TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Taxpayer First Act: Implementation of Identity Theft Victim Assistance Provisions

September 10, 2020

Reference Number: 2020-45-070

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

HIGHLIGHTS: Taxpayer First Act: Implementation of Identity Theft Victim Assistance Provisions

Final Audit Report issued on September 10, 2020
Reference Number 2020-45-070

Why TIGTA Did This Audit

On July 1, 2019, the President signed the *Taxpayer First Act*, which aims to broadly redesign the IRS, expand and strengthen taxpayer rights, and enhance its cybersecurity. This Act includes four sections that require the IRS to increase protections and further assist identity theft victims. In addition, TIGTA has issued 13 reports since March 2010 with recommendations for the IRS to improve assistance to victims of identity theft. The overall objective of this review was to assess the IRS's efforts to assist victims of identity theft and implement the victim assistance provisions in the *Taxpayer First Act*.

Impact on Taxpayers

Identity theft refund fraud adversely affects the ability of innocent taxpayers to file their tax returns and timely receive their tax refunds, often imposing significant financial and emotional hardship. Similarly, employment identity theft can affect a taxpayer's account if it results in the IRS assessing additional tax to the innocent taxpayer, *i.e.*, the IRS could assess taxes to the innocent taxpayer if the IRS does not identify the theft. Furthermore, the taxpayer may incur problems with his or her Social Security Administration benefits if the income discrepancies are not resolved.

What TIGTA Found

The IRS established a single point of contact to assist identity theft victims and resolve their cases efficiently. The IRS is also taking actions to address other requirements in the *Taxpayer First Act*. For example, the IRS is developing information about the actions it takes to resolve stolen identity refund fraud cases for public distribution. In addition, the IRS's notifications to victims provide useful instructions about the actions they can take to reduce the burden of identity theft. However, TIGTA identified other areas that need improvement to better assist victims of identity theft and address the requirements in the *Taxpayer First Act*.

Taxpayers eligible to obtain an Identity Protection Personal Identification Number may not be aware of their eligibility due to a lack of IRS advertising for its Identity Protection Personal Identification Number Opt-In Program. In Processing Year 2019, only 25,130 individuals in the 10 eligible locations obtained an Identity Protection Personal Identification Number, compared to more than 48.5 million tax returns received from these locations.

The IRS did not issue its Employment-Related Identity Theft notice to the parents or legal guardians of 133,864 dependents that the IRS identified as employment identity theft victims in Processing Year 2019. In addition, systemic programming errors prevented the IRS from issuing the notice to 60,872 victims that the IRS identified.

Finally, the IRS's policy to notify repeat victims of employment identity theft every three years may result in many victims not being notified that identity thieves continued to use the victims' Taxpayer Identification Numbers nearly every year to work. The 75,451 victims that the IRS first notified in Processing Year 2017 were not sent a subsequent notice despite identity thieves using the victims' Taxpayer Identification Numbers again to gain employment in Processing Years 2018, 2019, or both years.

What TIGTA Recommended

TIGTA made nine recommendations to the IRS, including to: 1) develop a communication strategy to educate taxpayers about the availability of the Identity Protection Personal Identification Number, 2) develop a process to identify and notify parents and legal guardians in cases in which an identity thief uses their dependent's Taxpayer Identification Number to work, 3) correct programming errors to ensure that the Employment-Related Identity Theft notice is issued to all identified victims, and 4) issue the notice to victims of employment identity theft every year that they are identified as a victim.

The IRS agreed with six recommendations and disagreed with three. The IRS's decision to not notify the parents or legal guardians of dependents who are victims of identity theft is not in accordance with the *Taxpayer First Act* requirement to expand taxpayer rights and better assist victims.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 10, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Taxpayer First Act: Implementation of Identity Theft Victim Assistance Provisions (Audit # 201940027)

This report presents the results of our review to assess the Internal Revenue Service's (IRS) efforts to assist victims of identity theft and implement the victim assistance provisions in the *Taxpayer First Act*.[1] This audit is part of the Treasury Inspector General for Tax Administration's Fiscal Year 2020 discretionary audit coverage and addresses the major management and performance challenge of *Addressing Emerging Threats to Tax Administration*.

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

Copies of this report are also being sent to the IRS 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).

[1] Pub. L. 116-025.

Table of Contents

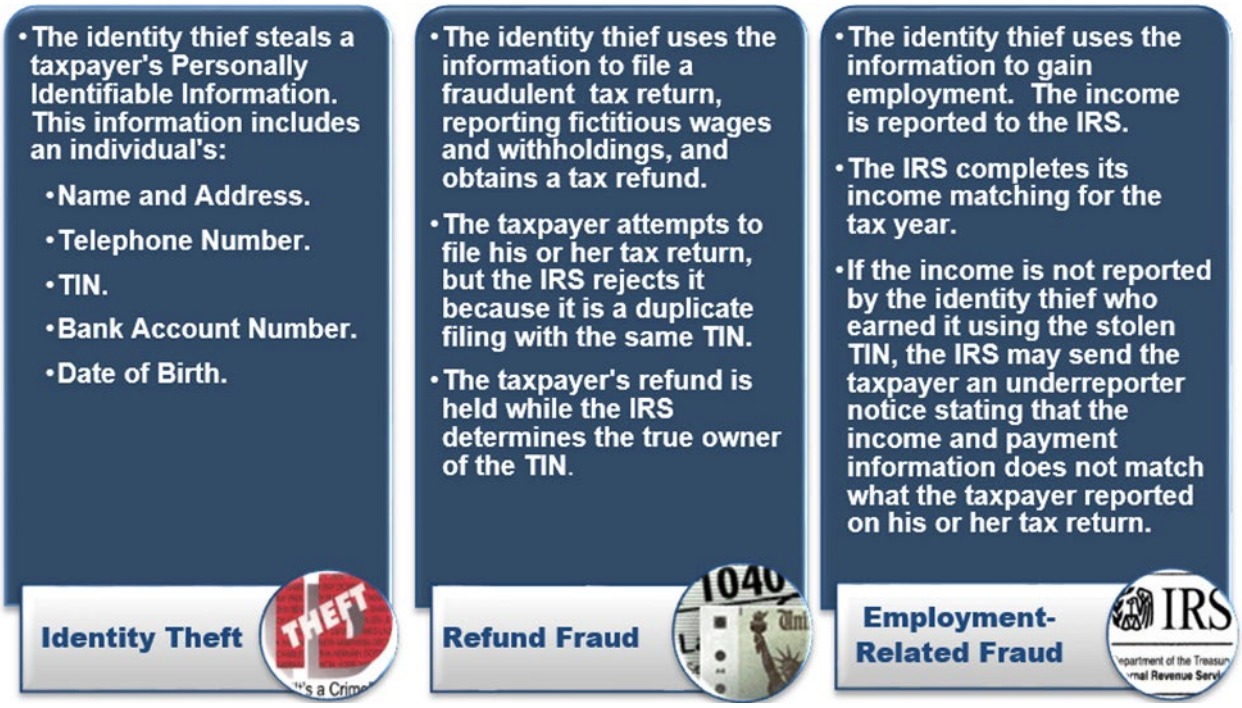
Appendices

Background

Identity theft occurs when an identity thief obtains and uses someone else's personal identifying information without that person's authorization. Personal identity information includes an individual's name, Taxpayer Identification Number (TIN),[1] or other identifying information. Victims of identity theft can spend months or years and considerable money repairing the harm that an identity thief inflicted to their good name and credit record. For example, victims may lose job opportunities or be refused loans, education, or housing.

Two types of identity theft affect tax administration. The first involves an identity thief using another person's identity to file a fraudulent tax return to steal a tax refund. The second involves an identity thief using another person's identity to gain employment. Although employment identity theft does not involve the filing of a fraudulent tax return, the income earned by the identity thief and reported on his or her tax return may affect the taxpayer's account if it results in the Internal Revenue Service (IRS) assessing additional tax to the innocent taxpayer, *i.e.*, the IRS could assess taxes to the innocent taxpayer if the IRS does not identify the theft. Furthermore, the taxpayer may incur problems with his or her Social Security Administration benefits if the income discrepancies are not resolved. Figure 1 describes the two types of identity theft that affect tax administration.

