TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft

August 20, 2018

Reference Number: 2018-40-061

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

Redaction Legend:
1 = Tax Return/Return Information
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

ADDITIONAL ACTIONS CAN BE TAKEN TO FURTHER REDUCE REFUND LOSSES ASSOCIATED WITH BUSINESS IDENTITY THEFT

Highlights

Final Report issued on August 20, 2018

Highlights of Reference Number: 2018-40-061 to the Commissioner of Internal Revenue.

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' identifying information without authority to claim tax benefits.

WHY TIGTA DID THE AUDIT

This audit was initiated because business identity theft patterns are constantly evolving, and as such, the IRS needs to continually adapt its detection and prevention processes. The overall objective of this review was to determine the effectiveness of the IRS's ongoing efforts to detect and prevent business identity theft.

WHAT TIGTA FOUND

Since TIGTA's first business identity theft report was issued in September 2015, the IRS has created 25 business identity theft filters and three dynamic selection lists to identify potential business identity theft returns. For Processing Year 2017, these filters identified 20,764 business returns with characteristics of identity theft and associated refunds totaling $2.2 billion.

However, TIGTA found that certain types of tax returns are not being evaluated for potential identity theft. For Processing Year 2017, TIGTA identified 15,127 returns with refunds totaling more than $200 million that would have been identified as potentially fraudulent if current business identity theft filters included an evaluation of these types of tax returns.

TIGTA also found that only 220 of 5,133 Employer Identification Numbers (EIN) on the IRS's *Suspicious EIN Listing* had the associated tax accounts locked. Although the IRS issued internal guidelines requiring the locking of tax accounts associated with bogus/fictitious EINs after January 2017, these guidelines were not consistently being followed. Moreover, the IRS removed 1,097 EINs from the *Suspicious EIN Listing* after completing a systemic analysis of filing and payment history. However, TIGTA's more in-depth analysis identified characteristics that indicate many of the EINs should not have been removed.

In addition, some business identity theft cases were not always accurately processed by the IRS. A review of a statistically valid sample found that 21 (23 percent) of the 91 cases TIGTA could review were not accurately processed. As such, TIGTA estimates that 188 cases may have been inaccurately processed. Finally, actions need to be taken to protect refunds associated with confirmed business identity theft from being erroneously released. TIGTA identified 872 tax returns identified by the IRS as identity theft returns in Processing Year 2016 for which refunds totaling more than $61 million appear to have been released in error.

WHAT TIGTA RECOMMENDED

TIGTA made 10 recommendations to improve the identification of business identity theft. Recommendations included expanding the use of business identity theft filters, reviewing and updating the *Suspicious EIN Listing* on a periodic basis, ensuring all EINs deemed to be bogus or fictitious are locked, developing processes and procedures to ensure that tax examiners accurately process business identity theft cases, and developing processes to ensure that refunds associated with Processing Year 2016 identity theft tax returns remain frozen.

The IRS agreed with eight recommendations and partially agreed with the other two. The IRS did not agree that all of the accounts TIGTA identified should be locked. It plans to lock accounts only when there are clear indications of identity theft fraud. It also believes the degree and the method of taxpayer contact should be determined on a case-by-case basis.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

August 20, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft (Audit # 201740037)

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

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

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

Table of Contents

Abbreviations

EIN	Employer Identification Number
IRS	Internal Revenue Service
PY	Processing Year
TIN	Taxpayer Identification Number

Background

Identity theft not only affects individuals, it can also affect businesses. 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********** **********2**********, claiming a fraudulent refund.
- An identity thief applies for and obtains an EIN using the name and Social Security Number 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

Business tax returns claiming refunds are systemically evaluated for potential fraud during tax return processing and prior to refund issuance via the business identity theft filters included in the Dependent Database.[2] In Processing Year (PY)[3] 2017, for those business tax returns identified as potential identity theft and selected for review, the IRS placed a hold on the associated tax account to prevent the return from posting to the IRS's Master File[4] and the refund from issuing. Once the potential identity theft returns are identified, the IRS screens the returns that meet certain filter criteria or have a high dollar refund[5] to determine whether they are

[1] 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] The Dependent Database is 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.
[3] The calendar year in which the IRS processes the tax return or document.
[4] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
[5] **********1**********.

identity theft returns. For example, research is performed to determine if payroll payments have been made, which may indicate the filing was a legitimate business, or to check if the characteristics of the return appear to be consistent with prior filings. For those returns determined to be legitimate, the return hold is released and the tax return continues to be processed. For those returns determined to be potential identity theft, taxpayers are sent Letter 5263C, *Entity Fabrication*.[6] After evaluating responses to the letters, returns that are confirmed as identity theft will have an identity theft indicator placed on their account. If the entity associated with the return is determined to be fabricated,[7] the IRS will deactivate the account, meaning that no future tax returns can be filed using that EIN.

