed with this recommendation and plans to analyze the accounts identified and share the results of the analysis with the appropriate functions. IRS management also plans to coordinate communications and other outreach with functional management to address errors or other issues identified in their analysis.

A Process Needs to Be Developed to Measure the Extent of Business Identity Theft and Efforts to Defend Against Fraudulent Refund Losses

Since 2014, the IRS annually reports *(Identity Theft Taxonomy Report)* on its efforts to defend against individual tax return identity theft filings. The IRS provides an estimate of the amount of fraudulent tax refunds detected and prevented from being issued along with the estimate of the amount identity thieves were successful in receiving. The IRS uses the later estimate to continue to analyze and refine its existing identity theft detection filters or to develop new detection filters.[24]

However, the IRS has yet to develop a similar measurement process as it relates to its efforts to defend against business tax return identity theft. 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. They plan to have this assessment completed by September 30, 2020. They will then determine next steps with respect to developing a Business Identity Theft Taxonomy Report. We will continue to assess the IRS's efforts to expand the use of business identity theft filters to other business tax return types as well as the development of a process to measure efforts to detect and prevent the issuance of fraudulent refunds.

Refunds Are Not Timely Released Once a Non–Identity Theft Determination Has Been Made

Our analysis of the 202,458 business tax accounts associated with returns selected as potential identity theft between October 1, 2018, and December 31, 2019, identified 821 taxpayer accounts for which the associated refund freeze was released 21 or more calendar days after a tax examiner determined that the return was valid, *i.e.*, return was not a fraudulent identity theft filing. The time frame for release ranged from 21 to 411 calendar days and resulted in additional interest paid totaling more than $1.3 million.

In our prior review, we reported that potential identity theft cases with large-dollar refunds were not promptly screened, which caused millions of dollars in interest to be paid. In response to our review, the IRS established procedures designating that the screening review must be completed within three cycles, *i.e.*, 21 calendar days, of return selection.[25] When we brought our concerns that refunds were not being timely released once the tax examiner determines the return is valid to IRS management's attention, they stated that the process to release a refund

[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] TIGTA, Ref. No. 2018-40-061, *Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft* (Aug. 2018).

freeze could take up to three weeks. However, the IRS has not established a process to monitor and ensure the timely release of refunds once it determines the tax return is a valid filing.

Efforts are being initiated to improve the efficiency of case processing

Currently, the IRS does not maintain responses to Letter 6042C for those suspected returns the IRS determines are legitimate. Instead, tax examiners are required to transcribe the responses provided to the verification questions into the Business Master File Identity Check and Account Management Services databases. The IRS indicated that it implemented this process because the storage and retrieval alternative for the correspondence is labor intensive when left in paper form only.

IRS management stated that they submitted a request for Information Technology organization support on April 9, 2019, to provide the capability to scan taxpayer responses to Letter 6042C into the IRS's Correspondence Imaging System. This is part of an overall initiative to improve the RICS function's efficiency, accuracy, and timeliness of case processing, *e.g.*, refundable credit examinations, automated questionable credit cases, by making it easier to move inventory electronically between the various RICS function locations. It would also provide other IRS employees with immediate access to the information should there be a need when assisting with taxpayer inquiries. This request was denied on October 2, 2019, due to higher priorities. The RICS function resubmitted the funding request on May 26, 2020. As of August 4, 2020, the funding request is still undergoing review and has not been approved or denied. In the interim, the IRS has installed four multifunctional devices to provide scanning capabilities. The IRS is in the process of training, testing, and implementing the interim process.

Recommendation 4: The Commissioner, Wage and Investment Division, should establish processes and procedures to ensure the prompt release of refunds once a non–identity theft determination is made in an effort to reduce taxpayer burden and to minimize unnecessarily paying interest.

Management's Response: The IRS agreed with this recommendation and plans to implement a periodic review of the account actions based on case determinations and provide feedback to its workgroups for timely case processing.