Figure 1: Description of Identity Theft Refund Fraud and Employment Identity Theft



Source: Our analysis of the identity theft process as it affects the IRS and taxpayers.

[1] The identifying number of a person required to file a tax return. This could be a Social Security Number, Individual Taxpayer Identification Number, or an Adoption Taxpayer Identification Number.

Cases of employment identity theft that the IRS identifies usually involve an Individual Taxpayer Identification Number (ITIN)[2] filer who used the TIN of another individual, *i.e.*, victim, to gain employment. The IRS identifies employment identity theft with its ITIN/Social Security Number (SSN) mismatch process. For electronically filed (e-filed) returns, the ITIN/SSN mismatch process detects instances in which an ITIN is listed as either the primary or secondary TIN on Form 1040, *U.S. Individual Income Tax Return*, and the Form W-2, *Wage and Tax Statement*, included with the return has a TIN that does not match the primary or secondary SSN. The TIN belongs to the employment identity theft victim. The IRS refers to these cases as ITIN/SSN mismatches. Paper-filed returns with potential ITIN/SSN mismatches are identified by the Error Resolution System when an ITIN is listed as either the primary or secondary taxpayer on the return and the return reports wages, on Form W-2, earned under an SSN that is different than the primary or secondary taxpayer's SSN.

Although the IRS created the ITIN to help individuals who cannot legally obtain an SSN comply with U.S. tax laws, these individuals generally cannot obtain a job in the United States without an SSN. Therefore, they may use someone else's SSN to obtain employment.

The *Taxpayer First Act*[3] requires the IRS to assist victims of identity theft

On July 1, 2019, the President signed the *Taxpayer First Act*, which aims to broadly redesign the IRS, expand and strengthen taxpayer rights, and enhance its cybersecurity. This Act includes the following four sections to increase protections and further assist identity theft victims:

- Section 2005: The IRS must create a program in which taxpayers, concerned that they may be a victim of identity theft, can request an Identity Protection Personal Identification Number (IP PIN) to file a tax return. An IP PIN is a six-digit number the IRS creates to allow it to process taxpayers' tax returns/refunds without delay. The IP PIN helps the IRS verify a taxpayer's identity and, as a result, accept his or her e-filed or paper tax return. For each calendar year beginning after the date of enactment, *i.e.*, July 1, 2019, the IRS shall provide numbers to residents of States it deems appropriate, provided that the total number of States served each year is greater than the total number of States served during the preceding year. Not later than five years after the date of enactment, the IRS must make the program available to any individual residing in the United States. This section has an implementation date of July 1, 2024.
- Section 2006: The IRS must establish a single point of contact for taxpayers who are a victim of identity theft. The single point of contact shall track the taxpayer's case to completion and coordinate with other IRS employees to resolve the case as quickly as possible. The single point of contact shall consist of a team or subset of specially trained employees who a) have the ability to work across functions to resolve the issues involved in the taxpayer's case and b) shall be accountable for handling the case until its resolution. The employees included within the team or subset may change as required to meet the needs of the IRS, provided that procedures have been established to ensure continuity of records and case history and notify the taxpayer when appropriate. This section has an implementation date of July 1, 2019.

[2] A tax processing number issued by the IRS to individuals who are required to have a TIN, but who do not have and are not eligible to obtain a Social Security Number.
[3] Pub. L. 116-025.

- Section 2007: The IRS must notify taxpayers when the IRS determines or suspects unauthorized use of the identity of an individual (identity theft), including the unauthorized use of the identity of the individual to obtain employment. As soon as practicable, the IRS must:
  - Notify the individual of such determination.
  - Provide instructions on how to file a report with law enforcement regarding the unauthorized use.
  - Identify any steps to be taken by the individual to permit law enforcement to access personal information of the individual during the investigation.
  - Provide information regarding actions the individual may take in order to protect the individual from harm related to the unauthorized use.
  - Offer identity protection measures to the individual, such as the use of an IP PIN.

  In addition, the IRS must issue additional notifications to individuals, or their designee, regarding:
  - Whether an investigation has been initiated in regards to such unauthorized use.
  - Whether the investigation substantiated an unauthorized use of the identity of the individual.
  - Whether any action has been taken against a person related to such unauthorized use or any referral has been made for criminal prosecution of such person and, to the extent such information is available, whether such person has been criminally charged by indictment or information.

  In addition, the IRS must review any information, submitted electronically or on paper, obtained from a statement described in Internal Revenue Code Section 6051 (Form W-2) or an information return related to compensation for services rendered other than as an employee, or provided by the Social Security Administration, which indicates that the SSN does not correspond with the name provided on such statement or information return or the name on the tax return reporting the income which is included on such statement or information return. Finally, the IRS shall establish procedures to ensure that income reported in connection with the unauthorized use of a taxpayer's identity is not taken into account in determining any penalty for underreporting of income by the taxpayer. This section applies to determinations made after January 1, 2020.
- Section 2008: The IRS must develop and implement publicly available guidelines for management of cases of stolen identity refund fraud. The IRS must consult with the National Taxpayer Advocate and implement the guidelines not later than one year after the date of enactment. This section has an implementation date of July 1, 2020. The guidelines may include:
  - Standards for the average length of time in which cases involving stolen identity refund fraud should be resolved; the maximum length of time, on average, a taxpayer who is a victim of stolen identity refund fraud and is entitled to a tax refund which has been stolen should have to wait to receive such refund; and the maximum number of offices and employees within the IRS with whom a taxpayer, who is a victim of stolen identity refund fraud, should be required to interact in order to resolve a case.

- Standards for opening, assigning, reassigning, or closing a case involving stolen identity refund fraud.
- Procedures for implementing and accomplishing the standards previously noted and measures for evaluating such procedures and determining whether such standards have been successfully implemented.

Since March 2010, we have issued 13 reports that included recommendations for the IRS to improve its assistance to victims of tax refund fraud and employment identity theft. Appendix III provides a list of the prior reports.

Results of Review

Taxpayers in "Opt-In" Locations May Not Be Aware That They Can Obtain an Identity Protection Personal Identification Number

The IRS first began issuing IP PINs to confirmed victims of identity theft in Fiscal Year[4] 2011. In January 2014, the IRS expanded its IP PIN issuance program to provide IP PINs through its Opt-In Program. The Opt-In Program enables taxpayers who are concerned about becoming a victim of identity theft to proactively request an IP PIN. For example, this could be a taxpayer whose wallet, containing their Personally Identifiable Information, was stolen. To obtain an IP PIN through the Opt-In Program, taxpayers must access the *Get an IP PIN* application on IRS.gov. They then register to establish an account, which requires them to authenticate their identity using the online authentication process. Taxpayers who successfully enroll will be issued a new IP PIN every year (prior to the start of the next filing season).[5] Taxpayers who obtained an IP PIN via the Opt-In Program would then access their online account to retrieve their issued IP PIN.

Insufficient advertising contributes to the small percentage of eligible taxpayers who proactively obtain an IP PIN.

When the Opt-In Program first stood up, the IRS allowed taxpayers residing in the District of Columbia, Florida, and Georgia to obtain an IP PIN. These locations were selected because, at the time, they had the highest per capita rate of identity theft as reported by the Federal Trade Commission. Since this time, the IRS has expanded the IP PIN Opt-In Program to additional States. For example, in Processing Year (PY)[6] 2019, the IRS expanded the program to seven additional states (California, Delaware, Illinois, Maryland, Michigan, Nevada, and Rhode Island). In PY 2020, the IRS further expanded the Program to 10 additional States (Arizona, Colorado, Connecticut, New Jersey, New Mexico, New York, North Carolina, Pennsylvania, Texas, and Washington).

[4] Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
[5] The period from January through mid-April when most individual income tax returns are filed.
[6] The calendar year in which the tax return or document is processed by the IRS.