This review was performed at the IRS Wage and Investment Division office in Atlanta, Georgia, during the period June 2017 through April 2018. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit evidence. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[6] See Appendix V for an example of the letter used.
[7] 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.

Results of Review

Actions Have Been Taken to Improve Business Identity Theft Detection in Response to Our Prior Audit

In September 2015, we reported that the IRS recognizes that new identity theft patterns are constantly evolving and, in response, it needs to continuously adapt its detection and prevention processes that include detecting identity theft on business returns. In response, the IRS expanded its processes and procedures in an effort to improve detection and prevention of business identity theft.[8] For example, the IRS has:

- Increased the number of business identity theft detection filters[9] from seven in PY 2015 to 25 in PY 2017. The types of business returns for which the filters detect potential identity theft have also been expanded to include **********2**********, filings. It should be noted that seven of these filters were developed in response to our prior report recommendations. The IRS reports that these seven filters have identified 2,868 potential identity theft returns and have stopped more than $258 million in potentially fraudulent refunds during PYs 2015 through 2017.
- Created three dynamic selection lists to identify potential business identity theft returns. If a business return is identified during processing as meeting any the following dynamic selection list criteria, the return is selected for additional review. These lists include:
  - The EINs identified by the IRS as questionable or were associated with a business that was part of a reported data breach.
  - Questionable addresses or addresses associated with businesses that were part of a reported data breach.
  - Social Security Numbers associated with the filing of a questionable business tax return or suspected data breach.

Overall, via the use of its filters and dynamic selection lists, the IRS reported that between January 1 and December 31, 2017, it identified 20,764 business returns with characteristics of identity theft that had associated refunds totaling $2.2 billion. Figure 1 provides volumes and

[8] Treasury Inspector General for Tax Administration, Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).
[9] Twenty-five business identity theft filters and three dynamic selection lists were in place as of December 31, 2017.

refund amounts associated with business identity theft returns the IRS identified in PYs 2015 through 2017.

Figure 1: Business Identity Theft Statistics PYs 2015 Through 2017

Statistic	PY		
	2015	2016	2017
Number of business identity theft filters	7	25[10]	25
Number of business identity theft returns identified	350	5,780	20,764
Total refunds	$122 Million	$534 Million	$2.2 Billion

Source: The IRS's Return Integrity and Compliance Services function.

Business Identity Theft Filters Should Continue to Be Expanded to Include Other Types of Business Tax Return Filings

For PY 2017, the business identity theft filters identify potential fraudulent filings associated with **********2**********. However, our review of PY 2017 ***2*** identified 15,127 **********2******** with refunds totaling more than $200 million[11] that the IRS would have identified as potentially fraudulent if current business identity theft filters included an evaluation of these types of tax returns. For example, we identified ***2*** with no filing requirement or with an associated cross-reference Taxpayer Identification Number (TIN)[12] that has an identity theft marker present. When we brought our concern to IRS management's attention, they agreed that the filters should be expanded to evaluate ********2******* for potential identity theft.

Recommendation

Recommendation 1*:* The Commissioner, Wage and Investment Division, should expand the use of business identity theft filters to include **********2**********
**********2**********

[10] The IRS used seven filters from January 1, 2016, through July 31, 2016. On August 1, 2016, the IRS added 18 more filters.

[11] **********2**********.

[12] A cross-reference TIN is a nine-digit taxpayer identification number that is generally associated with the responsible party for an EIN. A TIN is a nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an EIN, a Social Security Number, or an Individual TIN.

**********2**********
**********2**********.

Management's Response: The IRS agreed with this recommendation and is currently developing employment tax form identity theft filters for ********2********* ***2***. IRS management is also performing research to develop filters for additional *********2*********.