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:

- Identified and evaluated the IRS's existing business identity theft filters to determine if they can be improved or expanded.
  - Determined what systems the IRS is currently using to identify business identity theft, *i.e.*, DDb, RRP, offline model.
  - Identified all current business identity theft filters, making note of new filters that have been added since the previous audit.
  - Identified and evaluated the IRS's use of business identity theft filters for employment tax returns.
    - Evaluated PY 2018 filter criteria for ****2**** relative to **********2********** **********2**********.
- Evaluated the IRS's business identity theft case processing procedures.
  - Evaluated procedures used to generate business identity theft letters to taxpayers.
  - Reviewed a statistical sample of 95 case selections from a total population of 3,476 determined by the IRS to be legitimate return filings between October 29, 2019, and December 7, 2019, and reviewed the sample to evaluate whether a proper determination was made on each case. To select our sample, we used an unknown expected error rate, a ±10 percent precision rate, and a 95 percent confidence interval. A contract statistician assisted with developing the sampling plan.
  - Assessed the effectiveness of controls to ensure that refunds associated with business identity theft returns are not erroneously released and are timely released when tax examiners determined the tax return to be valid.
- Evaluated the IRS's plan to include authentication data elements for business tax returns into its business identity theft filters.
- Evaluated the IRS's efforts to work with the Security Summit and measure the extent of business identity theft.

Performance of This Review

This review was performed at the IRS Wage and Investment Division in Atlanta, Georgia, and the Tax Processing Center located in Ogden, Utah, during the period July 2019 through August 2020. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit 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; Darryl Roth, Audit Manager; Jennifer Bailey, Lead Auditor; Tanya Boone, Senior Auditor; and Benjamin Meeks, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

During this review, we relied on the Business Master File and Business Return Transaction File data stored on the TIGTA Data Center Warehouse.[1] We also relied on data extracted from the IRS's Business Master File Identity Check inventory database that were 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 the specific data we needed and that the data were accurate. In addition, we selected random samples from all extracts and verified that the data in the extracts were the same as the data captured in the IRS's Integrated Data Retrieval System. 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, other policies and procedures followed when processing business identity theft returns, and the systems/programming used to process the returns. We evaluated the controls by reviewing the IRS's internal guidelines,[2] interviewing IRS management, and evaluating applicable documentation and management information reports.

[1] A TIGTA repository of IRS data.
[2] Internal guidelines include the Internal Revenue Manual, desk guides, *etc.*

Appendix II

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:

- Cost Savings – Funds Put to Better Use – Potential; implementation of these 34 business identity theft filters for employment tax returns has resulted in identification of 2,382 potential identity theft returns and has stopped more than $248 million in potentially fraudulent refunds (see Page 3).

Methodology Used to Measure the Reported Benefit:

In August 2018, we reported that business identity theft filters should continue to be expanded to include other types of business tax return filings. We recommended that the IRS expand the use of business identity theft filters to include employment tax returns. In response to our report, the IRS created 34 business identity theft filters to evaluate employment tax returns for potential identity theft.

Using the IRS's Business Master File Identity Check inventory as of June 30, 2020, we identified 6,878 business tax accounts with employment tax returns that were selected as potential identity theft. Using this information, we identified 2,382 taxpayer accounts that were still being worked as potential identity theft with potentially fraudulent refunds totaling $248,763,317. This includes 2,249 **********2********** with refunds claimed totaling $241,042,902, and 133 **********2********** with refunds claimed totaling $7,720,415.

Type and Value of Outcome Measure:

- Cost Savings – Funds Put to Better Use – Potential; more than $1.3 million in interest paid due to delays in the IRS releasing refunds after determining the return was valid (see Recommendation 4).

Methodology Used to Measure the Reported Benefit:

Using the IRS's Business Master File Identity Check inventory database, we identified 202,458 business tax accounts associated with returns that were selected as potential identity theft between October 1, 2018, and December 31, 2019.

Our analysis of the business tax accounts identified 821 taxpayer accounts for which the associated refund freeze was released in 21 or more calendar days after a tax examiner determined the return was valid, *i.e.*, return was not a fraudulent identity theft filing. As of December 31, 2019, we identified 133 taxpayer accounts that had the refund released, of which 124 had interest paid on the account. We determined that the IRS paid $1,946,101 in total interest on these accounts. We prorated the interest payments based on the computed total interest paid daily multiplied by the total calendar days delayed from having the refund

released. As a hypothetical example, a refund was held 50 calendar days, which consisted of 20 days to be worked and 30 days from the determination to input the refund release. The IRS paid $1,000 in total interest. We determined the daily rate of $20 ($1,000/50 days) and then determined the portion attributed to the delay as $600 ($20 times the 30 days of delay). We applied this to each of the 124 tax accounts with interest paid as of December 31, 2019, and determined that $1,318,181 of the $1,946,101 interest assessed was paid as a result of delays in releasing the refund once the IRS determined the return was valid. We note that this does not include any interest on the remaining 688 taxpayer accounts that had the refunds released after December 31, 2019.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