Section 2005 of the *Taxpayer First Act* establishes time frames for a nationwide rollout of the Opt-In Program

Section 2005 of the *Taxpayer First Act* requires the IRS to expand the availability of the Opt-In Program to additional States each calendar year beginning after the date of enactment, *i.e.,* July 1, 2019. Therefore, not later than five years after the date of the *Taxpayer First Act's* enactment, the Opt-In Program should be available to all individuals residing in the United States. IRS management stated that they plan to make the Program available to individuals in all States[7] in January 2021, which is more than three years before the *Taxpayer First Act* deadline. Figure 2 shows the locations and dates that the locations have been or will be added.

Figure 2: Locations Added to the IP PIN Opt-In Program and Dates They Will Be Added

Date	Locations
Prior to 2020	California, Delaware, District of Columbia, Florida, Georgia, Illinois, Maryland, Michigan, Nevada, Rhode Island
January 2020	Arizona, Colorado, Connecticut, New Jersey, New Mexico, New York, North Carolina, Pennsylvania, Texas, Washington
January 2021	Alabama, Alaska, Arkansas, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, North Dakota, Ohio, Oklahoma, Oregon, Puerto Rico, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, West Virginia, Wisconsin, Wyoming

Source: IRS Expansion Schedule.

A prior audit reported that taxpayers may not be aware of the IP PIN Opt-In Program

In March 2017,[8] we reported that taxpayers in IP PIN Opt-In Program locations may not be aware of their option to obtain an IP PIN because of insufficient advertising for the Opt-In Program. For example, we reported that, in PY 2016, only 11,831 individuals in the three eligible locations (District of Columbia, Florida, and Georgia) participated in the Program, despite the fact that the IRS receives 13.4 million tax returns from these locations. Our current review again

[7] Residents in the District of Columbia and Puerto Rico will also be able to participate in the Opt-In Program.
[8] Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2017-40-026, *Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers* (Mar. 2017).

found that only a small percentage of taxpayers in eligible locations obtained an IP PIN via the Opt-In Program. In PY 2019, only 25,130 individuals in the 10 eligible locations obtained an IP PIN, compared to more than 48.5 million tax returns received from these locations in PY 2019. Figure 3 provides the number of participants in each eligible location since the Program started.

Figure 3: Number of Individuals Who Obtained an IP PIN Through the Opt-In Program in PY 2014 Through PY 2020

Location	PY 2014 to PY 2017	PY 2018	PY 2019	PY 2020 (as of May 12, 2020)	Totals
District of Columbia	1,262	169	197	186	**1,814**
Florida	52,699	6,767	7,128	6,927	**73,521**
Georgia	17,282	2,482	2,710	3,202	**25,676**
Seven States Added in PY 2019					
California	--	--	7,614	7,646	**15,260**
Delaware	--	--	213	266	**479**
Illinois	--	--	3,363	4,052	**7,415**
Maryland	--	--	1,383	1,409	**2,792**
Michigan	--	--	1,735	1,987	**3,722**
Nevada	--	--	624	781	**1,405**
Rhode Island	--	--	163	180	**343**
10 States Added in PY 2020					
Arizona	--	--	--	1,735	**1,735**
Colorado	--	--	--	1,387	**1,387**
Connecticut	--	--	--	775	**775**
New Jersey	--	--	--	1,453	**1,453**
New Mexico	--	--	--	423	**423**
New York	--	--	--	3,035	**3,035**
North Carolina	--	--	--	2,354	**2,354**
Pennsylvania	--	--	--	2,418	**2,418**
Texas	--	--	--	7,070	**7,070**
Washington	--	--	--	2,010	**2,010**
Total	**71,243**	**9,418**	**25,130**	**49,296**	**155,087**

Source: Identity Protection Strategy and Oversight management, as of May 12, 2020.

In PY 2019, taxpayers were made aware of this Program through targeted news articles aimed at tax practitioners or via web pages on IRS.gov. The IRS also relied on its stakeholder network, *e.g.*, national association leaders, State tax agency leaders, and tax software providers, to cascade IRS messages to their members, colleagues, and customers. When we asked management why a broader scoped effort was not undertaken to raise awareness of this Program, they cited concerns raised by the Information Technology organization about the potential adverse effects to e-filing and other online tools, on IRS.gov, if the volume of IP PIN requests increased. For example, there could be an increase in rejected e-filed returns due to taxpayer errors in recording their IP PIN on their e-filed return.

To address the potential concerns raised by the Information Technology organization, management used a "soft launch" advertising approach in PY 2019. Soft launch means the IRS communicated with tax return preparers, tax software providers, and State tax agencies to increase awareness of the Program in the 10 eligible locations. In PY 2020, the IRS:

- Included an explanation of the IP PIN Opt-In Program when it announced the start of the 2020 Filing Season, and provided news releases about IP PIN availability to media outlets in the 20 States in which the Program was expanded.
- Created Publication 5367, *Identity Protection PIN Opt-In Program for Taxpayers*, which explains how taxpayers can proactively obtain an IP PIN. The IRS provided this publication to stakeholders in the 20 eligible locations, especially tax professionals, to share with their clients.
- Posted Publication 5367 to the Get an IP PIN web page on IRS.gov.

IRS management believes the above actions increased taxpayer awareness of the Program because the number of taxpayers who successfully passed authentication and obtained an IP PIN has nearly doubled to 49,296 in PY 2020 over PY 2019. When we asked management about their efforts to promote the program via social media, they stated that they do not promote the Opt-In Program on social media because they believe the Program's availability in only 20 locations could confuse taxpayers who reside in locations currently not eligible for the Program. With the IRS's planned expansion of the Opt-In Program, a widespread communication strategy needs to be developed to inform taxpayers of this option.

Recommendation 1: The Commissioner, Wage and Investment Division, should develop a multifaceted communication strategy to educate taxpayers on the availability of the IP PIN Opt-In Program and the IRS's plan to implement the provision of the *Taxpayer First Act*, which requires expansion of this program to all taxpayers.

Management's Response: The IRS agreed with this recommendation. The IRS is taking several actions to develop a multifaceted communication strategy to educate taxpayers on the availability of the IP PIN Opt-In Program and implement the provisions of the *Taxpayer First Act*. Some of these actions include: communicating with tax professionals and tax software providers through various IRS outreach functions, including the expansion message in the 2020 Tax Forum topics being planned for tax preparers; creating how-to videos for taxpayers and updating Publication 5367 by December 31, 2020; using traditional and social media platforms to generate nationwide publicity when the *Get an IP PIN* tool is online; leveraging its relationship with tax professionals and tax software providers to include the IP PIN option as part of their communication with their clients, as well as leveraging relationships with States,

congressional offices, and businesses to provide them with information they may share with stakeholders. The IP PIN and its purpose will also be part of the November/December National Tax Security Awareness messaging, which engages Security Summit members in outreach to taxpayers.

A Single Point of Contact Was Created to Assist Identity Theft Victims and Efficiently Resolve Their Cases

The IRS took actions prior to passage of the *Taxpayer First Act* to provide victims of identity theft with a single point of contact. In July 2015, the IRS centralized its identity theft functions into its newly created Identity Theft Victim Assistance (IDTVA)[9] Directorate. This Directorate combines the skills of employees working in multiple functions into one directorate to resolve identity theft cases, including cases initiated by the taxpayer.[10] The Directorate's goal is to improve the taxpayer's experience when working with the IRS to resolve his or her identity theft case. Case processing guidelines for the IDTVA outline actions to better assist the taxpayer and ensure end-to-end account resolution. For example, one employee will take responsibility for resolving a victim's case.

The IDTVA Directorate also provides an identity theft toll-free telephone hotline for victims to reach a trained assistor from 7:00 a.m. to 7:00 p.m. local time. Assistors who answer this specialty line are part of the overall team trained to review taxpayers' case files and answer their questions.

In June 2017, we reported[11] that centralizing the identity theft assistance functions into the IDTVA Directorate reduced the length of time the IRS took to resolve cases and the number of errors employees committed while resolving the cases. In this review, we confirmed that the effective processes we evaluated in our prior audit are still in place. These processes include:

- A decision matrix for tax examiners and managers to better determine which function, such as Examination or Accounts Management, can best work a case.
- Transfer of cases to another IDTVA function requires tax examiners to check the Integrated Data Retrieval System[12] for multiple open control bases[13] on the taxpayer's account. Also, the same employee is required to resolve all issues to prevent duplication of work and incorrect adjustments to the account.
- The Identity Protection Specialized Unit monitors victim cases that require transfer within or outside of the IDTVA Directorate until the case is resolved.

