TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection

September 9, 2015

Reference Number: 2015-40-082

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

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

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

PROCESSES ARE BEING ESTABLISHED TO DETECT BUSINESS IDENTITY THEFT; HOWEVER, ADDITIONAL ACTIONS CAN HELP IMPROVE DETECTION

Highlights

Final Report issued on September 9, 2015

Highlights of Reference Number: 2015-40-082 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

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

The IRS recognizes that new identity theft patterns are constantly evolving and, as such, it needs to continually adapt its detection and prevention processes. The overall objective of this review was to determine the effectiveness of the IRS's efforts to implement a business return program to detect and prevent identity theft.

WHAT TIGTA FOUND

TIGTA found that the IRS recognizes continued efforts are needed to develop and implement systemic processes to detect identity theft. To date, the IRS has taken actions that include defining business identity theft, creating procedures for IRS employees to follow when they are made aware of a potential business identity theft situation, and conducting a Business Identity Theft Project to detect potential business identity theft relating to corporate tax returns.

However, TIGTA also found that the IRS ***2** **********2********** **********2********** **********2********** **********2**********. For example, the IRS maintains a list of suspicious Employer Identification Numbers (EINs) determined to be associated with a fictitious business. Our analysis of business returns filed during Processing Year 2014 identified that 233 tax returns were filed using a known suspicious EIN. Of these, 97 claimed refunds totaling over $2.5 million.

In addition, TIGTA determined that processing filters could be developed to identify returns containing certain characteristics that could indicate potential identity theft cases. For example, the IRS has data to proactively identify business tax returns filed using an EIN the IRS assigned to a business that *******2********* ******2**********. TIGTA also found that State information sharing agreements do not address business identity theft. The agreements only address the detection of individual identity theft. Finally, TIGTA also identified that actions are needed to better promote awareness of business identity theft.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Commissioner, Wage and Investment Division, ensure that processes and procedures are in place **2*** **********2********** associated with suspicious EINs; establish a systemic process to identify tax returns filed with an *******2********* **********2********** to file a tax return to ensure the legitimacy of the filing and any refund claimed; establish a filter to identify **********2**********; evaluate the potential for expanding information sharing agreements to include the sharing of suspicious or potentially fraudulent business tax return filings; and continue to develop and offer additional outreach materials that directly inform businesses about business identity theft.

The IRS agreed with our recommendations. It plans to **********2********** with suspicious EINs, develop a process to systemically identify tax returns with **********2********, work with stakeholders to assess expanding the State Suspicious Filer Exchange to include business returns, and update business outreach materials. In addition, the IRS has established filters for certain corporate returns with **2*** ***2*****and plans to evaluate expanding these filters to other business returns.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 9, 2015

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection (Audit # 201440004)

This report presents the results of our review to determine the effectiveness of the Internal Revenue Service's efforts to implement a business return program to detect and prevent identity theft. This audit is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenges of Taxpayer Protection and Rights and of Fraudulent Claims and Improper Payments.

Management's response to the draft report is included in Appendix IV.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have 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

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 (*e.g.*, Form 1120, *U.S. Corporation Income Tax Return*, or Form 720, *Quarterly Federal Excise Tax Return*) 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 Forms 941, *Employer's QUARTERLY Federal Tax Return*, or Forms W-2, *Wage and Tax Statement*, to support bogus Forms 1040, *U.S. Individual Income Tax Return*, 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 (*e.g.*, Form 941, Form 1120, or Form 1041, *U.S. Income Tax Return for Estates and Trusts*), avoid paying taxes, obtain a refund, or further perpetuate individual identity theft or refund fraud.

In addition, certain refundable credits can be claimed by business filers. Refundable credits are sometimes claimed by identity thieves on individual tax returns to increase fraudulent refunds. A refundable credit is not limited to the amount of a business tax liability and can result in a tax refund that is larger than the amount of the business tax owed. In contrast, a nonrefundable credit can only reduce a business tax liability to zero. Figure 1 provides the number of returns and refundable tax credit amounts claimed on Forms 1120 for Processing Years (PY)[2] 2012 through 2014.

[1] An EIN is 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] The calendar year in which the tax return or document is processed by the IRS.