Existing Detection Processes and Procedures Need to Be Improved

Our review identified that information maintained by the IRS should be added to its dynamic selection lists to further improve identification of potentially fraudulent tax returns. This information includes:

- ********2********* of the responsible parties associated with businesses listed on the IRS's *Suspicious EIN Listing*.[13] During PY 2017, we identified 53 business tax returns with refunds totaling nearly $2.5 million in which the EIN associated with the filing had the same *******2******* that was associated with a previously identified suspicious EIN.
- ****2*** associated with cross-referenced TINs or addresses of businesses on the IRS's *Suspicious EIN Listing*. The IRS's *Suspicious EIN Listing* contained 5,133 suspicious EINs[14] as of November 1, 2017. Because the IRS has determined that these EINs are suspicious, it is likely that the ****2*** associated with these EINs and *****2***** **2** are also suspicious.

When we brought our concerns to IRS management's attention, they stated that they agreed that information from the IRS's *Suspicious EIN Listing* should be reviewed for possible inclusion on a dynamic selection list. In addition, management noted that this information would be beneficial in identifying potential questionable refund returns filed using *********2******** to these suspicious businesses.

Required account locks were not added to the majority of tax accounts associated with entities listed on the Suspicious EIN Listing

In response to a recommendation in our prior report, IRS management indicated that processes and procedures were developed to lock business tax accounts associated with suspicious EINs.

[13] Suspicious EINs are identified by the IRS when examiners call businesses to verify the tax withholding amounts claimed on certain Forms W-2. They can also be identified when the IRS corresponds with certain businesses deemed as potentially fictitious by the IRS. If the IRS receives information that a business is fictitious or bogus, as a result of these calls or correspondence, the business's EIN is added to the listing.
[14] The IRS's *Suspicious EIN Listing* actually contained 6,824 EINs. However, only 5,133 had accounts listed on the IRS's Master File.

Specifically, the IRS issued internal guidelines[15] requiring the locking of the tax accounts associated with bogus/fictitious EINs after January 2017. However, our review of the 5,133 EINs on the IRS's *Suspicious EIN Listing* as of November 2017 identified that only 220 (4 percent) had the associated tax account locked. To lock an account, the IRS inputs a specific transaction code to the taxpayer's account that deactivates the account, thus ensuring that a business return cannot be filed using the suspicious EIN.

When we discussed our analysis with management, they stated that they did not lock all EINs on the *Suspicious EIN Listing* because after reviewing the list, they identified some EINs that appeared to be associated with legitimate or active businesses, *i.e.*, not bogus/fictitious. Management noted that although the EINs were considered bogus or fabricated at the time they were placed on the list, some of the EINs could later be determined to be legitimate or valid businesses. As a result, the IRS reviewed the list in February 2018 and removed 1,097 EINs previously added to the list as a bogus or fabricated entity as being a legitimate or valid business. To make this determination, management indicated that it performed a systemic analysis of the payment and filing history for each of the suspicious EINs on the list. For those EINs that had a tax return filed or payment(s) made, regardless of when this activity occurred, the IRS concluded the business was legitimate and removed it from the list.

To confirm management's assertion that the businesses were legitimate, we performed a more in-depth analysis of payment and/or filing history associated with the 1,097 EINs. Our analysis found that many of the EINs the IRS removed from the list are in fact not legitimate businesses. We identified the following:

- 1,072 (98 percent) of the businesses removed had no income or payroll tax payments on their accounts.
- 788 (72 percent) of the EINs had no income tax or employment tax returns filed for that EIN. Of the 309 EINs with a return filing, a total of 187 (61 percent) were returns filed by the IRS, not the taxpayer. These returns were filed by the IRS's Substitute for Return program.[16] In addition, even though the IRS classifies these returns as official tax returns, only a few had payments made to these accounts by the businesses.

As previously noted, management relied solely on the results of its systemic analysis and took no additional actions, such as attempting to contact, authenticate, and verify the business was in fact legitimate, prior to removing the EIN from the list. As a result, the IRS could be removing businesses for which return filings and/or payments were the result of a *********2********** **********2**********.

[15] Internal guidelines include the Internal Revenue Manual, desk guides, *etc*.
[16] The Substitute for Return program is a nonfiler or return delinquency program for individual and individual business nonfilers who are identified via matching programs.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 2**:** Review the IRS's *Suspicious EIN Listing* on a periodic basis to ensure that the dynamic selection lists include **********2********** information associated with the EINs on the IRS's *Suspicious EIN Listing*.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to adjust its monitoring process to include the use of applicable **********2********** ***2*** information associated with the EINs on the IRS's *Suspicious EIN Listing.*

Recommendation 3: Ensure that the remaining 3,816[17] tax accounts on the IRS's November 2017 *Suspicious EIN Listing* are locked.