[9] The IDTVA Directorate is in the Wage and Investment Division's Accounts Management function.
[10] A taxpayer-initiated identity theft case is created when a taxpayer contacts the IRS to report that, after filing a tax return, he or she received a notice indicating that the return was rejected because someone (an identity thief) already filed a return using the same SSN and name.
[11] TIGTA, Ref. No. 2017-40-036, *Centralization of Identity Theft Victim Assistance Reduced Case Closure Time Frames and Tax Account Errors* (June 2017).
[12] An IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.
[13] An entry on a tax account that indicates correspondence, an adjustment, or other action.

Many Victims of Employment Identity Theft Were Not Notified

Section 2007 of the *Taxpayer First Act* requires the IRS to notify victims of employment identity theft, once identified. Our review found that the IRS has processes to identify individuals who are or may be a victim of identity theft refund fraud and employment identity theft. For example:

- ***Identity Theft Refund Fraud*** - The IRS notifies taxpayers identified as a victim of identity theft refund fraud. The notification is provided when the IRS rejects the taxpayer's e-filed tax return due to its processing another return with the same TIN. The IRS coordinated with tax software providers to issue a reject code to taxpayers who attempt to e-file their return with a TIN that was used on a previously filed tax return. The reject code informs taxpayers that they must file a paper tax return. When the IRS receives and attempts to process this paper return with the same TIN that was used on another filed return, the IRS identifies the return as a duplicate filing. Once identified, tax examiners send Letter 4674C, *Identity Theft Post-Adjustment Victim Notification Letter – ID Theft*. This letter provides the taxpayer with information about actions the IRS took to resolve the taxpayer's case and helpful actions the taxpayer should take, such as obtaining an IP PIN and contacting the Social Security Administration to verify his or her earnings record.

Although the process to notify victims of identity theft refund fraud is effective, our reviews continue to identify deficiencies in IRS notification to victims of employment identity theft.

- ***Employment Identity Theft*** – The IRS developed the Computer Paragraph (CP) 01E Notice, *Employment-Related Identity Theft Notice*, to notify victims of employment identity theft. This notice informs the victim that the IRS believes another person used the victim's SSN to obtain employment and provides helpful actions the victim can take to mitigate the burden of identity theft. However, this notice will only be issued if the IRS correctly updates the victim's account on the Master File[14] with an employment identity theft marker. This marker is crucial because it generates the CP01E Notice to the taxpayer. Our reviews continue to identify programming errors that result in this marker not being added to victims' accounts. As such, the notice is not sent to the taxpayers. In addition, the IRS established policies that result in some victims not receiving the notice.

Management does not notify the parents and legal guardians of dependents when their TINs are used by other individuals to gain employment

Our review of 1,031,345 PY 2019 tax returns with an ITIN/SSN mismatch identified 883,114 (85.6 percent) returns for which an ITIN filer used an identity theft victim's valid TIN[15] to gain employment. Further analysis of these returns identified 392,949 victims who were not notified. The IRS was unable to notify 198,213 of these victims because they did not have an active tax account. Without a tax account, the IRS does not have a current address to send the CP01E Notice. For the remaining 194,736 victims:

[14] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
[15] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, a valid TIN is either an Employer Identification Number or ITIN issued by the IRS or an SSN issued by the Social Security Administration.

- 133,864 did not have an active tax account but were claimed as a dependent on a filed tax return, *e.g.*, by a parent or legal guardian. We provided the 133,864 dependent TINs to the IRS. Management stated that 960 of the 133,864 dependents we identified were claimed on more than one tax return. Thus, the IRS could not be sure which parent/guardian should receive a notification about possible TIN misuse. The dependents claimed on more than one tax return are less than 1 percent of the 133,864 accounts we identified.

  We raised this same concern in our prior review[16] and recommended that the IRS develop a process to notify the parents and legal guardians who claimed these dependents on their tax returns. Management disagreed with our recommendation, noting that the IRS previously considered processes to address this recommendation. In our prior review, we requested information detailing the processes that management "previously considered." However, the IRS did not provide this information.

  As it relates to the 133,864 accounts we identified, management stated that they would have to manually research the accounts, consuming significant resources, to determine the rightful parent/guardian. However, as we detailed in our prior report, management could use the same notification process they used to notify parents and guardians of dependents associated with the Get Transcript breach.[17] The IRS could implement the following process to notify these parents and legal guardians:

  - The IRS identifies that a dependent's TIN was used by an ITIN filer to gain employment.
  - The IRS issues a precautionary letter to the parent or guardian who claimed this dependent on his or her tax return. To address any concerns about the risk of exposing dependents' Personally Identifiable Information to individuals not entitled to receive this information, the notice should not contain Personally Identifiable Information.
  - The letter advises the parents or legal guardians that the dependent's TIN was used by another person to gain employment and advises them of actions they can take to protect the dependent's identity.

  As previously detailed, management took no action to address our recommendation. In this review, management again noted that they cannot add the identity theft marker to these accounts as they are not active. Without the marker, the CP01E Notice is not issued. In addition, management indicated that the dependent's SSN is often identified on an ITIN return before the parent/legal guardian's tax return has been processed. Therefore, the IRS cannot send the notice because it does not have a tax return to use to identify the parent/legal guardian who claimed the dependent.

  However, provisions in the *Taxpayer First Act* require the IRS to review any information submitted electronically or on paper, *e.g.*, Form W-2, which indicates that the SSN does not correspond with the name provided on such statement or information return or the name on the tax return reporting the income which is included on such statement or

[16] TIGTA, Ref. No. 2017-40-031, *The Number of Employment-Related Identity Theft Victims Is Significantly Greater Than Identified* (June 2017).

[17] The Get Transcript application allows taxpayers to view and download their tax information on the IRS public website. On May 21, 2015, the IRS removed this application from its website after discovering it was being used for unauthorized accesses to taxpayer data.

information return. Once identified, the IRS must notify individuals of the unauthorized use. Since management has stated that notifying these victims falls outside its usual notification process, the IRS should develop a different process.

The IRS's unwillingness to take any action in an effort to notify parents or legal guardians is problematic because of the impact and damage that theft of a child's identity can have on future credit and employment history. The IRS is in a unique position to identify this type of child identity theft and provide individuals with the information they need to minimize the impact. However, without notification, parents and legal guardians cannot take the same proactive steps the IRS suggests when an adult's TIN is identified as being used to fraudulently obtain employment.

- 60,872 victims had an active tax account, but systemic programing errors continue to result in some accounts not being updated with the employment identity theft marker. These errors prevented the marker from posting to the account in cases in which ITIN filers filed a return with two or more Forms W-2, each with a different SSN used for work, and in cases in which the victim is deceased or a minor. We reported these same programming errors in our June 2017 report and recommended that the IRS correct the programming to ensure that the marker is placed on all victims' tax accounts for ITIN/SSN mismatches on e-filed tax returns. In response, management stated that, after our prior review, they submitted a request for programming changes to the Information Technology organization, and the programming changes should have placed the marker on the 60,872 accounts. After analyzing our results in this review, management stated that the programming was corrected, in June 2019, to place the marker on the accounts of the first two victims identified on ITIN-filed returns. We confirmed that the programming was corrected in June 2019. However, it was not corrected to place the marker on victims' accounts in cases in which the ITIN filer filed a return with three or more Forms W-2, each with a different SSN used for work. The programming also does not place the marker on the accounts of some victims who are deceased or a minor.

The Commissioner, Wage and Investment Division, should:

Recommendation 2: In order to comply with the *Taxpayer First Act*, develop a process to identify and notify the parents and legal guardians of the fraudulent use of a claimed dependent's TIN to gain employment.