Figure 1: Refundable Credits Claimed on Corporate Tax Returns (PYs 2012–2014)

Credit Type		2012	2013	2014
Fuel Tax Credit[3]	Tax Returns	18,235	17,134	16,862
	Credit Amount	$265,344,504	$319,508,998	$267,451,024
Refundable Minimum Tax Credit[4]	Tax Returns	452	197	160
	Credit Amount	$230,119,298	$63,263,554	$209,667,492
Other Refundable Credits[5]	Tax Returns	239	330	378
	Credit Amount	$17,077,501	$45,356,385	$31,532,691
Totals	Tax Returns	**18,926**	**17,661**	**17,400**
	Credit Amount	**$512,541,303**	**$428,128,937**	**$508,651,207**

Source: Our analysis of the Business Return Transaction File,[6] PYs 2012 through 2014.

The IRS Advisory Council[7] raised concerns about business identity theft

In November 2014, the IRS Advisory Council[8] included the following statement concerning business identity theft in its report:

> *Business identity theft can be a more complex issue than individual identity theft. While individual identity theft with the IRS is accomplished by filing one fraudulent tax return at a time, business identity theft can occur in many ways. A fraudulent business entity tax return can be filed that generates a larger refund than would be obtained on an individual income tax return due to available refundable business tax credits, or fraudulent W-2 forms with fictitious withholding may be filed and the information subsequently used to file multiple fraudulent individual income tax returns claiming refunds. Similar to individual identity theft, business identity theft also impacts the banking and business communities. Because of the potentially larger payoffs available, business identity theft is on the rise.*

[3] A credit for certain nontaxable uses or sales of fuel during the income tax year claimed on Form 4136, *Credit for Federal Tax Paid on Fuels*.
[4] An election to claim certain unused minimum tax credits instead of claiming any additional first-year special depreciation allowance for eligible property claimed on line 8c of Form 8827, *Credit for Prior Year Minimum Tax – Corporations*.
[5] Various other miscellaneous refundable credits claimed that include, but are not limited to, credit for tax on ozone-depleting chemicals or credit under Internal Revenue Code Section 960(b).
[6] An IRS database of transcribed line items on all business returns and their accompanying forms and schedules.
[7] The primary purpose of the IRS Advisory Council is to provide an organized public forum for discussion of relevant tax administration issues between IRS officials and representatives of the public.
[8] Internal Revenue Service Advisory Council 2014 Public Report.

Figure 2 includes a summary of recommendations included in the report, along with the IRS's responses to those recommendations.

Figure 2: Internal Revenue Service Advisory Council 2014 Public Report – Business Identity Theft Recommendations for IRS

IRS Advisory Council Recommendations	IRS Response
Expand guidance to include truncated EINs of issuers on any copies of IRS filings that are provided to outside parties or made public or to any forms not submitted to the IRS.	The IRS agreed that implementation would reduce the number of documents with full EINs and may have a positive impact on business EIN identity theft. However, other Federal agencies require the reporting of EINs on forms that are filed. Changes to procedures of other government agencies would be needed to allow truncated EINs and/or further reduce access to fully listed EINs. Therefore, the IRS cannot implement this recommendation.
Develop and implement procedures that a taxpayer must surrender an EIN no longer in use because the business is closed or no longer in service.	**********2********** **********2********** **********2********** **********2********** **********2********** **********2**********.
Include a specific web page at IRS.gov that describes what to do if a taxpayer has been a victim of business identity theft.	The IRS previously published a web page on IRS.gov specific to business identity theft.
Increase awareness of Form 14039-B, *Business Identity Theft Affidavit*, and make it more readily available to taxpayers who are victims.	The IRS disagreed with this recommendation. Form 14039-B is provided to businesses only when the IRS needs additional information from the taxpayer to determine if business identity theft occurred.
Provide a dedicated point of contact for victims of business identity theft.	The IRS is evaluating Calendar Year 2014 business identity theft data. These include consistent taxpayer treatment, trained IRS personnel able to understand all of the complexities of business identity theft, and, ultimately, improved customer services.

