



*Most Employment Identity Theft Victims
Have Not Been Notified That Their Identities
Are Being Used by Others for Employment*

February 12, 2018

Reference Number: 2018-40-016

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.

Phone Number / 202-622-6500

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

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



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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.



HIGHLIGHTS

MOST EMPLOYMENT IDENTITY THEFT VICTIMS HAVE NOT BEEN NOTIFIED THAT THEIR IDENTITIES ARE BEING USED BY OTHERS FOR EMPLOYMENT

Highlights

Final Report issued on February 12, 2018

Highlights of Reference Number: 2018-40-016 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

Employment-related identity theft (hereafter referred to as employment identity theft) occurs when an identity thief uses another person's identity to gain employment. Employment identity theft can cause a significant burden to innocent taxpayers, including the incorrect computation of taxes based on income that does not belong to them.

WHY TIGTA DID THE AUDIT

This audit was initiated to assess the IRS's processes to notify employment identity theft victims in Processing Year (PY) 2017. This includes assessing the impact of the IRS's decision to notify only newly identified victims.

WHAT TIGTA FOUND

Most identified victims remain unaware that their identities are being used by other individuals for employment. A programming error limited the IRS notifications to only those victims who were not identified in prior years. As a result, the IRS did not notify 458,658 repeat victims of employment identity theft that it identified in PY 2017 and on a tax return processed prior to PY 2017. On September 27, 2017, the IRS prepared an information technology request to correct this programming error.

In addition, the IRS plans to evaluate the results of its notice program after the first year of implementation and determine an appropriate course of action with respect to previously identified potential victims of employment identity theft who were not victims in PY 2017.

TIGTA also identified that 15,168 (13.5 percent) of the 112,445 employment identity theft notices were erroneously sent to taxpayers who were not employment identity theft victims. In most instances, these taxpayers were the spouses of taxpayers who filed legitimate tax returns reporting the spouses' wages and Social Security Numbers. The IRS erroneously placed an employment identity theft marker on the spouses' tax accounts, which then generated the notices.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS: 1) send the employment identity theft notice to the 458,658 victims identified in PY 2017 informing them that their Social Security Number was used by another person to obtain employment; 2) reverse the employment identity theft marker on the 15,168 taxpayers' accounts and notify them that the notice was sent to them in error; 3) revise programming to ensure that the employment identity theft marker is not erroneously placed on tax accounts; and 4) identify instances, prior to PY 2017, in which the IRS erroneously placed the employment identity theft marker on taxpayers' accounts.

The IRS agreed with TIGTA's recommendations and plans to take corrective actions.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 12, 2018

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Most Employment Identity Theft Victims Have Not Been Notified That Their Identities Are Being Used by Others for Employment (Audit # 201740033)

This report presents the results of our review to assess the Internal Revenue Service's processes to notify employment-related identity theft victims in Processing Year 2017. This audit was included in our Fiscal Year 2017 Discretionary Audit Coverage and addresses the major management challenge of Providing Quality Taxpayer Service Operations.

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).



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Table of Contents

Background	Page 1
Results of Review	Page 3
Most Identified Victims Remain Unaware That Their Identities Are Being Used by Other Individuals for Employment	Page 3
Recommendation 1:	Page 4
Notifications Were Erroneously Sent to Some Taxpayers	Page 4
Recommendations 2 through 4:	Page 5
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 6
Appendix II – Major Contributors to This Report	Page 9
Appendix III – Report Distribution List	Page 10
Appendix IV – Outcome Measures	Page 11
Appendix V – CP01E, Employment Related Identity Theft Notice	Page 12
Appendix VI – Management’s Response to the Draft Report	Page 13



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Abbreviations

e-file(d)	Electronically File(d)
IRS	Internal Revenue Service
ITIN	Individual Taxpayer Identification Number
PY	Processing Year
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Background

Employment-related identity theft (hereafter referred to as employment identity theft) involves using another person's identity to gain employment. Employment identity theft can cause a significant burden to innocent taxpayers, including the incorrect computation of taxes based on income that does not belong to them. Cases of employment identity theft identified by the Internal Revenue Service (IRS) usually involve an Individual Taxpayer Identification Number (ITIN)¹ filer who used the Social Security Number (SSN) of another individual, *i.e.*, victim, to gain employment.