Management's Response: The IRS disagreed with this recommendation. IRS management stated it notifies victims of employment-related identity theft if they have an active tax account. Management does not intend to notify individuals without active tax accounts.

Office of Audit Comment: We agree that this population of victims presents notification challenges. However, taking no action is contrary to the overall intent of provisions included in the *Taxpayer First Act* to better assist victims of identity theft. As our report notes, theft of a child's identity can affect and damage future credit and employment history. Without notification, parents and legal guardians cannot take the same proactive steps the IRS suggests when an adult's TIN is identified as being used to fraudulently obtain employment. As such, the IRS should work to address these notification challenges.

Recommendation 3: Add employment identity theft markers to the 60,872 victims' tax accounts we identified.

> **Management's Response:** The IRS agreed with this recommendation and plans to review the 60,872 accounts to determine if they were marked with the employment identity theft markers or another identity theft indicator during 2020. IRS management also plans to review the accounts that did not receive an identity theft marker to determine if those accounts should be marked and will manually apply the necessary markers to the accounts.

Recommendation 4: Develop procedures to identify and manually add identity theft markers on victims' tax accounts until programming errors are corrected, when appropriate.

> **Management's Response:** The IRS agreed with this recommendation and is currently working on procedures to identify situations where an indicator should have been applied and to manually apply the indicators as necessary.

Recommendation 5: Correct the programming to ensure that all taxpayers' accounts are updated with the employment identity theft marker, as required.

> **Management's Response:** The IRS agreed with this recommendation and is currently working with the Information Technology organization to resolve incorrect programming as it is identified. This is a collaborative, continuous, and ongoing process.

The IRS intentionally suppresses the CP01E Notice to decedents

Our review of employment identity theft markers placed on tax accounts in PY 2019 identified 1,766 deceased individuals for whom the IRS intentionally suppressed the CP01E Notice. As a result, the decedents' heirs were not notified that an identity thief used the decedent's TIN to work. When we raised this issue to management, they stated that their review of calls made to the Identity Theft Hotline determined that the emotional burden of notifying decedent's heirs outweighs the benefit. Callers who received a CP01E Notice expressed grief, frustration, and extreme anger. Thus, the IRS began suppressing the CP01E Notice to decedents on June 30, 2019. While the IRS's conclusion is understandable, there is a downside to this action. Suppressing these notifications means that the IRS is not providing the decedent's heirs an opportunity to protect against the unauthorized use of the decedent's TIN.

Recommendation 6: The Commissioner, Wage and Investment Division, should reconsider its policy and resume issuing the CP01E Notice to decedents to ensure that their heirs are aware that the decedent's TIN was used by an identity thief to gain employment.

> **Management's Response:** The IRS disagreed with this recommendation and does not intend to resume issuing notifications to decedents. A review of affected decedent accounts indicates that 80 percent have been deceased for three or more years.
>
> **Office of Audit Comment:** The IRS not sending this notification is contrary to the *Taxpayer First Act* provision that requires the IRS to provide notification when employment identity theft is identified. In addition, it disregards the financial losses and burden to family members whose decedent is a victim of "Ghosting." Ghosting is a form of identity theft in which an identity thief uses the Personally Identifiable Information of a deceased individual to commit fraud such as gaining employment under a false identity. Although some of the individuals we identified have been deceased for years,

their Personally Identifiable Information is currently and actively being used to fraudulently gain employment. Notification from the IRS could be the only way in which family members are alerted to this crime. This notification would allow family members to take the steps needed to protect their deceased family member's Personally Identifiable Information.

Programming glitch suppresses some CP01E Notices

Our review of employment identity theft markers placed on taxpayers' accounts in PYs 2017 through 2019 identified 1,268 victims who were not issued a CP01E Notice. The ITIN-filed returns associated with these victims were filed and processed in the **********2**********
**********2**********. For each of these returns, the mismatch was identified and an identity theft marker was added to the victims' tax accounts. However, **********2**********
**********2**********.

When we raised this issue to management, they issued a programming change ticket, in March 2020, to correct the programming glitch. In addition, management stated that they will ensure that the CP01E Notice is issued to the 1,268 victims we identified. Finally, management's review of this issue identified an additional 2,024 victims who were not issued the CP01E Notice as required. Thus, a total of 3,292 victims were not issued the notice.

The Commissioner, Wage and Investment Division, should:

Recommendation 7: Ensure that systemic programming changes are implemented and effective to address the programming glitch that prevents the CP01E Notice from being issued to employment identity theft victims **********2**********
2.

Management's Response: The IRS agreed with this recommendation and has implemented the programming change to issue a CP01E Notice to victims of employment-related identity theft **********2**********. IRS management also plans to monitor accounts identified **********2**********
2 to ensure that the programming change is working as intended by verifying that the CP01E Notice is issued in 2021.

Recommendation 8: Ensure that the CP01E Notice is issued to the 3,292 victims.

Management's Response: The IRS agreed with this recommendation and plans to review the 3,292 accounts and issue the notices where applicable.

Due to the IRS's policy to notify repeat victims every three years, many victims are not notified that their TIN continues to be used to unlawfully gain employment

The IRS set a policy to issue the CP01E Notice to an employment identity theft victim when they are first identified. This same individual would then only receive an additional CP01E Notice if *identified as a victim in the third year after they were first issued the notice.* For example, we identified 75,451 victims that the IRS first notified in PY 2017 whose TIN was used again to fraudulently gain employment in PY 2018, PY 2019, or both years. According to the IRS's three-year notification policy, these victims were not notified in these subsequent years that their TINs were used by an identity thief to obtain employment. These victims will only be notified if they are identified as a victim in PY 2020.

IRS management stated that they set a three-year notification policy to avoid the high cost of issuing CP01E Notices and reduce the resources used to respond to the high number of taxpayer inquiries about the notice. We determined that it would have cost the IRS about $50,000[18] over the two-year period to mail a CP01E Notice to these 75,451 repeat victims. Furthermore, of the 158,597 CP01E Notices the IRS issued in Calendar Year 2019, management noted that IRS employees answered 11,306 telephone calls[19] to the dedicated telephone line listed at the bottom of the notice.

Management also stated that their notification policy is based on their December 2015 analysis of employment identity theft markers placed on taxpayers' accounts from Calendar Year 2011 to Calendar Year 2015, which revealed that only 2 percent of the taxpayers are victims in multiple years. However, in our February 2020 analysis of the 170,171 accounts updated with the employment identity theft marker in PY 2017, we found 75,451 (44 percent) were identified as repeat victims in PY 2018, PY 2019, or both years. It should be noted that as identity thieves use victims' SSNs year after year to unlawfully gain employment, the IRS's costs to notify the victims may increase.

The IRS's three-year notification policy is contrary to the intent of the *Taxpayer First Act* and could lead victims to the false conclusion that their TIN is no longer used by an identity thief. These victims may forego actions to protect their identity and mitigate their financial burden.

Recommendation 9: The Commissioner, Wage and Investment Division, should revise its policy and issue CP01E Notices to victims of employment identity theft every year that they are identified as a victim.

Management's Response: The IRS disagreed with this recommendation. IRS management does not believe issuing additional notices each year would provide additional information to victims of employment-related identity theft. As a result, the IRS plans to maintain its current policy.

Office of Audit Comment: The IRS's decision to not send this notification is contrary to the *Taxpayer First Act* provision that requires IRS to provide notification when employment identity theft is identified. Sending notifications each time an individual's Personally Identifiable Information is used to commit employment identity theft would inform these taxpayers that their TIN continues to be used by an identity thief to fraudulently gain employment.

IRS notifications provide victims with instructions on how to reduce the burden of identity theft

Our review of the Letter 4674C and CP01E Notice found that these notifications alert victims to identity theft and provide instructions on how they can reduce the burden of this crime. Both notifications meet the requirements in Section 2007 of the *Taxpayer First Act*. For example, these notifications include:

[18] We identified 75,451 victims in PY 2017, of which 37,934 were victimized in one of the following two processing years and 37,517 were victimized in both of the following two processing years. Each letter costs 44 cents. ((37,934 + (37,517 X 2)) X $0.44= $49,705).