> ***Management's Response:*** The IRS partially agreed with this recommendation. IRS management plans to review the remaining 3,816 tax accounts and will lock those found to have clear indications of being bogus or fabricated, rather than showing only indications of filing and/or payment noncompliance.

Recommendation 4: Develop a process to periodically review the IRS's *Suspicious EIN Listing* to ensure that the EINs on the list are still considered bogus or fictitious businesses. This should include taking actions to research the accounts and contact the businesses.

> ***Management's Response:*** The IRS partially agreed with this recommendation. IRS management plans to implement a periodic review process to ensure that the EINs on the *Suspicious EIN Listing* continue to meet established criteria for monitoring. Accounts will be researched; however, the degree and the method of taxpayer contact will be determined on a case-by-case basis.

Recommendation 5: After performing each periodic review of the IRS's *Suspicious EIN Listing*, ensure that the EINs still deemed to be bogus or fictitious are locked.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to update its procedures to require accounts are locked when applicable.

Recommendation 6: Review each of the 1,097 EINs removed from the *Suspicious EIN Listing* and determine which EINs should remain on the listing. Ensure that any EINs that remain are properly locked.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to review the subject accounts to determine if any should be restored to the *Suspicious EIN Listing* and locked.

[17] The 3,816 figure is computed as follows: 5,133 original suspicious EINs minus 220 locked EINs minus 1,097 EINs removed from the list equals 3,816 remaining EINs.

Some Business Identity Theft Cases Were Not Accurately Processed

Our review of a statistically valid sample of 113[18] business tax return filings identified between January 1 and November 11, 2017, as potential business identity theft and subsequently determined to be legitimate return filings identified that for:

- 22 (19 percent) of the cases we selected, we could not assess the accuracy of case processing because the IRS was unable to locate documentation associated with these cases. Management indicated that shipping issues between Tax Processing Centers working these cases resulted in case file information being unlocatable. In response to our bringing this to management's attention, shipping and confirmation procedures were updated. As such, we are not making a recommendation.
- 21 (23 percent) of the 91 cases we could review, we determined the cases were not accurately processed. Based on the results of our statistically valid sample, we estimate that 188 cases[19] may have been inaccurately processed. The errors associated with the 21 cases included incomplete information received by the business in response to the IRS's request to make a proper determination as to whether the return filing was identity theft, improper disclosure of taxpayer information, and procedural case processing errors on the part of tax examiners, *e.g.*, inputting transaction codes as required.

When we discussed the results of our case analysis with IRS management, they disagreed with our conclusion that 13 cases were inaccurately processed because there was not sufficient information from the business to accurately conclude that the return filing was valid. IRS management indicated that there was sufficient information available to make the determination without a conclusive response from the taxpayer on these cases. However, management did not provide documentation to support their conclusion that there was sufficient information to determine that the filing did not involve identity theft. For the cases in which there was an improper disclosure of taxpayer information, management indicated that this occurred because information sent out was not properly verified before being sent to the taxpayer. IRS management noted that they implemented changes to their procedures to perform additional quality review steps prior to sending information.

Potential identity theft cases with large dollar refunds were not promptly screened, which caused millions of dollars in interest to be paid

Our review of 134 PY 2017 returns with large dollar refund claims, *i.e.*, **********2********** ****2****, identified as potential business identity theft found that 25 were not promptly

[18] Our sample of 113 was randomly selected from a total population of 1,011 cases, following the guidance of our contract statistician. The sample was selected with an expected error rate of 50 percent, a precision rate of ± 9 percent, and a confidence interval of 95 percent.

[19] The point estimate projection, based on a 95 percent confidence interval, is that between 124 and 268 cases determined to be non–identity theft were not accurately processed.

screened. As a result, the IRS unnecessarily paid interest totaling more than $4 million to these 25 businesses subsequently found to be legitimate. Internal guidelines require business returns with large dollar refunds identified as potential identity theft to receive prompt additional scrutiny to help determine if the returns are legitimate. Refunds that are not processed within 45 days of IRS receipt or due date of the return, whichever is later, require the IRS to pay interest.