IRS Advisory Council Recommendations	IRS Response
Use the e-authentication system out-of-wallet[9] questions to verify the identity of anyone requesting a new EIN. This would require that anyone wishing to obtain an EIN verify his or her identity through a series of personal questions that only that individual would know.	The IRS agrees that positive taxpayer authentication is integral to issuing an EIN. The benefits of having an e-authentication system using out-of-wallet questions to verify identity may prevent an identity thief from using someone else's identity to apply for an EIN. ***2****** **********2********** **********2********** **********2********** **********2********** **********2********** **********2********** **********2**********.

Source: Our analysis of the IRS Advisory Council recommendations.

This review was performed at the IRS Wage and Investment Division office in Atlanta, Georgia, during the period August 2014 through May 2015. 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.

[9] These questions are based on information that only the taxpayer should know, such as the amount of their car payment or other personal information.

Results of Review

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. To date, the IRS has taken the following steps:

- Defined business identity theft.
- Created procedures for IRS employees to follow when they are made aware of a potential business identity theft situation. An IRS employee can become aware of a potential business identity theft issue when a taxpayer calls or writes in as a result of receiving a balance due notice. After becoming aware of the issue, the IRS places an indicator on the business tax account.
- Created Form 14039-B to gather information used to determine whether a business's identity has been stolen.
- Conducted a Business Identity Theft Project to detect potential business identity theft relating to the filing of Forms 1120 reporting overpayments and claiming refundable credits. Based on its preliminary results, the IRS plans on developing additional criteria for filters to detect potential business identity theft.

The IRS recognizes that continued efforts are needed to develop and implement systemic processes to detect identity theft at the time a business tax return is processed. For example, EINs are printed on each individual employee's Form W-2 and are also sent to every vendor, investor, individual, or business to whom the entity issues Forms 1099.[10] This creates a real challenge for the IRS and additional opportunities for identity thieves. While the IRS combats identity theft with an aggressive strategy of prevention, detection, and victim assistance, we identified the following areas where this strategy can be further expanded to include business tax returns.

Data Maintained by the IRS Can Be Used to Proactively Detect Potential Identity Theft on Business Tax Returns

**********2**********
**********2**********

[10] The 1099 form is a series of documents the IRS refers to as "information returns." There are a number of different 1099 forms that report the various types of income that can be received throughout the year. Some of these include Form 1099-MISC, *Miscellaneous Income*, or Form 1099-INT, *Interest Income*.

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

The suspicious EIN list could be used *******2**********

The IRS maintains a list of the suspicious EINs used to identify tax returns that have income reported using those EINs. The list is cumulative, and the IRS confirmed 6,176 suspicious EINs as of March 24, 2015. Our analysis of business returns filed during PY 2014 identified 233 returns that were filed using a known suspicious EIN. Of these, 97 businesses claimed refunds totaling over $2.5 million.

An EIN is identified as suspicious when a tax examiner screens a tax return for fraud potential in the IRS's Integrity and Verification Operations function within the Return Integrity and Compliance Services organization and performs extensive research in an attempt to locate the employers associated with the EIN. If the business is ultimately determined to be a fictitious business, tax examiners designate the associated EIN as suspicious.

When we discussed the potential for **********2 **********2**, IRS management indicated that they are developing procedures that would allow the IRS to *********2*********. Electronically filed tax returns with these EINs would be rejected, and paper tax returns would be prevented from posting to the Master File.[11] These procedures would allow a certain transaction code to be entered to **********2**********. While processes have not been established specifying which particular types of accounts would receive the transaction code, IRS management indicated that a programming request has been submitted to **********2**********. The IRS expects the programming to be in place and functional by July 2016. Once this programming is in place, the IRS would have the capability to *****2*********.

**********2**********2**********

**********2**********
**********2**********
**********2********** is one criterion the IRS uses when making a business identity theft determination. For example, business identity theft internal guidelines alert tax examiners researching a business tax return

[11] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.

filing for possible identity theft to look for indications that a tax return was filed using an EIN for ********2********[12] ********2**********.

The IRS has a process to identify when a business **********2********** ***2**. A code is assigned to the taxpayer's account. **********2********** **********2**********.

**********2**********. Tax returns identified would be held until the IRS could verify the legitimacy of the return filing and any associated refund being claimed. Once the legitimacy is confirmed, the tax return would be released for processing and the tax refund would be issued. If the legitimacy is not confirmed, the IRS would remove the tax return from processing, thus preventing the issuance of a fraudulent tax refund.