The IRS identifies employment identity theft with its ITIN/SSN mismatch process. This process detects instances in which an ITIN is listed as either the primary or secondary Taxpayer Identification Number on Form 1040, *U.S. Individual Income Tax Return*, and the Form W-2, *Wage and Tax Statement*, included with the return has an SSN. The SSN belongs to the employment identity theft victim. The IRS refers to these cases as ITIN/SSN mismatches.

When the IRS receives electronically filed (e-filed) returns, systemic programming is in place to identify an ITIN/SSN mismatch on the returns. Once identified, the program creates an e-file ITIN/SSN mismatch marker, which is placed on the SSN owner's tax account. This marker keeps victims from being identified by the IRS Automated Underreporter Program² as having income discrepancies, and alerts employees who may be assisting the SSN owner that he or she may be a victim of employment identity theft.

A process to identify and notify victims of employment identity theft reported on paper-filed returns will be in place for the 2018 Filing Season³

In August 2016, we first reported⁴ that the IRS had not established a process to identify mismatches and set an identity theft marker on victims' tax accounts for paper tax returns. In our June 2017 report,⁵ we recommended that the Commissioner, Wage and Investment Division, develop processes and procedures to identify ITIN/SSN mismatches on ITIN paper tax returns

¹ An ITIN is a nine-digit tax processing number issued by the IRS to individuals who do not have, and are not eligible to obtain, a Social Security Number. Generally, individuals who have a tax return filing requirement or are filing a tax return to claim a refund of over-withheld tax are eligible to receive an ITIN.

² The Automated Underreporter Program matches taxpayer income and deductions submitted on information returns by third parties, *e.g.*, employers, banks, or brokerage firms, against amounts reported by taxpayers on their individual income tax returns to identify discrepancies.

³ The period from January through mid-April when most individual income tax returns are filed.

⁴ Treasury Inspector General for Tax Administration (TIGTA), Ref. 2016-40-065, *Processes Are Not Sufficient to Assist Victims of Employment-Related Identity Theft* (August 2016).

⁵ TIGTA, Ref. 2017-40-031, *The Number of Employment-Related Identity Theft Victims Is Significantly Greater Than Identified* (June 2017).



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

with a Form W-2 attached, and add an employment identity theft marker to the SSN owners' tax accounts. The IRS agreed and requested programming changes that are expected to be in place for the 2018 Filing Season. This programming will systemically identify SSN mismatches on paper returns filed with an ITIN and forward those returns for special handling that will add the SSN data to the return record and permit markers to be applied on eligible accounts.

This review was performed with information obtained from the Identity Theft Protection Strategy and Oversight office in Washington, D.C., during the period March through November 2017. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Results of Review

In response to prior Treasury Inspector General for Tax Administration (TIGTA) audit recommendations, the IRS developed processes to notify taxpayers identified as victims of employment identity theft. Specifically, the IRS began notifying SSN owners⁶ who have an employment identity theft marker placed on their account on or after January 1, 2017. Once identified, the IRS sends the victims a CP01E (701E in Spanish) notice.⁷ This notice informs the recipient that the IRS believes another person used the taxpayer's SSN to obtain employment and provides actions the taxpayer can take to mitigate the effects of identity theft. For example, taxpayers are encouraged to review their earnings with the Social Security Administration to ensure that their records are correct. Taxpayers are also encouraged to contact one of the three major credit bureaus to have a no-cost temporary "fraud alert" placed on their accounts.

The IRS's Correspondence Production Services sites in Detroit, Michigan, and Ogden, Utah, print and mail the CP01E notices. The IRS systemically adds a confirmation marker to the taxpayers' accounts confirming the printing and mailing of the notice. In addition to sending the notifications, the IRS established a dedicated telephone line and included that number on the notice so victims can contact the IRS directly if they have questions or need assistance.

Most Identified Victims Remain Unaware That Their Identities Are Being Used by Other Individuals for Employment

Our review of Processing Year (PY) 2017 e-filed returns processed between February 27, 2017, and May 22, 2017, identified that the IRS did not send the CP01E notice to 458,658 taxpayers whose SSNs were used to report income by an ITIN filer on a PY 2017 e-filed tax return. A programming error limited notifications to only those victims whose information was identified on an ITIN/SSN mismatch return *who were not previously identified as a victim*. Each of these 458,658 taxpayer's SSNs were used by an ITIN filer prior to PY 2017 and identified by the IRS as a victim of employment identity theft. Without receiving the notice, the 458,658 victims remain unaware that their SSNs were used by someone else.