October 5, 2020

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report - Refinement and Expansion of Filters to Include Additional Business Returns Will Continue to Improve Business Identity Theft Detection Efforts (Audit # 201940020)

Thank you for the opportunity to review and comment on the subject draft report. Business identity theft is the creation, use, or attempted use of businesses' identifying information, without authority, to obtain tax benefits. The detection of business identity theft can be challenging in that it shares many characteristics of noncompliance or attempts to defraud by individuals with legitimate authorization to use the businesses' information. Since 2015, we have improved and expanded our ability to detect both conventional fraud and identity theft fraud associated with the filing of business tax returns. As noted, the number of filters being used to detect business identity theft has expanded from 35 in 2018 to 84 in 2020. We also increased both the number of Dynamic Selection Lists and our detection coverage to include additional business tax returns. The volume of filings for these business tax returns, processed in 2019, accounted for 82 percent of the refunds issued to businesses that year.

New filters and fraud detection models have increased the scope of business return protection to include **********2********** and focus on emerging schemes. We recognize there is more work yet to be done in this area and are actively engaged in expanding protection coverage to additional types of business returns. We have established an inventory control system to more effectively process and document actions taken to resolve business identity theft cases and we continue to actively work with Security Summit partners in efforts to improve the authentication of those that file business returns.

The report states filters have not been updated to identify business returns with inconsistencies in reported **********2********** as potentially fraudulent, despite this being a known refund scheme. We have conducted two separate analyses and

found no incidents of identity theft occurring for business tax returns in relation to the known refund scheme. Additionally, none of the discrepancies identified in the report were a result of any claims of identity theft after the refund was issued. Discrepancies with **********2********** for business taxpayers are identified during return processing and are reviewed by our Submission Processing function.

The report also states that we continue to use processes that do not protect potentially fraudulent refunds from erroneous release. We changed our procedures in 2017 to further prevent the risk associated with erroneously released refunds on business accounts where the source tax returns were identified as potential identity theft. We also submitted requests to change programming related to how refunds are held when the business return filing is suspected of being identity theft; however, these requests have not been fulfilled due to competing priorities for limited programming resources and funding.

We appreciate the identification of opportunities for improving business identity theft detection and prevention processes, as well as your acknowledgement of the corrective actions implemented in response to the previous review of this program. We continue to improve our detection of business identity theft and our abilities to prevent issuance of fraudulent refunds.

Our responses to the recommendations made in the report are enclosed. If you have any questions, please contact me, or a member of your staff may contact Michael Beebe, Director, Return Integrity and Compliance Services, at (470) 639-3250.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Expand the ******2****** business identity theft filters to include the use of ******2****** reported on third-party information documents as a characteristic of potential identity theft.

CORRECTIVE ACTION
We will conduct an analysis to determine the effectiveness of incorporating *****2***** discrepancies in our filtering process as a characteristic of potential identity theft.

IMPLEMENTATION DATE
February 15, 2022

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification 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
Revise the Form 1041 business identity theft filters to use ********2******** that post to the taxpayer's account.

CORRECTIVE ACTION
We will conduct an analysis to determine the effectiveness of using *********2********* that post to the taxpayer's account in our filtering process for the ******2****** business identity theft filters.

IMPLEMENTATION DATE
February 15, 2022

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification 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 3
Analyze the 1,966 accounts we identified to detect any trends regarding the IRS functional areas releasing the refunds and send alerts targeted at those functions emphasizing that refunds associated with returns under RICS function control are not to be released.

CORRECTIVE ACTION
We will analyze the accounts identified and will share the results of the analysis with the appropriate functions. Communications and/or other educational outreach will be coordinated with functional management to address errors or other issues identified in our analysis.

IMPLEMENTATION DATE
February 15, 2021

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification 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 4
Establish processes and procedures to ensure the prompt release of refunds once a non-identity theft determination is made in an effort to reduce taxpayer burden and to minimize unnecessarily paying interest.

CORRECTIVE ACTION
We will implement a periodic review of account actions based on case determinations and will provide feedback to our workgroups for timely case processing.

IMPLEMENTATION DATE
May 15, 2021

RESPONSIBLE OFFICIAL
Director, Return Integrity Verification 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.

Appendix IV

Abbreviations

DDb	Dependent Database
e-file(d)	Electronically file(d)
EIN	Employer Identification Number
IRS	Internal Revenue Service
PY	Processing Year
RICS	Return Integrity and Compliance Services
RRP	Return Review Program
TIGTA	Treasury Inspector General for Tax Administration