Processing filters could also be developed to identify business tax filings ***2** **********2*******

Of the approximately 82 million EINs issued to businesses, we identified almost *****2****** ********2******** ********2******** ********2******** ********2******** ********2******** *******2****** Establishing a filtering tool to identify *********2********** ****2******* would give the IRS the ability to review these returns before issuing a refund.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Ensure that processes and procedures are in place to ******2****** ******2*****associated with suspicious EINs.

> ***Management's Response:*** The IRS agreed with this recommendation and already has manual processes in place ****2*******using suspicious EINs. Programming changes are expected to be completed in mid-2016 that will **********2*******

[12] **********2********** **********2********** **********2********** **********2**********.

of suspicious accounts, and procedures will be reviewed and updated accordingly to recognize the improved ****2********* capability.

Recommendation 2: Establish a systemic process to identify tax returns filed using **2*** **********2********** to ensure the legitimacy of the filing and any refund claimed.

Management's Response: The IRS agreed with this recommendation and will evaluate existing data attributes of business accounts and develop a process that can be used to systemically identify tax returns that have been filed under ******2********** **********2**********. Identified returns will be directed to an appropriate treatment stream for additional scrutiny to determine if they should be allowed to post to the Master File.

Recommendation 3: Establish a filter to identify **********2********** ****2***. Processes and procedures should also be developed to verify the legitimacy of the tax return filing prior to processing and issuance of a refund.

Management's Response: The IRS agreed with this recommendation. On June 26, 2015, the IRS initiated a pilot program in which seven rules-based decision models were added to its suite of fraud filters. These models are designed to detect potentially fraudulent *****2****** and specifically evaluate EINs that have had a ****2*****. These rules are currently in use for ********2******* filings, and their effectiveness will be evaluated for possible expansion to other business return filings in Calendar Year 2016.

State Information Sharing Agreements Do Not Address Business Identity Theft

Although the IRS has information sharing agreements in place with several States, the agreements only address the detection and prevention of individual tax return filing fraud. For example, the IRS participates with the States in a Suspicious Filer Exchange Program. In Calendar Year 2014, the IRS began working with the States to have them provide information relating to fraud and identity theft that they were identifying. Figure 4 provides a summary of the number of States currently sharing information with the IRS.

Figure 4: State Information Sharing

	Number of States
States Indicating That They Would Share Information	**31**
States Actually Sharing Information	19
States That Want to Share, But Are Not[13]	12
States That Are Not Sharing	**16**
States Not Sharing Because They Are Partial or No Income Tax States	9
No Reason Provided for Not Sharing	7
States Whose Systems Are Not Compatible for Sharing	**2**
State Still Working With the IRS to Receive Information	**1**

Source: IRS management, January 2015.

During Calendar Year 2014, 19 States submitted 302 Suspicious Filer Exchange referrals to the IRS that included approximately 157,000 taxpayers. Using these referrals, the IRS was able to identify approximately 2,600 questionable returns totaling $16 million in refunds claimed.

For PY 2015, the IRS began a pilot program to share limited information with four States to assist them in stopping potentially fraudulent refunds. On a daily basis, a file containing specific return details relating to questionable tax returns identified by the IRS is sent to these four pilot States. Each State receives the entire listing of questionable returns, not just the returns with addresses in their State. According to IRS management, between January 1 and May 1, 2015, the IRS has shared approximately 865,000 questionable returns with the pilot States. In addition, IRS management indicated that the IRS provided these pilot States with 2.5 million confirmed individual identity theft cases from PY 2014. Currently, the IRS is collecting feedback from the pilot States. If the pilot is successful, this program will be expanded to include all States interested in participating. We contacted three of the four States involved in the pilot to obtain their feedback regarding the usefulness of the information being provided by the IRS. The three States we contacted stated that the information shared by the IRS was very useful in identifying potential fraudulent tax returns filed in their States.

[13] These 12 States have indicated a willingness to share information, but have not done so at this time.

Sharing individual tax return information with the States has improved detection and prevention. Without this same type of information sharing for business tax returns, the IRS increases the risk that it will not be able to identify potential business identity theft cases. It also increases the same risk for the States. When we brought this issue to IRS management's attention, they indicated that before they can share such information, they will need to justify the "need for and use of" such data with the IRS Disclosure Office.