On April 13, 2017, we notified IRS management of our concerns that repeat victims were not being notified. In response, the IRS prepared an information technology request, on September 27, 2017, to correct the programming error that limited notifications to only those victims whose information was identified on an ITIN/SSN mismatch return and were not

⁶ The IRS will not issue notice CP01E if the marker has been reversed, the notice was previously issued, or the taxpayer's address on the Individual Master File is an IRS campus address. The Individual Master File is the database that maintains transactions or records of individual tax accounts.

⁷ See Appendix V for an example of the notice.



Most Employment Identity Theft Victims Have Not Been Notified That Their Identities Are Being Used by Others for Employment

previously identified as a victim. The IRS stated the correction to the programming will be implemented by January 27, 2018.

In addition, IRS management noted that they will evaluate the results of the CP01E notice program after the first year and determine an appropriate course of action with respect to the previously identified potential victims who were not victims in PY 2017. IRS management also stated that they decided to send notices to only taxpayers victimized in PY 2017 because they wanted to use their limited resources efficiently and prevent taxpayer confusion by preventing multiple notices from being issued to the same taxpayer.

Recommendation

Recommendation 1: The Commissioner, Wage and Investment Division, should send the CP01E notice to the 458,658 repeat victims identified in PY 2017 informing them that their SSN was used by another person to obtain employment.

Management's Response: The IRS agreed with this recommendation and plans to send a CP01E notice to the 458,658 repeat victims identified in PY 2017 and in PY 2018.

Notifications Were Erroneously Sent to Some Taxpayers

Our review of the 112,445 CP01E employment identity theft notices issued by the IRS between February 27, 2017, and May 22, 2017, identified that 15,168 (13.5 percent) notices were erroneously sent to taxpayers. The majority of these cases involved an ITIN filer *whose spouse had an SSN* that was used to report income on the ITIN filer's e-filed tax return. The IRS erroneously placed the employment identity theft marker on the SSN owners' tax account, which then generated the notices.

The erroneous notices resulted from an IRS programming deficiency that did not identify situations in which an ITIN filer's return includes a spouse with a valid SSN that is also listed on the Form W-2 associated with the tax return. These returns are not ITIN/SSN mismatch returns, yet the IRS's programming identified them as such.

IRS management has not reviewed the programming of the employment identity theft marker since it was implemented in January 2011. When we brought our concerns to IRS management's attention, they stated that they would monitor the notification process and determine by July 2018 the requisite programming changes needed to ensure that markers are properly applied. The IRS also stated that it could not provide an implementation date for this corrective action because its information technology resources are subject to competing priorities and budget constraints.

Erroneously marking taxpayers' accounts with the employment identity theft marker causes taxpayer burden and confusion when they receive the CP01E notice. For example, the taxpayer might spend time completing the steps listed on the notice, such as contacting the Social Security



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Administration, the credit bureaus, and the IRS, to protect their identity, then later discover that they were never a victim of employment identity theft.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 2: Reverse the employment identity theft marker placed on the 15,168 taxpayers' accounts and notify them that the prior notice was sent erroneously.

Management's Response: The IRS agreed with this recommendation and plans to take the necessary actions to reverse the indicators. IRS management also plans to notify the taxpayers that the prior CP01E notice was sent erroneously, if there are no indications that they are a victim of another type of identity theft.

Recommendation 3: Revise ITIN/SSN mismatch programming to ensure that it does not place the employment identity theft marker on the accounts of SSN owners who are spouses of ITIN holders.

Management's Response: The IRS agreed with this recommendation. IRS management is reviewing the current programming and plans to implement the necessary programming changes when the root cause of the problem is identified.

Recommendation 4: Identify instances, prior to PY 2017, in which the ITIN/SSN mismatch process erroneously placed the employment identity theft marker on the tax accounts of SSN owners who are spouses of ITIN holders. The marker should be reversed on those accounts.

Management's Response: The IRS agreed with this recommendation and plans to reverse the appropriate employment identity theft markers.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the IRS's processes to notify employment-related identity theft victims in PY 2017. To accomplish our objective, we:

- I. Assessed the IRS's notice, CP01E/701E,¹ to victims of employment identity theft for clarity and accuracy.
 - A. Evaluated the notice for clarity.
 - B. Reviewed the notice information for accuracy, including telephone numbers and web addresses.
- II. Determined if the notice is sent to all victims identified by ITIN/SSN mismatch programming.
 - A. Analyzed taxpayer data to ensure that all victims identified by the ITIN/SSN mismatch programming received the employment identity theft notification marker.
 1. Identified 112,445 taxpayers who received the employment identity theft marker between February 27 and May 22, 2017.
 2. Compared the tax accounts marked with the employment identity theft marker in PY 2017 to the accounts with the employment identity theft notification marker to identify accounts that were not properly marked, *i.e.*, taxpayer did not get the required CP01E notice.
 3. Determined the cause for tax accounts with the employment identity theft marker that did not have the employment identity theft notification marker placed on the account.
 - B. Analyzed IRS print files data to ensure that a CP01E notice was actually generated for all victims in the print files.
 1. Obtained IRS print file data for cycles 201713 and 201714 that were sent for notice printing.
 2. Compared the print file data to the tax accounts that received the employment identity theft marker and the employment identity theft notification marker for the associated cycles to verify notice accuracy and completeness.

¹ See Appendix V for an example of the notice.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

- C. Determined whether the 112,445 taxpayers receiving the employment identity theft notice were associated with an ITIN/SSN mismatch return.
- III. Assessed the impact of the IRS's decision to notify only newly identified employment identity theft victims in PY 2017.
- A. Identified 1,346,485 tax accounts marked with the employment identity theft marker prior to PY 2017 using data provided by Strategic Data Services.
 - B. Analyzed IRS e-filed tax returns and corresponding Forms W-2, *Wage and Tax Statement*, processed in PY 2017 through April 18, 2017, to identify ITIN/SSN mismatches.
 - 1. Identified PY 2017 e-filed tax returns with an ITIN and respective Form W-2 data from the Modernized Tax Return Database² files on the TIGTA Data Center Warehouse.³
 - 2. Matched the PY 2017 e-filed tax return data and respective W-2 data by return unique keys into one data file.
 - 3. Identified 1,227,579 tax returns in step III.B.2. in which the ITIN on the return does not match the SSN on the Form W-2.
 - C. Compared the PY 2017 ITIN/SSN mismatch results from Step III.B. to the accounts identified in Step III.A. that were marked with an employment identity theft marker prior to PY 2017 and identified 458,658 repeat victims who did not get a CP01E notice in PY 2017.

Validity and reliability of data from computer-based systems

We validated the data from the Modernized Tax Return Database, the Individual Returns Transaction Files,⁴ and the Form W-2 File obtained from the TIGTA Data Center Warehouse by: 1) reviewing the data for obvious errors in accuracy and completeness and 2) selecting a random sample of cases from each extract to verify that the data elements extracted matched the taxpayer account information in the Integrated Data Retrieval System⁵ and the Employee User Portal. We determined that the data were valid and reliable for the purposes of this report.

² The legal repository for original e-filed returns received by the IRS through the Modernized e-File system.

³ A secured centralized storage of IRS database files used to maintain critical historical data that have been extracted from operational data storage and transformed into formats accessible to TIGTA employees.

⁴ Contains data transcribed from initial input of the original individual tax returns during return processing.

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



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRS's systemic processes for placing employment identity theft markers on taxpayer accounts and issuing the CP01E notice to taxpayers, which notifies them that they are a victim of employment identity theft. We evaluated these controls by interviewing officials in the Identity Theft Protection Strategy and Oversight office, reviewing the IRS data validation and quality assurance procedures, and analyzing the IRS processed taxpayer data.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Appendix II

Major Contributors to This Report

Russell Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Allen Gray, Director
Levi Dickson, Audit Manager
Erica Law, Lead Auditor
Ann Ring, Auditor



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Associate Chief Information Officer, Applications Development
Deputy Commissioner, Wage and Investment Division
Director, Corporate Data
Director, Customer Account Services
Director, Submission Processing
Director, Office of Audit Coordination



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Appendix IV

Outcome Measures

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

Type and Value of Outcome Measure:

- Taxpayer Rights and Entitlements – Potential; 458,658 repeat taxpayer employment identity theft victims identified in PY 2017 (see page 3).

Methodology Used to Measure the Reported Benefit:

The IRS placed the employment identity theft marker on 1,346,485 taxpayer accounts between PYs 2011 and 2016 through the e-file ITIN/SSN mismatch process. Our analysis identified 458,658 taxpayers whose information was once again identified in PY 2017 on an ITIN/SSN mismatch tax return. These taxpayers did not receive the CP01E notice because a programming error limited the notifications to only those victims whose information was identified on an ITIN/SSN mismatch return and who were not previously identified as a victim.

Type and Value of Outcome Measure:

- Taxpayer Burden – Potential; 15,168 taxpayers who were erroneously issued notice CP01E. The IRS had no evidence that these taxpayers were victims of employment identity theft (see page 4).