When we brought our concern to IRS management's attention, they acknowledged that the delay in addressing these 25 returns resulted in the payment of interest. They also stated that they now have a process to consistently review large dollar refund cases when a response from the business has not been returned within 60 days.

Actions need to be taken to protect refunds associated with confirmed business identity theft tax returns from being erroneously released

Our review of 2,606[20] PY 2016 business identity theft tax returns identified 872 returns with refunds totaling more than $61 million that appear to have been released in error. This occurred because prior to PY 2017, the IRS allowed potential business identity theft tax returns to be processed and posted to the taxpayer's tax account. At the time the return posted, the refund was also frozen. However, this process created a situation in which other areas within the IRS could erroneously release the refund without notifying the Return Integrity and Compliance Services function. It should be noted that the remaining 1,593 returns with refunds totaling more than $93 million are at risk of being erroneously released.[21]

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. Returns that are identified as potential identity theft during PY 2017 will have a hold placed on the account that will prevent the return from posting to the Master File. This eliminates the risk of the refund associated with the return from being released in error.

[20] After providing our methodology to IRS management and receiving their feedback, we removed a total of 141 returns either because they were later determined to not be identity theft (122) or the refund was issued prior to the return being detected as identity theft (19).
[21] As of April 21, 2017.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 7**:** Develop processes and procedures to ensure that tax examiners accurately process and document the actions taken to resolve business identity theft cases.

> ***Management's Response:*** The IRS agreed with this recommendation. In June 2018, IRS management updated its procedures and training materials to provide guidance on all processes and actions required when addressing business identity theft cases.

Recommendation 8: Develop processes and procedures to ensure that transaction codes are properly input, released, and updated when necessary on business identity theft tax accounts.

> ***Management's Response:*** The IRS agreed with this recommendation. IRS management updated its procedures and training materials to include guidance on transaction code usage for business identity theft tax accounts.

Recommendation 9: Develop processes to ensure prompt screening of potential business identity theft returns with high dollar refunds to minimize unnecessarily paying interest.

> ***Management's Response:*** The IRS agreed with this recommendation. IRS management plans to develop a review process for selected business identity theft returns, including issuing procedural guidance and establishing acceptable time frames for actions to be completed.

Recommendation 10: Develop processes to ensure that refunds associated with the 1,593 confirmed PY 2016 business identity theft tax returns remain frozen from erroneous release.

> ***Management's Response:*** The IRS agreed with this recommendation and has placed controls on affected accounts to prevent the erroneous release of frozen refunds by other operating functions. The controls identify the accounts as being assigned to the Return Integrity Operation function and are not to be released by any other function. The control assignment is visible to all users who can potentially release the refund freeze.

Appendix I

Detailed Objective, Scope, and Methodology

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

I. Determined if the IRS adequately addressed concerns raised in a prior Treasury Inspector General for Tax Administration business identity theft report.[1]

- A. Reviewed the prior report and summarized recommendations and the IRS's planned corrective actions concerning business identity theft.
- B. Quantified the outcomes associated with the recommendations from the prior business identity theft report.

II. Evaluated the IRS's existing business identity theft filters to determine if they could be improved or expanded.

- A. Determined if the IRS is properly using the dynamic selection lists.
- B. Determined if current filter criteria can be expanded to other business returns.

III. Assessed the effectiveness of the IRS's screening procedures.

- A. Reviewed the current criteria established for screening out business returns selected by the business identity theft filters.
- B. Reviewed business identity theft returns with high dollar refunds[2] to determine if they were reviewed properly as per IRS screening procedures.

IV. Evaluated the effectiveness of the IRS's business identity theft case processing procedures.

- A. Identified and reviewed current procedures used to process business identity returns.
- B. Reviewed a statistical sample[3] of 113 business tax returns from a total population of 1,011 cases[4] closed as non–identity theft in PY 2017 from the IRS's inventory

[1] Treasury Inspector General for Tax Administration, Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).
[2] **********2**********.
[3] A statistical sample was selected so that the result of the sample review could be projected to the population. The sample of 113 business tax returns selected for review were determined to be non–identity theft by the IRS between January 1 and November 11, 2017.
[4] The 1,011 business tax returns were determined to be non–identity theft by the IRS between January 1 and November 11, 2017.

tracking spreadsheet and reviewed the sample to evaluate whether a proper determination was made on each case. To select our sample, we used an expected error rate of 50 percent, a precision rate of ± 9 percent, and a confidence interval of 95 percent. A contract statistician assisted with developing the sampling plan and projections.