Recommendation

Recommendation 4: The Commissioner, Wage and Investment Division, should evaluate the potential for expanding State Suspicious Filer information sharing agreements to include suspicious or potentially fraudulent business tax return filings.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will work with stakeholders in assessing the potential benefits to be obtained from expanding the State Suspicious Filer Exchange to include suspicious or potentially fraudulent business tax returns.

Further Actions Are Needed to Promote Awareness of Business Identity Theft

The IRS needs to take additional actions to increase awareness of business identity theft. Although the IRS offers some outreach information through its tax forums, the information is limited. For example, there is minimal information provided to let businesses know how to identify potential identity theft, how to protect themselves from identity theft, and what to do and who to contact if they feel their identity has been stolen. The IRS currently provides a significant amount of educational information regarding individual identity theft. Some of this information addresses business identity theft. Figure 5 summarizes the source materials that discuss identity theft and a description of the information provided.

Figure 5: Identity Theft Information Provided by the IRS

Source	Description of Information Provided
IRS.gov/Individuals/Identity-Protection	Includes resource information, identity theft information for tax practitioners and businesses, and other valuable identity theft information. However, the section dealing with identity theft for businesses mainly includes information on what to do if your business experiences a data breach.
IRS Publication 5027, *Identity Theft Information for Taxpayers*	Defines what identity theft is, what the warning signs of identity theft are, how to reduce your risk of having your identity stolen, and the steps to take for victims of identity theft.

Source	Description of Information Provided
IRS Publication 5199, *Tax Preparer Guide to Identity Theft*	Defines what identity theft is, describes the warning signs for individual and business clients, and provides information for victims of identity theft.
Identity Theft News and Outreach	An ongoing compilation of the latest information (news releases, fact sheets, videos, podcasts, *etc*.) being issued by the IRS.
YouTube videos	The IRS has a number of YouTube videos. These include *IRS Identity Theft Frequently Asked Questions, IRS Efforts on Identity Theft, Protecting Yourself From Identity Theft, Are You a Victim of Identity Theft?,* and *Phishing-Malware*.

Source: Information taken from IRS.gov.

After we brought our concerns about the lack of sufficient information available to inform taxpayers about business identity theft, the IRS added information to the IRS.gov website titled *"Tax Practitioner Guide to Business Identity Theft."* This guide contains information for tax practitioners relating to what business identity theft is, how to know if a business has been affected, and what protective actions to take if a business has been compromised.

Although the information provided in the new guide is very good, information should also be provided specifically for business taxpayers because not all businesses use tax practitioners. As the IRS gains more information from its business identity theft projects and from resolving actual business identity theft cases, it should use this information to further educate business taxpayers concerning the risks of business identity theft and how to identify it. In addition, while the IRS has not identified a large number of business identity theft cases, it should be prepared to proactively address this type of identity theft and its potential effects on tax administration. Identity theft outreach has been an important vehicle for combating individual identity theft and should also be used as an important tool for business identity theft. If business taxpayers do not have the needed information, they may not recognize identity theft and take the proper steps to minimize its effects until the damage has already been done.

Recommendation

Recommendation 5: The Commissioner, Wage and Investment Division, should continue to develop and offer additional outreach material that directly informs businesses about business identity theft, the risks involved, how to protect themselves, and who to contact if they suspect their business's identity has been stolen.

> ***Management's Response:*** The IRS agreed with this recommendation and is currently in the process of evaluating the content of outreach materials and other sources of information addressing business-related identity theft. It will identify areas for improvement and update the messaging accordingly.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of IRS efforts to implement a business return program to detect and prevent identity theft. To accomplish this objective, we:

I. Assessed the effectiveness of IRS processes and controls to proactively detect and prevent potential business identity theft at the time returns are processed.

A. Requested a computer extract from the IRS's Business Master File[1] of all EINs. We identified those EINs for which there was **********2**********.

B. Compared the **2***** EINs to the Business Return Transaction File[2] from the Treasury Inspector General for Tax Administration's Data Center Warehouse[3] to determine if an ****2**** EIN was used to file a business return in PY[4] 2014. We identified 46,100 business returns that were filed using ***2*** EINs, and 1,203 of these returns claimed a refund.