Methodology Used to Measure the Reported Benefit:

The IRS issued 112,445 CP01E employment identity theft notices between February 27, 2017, and May 22, 2017. We compared the 112,445 taxpayers receiving the notification with the ITIN/SSN mismatch returns and found 15,168 taxpayers who were erroneously issued the notice. In most cases, these taxpayers were spouses of ITIN owners who filed returns listing their ITIN and their spouse's SSN on the return. We found that the employment identity theft marker was erroneously placed on the SSN owner's tax account, which then generated the notice.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Appendix V

CP01E, Employment Related Identity Theft Notice



Department of the Treasury
Internal Revenue Service
Fresno, CA 93888-0025

Notice	CP01E
Tax year	2016
Notice date	January 30, 2017
To contact us	1-800-908-4490 ext. 477
Your caller ID	NNNN
Page 1 of 1	

0000000000
JAMES Q. HINDS
22 BOULDER STREET
HANSON, CT 00000-7253

Important message about your tax account

Employment Related Identity Theft Notice

We believe another person used your social security number (SSN) to obtain employment.

We are sending this notice to make you aware of this incident so you can take appropriate steps to protect yourself from any potential effects of identity theft. We'll not provide you specific details regarding the identity of the individual who used your SSN for employment purposes.

There is currently no known impact to your tax account as a result of this potential misuse. We placed a marker on your tax account to identify that you may have been a victim of identity theft.

What you need to do

Continue to timely file all federal tax returns.

You should review your earnings with the Social Security Administration to ensure their records are correct. You can create an account online at www.ssa.gov.

We strongly suggest you monitor your credit reports and all financial accounts for signs of misuse of your personal information.

As a precaution, you can contact one of the three major credit bureaus to have a no-cost temporary "fraud alert" placed on your account:

- Equifax: 1-888-766-0008, www.equifax.com
- Experian: 1-888-397-3742, www.experian.com
- TransUnion: 1-800-680-7289, www.transunion.com

You only need to contact one of the credit bureaus. When requesting a "fraud alert," the bureau you contact must contact the other two bureaus.

Additional information about Identity Theft

- Visit www.irs.gov/identitytheft
- If you need assistance, don't hesitate to contact us at 1-800-908-4490 ext. 477. If you are out of the country and need assistance, call us at 01-267-941-1000 (not toll free).
- For additional information about identity theft and actions you can take to protect yourself, visit the Federal Trade Commission's website at www.ftc.gov/idtheft. You can also find additional information at www.irs.gov (search terms "identity theft" and "phishing").
- Visit the Social Security Administration at www.ssa.gov and search for "Identity Theft."



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Appendix VI

Management's Response to the Draft Report




COMMISSIONER
WAGE AND INVESTMENT DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

January 17, 2018

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report – Most Employment Identity Theft Victims
Have Not Been Notified That Their Identities Are Being Used by
Others for Employment (Audit # 201740033)

Thank you for the opportunity to review and provide comments on the subject draft report and its recommendations. Employment-related identity theft (IDT) is the misuse of another person's Social Security Number (SSN) to obtain employment. Individuals engaging in employment-related IDT have a legal obligation to file their tax returns and report income. Tax-related IDT is not the same as employment-related IDT, but instead is a filing of a false return using the name and SSN of another taxpayer to obtain a tax refund fraudulently.

Regardless of the type, the IRS takes IDT fraud very seriously and has expended substantial resources to identify and stop tax fraud and the victimization of innocent taxpayers when their personally identifiable information (PII) is misused. Since February 2011, we have been identifying returns that reflect discrepancies between the wages self-reported by a taxpayer and wages attributed to the taxpayer as reported by an individual using that taxpayer's SSN. In those cases, we have placed an indicator code on the associated accounts to prevent unnecessary compliance contacts because of these discrepancies. The code also alerts IRS employees who may be assisting the taxpayer that the taxpayer may be the victim of IDT. In 2014, we completed a pilot program to notify such victims that their SSNs were used by another person to obtain employment. This notification alerted them that we've taken actions to ensure there is no impact to their tax return or tax account, that they may wish to review the earnings posted to their account with the Social Security Administration (SSA) (because this incident could result in additional amounts being credited to their SSA account), and that they should consider credit monitoring options. Based on the results of the pilot, we began, in January 2017, notifying the victims of such employment-related IDT that we identify.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