[19] IRS Joint Operations Center Reports, *Identity Protection Specialized Unit Volumes by Extension*.

- An explanation of why the victim received the notification and steps the victim should take.
- References to access information on the IRS's website where victims can obtain extensive assistance. For example, information on the website explains the purpose of the notification and offers several suggestions on actions the individual can take, including reviewing earnings with the Social Security Administration to ensure that earnings records are correct, monitoring credit reports, and placing a one-year fraud alert on credit accounts. The IRS provides the individual with the names and contact numbers for the credit bureaus. The IRS also provides information on how a victim can file a report with law enforcement.
- References to identitytheft.gov for information about various types of identity theft and actions that victims can take to protect themselves. This is the Federal Government's one-stop resource for identity theft victims. It provides streamlined checklists and sample letters to guide victims through the recovery process.
- Information on how to obtain an IP PIN.

The *Taxpayer First Act* also requires the IRS to establish procedures to ensure that income reported in connection with the unauthorized use of a taxpayer's identity is not taken into account in determining any penalty for underreporting of income by the victim of identity theft. Our review identified that the Automated Underreporter Program's[20] procedures address this requirement. The procedures provide employees detailed instructions on how to abate tax assessments and penalties in identity theft cases for which the taxpayer notifies the IRS that he or she did not earn the income.

Finally, the *Taxpayer First Act* requires the IRS to issue additional notifications to victims regarding whether: 1) an investigation has been initiated in regard to the unauthorized use of the victim's identity, 2) the investigation substantiated an unauthorized use of the identity of the individual, and 3) action has been taken against a person related to such unauthorized use. When we asked Accounts Management function management what actions they took to comply with these requirements, management stated that, as it relates to victims of employment identity theft, the IRS does not investigate instances of individuals using the identity of another person to fraudulently obtain employment. Such an investigation is beyond the scope of the IRS's authority under the Internal Revenue Code. However, Accounts Management function management stated they are coordinating with Criminal Investigation to create additional notifications when an investigation of identity theft has been opened. They do not have an estimated time for when these notifications will be sent to taxpayers.

Information Detailing Actions the Internal Revenue Service Takes to Work Stolen Identity Refund Fraud Cases Is Being Developed for Public Distribution

Section 2008 of the *Taxpayer First Act* requires the IRS to develop and implement publicly available guidelines for management of cases of stolen identity refund fraud. The IRS must consult with the National Taxpayer Advocate to develop the guidelines and must implement them by July 1, 2020. The intent is to provide information that will reduce the administrative

[20] The Automated Underreporter Program matches taxpayer income reported on third-party information returns, *e.g.*, Forms W-2, to amounts reported by the taxpayers on their individual income tax returns.

burden on victims of identity theft. The legislation provides examples of information that should be included in the guidelines.

- The average time frame that identity theft refund fraud cases should be resolved.
- The maximum length of time, on average, that a victim of identity theft refund fraud, who is entitled to a tax refund, should have to wait to receive the refund.
- The maximum number of IRS offices and employees with whom a victim should be required to interact to resolve his or her case.

In response to this provision, the IRS formed a task force in November 2019 that meets weekly to identify improvements to the case management guidelines and resources needed to implement new guidelines. When we asked task force members, such as the IDTVA Director, about the actions taken to comply with this provision, they stated that they are coordinating with Taxpayer Advocate Service management to develop the new guidelines. However, this task force did not start meeting until five months after the *Taxpayer First Act* was enacted. In addition, the task force members stated that IRS office closures and shifting business priorities caused by the coronavirus pandemic are affecting the planned timeline to complete the guidelines. Due to IRS office closures and efforts to issue economic stimulus payments related to the coronavirus pandemic, on May 6, 2020, the Commissioner, Wage and Investment Division, submitted a request for an extension to the IRS's Taxpayer First Act Office. This office coordinates functions' implementation actions and will submit the request for a July 1, 2021, implementation date to Congress.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the IRS's efforts to assist victims of identity theft and implement the victim assistance provisions in the *Taxpayer First Act*. To accomplish our objective, we:

- Assessed the IRS's corrective actions to expand and improve the IP PIN Program.
- Assessed the IRS's plans to implement Provisions 2005, 2006, 2007, and 2008 in the *Taxpayer First Act*.
- Determined if the centralization of identity theft functions in the IDTVA Directorate continues to improve processing and resolution time for cases.
- Evaluated the IRS's corrective actions to prior Treasury Inspector General for Tax Administration (TIGTA) recommendations for employment identity theft. We determined the effectiveness of the processes the IRS implemented to ensure that SSN owners' accounts are marked and notifications sent.
- Identified the number of Individual Master File Transaction Code 971 Action Code 525 – employment identity theft markers placed on taxpayers' accounts in PY 2019.
- Evaluated e-filed tax returns with an ITIN/SSN mismatch filed in PY 2019 (as of November 16, 2019) for which the IRS did not identify and place employment identity theft markers on impacted individual tax accounts. To determine the cause, we selected and reviewed the following statistically valid samples:
    - 85 minor victims from the 1,217 e-filed employment identity theft tax returns processed during PY 2019 that resulted in the IRS not placing an employment identity theft indicator on the individuals' tax accounts.
    - 95 deceased victims from the 5,511 e-filed employment identity theft tax returns processed during PY 2019 that resulted in the IRS not placing an employment identity theft indicator on the individuals' tax accounts.
    - 96 Forms W-2 from the 63,004 e-filed employment identity theft tax returns processed during PY 2019 that resulted in the IRS not placing an employment identity theft indicator on the individuals' tax accounts.

    All samples were based on an expected error rate of 5 percent, a precision rate of ±10 percent, and a confidence interval of 95 percent. Samples were provided to the IRS for concurrence. The contracted statistician assisted with developing sampling plans and projections.
- Identified the number of CP01E Notices (Individual Master File Transaction Code 971 Action Code 804 MISC) the IRS sent to victims in PY 2019.
- Analyzed the Modernized Tax Return Database to identify the number of ITIN/SSN mismatches in PY 2019.

Performance of This Review

This review was performed at the Wage and Investment Division offices in Fresno, California; Atlanta, Georgia; Andover, Massachusetts; and Austin, Texas, during the period October 2019 through May 2020. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Russell Martin, Assistant Inspector General for Audit (Returns Processing and Account Services); Allen Gray, Director; Paula Johnson, Audit Manager; Ashley Burton, Lead Auditor; Ann Ring, Senior Auditor; Nathan Cabello, Auditor; and Laura Christoffersen, Auditor.

Validity and Reliability of Data From Computer-Based Systems

We validated the data from the Modernized Tax Return Database, the Individual Returns Transaction Files, and the Form W-2 File obtained from TIGTA's 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 System.[1] We determined that the data were valid and reliable for the purposes of this audit.

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, and the IRS's procedures for planning and compliance with the provisions of the *Taxpayer First Act*. We evaluated these controls by interviewing officials in the Identity Theft Protection Strategy and Oversight office, reviewing IRS data validation and quality assurance procedures, analyzing IRS-processed taxpayer data, and reviewing the Internal Revenue Manual and key system documentation related to the tracking of tax provisions related to identity theft in the *Taxpayer First Act*.

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

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Taxpayer Rights and Entitlements – Potential; 133,864 taxpayers' accounts were not notified that their dependents' TINs were used by identity thieves (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

The IRS has not developed a process to notify parents and legal guardians when identity thieves use their dependents' SSNs to gain employment. Our review found the IRS did not send the CP01E Notice to 133,864 taxpayers who are the parent or legal guardian of a dependent the IRS identified as a victim of employment identity theft. These dependents are identity theft victims because their SSNs are on Forms W-2 attached to ITIN filers' tax returns in PY 2019.

Type and Value of Outcome Measure

- Taxpayer Rights and Entitlements – Potential; 60,872 taxpayers' accounts were not updated with the employment identity theft marker due to systemic programing errors (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

Our review of 1,031,345 PY 2019 e-filed tax returns with an ITIN/SSN mismatch identified 60,872 victims who had an active tax account in PY 2019, but their account was not updated with an employment identity theft marker. When this marker is not placed on victims' tax accounts, they are not issued a CP01E Notice, which provides helpful actions the victim can take to mitigate the burden of identity theft.