C. Analyzed business returns filed in PY 2014 to identify characteristics of potential identity theft. We identified 627 business returns that were filed using EINs with no *******2*********, and 32 of these returns claimed a refund.

D. Analyzed business refunds sent by the IRS to the Bureau of the Fiscal Service during PY 2014. We identified 393,567 refunds that were issued to the ******2********** **********2**********.

E. Interviewed IRS management to determine the status of implementing a process to ******2**********.

F. Obtained from the IRS the suspicious EIN listing. We analyzed business returns filed in PY 2014 to determine if a suspicious EIN was used to file a business return. We identified 233 business returns that were filed using suspicious EINs, and 97 of these returns claimed a refund.

[1] The IRS database that consists of Federal tax-related transactions and accounts for businesses. These include employment taxes, income taxes on businesses, and excise taxes.
[2] An IRS database of transcribed line items on all business returns and their accompanying forms and schedules.
[3] A collection of IRS databases containing various types of taxpayer account information that is maintained by the Treasury Inspector General for Tax Administration for the purpose of analyzing data for ongoing audits.
[4] The calendar year in which the tax return or document is processed by the IRS.

G. Reviewed the IRS Advisory Council's 2014 Public Report and the IRS's responses to the Council's recommendations.

II. Determined what information the States could provide to help the IRS proactively identify business returns with potential identity theft.

A. Reviewed agreements between the States and the IRS regarding individual identity theft information sharing and determined if similar agreements could be beneficial for business identity theft.

B. Contacted three States that are actively involved with business identity theft at a State level and determined if the information shared by the IRS was useful and could assist States in identifying business identity theft.

III. Evaluated the effectiveness of the IRS's outreach efforts to inform business taxpayers of the risks associated with business identity theft and the processes that should be followed to reduce those risks.

A. Reviewed business identity theft Internal Revenue Manual instructions, publications, information on the IRS's website, and tax forum information to determine if outreach information is accurate, consistent, and clear.

B. Interviewed IRS management to determine current and future outreach efforts that are planned for business identity theft.

Data validation methodology

During this review, we relied on data stored at the Treasury Inspector General for Tax Administration's Data Center Warehouse and performed analysis of data extracted from the Business Return Transaction File and business refunds file. We also relied on data extracted from the IRS's Business Master File that were provided by programmers from the Data Center Warehouse. To assess the reliability of computer-processed data, programmers within the Data Center Warehouse validated the data files extracted and provided, while 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 extracted and verified that the data were the same as the data captured in the IRS's Integrated Data Retrieval System.[5] In addition, we compared data to the electronically filed returns as appropriate to verify that the amounts were supported. As a result of our testing, we determined that the data used in our review were reliable and accurate.

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

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: policies and procedures followed when processing these returns and the systems/programming used. We evaluated the controls by reviewing the IRS's Internal Revenue Manual sections used by various business operating divisions, interviewing IRS management, and evaluating applicable documentation and management information reports.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Diana M. Tengesdal, Director
Larry Madsen, Audit Manager
Kyle Bambrough, Lead Auditor
Steven Stephens, Senior Auditor
Jeremy Berry, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Deputy Commissioner, Wage and Investment Division SE:W
Director, Customer Account Services, Wage and Investment Division SE:W:CAS
Director, Customer Assistance, Relationships and Education SE:W:CAR
Director, Return Integrity and Compliance Services SE:W:RICS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Chief, Program Evaluation and Improvement, Wage and Investment Division SE:W:S:PEI

Appendix IV

Management's Response to the Draft Report

DEPARTMENTOF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

August 18, 2015

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Debra Holland /s/ Debra S. Holland
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report - Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection (Audit# 201440004)

Thank you for the opportunity to review and provide feedback on the subject draft audit report. As the tactics employed by the perpetrators of tax-related identity theft (IDT) continue to evolve, the IRS has likewise expanded its efforts at improving defensive controls and exploring proactive measures intended to stop new tactics from yielding successful results for the identity thieves. We appreciate the Treasury Inspector General for Tax Administration's acknowledgement of the IRS' continued efforts in fighting IDT-related refund fraud in both the individual and business environments.