2

The 2017 Filing Season was the initial season for the employment-related IDT notification program. Throughout this season, we monitored the notification program to not only identify any programming issues, but to continue to refine and improve our process for notifying individuals when their SSNs were being misused by others for employment purposes. The programming for the employment-related IDT notification program was intended to place a marker on every SSN when an incident of employment-related IDT was identified during the processing of tax returns throughout each filing season. This includes newly identified victims and repeat victims. Although the intent of the programming was to mark repeat victims accounts every year that their SSN was used for employment, the programming did not work as intended, therefore preventing repeat victims accounts from receiving the marker and the CP 01E, *Employment-Related Identity Theft Notice*. A programming change has been initiated and is scheduled for implementation in January 2018 to correct this issue. Once the programming change is implemented, the 458,658 individuals identified in the audit will be notified during the 2018 filing season.

Our monitoring of the program also identified that some taxpayers were not issued a CP 01E although they were eligible to receive a notice. A review of the programming revealed that although the programming was intended not to issue another CP 01E if one was previously issued within the past three years, the programming did not issue a CP 01E if a previous CP 01 notice, regardless of the identifier (CP 01A, CP 01B, CP 01C, etc.) was issued. The programming change was implemented in June 2017 and a CP 01E was issued to these taxpayers who were not previously notified due to the programming issue.

In the report, it is noted that 15,168 notices were sent erroneously to the spouse of an Individual Taxpayer Identification Number (ITIN) filer resulting from a programming deficiency. We agree with your findings and are taking the necessary actions to identify and correct this programming deficiency. Although we feel that sending a notice to these taxpayers explaining that the previously issued notice of employment-related IDT was issued in error may cause confusion for the taxpayer due to the amount of time that has expired during the issuance of both notices, we agree that it is the appropriate action to take. However, if there is any indication that the individuals who were issued the CP 01E in error were victims of another type of identity theft, then we will not send them the additional notification.

We are continuing to analyze the data collected during this initial year of implementing the employment-related IDT notification program and based on our analysis we will make the necessary changes to improve the notification process. For example, from our monitoring of phone calls received related to the CP 01E notice, we are updating the information provided on IRS.gov, Frequently Asked Questions, and procedural changes.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

3

As noted, the IRS is committed to providing all assistance possible to taxpayers whose SSNs are being misused. Working within the confines of our limited resources, we will continue to leverage existing systems to the greatest extent possible to improve the notification process to the taxpayer.

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 James P. Clifford, Director, Customer Account Services, Wage and Investment Division, at (470) 639-3504.

Attachment



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

Attachment

Recommendations

RECOMMENDATION 1

The Commissioner, Wage and Investment Division, should send the CP01E notice to the 458,658 repeat victims identified in PY 2017 informing them that their SSN was used by another person to obtain employment.

CORRECTIVE ACTION

We agree with this recommendation and will send a CP 01E, *Employment-Related Identity Theft Notice*, to the 458,658 repeat victims identified in Processing Year (PY) 2017 and in PY 2018.

IMPLEMENTATION DATE

November 15, 2018

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

Reverse the employment identity theft marker placed on the 15,168 taxpayers' accounts and notify them that the prior notice was sent erroneously.

CORRECTIVE ACTION

We agree with this recommendation and will take the necessary actions to reverse the indicators. We will notify the taxpayers that the prior notice, CP 01E, was sent erroneously if there are no indications that they have been a victim of another type of identity theft.

IMPLEMENTATION DATE

December 15, 2018

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.



*Most Employment Identity Theft Victims Have Not Been Notified
That Their Identities Are Being Used by Others for Employment*

2

RECOMMENDATION 3

Revise ITIN/SSN mismatch programming to ensure that it does not place the employment identity theft marker on the accounts of SSN owners who are spouses of ITIN holders.

CORRECTIVE ACTION

We agree with this recommendation. We are reviewing the current programming and, when the root cause is identified, we will implement the necessary programming changes. The implementation of required programming changes to accomplish this objective are subject to budgetary constraints, limited resources, and competing priorities. Consequently, and due solely to those constraints, the IRS cannot provide an implementation date at this time.

IMPLEMENTATION DATE

N/A

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 4

Identify instances, prior to PY 2017, in which the ITIN/SSN mismatch process erroneously placed the employment identity theft marker on the tax accounts of SSN owners who are spouses of ITIN holders. The marker should be reversed on those accounts.

CORRECTIVE ACTION

We agree with this recommendation and will reverse the appropriate indicators.

IMPLEMENTATION DATE

December 15, 2018

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.