Type and Value of Outcome Measure:

- Taxpayer Rights and Entitlements – Potential; 1,766 deceased taxpayers' heirs were not notified that an identity thief used the decedent's TIN to gain employment (see Recommendation 6).

Methodology Used to Measure the Reported Benefit:

Our review of employment identity theft markers placed on tax accounts in PY 2019 identified 1,766 deceased individuals for whom the IRS intentionally suppressed the CP01E Notice. As a result, the decedents' heirs were not notified that an identity thief used the decedents' TINs to gain employment.

Type and Value of Outcome Measure:

- Taxpayer Rights and Entitlements – Potential; 3,292 taxpayers were not issued the CP01E Notice (see Recommendations 7 and 8).

Methodology Used to Measure the Reported Benefit:

Our review of employment identity theft markers placed on taxpayers' accounts in PYs 2017 through 2019 identified 1,268 victims who were not issued the CP01E Notice. The IRS's systemic programming identified these victims as having an ITIN/SSN mismatch on returns filed and processed in the two weeks before the end of the processing year. Once identified, an identity theft marker was added to the victims' tax accounts. Therefore, the notice should have been automatically issued to these victims. However, because many systems are down for maintenance during the last two weeks of the processing year, the notices were not issued. After we raised this issue to management's attention, they identified another 2,024 taxpayers who were not issued the notice because of this programming glitch (1,268 + 2,024 = 3,292).

Type and Value of Outcome Measure:

- Taxpayer Rights and Entitlements – Potential; 75,451 taxpayers were not notified in subsequent years that their TINs continued to be used by identity thieves to gain employment (see Recommendation 9).

Methodology Used to Measure the Reported Benefit:

The IRS sets a policy to issue the CP01E Notice to an employment identity theft victim when the taxpayer is first identified. However, this same individual would receive an additional notice only if identified as a victim in the third year after being issued the notice. Our review found 75,451 victims that the IRS notified in PY 2017 who were identified as victims again in PY 2018, PY 2019, or both years. However, these taxpayers were not notified in the subsequent years that their TINs continued to be used by identity thieves to gain employment. The IRS's three-year notification policy contravenes the intent of the *Taxpayer First Act* and could lead victims to the false conclusion that their TIN is no longer used by an identity thief.

Appendix III

Prior Treasury Inspector General for Tax Administration Reports Related to Identity Theft

Procedures Need to Be Developed for Collection Issues Associated With Individual Taxpayer Identification Numbers (Reference Number 2010-40-040, dated Mar. 2010).

Individuals Who Are Not Authorized to Work in the United States Were Paid $4.2 Billion in Refundable Credits (Reference Number 2011-41-061, dated July 2011).

Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service (Reference Number 2012-40-050, dated May 2012).

Case Processing Delays and Tax Account Errors Increased Hardship for Victims of Identity Theft (Reference Number 2013-40-129, dated Sept. 2013).

Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds (Reference Number 2015-40-024, dated Mar. 2015).

Improvements Are Needed in the Identity Protection Specialized Unit to Better Assist Victims of Identity Theft (Reference Number 2016-40-003, dated Oct. 2015).

Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection (Reference Number 2016-40-008, dated Dec. 2015).

Processes Are Not Sufficient to Assist Victims of Employment-Related Identity Theft (Reference Number 2016-40-065, dated Aug. 2016).

Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers (Reference Number 2017-40-026, dated Mar. 2017).

Centralization of Identity Theft Victim Assistance Reduced Case Closure Time Frames and Tax Account Errors (Reference Number 2017-40-036, dated June 2017).

The Number of Employment-Related Identity Theft Victims Is Significantly Greater Than Identified (Reference Number 2017-40-031, dated June 2017).

Most Employment Identity Theft Victims Have Not Been Notified That Their Identities Are Being Used by Others for Employment (Reference Number 2018-40-016, dated Feb. 2018).

Results of the 2018 Filing Season (Reference Number 2019-40-013, dated Dec. 2018).

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

August 21, 2020

MEMORANDUM FOR MICHAEL E MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

Digitally signed by Kenneth C. Corbin
Date: 2020.08.21 15:14:37 -04'00'

SUBJECT: Draft Report – Taxpayer First Act: Implementation of Identity Theft Assistance Provisions (Audit # 201940027)

Thank you for the opportunity to review and comment on the subject draft report. The IRS defines tax-related identity theft as the filing of a fraudulent tax return using the name and Social Security Number (SSN) of another taxpayer to obtain a tax refund. Employment-related identity theft is the misuse of another person's SSN for the purpose of obtaining employment. Regardless of the type, the IRS takes identity theft fraud very seriously and has expended substantial resources to identify and stop tax fraud and the victimization of innocent individuals when their personally identifiable information (PII) is misused. We appreciate your acknowledgement of the actions we took to identify and prevent identity theft prior to the enactment of the Taxpayer First Act,[1] as well as those we have taken after enactment to implement its provisions that address employment-related identity theft.

We are disappointed that the report does not discuss the leading cause of employment-related identity theft, which is that most employers are not required to confirm the identities of the individuals whom they hire. Individuals who are ineligible to obtain employment in the United States may use the SSN of another individual, provided to them voluntarily or involuntarily, or may create a SSN that coincidentally matches one already assigned to another person. These misuses would be detectable through use of the E-Verify service provided by the Department of Homeland Security (DHS). The E-Verify program is a web-based system[2] that allows enrolled employers to confirm the eligibility of their employees to work in the United States. Using E-Verify, employers verify the identity and employment eligibility of newly hired employees by electronically matching information provided by employees on the Form I-9, *Employment Eligibility Verification*, against records available to the Social Security Administration and DHS.

[1] Taxpayer First Act (Pub. L. No. 116-25), enacted July 1, 2019.
[2] https://www.e-verify.gov/.

The use of E-Verify is required only for employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation E-Verify clause that requires enrollment in E-Verify as a condition of federal contracting; employers in states with legislation mandating its use, such as a condition of business licensing; or as a result of a legal ruling specific to the employer that mandates its use. The E-Verify service is available in all 50 states, the District of Columbia, Puerto Rico, Guam, the U.S. Virgin Islands, and Commonwealth of Northern Mariana Islands. Its required use by all employers could eliminate most instances of employment-related IDT.

Portions of the 2019 Taxpayer First Act codified IRS initiatives that were already underway. For example, section 2005, *Identity Protection Personal Identification Numbers*, states that the IRS must create a program for taxpayers to request an Identity Protection Personal Identification Number (IP PIN) to file a tax return, and to expand the program nationwide within five years after the date of enactment. The IP PIN is an effective tool in preventing the misuse of taxpayers' SSNs on fraudulent tax returns because it is an identifier that is unique to the taxpayer, changes annually, and is known only to the IRS and the taxpayer to whom it is assigned. As the IP PIN program was being piloted, it was available only to individuals who were confirmed victims of identity theft plus residents of two states and the District of Columbia. We have increased to 20 the number of states whose residents are eligible to request an IP PIN without having previously been victimized by identity theft and are continuing with nationwide rollout of the program in 2021.

As another example, section 2006, *Single Point of Contact for Tax-Related Identity Theft Victims*, requires the IRS to establish a single point of contact for any taxpayer whose return has been delayed or otherwise adversely affected due to tax-related identity theft. We implemented the single point of contact for victims of identity theft prior to enactment of the Act. Our Identity Theft Victim Assistance program has centralized assistance-related casework since 2015. It also provides a toll-free identity theft hotline, and other processes to ensure that all taxpayers affected by identity theft have their cases assigned to a single employee with the highest level of skills needed to resolve their issues.