One of the approaches the IRS is applying to defending against IDT using business accounts is preventing suspect returns from fully processing and posting to the Master File. This approach has been very successful in combating attempted IDT using the stolen account information of individuals, and we believe it will also be an effective control for protecting business accounts. Further, when expected programming is completed in mid-2016, we will have the ability to systemically lock fraudulently used business accounts when those accounts are found to be used to perpetrate refund fraud on individual tax returns.

We believe other existing processes can be updated to better position them as protective controls against business account IDT. We are evaluating procedures that, similar to controls that will prevent the posting of deactivated accounts, will also prevent the posting of returns that are filed under the Employer Identification Numbers (EIN) of inactive accounts. While these long-time procedures have been in place to detect and prevent potential errors, we will adapt them to also recognize the potential for identity theft and treat the returns accordingly. *******2********** **********2**********.

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

We would like to address a statement included in the report that we believe may confuse an outside reader as to our commitment to fight all forms of tax-related IDT. Regarding the sharing of business identity theft information with the states participating in the Suspicious Filer Exchange Program, it is important to note that the sharing of individual information has been piloted during 2015 and we, along with the participating states, are evaluating the effectiveness of the program. Sharing business-related information is a logical next step in the evolution of the program; however, it will be necessary to assess the cost of compiling and providing the information and the degree to which it would be useful to our outside partners. Further, as with the sharing of any taxpayer information protected under the authority of Internal Revenue Code Section 6103, our agreements with the participating states are subject to review by the IRS Disclosure Office.

Attached are our comments to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Ivy McChesney, Director, Customer Account Services, Wage and Investment Division, at (404) 338-8910.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Ensure that processes and procedures are in place *****2********** associated with suspicious EINs.

CORRECTIVE ACTION
We agree with this recommendation and already have manual processes in place ****2*** using suspicious Employer Identification Numbers (EIN). Programming changes are expected to be completed in mid-2016 that will ******2********** of suspicious accounts and, at that time, procedures will be reviewed and updated accordingly to recognize the improved ********2**********.

IMPLEMENTATION DATE
October 15, 2016

RESPONSIBLE OFFICIAL
Director, Accounts Management, Customer Account 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
Establish a systemic process to identify tax returns filed using **********2********** **********2********** to ensure the legitimacy of the filing and any refund claimed.

CORRECTIVE ACTION
We will evaluate existing data attributes of business accounts and develop a process that can be used to systemically identify tax returns that have been filed under **********2**********. Identified returns will be directed to an appropriate treatment stream for additional scrutiny and to determine if they should be allowed to post to the Master File.

IMPLEMENTATION DATE
February 15, 2017

RESPONSIBLE OFFICIAL
Director, 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
Establish a filter to identify**********2**********. Processes and procedures should also be developed to verify the legitimacy of the tax return filing prior to processing and issuance of a refund.

CORRECTIVE ACTION
We agree with this recommendation. On June 26, 2015, the IRS initiated a pilot program where seven rules-based decision models were added to our suite of fraud filters. These models are designed to detect potentially fraudulent ****2**********, and specifically evaluate EINs that have had a ********2**********. These rules are currently in use for **********2**********, filings and their effectiveness will be evaluated for possible expansion to other business return filings in
2016.

IMPLEMENTATION DATE
February 15, 2016

RESPONSIBLE OFFICIAL
Director, 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
The Commissioner, Wage and Investment Division, should evaluate the potential for expanding State Suspicious Filer information sharing agreements to include suspicious or potentially fraudulent business tax return filings.

CORRECTIVE ACTION
The IRS will work with stakeholders in assessing the potential benefits to be obtained from expanding the State Suspicious Filer Exchange to include suspicious or potentially fraudulent business tax returns.

IMPLEMENTATION DATE
October 15, 2016

RESPONSIBLE OFFICIAL
Director, 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
The Commissioner, Wage and Investment Division, should continue to develop and offer additional outreach material that directly informs businesses about business identity theft, the risks involved, how to protect themselves, and who to contact if they suspect their business's identity has been stolen.

CORRECTIVE ACTION
We are currently in the process of evaluating the content of outreach materials and other sources of information addressing business-related IDT. We will identify areas for improvement and update the messaging accordingly.

IMPLEMENTATION DATE
October 15, 2016

RESPONSIBLE OFFICIAL
Director, Accounts Management, Customer Account Services, Wage and Investment Division

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