V. Assessed the effectiveness of controls to ensure that refunds for PY 2016 business identity theft returns were not erroneously released.

A. Identified and reviewed procedures used to process business identity theft returns in PY 2016.

B. Determined if these procedures are adequate to ensure that refunds are not improperly released.

C. Evaluated whether any refunds were erroneously released and determined the associated dollar amounts.

Data validation methodology

During this review, we relied on data stored at the Treasury Inspector General for Tax Administration's Data Center Warehouse[5] and performed analysis of data extracted from the IRS Dependent Database.[6] To access the reliability of computer-processed data, programmers within the Data Center Warehouse validated the data files we extracted, and we ensured that each data extract contained the specific data elements we requested and that the data elements were accurate. For example, we reviewed judgmental samples of the data extracts and verified that the data in the extracts were the same as the data captured in the IRS's Integrated Data Retrieval System[7] or other systems, if possible. As a result of our testing, we determined 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

[5] The Data Center Warehouse provides data and data access services through the Treasury Inspector General for Tax Administration's intranet.
[6] The Dependent Database is 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.
[7] IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.

systems/programming used to process the returns. We evaluated the controls by reviewing the IRS's internal guidelines,[8] interviewing IRS management, and evaluating applicable documentation and management information reports.

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

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Diana Tengesdal, Director
Larry Madsen, Audit Manager
Jeremy Berry, Lead Auditor
Jennifer Bailey, Auditor
Jaclynne Durrant, Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Services and Enforcement
Commissioner, Wage and Investment Division
Deputy Commissioner, Wage and Investment Division
Director, Customer Account Services, W age and Investment Division
Director, Customer Assistance, Relationships, and Education, Wage and Investment Division
Director, Return Integrity and Compliance Services, Wage and Investment Division
Director, Return Integrity Operations, Wage and Investment Division
Director, Office of Audit Coordination

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective action 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 – Actual; implementation of these seven business identity theft filters has resulted in identification of 2,868 potential identity theft returns and has stopped $258,459,550 in fraudulent refunds (see page 3).

Methodology Used to Measure the Reported Benefit:

In September 2015, we reported that the IRS recognizes that new identity theft patterns are constantly evolving and, as such, it needs to continuously adapt its detection and prevention processes. This includes implementing processes to detect identity theft on business returns. In response to our report, the IRS created seven business filters to identify business returns using an EIN[1] that had no associated *******2******* or that was ***2***. These seven filters have identified 2,868 potential identity theft returns and have stopped more than $258 million in fraudulent refunds during PYs[2] 2015 through 2017.

Type and Value of Outcome Measure:

- Cost Savings, Funds Put to Better Use – Potential; 1,593 business identity theft tax returns with refunds totaling $93,164,881 (see page 8).

Methodology Used to Measure the Reported Benefit:

Our review of 2,606[3] PY 2016 business identity theft tax returns identified 872 returns with refunds totaling more than $61 million that appear to have been released in error. This occurred because prior to PY 2017, the IRS allowed potential business identity theft tax returns to be processed and posted to an associated tax account. At the time the return posted, the refund was

[1] 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] The calendar year in which the IRS processes the tax return or document.
[3] After providing our methodology to IRS management and receiving their feedback, we removed a total of 141 returns either because they were later determined to not be identity theft (122) or the refund was issued prior to the return being detected as identity theft (19).

also frozen. However, this process created a situation whereby other areas within the IRS could erroneously release the refund without notifying the Return Integrity and Compliance Services function. It should be noted that, the remaining 1,593 returns with refunds totaling more than $93 million are at risk of being erroneously released.[4]

[4] As of April 21, 2017.

Appendix V

Letter 5263C, Entity Fabrication

Ogden Service Center
OGDEN UT 84201-0062

In reply refer to:
LTR 5263C

BODC:

Employer identification number:
Tax periods:

Contact telephone number:
Contact fax number:

Dear TAXPAYER:

Our records indicate you may be the responsible party for the entity above. A "responsible party" is, for example, the principal officer of a publicly-traded corporation or a general partner of a partnership. For a full definition of "responsible party," see the instructions for Form SS-4, Application for Employer Identification Number. If you're not the responsible party for this business, select the check box below indicating so. Sign and send this response to the address or fax number at the top of this page, within 30 days from the date of this letter.