In addition, section 2007, *Notification of Suspected Identity Theft*, requires the IRS to notify an individual if we have determined that there has been, or may have been, an unauthorized use of their identity. To meet this provision, we have included information in our letters and notices advising taxpayers of the steps they should take to protect themselves when they suspect their PII has been compromised. This includes instructions on reporting the incident to law enforcement agencies, steps they can take to permit law enforcement access to their personal information, and other actions they can take, such as applying for an IP PIN to protect themselves from future victimization. We also proactively notify taxpayers when we become aware of their PII being used by other individuals, including through suspected employment-related identity theft activities. Employment-related identity theft is most commonly detected during tax return

processing, when the Form W-2, *Wage and Tax Statement*, attached to the tax return, to support wages and income taxes withheld reported on it, is shown to have been issued to an individual who is not the filer of the tax return.

We disagree with conclusions stated in the report regarding our policies for notifying individuals whose PII appears to have been used improperly to obtain employment. Specifically, regarding the use of SSNs assigned to minors and other individuals claimed as dependents on tax returns, the report accurately states that an indicator cannot be applied to an account that does not exist; however, the suggested treatment described oversimplifies the process and does not take into account resources needed to implement it. Comparison to the process we used in responding to the Get Transcript incident, where bad actors successfully impersonated taxpayers by using PII obtained from outside sources to receive account transcripts, is not valid. In that incident, we were able to identify the specific accounts that had been compromised and identified all taxpayer identification numbers that had been revealed. Even with that degree of specificity, the notification process was manual, labor-intensive, and could not be replicated in a way that would be feasible for addressing dependents whose SSNs are reflected on Forms W-2 attached to the returns of other individuals.

When an SSN mismatch between Form W-2 and a tax return occurs, the notification process is triggered at the time the tax return is being processed. We do not have contact information for an individual who does not have a tax account and it is possible a tax return claiming the same SSN as a dependent has not already been filed or will not be filed for months. The value of such notification would be minimal in consideration of the restraints against disclosing PII imposed by Internal Revenue Code § 6103. Rather than identifying the dependent SSN affected, we could state only that the SSN "of a dependent claimed on your tax return" was misused.

Unlike identity theft refund fraud, which has a direct impact on tax accounts for each period that it occurs, employment-related identity theft generally does not affect tax accounts. In situations where it could, our compliance functions have procedures in place to recognize and appropriately address conditions that may appear to reveal unreported income. With limited resources and in consideration of the feedback we received from the surviving relatives of decedents, we do not believe there is value in providing notifications when the use of decedent SSNs is detected. If such notices were issued, they could continue indefinitely. Similarly, with those SSNs that are detected as misused each year, providing notification more than every three years raises the question of how useful the notices would be if the same information, which does not include the identity of the person using the number, is sent continuously.

As previously stated, we believe many of the causes of employment-related identity theft could be reduced if employers confirm employment eligibility through the use of E-Verify. Employment-related identity theft impacts labor and immigration laws, both of which are outside the scope of the IRS's authority to administer or enforce. The IRS

remains committed to do all we can with our limited resources to address the tax aspects of employment-related identity theft. We will continue to pursue corrections to programming found not to be performing to the specifications defined by the business requirements.

Attached are our comments and planned corrective actions to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Dietra Grant, Director, Customer Account Services, Wage and Investment Division, at (470) 639-3504.

Attachment

Attachment

Recommendation

RECOMMENDATION 1
The Commissioner, Wage and Investment Division, should develop a multifaceted communication strategy to educate taxpayers on the availability of the IP PIN Opt-In Program and the IRS's plan to implement the provision of the *Taxpayer First Act*, which requires expansion of this program to all taxpayers.

CORRECTIVE ACTION
The 2021 Identity Protection Personal Identification Number (IP PIN) Opt-In Program communications strategy depends on whether the IRS decides to continue gradual expansion by adding more states to the 20 already in the program, or to expand it nationwide. If the decision is to expand nationwide, the communications will immediately begin by informing critical stakeholders such as tax professionals and tax software providers. This information will be shared through various IRS outreach functions.

The fact that the IRS is considering a broader expansion is already included in the 2020 Tax Forum messages being planned for tax preparers. In preparation for the 2021 filing season, the IRS will also create a how-to video for taxpayers and will update publications such as Publication 5367, *Identity Protection PIN Opt-In Program for Taxpayers*, by December 31, 2020. The IP PIN and its purpose will also be part of the November/December National Tax Security Awareness Week messaging, which engages Security Summit members in outreach to taxpayers. Focusing messaging about the Opt-In Program directly to taxpayers is most effective when the tool is available, so taxpayer communications are paused when the *Get an IP PIN* tool is offline from November until the tax filing season begins.

When the tool is online, we will use traditional and social media platforms to generate nationwide publicity. This includes a national news release to generate broad taxpayer awareness and linking to information that will educate taxpayers, including the how-to video, updated web pages, and the revised Publication 5367. Tax tips and posts on Twitter, Facebook, and Instagram will also point to these resources. We will also leverage our relationships with tax professionals and tax software providers to include the IP PIN option as part of their communications with their clients. Further, the IRS will leverage its relationships with states, congressional offices, and businesses to provide them with information they may share with stakeholders.

IMPLEMENTATION DATE
February 15, 2021

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.

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 2
In order to comply with the *Taxpayer First Act*, develop a process to identify and notify the parents and legal guardians of the fraudulent use of a claimed dependent's TIN to gain employment.

CORRECTIVE ACTION
We are notifying victims of employment-related identity theft if they have an active tax account with their name and address in order to send the Computer Paragraph (CP) 01E, *Employment Related Identity Theft* notice to the victim. We do not intend to notify individuals without active tax accounts.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 3
Add employment identity theft markers to the 60,872 victims' tax accounts we identified.

CORRECTIVE ACTION
We will review the 60,872 accounts to determine if they were marked with the employment-related identity theft transaction or another identity theft indicator during 2020. We will review the accounts that did not receive an identity theft marker to determine if their account should be marked and will manually apply the necessary markers to the accounts.

IMPLEMENTATION DATE
January 15, 2021

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
Develop procedures to identify and manually add identity theft markers on victims' tax accounts until programming errors are corrected, when appropriate.

CORRECTIVE ACTION
We are working on procedures to identify situations where an indicator should have been applied, and to manually apply the indicators as necessary.

IMPLEMENTATION DATE
January 15, 2021

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 5
Correct the programming to ensure that all taxpayers' accounts are updated with the employment identity theft marker, as required.

CORRECTIVE ACTION
We are working with the Information Technology function to resolve incorrect programming as it is identified. This is a collaborative, continuous, and ongoing process.

IMPLEMENTATION DATE
Implemented

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

RECOMMENDATION 6
The Commissioner, Wage and Investment Division, should reconsider its policy and resume issuing the CP01E Notice to decedents to ensure that their heirs are aware that the decedent's TIN was used by an identity thief to gain employment.

CORRECTIVE ACTION
A review of affected decedent accounts indicate that 80 percent have been deceased for three or more years. We do not intend to resume issuing notifications to decedents.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 7
Ensure that systemic programming changes are implemented and effective to address the programming glitch that prevents the CP01E Notice from being issued to employment identity theft victims **********2********** ********2*******.

CORRECTIVE ACTION
The programming change to issue a CP 01E notice to victims of employment-related identity theft, identified **********2**********, was implemented on June 29, 2020. We will monitor accounts identified **********2********** to ensure the program change is working as intended by verifying that the CP 01E is issued in 2021.

IMPLEMENTATION DATE
March 15, 2021

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 8
Ensure that the CP01E Notice is issued to the 3,292 victims.

CORRECTIVE ACTION
We will review the 3,292 accounts and issue the notices where applicable.

IMPLEMENTATION DATE
January 15, 2021

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

RECOMMENDATION 9
The Commissioner, Wage and Investment Division, should revise its policy and issue CP01E Notices to victims of employment identity theft every year that they are identified as a victim.

CORRECTIVE ACTION
Issuing the additional notices each year does not provide any additional information to the victims of employment-related identity theft and if they contact us in response to receiving additional CP01E notices, we cannot provide them with any additional information. We will maintain our current policy.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A

Appendix V

Abbreviations

CP	Computer Paragraph
e-filed	Electronically Filed
IDTVA	Identity Theft Victim Assistance
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
ITIN	Individual Taxpayer Identification Number
PY	Processing Year
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number