_____ I have no affiliation with this entity.

_____ I am affiliated with this entity, but I'm not the responsible person because:
(Describe your affiliation)

_____

_____

_____.

The responsible person is _____.

Please fill out the remainder of the form with information about the business to the best of your knowledge.

_____ I was previously affiliated with this entity, but I wasn't the responsible party. I haven't affiliated with it since [provide date].
(Describe your prior affiliation)

_____

LTR 5263C

- Provide an officer's name, title, telephone number, and most convenient time for us to call if we need to speak with someone about your organization

Name and title _____

Telephone number ( )_____ Hours_____

If you don't respond to this letter, we'll assume you are responsible for the business and will consider holding you liable for any taxes this business owes.

DECLARATION

Under penalties of perjury, I declare that I have examined the information referred to in this letter, and to the best of my knowledge and belief it is true, correct, and complete.

_____ _____

Signature Date

Providing false information on this form can result in penalties for perjury.

For more information about ID theft, see Publication 5027, Identity Theft Information for Taxpayers at www.irs.gov/forms-pubs.

If you have questions, you can contact the telephone number or address at the top of this letter. When you call, please provide the indicator BMF on the message along with the EIN listed above.

When you write, include this letter and provide in the spaces below, the contact name and telephone number with the hours we can reach you. Keep a copy of this letter for your records.

Contact name: _____

Telephone number ( )_____ Hours_____

Appendix VI

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

August 1, 2018

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 - Additional Actions Can Be Taken to Further Reduce Refund Losses Associated With Business Identity Theft (Audit# 201740037)

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 seven, in 2015, to 25 in 2017, resulting in the protection of $2.2 billion of potentially fraudulent refund claims in 2017.

The new filters and fraud detection models have increased the scope of business return protection from **********2********** ********** returns. Further, in 2017, we implemented expanded techniques and processes to assist with monitoring business entities reporting they are victims of a tax-related data compromise. We recognize there is more work to be done in this area and are actively engaged in expanding protection coverage to additional types of business returns. One method used to protect business accounts from identity theft is by locking them. Locking an account is a treatment reserved for those accounts with confirmed identity theft activity or a high potential for it. An account lock prevents any returns or payments from posting to the account and is therefore used only when there are clear indications of identity theft fraud.

The report states several business accounts were not locked by the IRS as required. We agree that some of the accounts should have been locked; however, we do not

agree all should have been. Locking accounts prevents any returns and/or payments from posting to them and it is not appropriate to lock accounts without clearly determining an identity theft condition exists. A non-compliant business entity, for example, may appear to be a vehicle for identity theft activities based on certain behavior such as filing Form W-2, *Wage and Tax Statement*, for employees without filing the corresponding employment tax returns to report and pay the associated employment and withholding tax liabilities. Our Examination and Collection functions have established processes in place to identify and address instances where taxpayers do not comply with their filing and/or payment obligations. Those processes would be significantly impaired if the accounts were erroneously locked. The report concludes that non-filing and/or non-payment is synonymous with a fictitious entity or identity theft fraud.

Additionally, the report states that 98 percent of the businesses removed from our monitoring processes were erroneously removed because the businesses had no income or payroll tax payments on their accounts. The report concludes that non-payment confirms the business entities were not legitimate. That correlation does not necessarily support such a finding. Likewise, 72 percent of the businesses removed had also not filed income or payroll tax returns. We do not determine that businesses are not legitimate based on noncompliance with filing requirements. Of the 309 businesses that had filed returns, the report identifies 187 as having been returns filed by the IRS. When taxpayers do not comply with their requirements to file tax returns, and a filing requirement has been affirmed, the IRS may prepare a return for them as part of our compliance processes. A Substitute for Return permits unreported income or wages paid to be systemically processed as adjustments to the account and ensures the business is afforded the due process and appeal rights applicable to the respective tax being assessed. In cases where a Substitute for Return has been prepared by the IRS, an IRS employee has been in contact with the principals of the business entity or has otherwise evaluated evidence of business operations occurring.

We appreciate the identification of opportunities for improving business identity theft detection and prevention processes, as well as the acknowledgement that the seven corrective actions implemented in response to the previous review of this program directly resulted in the protection of $258 million in potentially fraudulent refunds. We also agree that $93 million in potential cost savings has been realized, associated with 1,593 at-risk refunds that posted and were frozen in 2016. Controls have been placed on those accounts to prevent the inadvertent release of those refunds.

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

Attachment

Attachment

RECOMMENDATION 1
The Commissioner, Wage and Investment Division, should expand the use of business identity theft filters to include **********2**********.

CORRECTIVE ACTION
We agree with this recommendation and are developing **********2********** identity theft filters. Filters **********2**********, are planned for implementation in January 2019. We are also performing research to develop filters for additional **********2********** that are expected to be implemented by June 2020. Both actions require the use of Information Technology resources that are limited and subject to competing priorities, which could affect the planned implementation timeline. Therefore, we cannot provide implementation dates.

IMPLEMENTATION DATES
**********2********** – N/A
Additional **********2********** – N/A

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

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

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 2
Review the IRS's *Suspicious EIN Listing* on a periodic basis to ensure that the dynamic selection lists include applicable **********2********** information associated with the EINs on the IRS's *Suspicious EIN Listing*.

CORRECTIVE ACTION
We agree with this recommendation and will adjust our monitoring processes to include the use of applicable **********2********** information, connected with the Employer Identification Numbers (EIN) contained in the *Suspicious EIN Listing*, when reviewing the dynamic selection lists.

IMPLEMENTATION DATE
April 15, 2019

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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
Ensure the remaining 3,816 tax accounts on the IRS's November 2017 *Suspicious EIN Listing* are locked.

CORRECTIVE ACTION
We partially agree with this recommendation. We will review the remaining 3,816 accounts and will lock those found to have clear indications of being bogus or fabricated, rather than showing only indications of filing and/or payment noncompliance.

IMPLEMENTATION DATE
April 15, 2019

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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
Develop a process for periodically reviewing the IRS's *Suspicious EIN Listing* to ensure that the EINs on the list are still considered bogus or fictitious businesses. This should include taking actions to research the accounts and contact the businesses.

CORRECTIVE ACTION
We partially agree with this recommendation. A periodic review process will be implemented to ensure the EINs on the *Suspicious EIN Listing* continue to meet established criteria for monitoring. Accounts will be researched; however, the degree and the method of taxpayer contact will be determined on a case-by-case basis.

IMPLEMENTATION DATE
April 15, 2019

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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 5
After performing each periodic review of the IRS's *Suspicious EIN Listing*, ensure that EINs still deemed to be bogus or fictitious are locked.

CORRECTIVE ACTION
We agree with this recommendation. Internal Revenue Manual (IRM) 25.25.3.4, *Bogus Employer Determination*, will be updated to require accounts are locked, when applicable.

IMPLEMENTATION DATE
April 15, 2019

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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 6
Review each of the 1,097 EINs removed from the *Suspicious EIN Listing* and determine which EINs should remain on the listing. Ensure any EINs that remain are properly locked.

CORRECTIVE ACTION
We agree with this recommendation and will review the subject accounts to determine if any should be restored to the *Suspicious EIN Listing* and locked.

IMPLEMENTATION DATE
November 15, 2018

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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 7
Develop processes and procedures to ensure that tax examiners accurately process and document the actions taken to resolve business identity theft cases.

CORRECTIVE ACTION
We agree with this recommendation. In June 2018, training materials and IRM 25.25.1, *Return Integrity and Verification Revenue Protection Programs*, were updated to provide guidance on all processes and actions that must be followed when addressing business identity theft cases.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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 8
Develop processes and procedures to ensure that transaction codes are properly input, released, and updated when necessary on business identity theft tax accounts.

CORRECTIVE ACTION
We agree with this recommendation. The previously-mentioned updates to training materials and IRM 25.25.1 include guidance on transaction code usage for business identity theft tax accounts.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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 9
Develop processes to ensure prompt screening of potential business identity theft returns with high dollar refunds to minimize unnecessarily paying interest.

CORRECTIVE ACTION
We agree with this recommendation and will develop a review process for selected business identity theft returns, including issuing procedural guidance and establishing acceptable timeframes for actions to be completed.

IMPLEMENTATION DATE
January 15, 2019

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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 10
Develop processes to ensure that refunds associated with the 1,593 confirmed PY 2016 business identity theft tax returns remain frozen from erroneous release.

CORRECTIVE ACTION
We agree with this recommendation and have placed controls on the affected accounts to prevent the erroneous release of frozen refunds by other operating functions. The controls identify the account as being assigned to the Return Integrity Operation and are not to be released by any other function. The control assignment is visible to all users who could potentially release the refund freeze.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, 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.